MULTIMEDIA SECURITY SYSTEM FOR SECURITY AND MEDICAL APPLICATIONS

A dissertation

submitted by

Yicong Zhou

In partial fulfillment of the requirements
for the degree of

Doctor of Philosophy

in

Electrical Engineering

TUFTS UNIVERSITY

August, 2010

Copyright (©) 2010 by Yicong Zhou

ADVISOR: Dr. Karen Panetta

www.manaraa.com

UMI Number: 3422402

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

UMI 3422402
Copyright 2010 by ProQuest LLC.
All rights reserved. This edition of the work is protected against
unauthorized copying under Title 17, United States Code.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

www.manaraa.com

Copyright (©) 2010 by Yicong Zhou

All rights reserved. Reproduction in whole or in part in any form requires the prior written permission of Yicong Zhou or designated representative.

www.manaraa.com

To my wife and son

www.manaraa.com

ACKNOWLEDGEMENTS

I would like to thank my wife, Dr. Yanwei Jia, for her unwavering encouragement, support and understanding throughout my research and the years I dedicated to achieving this milestone in my life and career. I am grateful to my son, Chenxiao Zhou, who brings happiness into my life.

I would like to thank my advisor, Dr. Karen Panetta, for the invaluable guidance, consistent encouragement and support that she has given me at each stage of my graduate studies and my research. Her knowledge, kindness, and patience have benefited my life and my future.

I want to show my sincere respect and appreciation to Dr. Sos Agaian at the University of Texas at San Antonio for his invaluable guidance and suggestions for my research and study. His knowledge, wisdom, persistence and kindness have nurtured my study and my future career.

I am grateful to Dr. Joseph Noonan and Dr. Ethan Danahy of my dissertation committee for their valued comments and suggestions on the dissertation draft. Special thanks must also go to Dr. Chorng Hwa Chang for the help and the suggestions he gave me when he was my course instructor, TA advisor and Master's thesis committee member.

I want to take this opportunity to show my special appreciation to Mr. George Preble for his consistent encouragement, considerate help, unlimited support and guidance. I also thank Simlab members, Shahan Nercessian, Li Lu, Junjun Xia, Sampathkumar

www.manaraa.com

Veeraraghavan, Sadaf Qazi, Eric Wharton, Barghavi Govindarajan, and Aaron Greenblatt, as well as my classmates in other research groups, Ruida Yun, Yiling Zhang, Yue Wu and Yuping Dong, for their insightful discussions during my study and research at Tufts.

www.manaraa.com

ABSTRACT

This dissertation introduces a new multimedia security system for the performance of object recognition and multimedia encryption in security and medical applications. The system embeds an enhancement and multimedia encryption process into the traditional recognition system in order to improve the efficiency and accuracy of object detection and recognition while protecting multimedia data. The dissertation then focuses on the system's enhancement and encryption processes, and presents contributions to the area of image enhancement and multimedia encryption.

For the purposes of image enhancement, a new enhancement measure called the second-derivative-like measure of enhancement (SDME) is introduced to quantitatively evaluate the enhancement algorithm's performance. This is followed by the introduction of a new 3D CT baggage image enhancement algorithm for homeland security applications. Computer simulations and comparisons demonstrate that the presented algorithm significantly improves the visual quality of objects in the original CT images while reducing background noise. The quantitative SDME measure results and 3D visualizations verify the algorithm's excellent enhancement performance.

To improve the visual quality of medical images and thereby improve the efficiency and accuracy of early cancer detection, a new nonlinear filter, called the Alpha-Weighted Quadratic Filter (AWQF), is integrated with human visual system based decomposition and unsharp masking techniques to enhance mammograms for breast cancer detection. To enhance prostate MR images for prostate cancer detection, the same filter is

www.manaraa.com

integrated with alpha-trimmed mean separation and logarithmic enhancement techniques. Simulation results and comparisons are given to demonstrate the enhancement algorithms' excellent performance when it comes to enhancing mammograms and prostate MR images.

In order to enhance the efficiency and security of existing encryption algorithms, five parametric recursive sequences and their transforms are developed and applied to multimedia scrambling/encryption. The recursive sequence transforms are integrated with the Fibonacci bit-plane decomposition method and the newly introduced *(n, k, p)*-Gray code bit-plane decomposition for image and object encryption. Based on the concept of using one set of security keys to encrypt the original image and a different set of security keys to reconstruct the image to obtain the final encrypted image, a discrete parametric cosine transform is used for image encryption.

Despite the fact that the edge map has been used traditionally for image compression, enhancement, and recognition, it has never been used for image encryption. This dissertation investigates the use of the edge map for applications in image encryption. The edge map is integrated with the 3D Cat Map for image encryption and with the chaotic logistic map for encrypting medical images for the sake of privacy protection. The concept of the edge map is then extended further to produce a binary "key-image", which can either be a bit-plane or an edge map obtained from any other image. Computer simulations, comparisons and security analysis demonstrate the excellent performance of the presented encryption algorithms when it comes to multimedia encryption.

The contributions of this dissertation are as follows:

www.manaraa.com

- ❖ A new multimedia security system for object detection and multimedia encryption

- ❖ Image enhancement:

  - A new SDME measure for quantitatively evaluating the enhancement algorithm's performance
  - A new 3D CT baggage image enhancement algorithm using alpha weighted mean separation for homeland security applications
  - A new alpha weighted quadratic filter for mammogram enhancement
  - A new human visual system decomposition based algorithm for mammogram enhancement
  - A new nonlinear unsharp masking scheme for mammogram enhancement
  - A new prostate MR image enhancement algorithm using the alpha-trimmed mean separation and nonlinear filtering
  - A new logarithmic enhancement algorithm using nonlinear filtering for prostate MR image enhancement

- ❖ Multimedia encryption:

  - Five new parametric recursive sequences and their transforms for multimedia encryption, including the truncated P-Fibonacci sequence, P-Lucas sequence, *(n, k, p)*-Gray code, P-recursive sequence and the parametric M-sequence.

www.manaraa.com

- A new 2D P-recursive transform
- Two P-recursive transform based multimedia encryption algorithms in the spatial and frequency domains
- A new truncated Fibonacci p-code bit-plane decomposition
- A new *(n, k, p)*-Gray code bit-plane decomposition
- A new image encryption algorithm using the P-Fibonacci transform and decomposition
- A new selective object encryption algorithm using the truncated Fibonacci p-code bit-plane decomposition
- A new image encryption algorithm using the *(n, k, p)*-Gray code and its decomposition
- A new image encryption algorithm using the Discrete Parametric Cosine Transform
- A new image encryption algorithm using the edge map and a new 3D Cat Map
- A new medical image encryption algorithm using the edge map and chaotic logistic map
- Two image encryption algorithms using binary key-images: one uses bit-plane and the other uses the edge map.

www.manaraa.com

ASSOCIATED PUBLICATIONS

Book:

[1] Yicong Zhou, Karen Panetta, and Sos Agaian, Multimedia Encryption Using Recursive Sequences. Saarbrücken, Germany: VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG, 2008.

Journal Papers:

[1] Karen Panetta, Sos Agaian, Yicong Zhou, and Eric Wharton, "Parameterized Logarithmic Framework for Image Enhancement," IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics, 2010 (Accepted).

[2] Karen Panetta, Yicong Zhou, and Sos Agaian, "Image Encryption Using P-Fibonacci Decomposition and Transform," Signal Processing: Image Communication, 2010 (Submitted).

[3] Karen Panetta, Yicong Zhou, and Sos Agaian, " (n, k, p)-Gray Code for Image Systems," IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, 2010 (Submitted).

[4] Karen Panetta, Yicong Zhou, and Sos Agaian, "Nonlinear Unsharp Masking for Mammogram Enhancement," IEEE Transactions on Image Processing, 2009 (Submitted).

Refereed Conference Publications:

[1] Yicong Zhou, Karen Panetta, and Sos Agaian, "3D CT Baggage Image Enhancement Based on Order Statistic Decomposition," in *2010 IEEE Conference on Technologies for Homeland Security*, Waltham, MA, USA, 2010 (Submitted).

[2] Yicong Zhou, Karen Panetta, and Sos Agaian, "Human Visual System Based Mammogram Enhancement and Analysis," in *2010 The International Conference on Image Processing Theory, Tools and Applications*, Paris, France, 2010 (Accepted).

[3] Yicong Zhou, Karen Panetta, and Sos Agaian, "Nonlinear Filtering for Enhancing Prostate MR Images via Alpha-Trimmed Mean Separation," in *2010 IEEE International Conference on Systems, Man and Cybernetics*, Istanbul,Turkey, 2010 (Accepted).

[4] Yicong Zhou, Karen Panetta, and Sos Agaian, "CT Baggage Image Enhancement Using a Combination of Alpha-Weighted Mean Separation and Histogram

www.manaraa.com

Equalization," in *SPIE Defense, Security, and Sensing 2010: Mobile Multimedia/Image Processing, Security, and Applications 2010*, Orlando, FL, USA, pp. 77080G-12.

[5] Yue Wu, Yicong Zhou, Joseph P. Noonan, Karen Panetta, and Sos Agaian, "Image Encryption Using Sudoku Matrix," in *SPIE Defense, Security, and Sensing 2010: Mobile Multimedia/Image Processing, Security, and Applications 2010*, Orlando, FL, USA, 2010 pp. 77080P-12.

[6] Li Lu, Yicong Zhou, Karen Panetta, and Sos Agaian, "Comparative Study of Histogram Equalization Algorithms for Image Enhancement," in *SPIE Defense, Security, and Sensing 2010: Mobile Multimedia/Image Processing, Security, and Applications 2010*, Orlando, FL, USA, 2010 pp. 770811-11.

[7] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image Encryption Using Discrete Parametric Cosine Transform," in *The 43rd Annual Asilomar IEEE Conference on Signals, Systems and Computers, ACSSC 2009*, Pacific Grove, CA, 2009, pp. 395-399.

[8] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image Encryption Algorithms Based on Generalized P-Gray Code Bit Plane Decomposition," in *The 43rd Annual Asilomar IEEE Conference on Signals, Systems and Computers, ACSSC 2009* Pacific Grove, CA, 2009, pp. 400-404.

[9] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image encryption using binary key-images," in *2009 IEEE International Conference on Systems, Man and Cybernetics, SMC 2009*, San Antonio, TX, 2009, pp. 4569-4574.

[10] Yicong Zhou, Karen Panetta, and Sos Agaian, "A lossless encryption method for medical images using edge maps," in *The 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS 2009*, Minneapolis, Minnesota, 2009, pp. 3707-3710.

[11] Yicong Zhou, K. Panetta, and S. Agaian, "Mammogram Enhancement Using Alpha Weighted Quadratic Filter," in *The 31st Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS 2009*, Minneapolis, Minnesota, 2009, pp. 3681-3684.

[12] Yicong Zhou, Karen Panetta, Ravindranath Cherukuri, and Sos Agaian, "Selective Object Encryption for Privacy Protection," in *SPIE Defense, Security, and Sensing 2009: Mobile Multimedia/Image Processing, Security, and Applications 2009*, Orlando, FL, USA, 2009, pp. 73510F-10.

[13] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image Encryption Based on Edge Information," in *IS&T / SPIE Electronic Imaging 2009: Multimedia on Mobile Devices 2009*, San Jose, CA, USA, 2009, pp. 725603-11.

www.manaraa.com

[14] Yicong Zhou, Karen Panetta, and Sos Agaian, "Comparison of Recursive Sequence Based Image Scrambling Algorithms," in *2008 IEEE International Conference on Systems, Man and Cybernetics* Singapore, 2008, pp. 697-701.

[15] Yicong Zhou, Karen Panetta, and Sos Agaian, "An Image Scrambling Algorithm Using Parameter Based M-sequences," in *2008 IEEE International Conference on Machine Learning and Cybernetics*, Kunming, China, 2008, pp. 3695-3698.

[16] Yicong Zhou, Karen Panetta, and Sos Agaian, "Partial Multimedia Encryption with Different Security Levels," in *2008 IEEE Conference on Technologies for Homeland Security*, Waltham, MA, USA, 2008, pp. 513-518.

[17] Yicong Zhou, Karen Panetta, and Sos Agaian, "P-recursive Sequence and Key-dependent Multimedia Scrambling," in *SPIE Defense, Security, and Sensing 2008: Mobile Multimedia/Image Processing, Security, and Applications 2008*, Orlando, FL, USA, 2008, pp. 69820H-12.

[18] Yicong Zhou, Sos Agaian, Valencia M. Joyner, and Karen Panetta, "Two Fibonacci P-code Based Image Scrambling Algorithms," in *IS&T / SPIE Electronic Imaging 2008: Image Processing: Algorithms and Systems VI*, San Jose, CA, USA, 2008, pp. 681215-12.

www.manaraa.com

CONTENTS

www.manaraa.com

www.manaraa.com

www.manaraa.com

www.manaraa.com

www.manaraa.com

www.manaraa.com

www.manaraa.com

FIGURES

www.manaraa.com

www.manaraa.com

www.manaraa.com

www.manaraa.com

www.manaraa.com

www.manaraa.com

Part I

Multimedia Security System

www.manaraa.com

Improving the security level of multimedia data and the accuracy and efficiency of object recognition in security and medical applications is always beneficial. Visual surveillance systems that monitor public or strategic locations, and computer tomography (CT) baggage scanning systems that scan luggage at security checkpoints, can be improved by developments in the following technologies: 1) video/image enhancement algorithms to help threat object detection processes for identifying suspected criminals and objects; and 2) encryption algorithms for securing communication and storage. Other systems that require object recognition include biometric identification systems (for identifying biometric traits such as fingerprints, irises and facial features) and medical imaging systems (for detecting different types of tumors and cancers). These systems also require encryption algorithms – in the case of biometric identification systems, to protect biometric data, and in the case of medical imaging systems, to protect the privacy of patients. As regards medical imaging systems (such as computer tomography, magnetic resonance (MR) and ultrasound imaging), any improvement that can be made in the area of the above mentioned technologies may result in the earlier detection of tumors and cancers. In the case of surveillance and scanning systems, improvements mean a safer, more secure environment for everyone.

The efficiency and accuracy of object detection and identification in traditional recognition systems is often limited by the fact that the input image/video sources are subject to low visual quality and/or noise. These recognition systems also do not provide security protection for the objects recognized or for multimedia sources. To address these problems, this dissertation embeds an enhancement and multimedia encryption process

www.manaraa.com

into the traditional recognition system in such a way that a new multimedia security system is generated, thereby improving the performance of object recognition and multimedia encryption.

www.manaraa.com

Chapter 1

Multimedia Security System

To improve the efficiency and accuracy of object detection and identification in the traditional recognition system while providing security for multimedia data, this chapter introduces a new multimedia security system. The system embeds an enhancement and multimedia encryption process into the traditional recognition system with the intention of performing object recognition and multimedia encryption for security and medical applications.

This chapter is organized as follows. Section 1.1 introduces the multimedia security system. Section 1.2 gives several application examples. Finally, Section 1.3 gives a brief introduction to the dissertation.

www.manaraa.com

1.1 Multimedia Security System

Integrating an enhancement process and an encryption process, this section introduces a multimedia security system to perform object recognition and multimedia encryption. Whereas the enhancement process is introduced to improve the efficiency and accuracy of object detection and recognition, the encryption process is introduced to provide security protection for multimedia data that exists in a given system before it is actually stored in that system. Figure 1.1 shows the architecture of the multimedia security system.

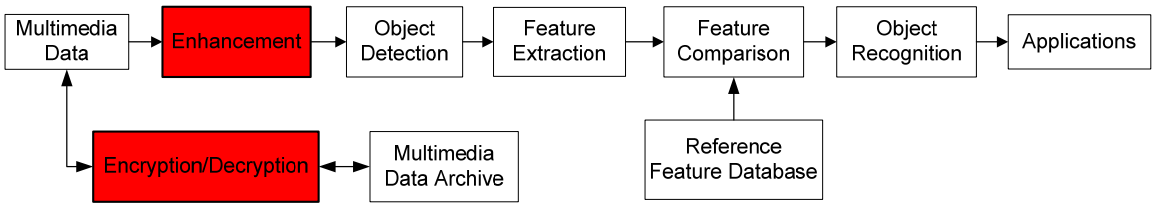


Figure 1.1: Block diagram of the multimedia security system

The system can be adapted to multiple source formats according to the multimedia data being processed, such as videos, images, biometrics and documentation. In order to perform real-time object recognition, an enhancement process is used to enhance the input multimedia data and an object detection process is used to segment the objects from that data. The features of the objects are extracted and the object recognition process then decides upon the recognition of the objects according to a comparison results between the objects' features and the reference features stored in the database.

www.manaraa.com

To provide security protection for multimedia data, an encryption process is used to encrypt the data before it is stored in the system. To inspect the saved data, the authorized user should use the correct security keys to decode the multimedia data.

Additionally, the multimedia security system being presented here is an open platform. Any algorithm for enhancement, encryption, object detection, feature extraction or object recognition can be used in this system.

In summary, the multimedia security system has the following features:

- It is able to perform object recognition.
- It provides security protection for multimedia data.
- It has improved efficiency and accuracy for object detection and recognition due to the enhancement process.
- It is adaptive to multiple source formats.
- It can be used for a broad range of applications.
- It provides users with an open platform to which any algorithm of enhancement, recognition and encryption can be applied.
- It can be customized into specific systems for different applications.

المنارة للاستشارات
www.manaraa.com

1.2 Requirements of the Multimedia Security System

The presented system can be used for a broad range of applications, including object recognition, traffic monitoring, baggage scanning and biometric identification (in homeland security applications) or for cancer detection in medical imaging systems (such as computer tomography (CT), magnetic resonance (MR) and ultrasound imaging).

Figure 1.2 gives an example of the presented multimedia security system for visual surveillance applications. For homeland security purposes, the system is able to identify and track suspected criminals using face detection and recognition. For the sake of privacy protection, the encryption process provides the system with security for images and videos. Only authorized personnel with the appropriate security keys can access and inspect protected images and videos.

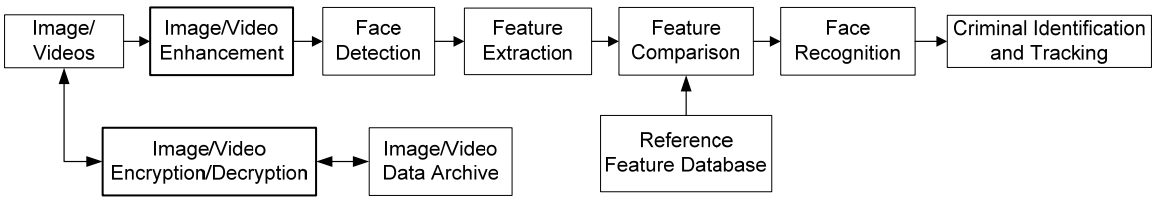


Figure 1.2: The multimedia security system for visual surveillance applications.

Figure 1.3 gives another application example for CT baggage scanning. The enhancement process improves the visual quality of CT baggage images and removes their background noise. The CT images are then processed by object detection and feature extraction. In

www.manaraa.com

order to recognize suspected explosives or prohibited objects, the extracted features are compared with referenced features in the database.

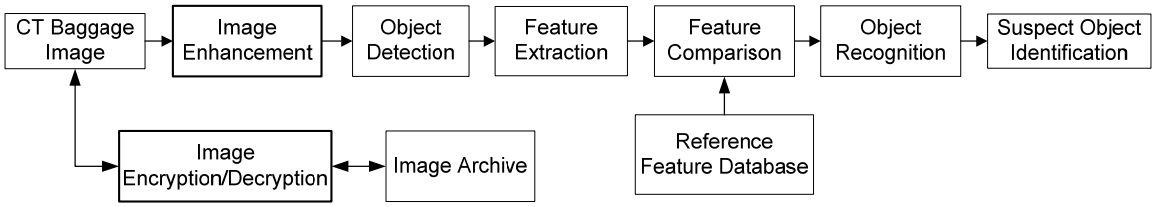


Figure 1.3: The multimedia security system for CT baggage scanning applications.

The presented system can also be used in biometric identification systems for securing access to classified locations. Examples of biometrics used in these systems include fingerprints, faces, irises and hands. As an example of biometric identification systems, Figure 1.4 shows a fingerprint access control system. The system first enhances the contrast of a fingerprint, then removes background noise, and then performs fingerprint detection and feature extraction. The extracted features are then compared to features referenced in the fingerprint database to verify whether the person is authorized or not. The recognition decision will result in the user being authorized or refused access to any region protected by the system.

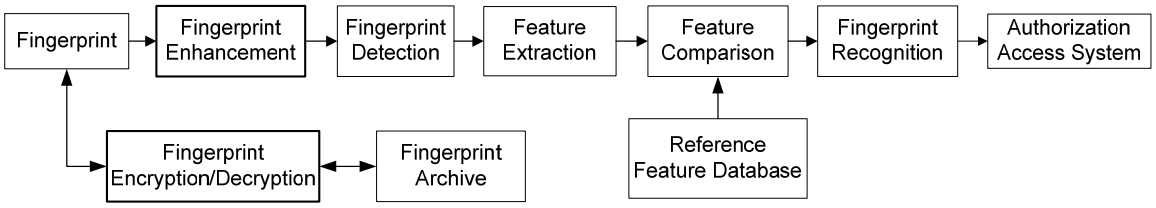


Figure 1.4: The multimedia security system for biometric identification applications.

www.manaraa.com

Cancer is a leading cause of death among human beings. The presented multimedia security system can be used in medical applications for the detection of early-stage tumors and cancers. The system is shown in Figure 1.5. In order to perform cancer detection, the reference feature database should be created for different types of cancers or tumors. The encryption process is used to protect the medical data.

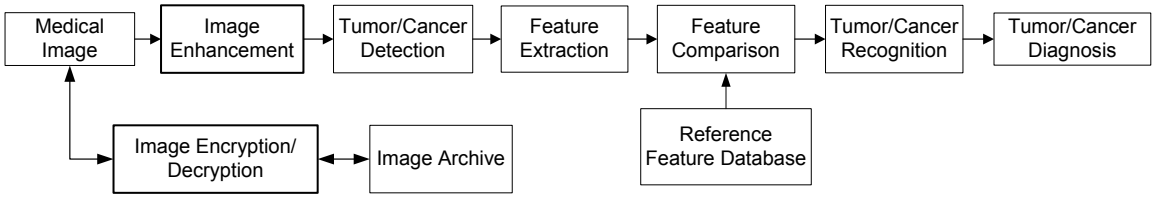


Figure 1.5: The multimedia security system for medical applications.

www.manaraa.com

1.3 Brief Introduction

The rest of this dissertation will focus on the enhancement and encryption portions of the presented multimedia security system and present contributions to image enhancement and multimedia encryption.

1.3.1 Introduction to Image Enhancement

Images and videos with high resolution and contrast can significantly improve the efficiency and accuracy of the presented multimedia security system when it comes to object detection and recognition. However, due to limitations of the system hardware and changes in background illumination conditions, images and videos may be of a low visual quality and/or contain noise. Image enhancement is a powerful tool to improve the visual quality of images and videos without affecting the image acquisition process or increasing system hardware costs. It can help the presented multimedia security system to recognize objects for security applications and detect cancer at an early stage for medical applications.

Many enhancement techniques have been employed to improve the contrast of images. They can be classified as the spatial domain techniques and the frequency domain techniques. Spatial domain techniques include histogram equalization [1-6], nonlinear filtering [7-12], adaptive neighborhood [13-17] and unsharp masking [18-22]. Frequency domain techniques are based on various transforms such as the Discrete Cosine

www.manaraa.com

Transform (DCT) [23-25], the Discrete Wavelet Transform (DWT) [26-30] and fuzzy set theory [31-34].

This dissertation introduces the following: a 3D CT baggage image enhancement algorithm for homeland security applications [35], three algorithms for mammogram enhancement (for breast cancer detection) [36-38] and two algorithms for enhancing prostate MR images (for prostate cancer detection) [39, 40]. A new enhancement measure called the Second-Derivative-like Measure of Enhancement (SDME) [35, 36, 38] is presented as a way to quantitatively evaluate the performance of the enhancement algorithms.

1.3.2 Introduction to Multimedia Encryption

Fast growing networking technologies and ubiquitous multimedia services have given people all over the world many opportunities to create, distribute, and access images and videos. For this reason, multimedia security is important for individuals, businesses, and governments in areas such as privacy and copyright protection. Multimedia encryption protects multimedia data by transforming it into an unrecognized format. Only authorized users with the correct security keys are able to decode and view protected data.

Images or videos can be encrypted either partially or fully using various technologies in the spatial or frequency domains. Image/video encryption in the frequency domain is often embedded in the compression process, which is mainly based on the Discrete Cosine Transform (DCT) [41-46] or Discrete Wavelet Transform (DWT) [47-49]. Image/video encryption in the spatial domain changes pixel locations and/or values using

www.manaraa.com

different techniques. Data Encryption Standard (DES) [50] and Advanced Encryption Standard (AES) [51, 52] are two examples of this method. However, they do have high computation costs [53]. Other techniques include chaos theory [54-58] and recursive sequences [59-62]. Nevertheless, due to their lack of security keys or the small key space, these approaches often involve either high computation costs or provide low levels of security.

To improve the efficiency and security level of existing encryption algorithms, this dissertation introduces five new recursive sequences and their corresponding transforms [63-68]. Since permutation-only based encryption methods are known to be vulnerable to some plaintext attacks [69, 70], this dissertation overcomes this weakness by offering a more secure encryption process that changes pixel data values as well as data positions. Bit-plane decomposition is an interesting method for changing multimedia data values. However, due to the fact that their decomposition results are sometimes predictable, several existing bit-plane decomposition based encryption methods [71-73] are subject to security limitations. To solve these problems, the dissertation introduces three new parametric bit-plane decomposition methods and uses them for image encryption [74-77]. A parametric Discrete Cosine Transform is also introduced for image encryption [78].

The edge map is a binary image containing all the edge information of an image. It has been used for many applications in image processing, including image enhancement, denoising, compression, segmentation and recognition, but it has never been used for image encryption. To investigate its applications for image encryption, this dissertation introduces three algorithms for image encryption [79-81].

www.manaraa.com

1.3.3 Dissertation Organization

This dissertation consists of four parts: Part I contains Chapter 1, which introduces *a new multimedia security system* for security and medical applications. Part II includes Chapter 2 and Chapter 3, which discuss *image enhancement for security and medical applications*. Part III consists of Chapter 4, Chapter 5 and Chapter 6, which present *multimedia encryption for security and medical applications*. Part IV draws *a conclusion and suggests several future directions*. Figure 1.6 gives the dissertation structure.

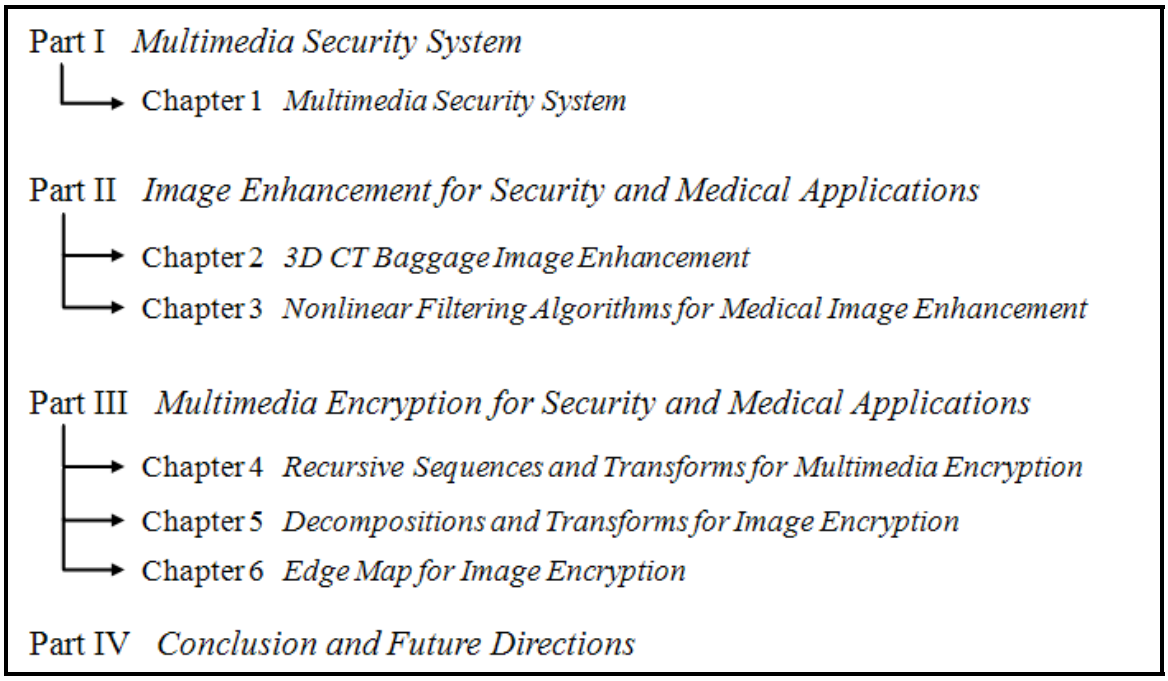


Figure 1.6: The structure of this dissertation.

www.manaraa.com

Part II

Image Enhancement for Security and Medical Applications

www.manaraa.com

Homeland security applications, visual surveillance systems, biometric identification systems and CT baggage scanning systems require video/image enhancement algorithms to help identify and track suspected criminals and aid in the detection of threatening objects. Due to limitations in system hardware and/or changes in background illumination conditions, these systems suffer from noise and low resolution of images or videos.

For medical applications, image enhancement algorithms can help aid the early detection of diseases and provide more accurate diagnoses. Breast cancer, for example, is the leading cause of death in women and prostate cancer is the single most common type of cancer occurring in men. Early detection of cancer using medical imaging technologies is an important and effective way to reduce mortality. Early treatment of breast cancer is most successful, while prostate cancer is curable at the early stage [82-84]. However, medical images may present characteristics such as poor resolution or low contrast due to the limitations of system hardware. Without affecting the image acquisition process or increasing system hardware costs, image enhancement is a powerful tool to improve the visual quality of images.

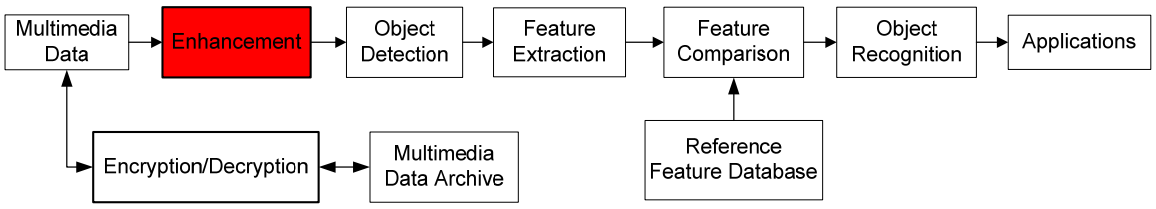


Figure II-1: Block diagram of the multimedia security system

To improve the efficiency and accuracy of the presented multimedia security system for object detection and recognition in security and medical applications, Part II discusses the

www.manaraa.com

enhancement process as shown in Figure II-1 and introduces several algorithms for enhancing both security images and medical images.

Part II first introduces a new enhancement measure to quantitatively evaluate the performance of the enhancement algorithms. It then introduces a 3D CT baggage image enhancement algorithm for homeland security applications, three mammogram enhancement algorithms for breast cancer detection, and two algorithms for enhancing prostate MR images for detecting prostate cancer.

Part II consists of Chapter 2 and Chapter 3. It is organized as follows.

Chapter 2 introduces:

1) An enhancement measure, called the Second-Derivative-like Measure of Enhancement (SDME) [35, 36, 38].

2) A 3D CT baggage image enhancement algorithm [35].

Chapter 3 presents:

1) Mammogram Enhancement Using the Alpha Weighted Quadratic Filter [37]

2) Human Visual System Based Mammogram Enhancement [38]

3) Nonlinear Unsharp Masking for Mammogram Enhancement [36]

4) Nonlinear Filtering for Enhancing Prostate MR Images via Alpha-Trimmed Mean Separation [39]

5) Logarithmic Enhancement for Prostate MR Images Using Nonlinear Filtering [40].

www.manaraa.com

Chapter 2

3D CT Baggage Image Enhancement

This chapter introduces a new SDME enhancement measure for quantitatively evaluating the performance of enhancement algorithms. It then presents a new 3D CT baggage image enhancement algorithm for homeland security applications.

www.manaraa.com

2.1 Introduction

Baggage scanning systems at security checkpoints in airports use computerized tomography (CT) scanning systems to scan and screen packages and luggage for the presence of explosives and other prohibited items [85, 86]. However, the CT baggage images often contain projection noise and are of a low resolution.

Many enhancement techniques have been employed to improve the contrast of images. Due to its simplicity and effectiveness, histogram equalization (HE) is one well-known technique for image enhancement [1]. However, this technique may significantly change the brightness of an input image and create visually undesirable artifacts [2]. To overcome this problem, Bi-histogram equalization was proposed, combining HE with a mean-separation technique [3]. This enhancement method strives to preserve the mean brightness of the original image. Many HE-based algorithms have been developed based on image decomposition such as minimum mean brightness error bi-histogram equalization [2], recursive mean-separate histogram equalization [4], dualistic sub-image histogram equalization [5], and recursively separated and weighted histogram equalization [6].

To develop enhancement algorithms that will improve the image's visual quality, remove noise and not create undesirable artifacts, a new enhancement algorithm is introduced for security images and demonstrate its performance on 3D CT baggage images.

www.manaraa.com

After analyzing the characteristics of the CT baggage images, this chapter introduces a new enhancement algorithm that combines alpha-weighted mean separation with the enhancement method, while removing background projection noise. Simulation results and a comparative analysis are given to demonstrate the presented algorithm's performance.

To provide a quantitative performance metric, this chapter introduces a new enhancement measure called the Second-Derivative-like Measure of Enhancement (SDME), using the concept of the second derivative for quantitative assessment of image enhancement.

The rest of this chapter is organized as follows. Section 2.2 introduces the SDME measure. Section 2.3 analyzes the CT baggage images and introduces an image denoising scheme. Section 2.4 introduces an algorithm for enhancing CT baggage images. Section 2.5 addresses a summary discussion and several future directions.

www.manaraa.com

2.2 Image Enhancement Measure

Quantitatively measuring and evaluating the enhancement performance of an algorithm can be extremely difficult due to the fact that the improvement of an enhanced image is often subjective and hard to measure. There is, therefore, no universal measure able to specify both the objective and subjective validity of an enhancement method [87]. Since image enhancement is intended to improve image contrast, the enhancement measure is usually based on contrast measure. This section first reviews several existing measures of image enhancement and then introduces a new enhancement measure using the concept of the second derivative.

2.2.1 Existing Enhancement Measures

Several measures of image enhancement have been developed using the contrast measure. The EME (measure of enhancement) and the EMEE (measure of enhancement by entropy) were developed in [88]. These two measures are based on Weber's Law [89]. Later, the AME (Michelson-Law measure of enhancement) and AMEE (Michelson-Law measure of enhancement by entropy) were introduced, incorporating the Michelson's Law [90, 91], to improve the measure performance of the EME and EMEE [23]. Since PLIP (Parameterized Logarithmic Image Processing) subtraction has been shown to be consistent with Weber's Law and with characteristics of the human visual system [92], the contrast information can be presented and processed more accurately. Finally, the

www.manaraa.com

logAME (logarithmic Michelson contrast measure) and the logAMEE (logarithmic AME by entropy) were developed, using the PLIP operators to improve these measures [93].

TABLE 2.1 THE DEFINITION OF SEVERAL ENHANCEMENT MEASURES

Name	Definition	Reference
EME	$EME_{k_1k_2} = \frac{1}{k_1k_2}\sum_{l=1}^{k_1}\sum_{k=1}^{k_2}\left[20\ln\left(\frac{I^W_{\max;k,l}}{I^W_{\min;k,l}+c}\right)\right]$	[88]
EMEE	$EMEE_{\alpha k_1k_2} = \frac{1}{k_1k_2}\sum_{l=1}^{k_1}\sum_{k=1}^{k_2}\left[\alpha\left(\frac{I^W_{\max;k,l}}{I^W_{\min;k,l}+c}\right)^{\alpha}\ln\left(\frac{I^W_{\max;k,l}}{I^W_{\min;k,l}+c}\right)\right]$	[88]
AME	$AME_{k_1k_2} = -\frac{1}{k_1k_2}\sum_{l=1}^{k_1}\sum_{k=1}^{k_2}\left[20\ln\left(\frac{I^W_{\max;k,l}-I^W_{\min;k,l}}{I^W_{\max;k,l}+I^W_{\min;k,l}+c}\right)\right]$	[23]
AMEE	$AMEE_{\alpha k_1k_2} = -\frac{1}{k_1k_2}\sum_{l=1}^{k_1}\sum_{k=1}^{k_2}\left[\alpha\left(\frac{I^W_{\max;k,l}-I^W_{\min;k,l}}{I^W_{\max;k,l}+I^W_{\min;k,l}+c}\right)^{\alpha}\ln\left(\frac{I^W_{\max;k,l}-I^W_{\min;k,l}}{I^W_{\max;k,l}+I^W_{\min;k,l}+c}\right)\right]$	[23]
logAME	$\log AME_{k_1k_2} = \frac{1}{k_1k_2}\otimes\sum_{l=1}^{k_1}\sum_{k=1}^{k_2}\left[\frac{1}{20}\otimes\ln\left(\frac{I^W_{\max;k,l}\Theta I^W_{\min;k,l}}{I^W_{\max;k,l}\oplus I^W_{\min;k,l}}\right)\right]$	[93]
logAMEE	$\log AMEE_{k_1k_2} = \frac{1}{k_1k_2}\otimes\sum_{l=1}^{k_1}\sum_{k=1}^{k_2}\left[\left(\frac{I^W_{\max;k,l}\Theta I^W_{\min;k,l}}{I^W_{\max;k,l}\oplus I^W_{\min;k,l}}\right)*\ln\left(\frac{I^W_{\max;k,l}\Theta I^W_{\min;k,l}}{I^W_{\max;k,l}\oplus I^W_{\min;k,l}}\right)\right]$	[93]

where the image is broken up into $k_1 \times k_2$ blocks, α, c are constants, and $c = 0.0001$ to avoid dividing by zero.

All these enhancement measures divide an image into $k_1 \times k_2$ blocks, and then calculate the average values of the measure results of all the blocks in the entire image. The definitions of these measures are listed in Table 2.1.

However, these enhancement measures only calculate the maximum and minimum values of the small regions or blocks in images. As a result, they are very sensitive to noise and to steep edges in images, which significantly increase the measure results. To overcome this problem, this section introduces a new enhancement measure using the concept of the second derivative.

www.manaraa.com

2.2.2 The New Enhancement Measure

Integrating the concept of the second derivative with the strengths of the reviewed measures, this section introduces a new enhancement measure using a second-derivative-like visibility operator [94].

The measure - the second-derivative-like measure of enhancement (SDME) – is defined by,

$$SDME = -\frac{1}{k_1 k_2}\sum_{l=1}^{k_1}\sum_{k=1}^{k_2} 20\ln\left|\frac{I_{\max;k,l} - 2I_{center;k,l} + I_{\min;k,l}}{I_{\max;k,l} + 2I_{center;k,l} + I_{\min;k,l}}\right| \quad (1)$$

where an image is divided into $k_1 \times k_2$ blocks, $I_{\max;k,l}, I_{\min;k,l}$ are the maximum and minimum values of the pixels in each block separately, and $I_{center;k,l}$ is the intensity of the center pixel in each block. Thus, the size of the blocks should be composed of an odd number of pixels such as 3×3 or 5×5.

The SDME definition can be modified by replacing the intensity of the center pixel in each block with the mean value of each block. The SDME is then defined by,

$$SDME = -\frac{1}{k_1 k_2}\sum_{l=1}^{k_1}\sum_{k=1}^{k_2} 20\ln\left|\frac{I_{\max;k,l} - 2I_{mean;k,l} + I_{\min;k,l}}{I_{\max;k,l} + 2I_{mean;k,l} + I_{\min;k,l}}\right| \quad (2)$$

where an image is divided into $k_1 \times k_2$ blocks, $I_{\max;k,l}, I_{\min;k,l}, I_{\text{mean};k,l}$ are the maximum, minimum, and mean values of pixels in each block separately. Thus, the users have flexibility to use any block size. Based on the definition above, the range of the SDME

www.manaraa.com

values should be between zero and $20\ln(2I_{max}+1)$. For grayscale image with data range between [0, 255], the SDME will be $[0,124.73)$.

2.2.3 Performance Comparison of Enhancement Measures

This section compares the measure performance of the SDME measure to that of several above mentioned enhancement measures under different conditions such as contrast laws, different image types, negative images, and the changes of background luminance and the levels of noise.

2.2.3.1 Adaptive to Different Contrast Laws

Table 2.2 shows that the enhancement measures are consistent with different Laws. The SDME is based on the concept of the second derivative. It is satisfied with Fechner's Law and Michelson's Law.

TABLE 2.2 COMPARISON OF ENHANCEMENT MEASURES BASED ON CONTRAST LAWS

Laws	EME	EMEE	AME	AMEE	logAME	logAMEE	SDME
Weber's Law	Yes	Yes					
Fechner's Law	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Michelson's Law			Yes	Yes	Yes	Yes	Yes
Entropy		Yes		Yes		Yes	

2.2.3.2 Different Types of Images

This section compares the SDME with other enhancement measure when it comes to measuring different types of images such as grayscale, medical and satellite images. These images are 8-bit images with image intensity range between 0 and 255. The 16-bit CT baggage images are also devalued by all these measures. Figure 2.1 shows these test

www.manaraa.com

images, including four grayscale images, four medical images, four satellite images and four CT baggage images.

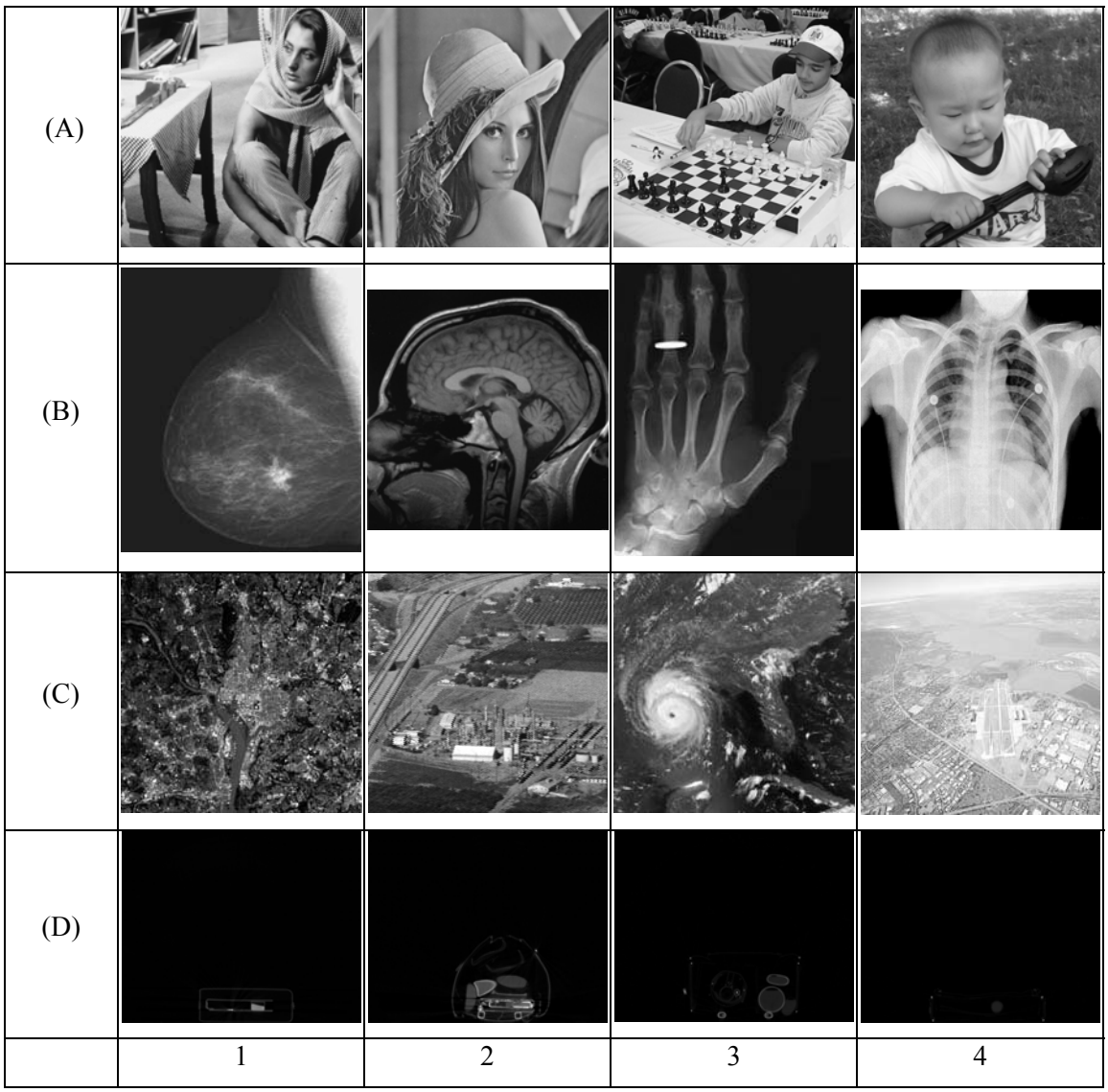


Figure 2.1: Different types of images. (A) Grayscale images; (B) Medical Images; (C) Satellite Images; (D) 16-bit CT baggage images.

All images in Figure 2.1 were measured using EME, EMEE, AME, AMEE, logAME, logAMEE and SDME, respectively. The measure results are shown in Table 2.3 and

www.manaraa.com

plotted in Figure 2.2. The measured results demonstrate that all measures show good measurement performance and are able to evaluate these types of images.

TABLE 2.3 MEASURE RESULTS OF IMAGES IN FIGURE 2.1 USING DIFFERENT ENHANCEMENT MEASURE

	EME	EMEE	AME	AMEE	logAME	logAMEE	SDME
(A)-1	4.0290	0.6400	18.3782	0.1023	0.0252	0.1139	31.5485
(A)-2	1.7110	0.1500	24.6483	0.0764	0.0412	0.1118	38.5153
(A)-3	4.2655	3.3384	22.0596	0.0783	0.0316	0.1079	34.5125
(A)-4	1.7050	0.1576	25.0700	0.0755	0.0412	0.1125	39.7486
(B)-1	0.9102	0.0566	23.2472	0.0801	0.0413	0.1179	37.3556
(B)-2	2.4011	0.2473	20.4615	0.0945	0.0378	0.1186	34.0295
(B)-3	2.0897	0.1719	19.9701	0.1004	0.0359	0.1287	31.5140
(B)-4	3.3868	0.9866	16.7115	0.1069	0.0136	0.1188	29.7590
(C)-1	9.2828	2.5315	7.4273	0.1253	0.0100	0.1002	20.9987
(C)-2	3.3460	0.3459	16.2683	0.1154	0.0248	0.1333	31.1690
(C)-3	3.2865	0.3913	18.0628	0.1106	0.0297	0.1295	31.8516
(C)-4	2.6348	0.4068	24.6025	0.0788	0.0265	0.1012	37.6527
(D)-1	10.5142	10.7755	6.5663	0.0982	0.0113	0.0941	18.3563
(D)-2	10.4752	9.4127	6.0755	0.1018	0.0103	0.0933	18.9684
(D)-3	15.4568	20.1601	2.5016	0.0467	0.0044	0.0431	14.5381
(D)-4	10.8976	8.7617	5.7731	0.0928	0.0099	0.0875	18.7597

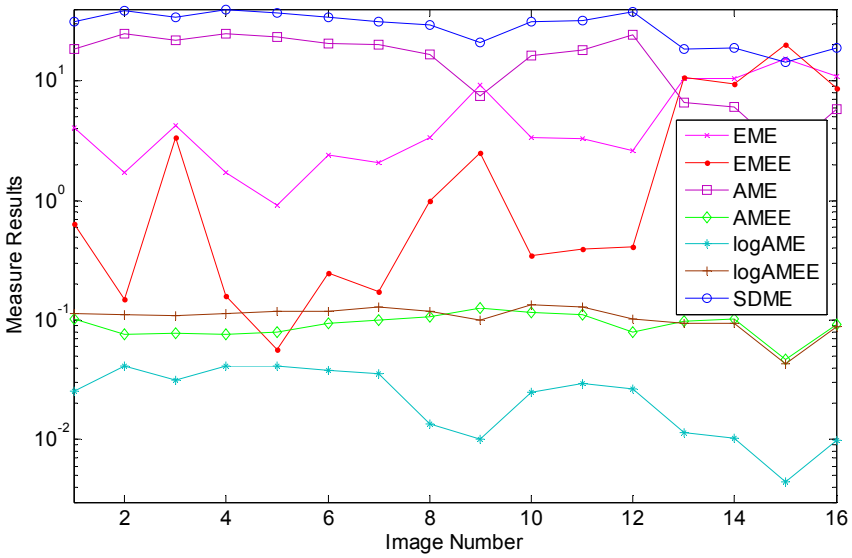


Figure 2.2: Plot measure results of several types of images using different enhancement measures.

www.manaraa.com

2.2.3.3 Different types of Negative Images

Figure 2.3 shows the negative photos of the images in Figure 2.1. These images are used to test the ability of the enhancement measure for assessing the negative images.

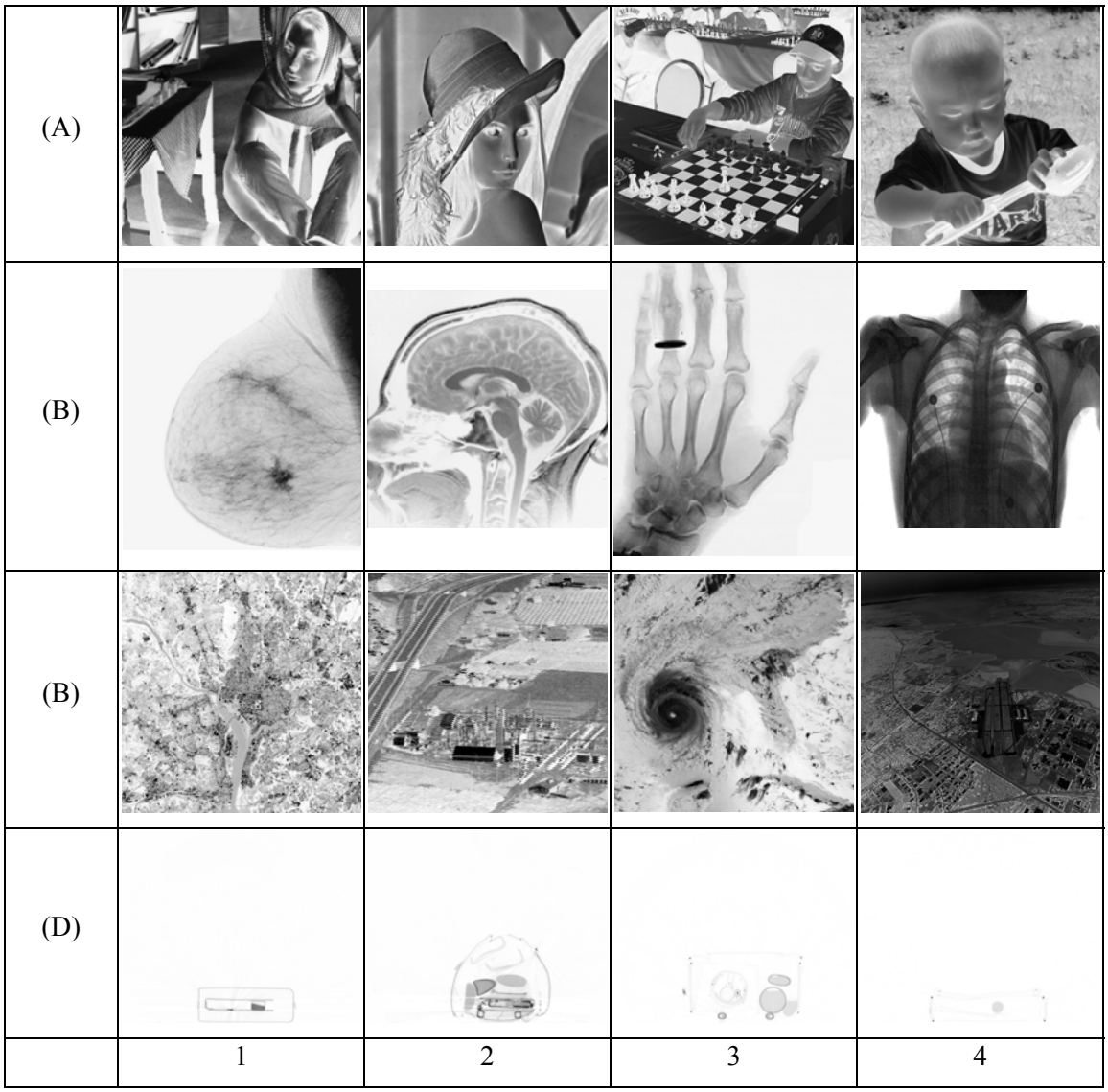


Figure 2.3: Negative photos of images in Figure 2.1. (A) Grayscale images; (B) Medical Images; (C) Satellite Images; (D) 16-bit CT baggage images.

All negative images in Figure 2.3 were measured using EME, EMEE, AME, AMEE, logAME, logAMEE and SDME, respectively. The measure results are shown in Table

www.manaraa.com

2.4 and plotted in Figure 2.4. The results show that all enhancement measures are able to evaluate negative images.

TABLE 2.4 MEASURE RESULTS OF IMAGES IN FIGURE 2.3 USING DIFFERENT ENHANCEMENT MEASURE

	EME	EMEE	AME	AMEE	logAME	logAMEE	SDME
(A)-1	4.2695	0.8588	18.8573	0.0968	0.0254	0.1133	31.9699
(A)-2	1.3482	0.1058	25.1715	0.0713	0.0412	0.1126	39.2257
(A)-3	3.3349	0.8382	21.5104	0.0859	0.0306	0.1103	34.1009
(A)-4	1.4221	0.1433	26.3966	0.0668	0.0421	0.1106	41.2321
(B)-1	0.5580	0.0382	30.0141	0.0523	0.0456	0.1072	44.1159
(B)-2	0.6694	0.0481	34.1264	0.0427	0.0438	0.1074	47.4854
(B)-3	0.6207	0.0623	33.7808	0.0426	0.0422	0.1162	45.3799
(B)-4	6.6515	3.0637	10.0137	0.1196	0.0117	0.1104	23.2939
(C)-1	3.6256	1.3519	17.6799	0.1036	0.0119	0.1064	31.6815
(C)-2	2.6236	0.6363	19.5995	0.0959	0.0266	0.1315	34.4847
(C)-3	1.8583	0.2387	25.4104	0.0776	0.0332	0.1250	39.1133
(C)-4	7.8577	10.1575	12.8956	0.1088	0.0223	0.1057	25.7752
(D)-1	0.0047	0.0002	72.8027	0.0010	0.0164	0.0982	85.7561
(D)-2	0.0085	0.0004	69.7396	0.0017	0.0152	0.1018	83.8189
(D)-3	0.0106	0.0005	66.3098	0.0020	0.0062	0.0467	80.0218
(D)-4	0.0047	0.0002	72.4838	0.0010	0.0144	0.0928	86.7122

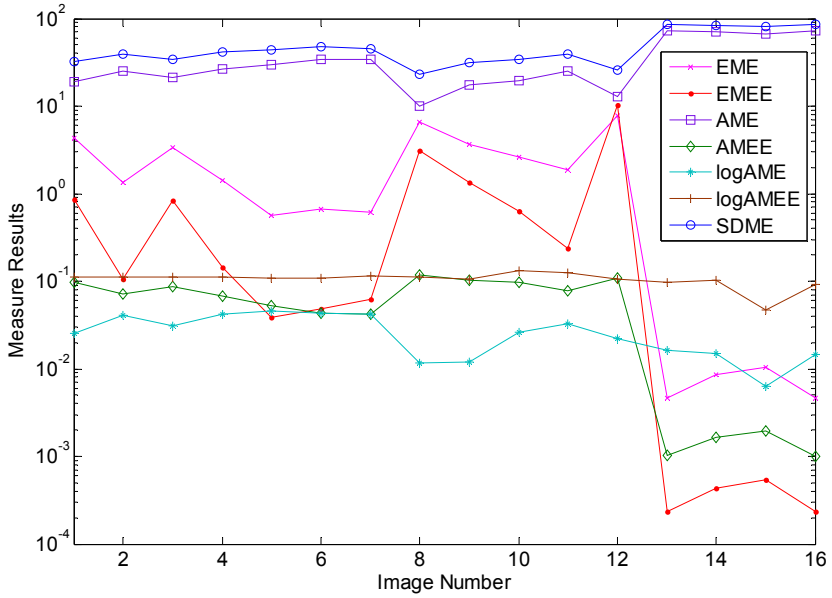


Figure 2.4: Plot measure results of negative photos of images in Figure 2.1 using different enhancement measures.

www.manaraa.com

2.2.3.4 Background luminance Change

This simulation investigates how the background luminance affects the measure results of different enhancement measures. Figure 2.5 shows 16 images which contain a lot of edges and different levels of background luminance. These images were also measured by the enhancement measures individually. The measured results are shown in Table 2.5 and plotted in Figure 2.6. The results demonstrate that higher background luminance will increase the SDME and AME results.

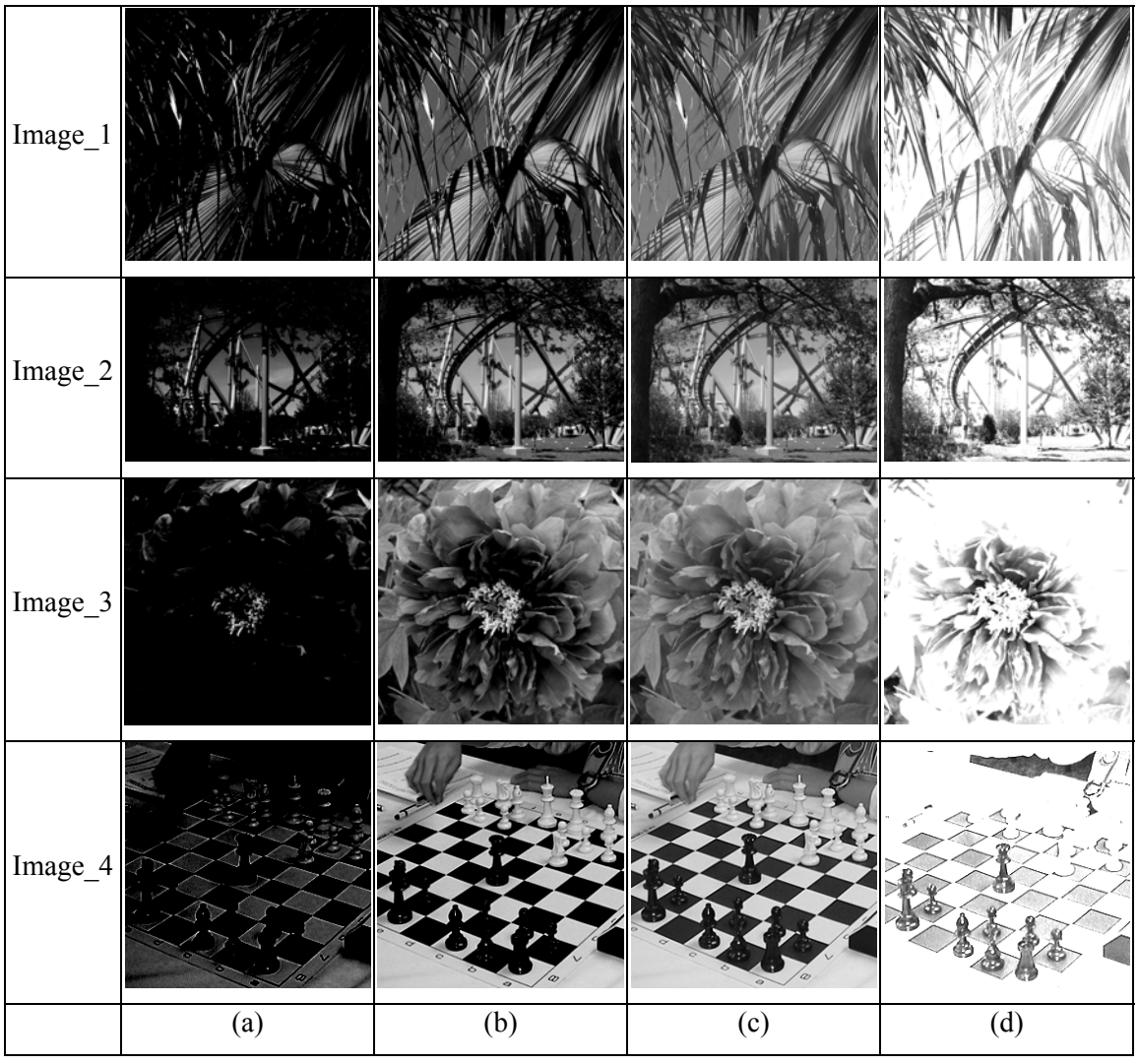


Figure 2.5: Images with background luminance change.

www.manaraa.com

TABLE 2.5 MEASURE RESULTS OF IMAGES IN FIGURE 2.5 USING DIFFERENT ENHANCEMENT MEASURE

	EME	EMEE	AME	AMEE	logAME	logAMEE	SDME
Image_1(a)	10.1701	7.1093	1.4497	0.0187	0.0034	0.0341	8.8899
Image_1(b)	11.1629	10.8697	7.8867	0.0781	0.0132	0.0795	19.1918
Image_1(c)	5.8083	1.6455	13.8182	0.1184	0.0209	0.1131	26.7210
Image_1(d)	1.0978	0.0711	24.3713	0.0782	0.0134	0.0551	35.8613
Image_2(a)	7.5734	4.7914	5.3130	0.0346	0.0109	0.0593	13.4711
Image_2(b)	12.1496	12.2265	7.2847	0.0587	0.0122	0.0634	17.6654
Image_2(c)	6.9183	1.2554	11.5844	0.1270	0.0167	0.1144	24.3707
Image_2(d)	1.6871	0.1162	20.5579	0.0974	0.0144	0.0713	32.9284
Image_3(a)	8.9890	3.8432	4.2404	0.0492	0.0095	0.0784	13.7414
Image_3(b)	4.3357	1.9816	17.2348	0.0883	0.0312	0.1120	30.9975
Image_3(c)	1.8171	0.2043	23.8117	0.0779	0.0411	0.1109	38.2081
Image_3(d)	0.2196	0.0125	32.6444	0.0410	0.0207	0.0706	45.5951
Image_4(a)	7.8073	2.9641	6.1197	0.0601	0.0123	0.0807	15.0407
Image_4(b)	5.6029	5.4403	17.5923	0.0573	0.0307	0.0776	28.7585
Image_4(c)	5.6086	4.3492	20.0424	0.0772	0.0287	0.0966	32.1571
Image_4(d)	0.3362	0.0194	27.7483	0.0547	0.0109	0.0537	39.8169

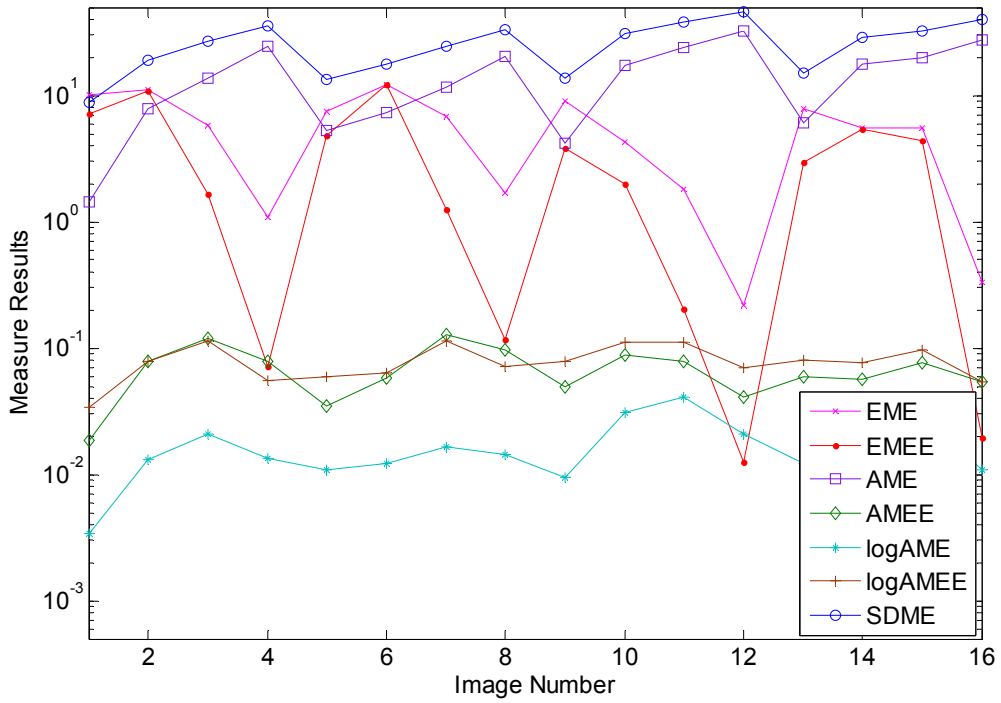


Figure 2.6: Plot measure results of images with background luminance change using different enhancement measures.

www.manaraa.com

2.2.3.5 Gaussian Noise Effect

Figure 2.7 shows 16 images embedded with different levels of Gaussian noise. This test is designed to investigate how Gaussian noise affects the measurement performance of these enhancement measures.

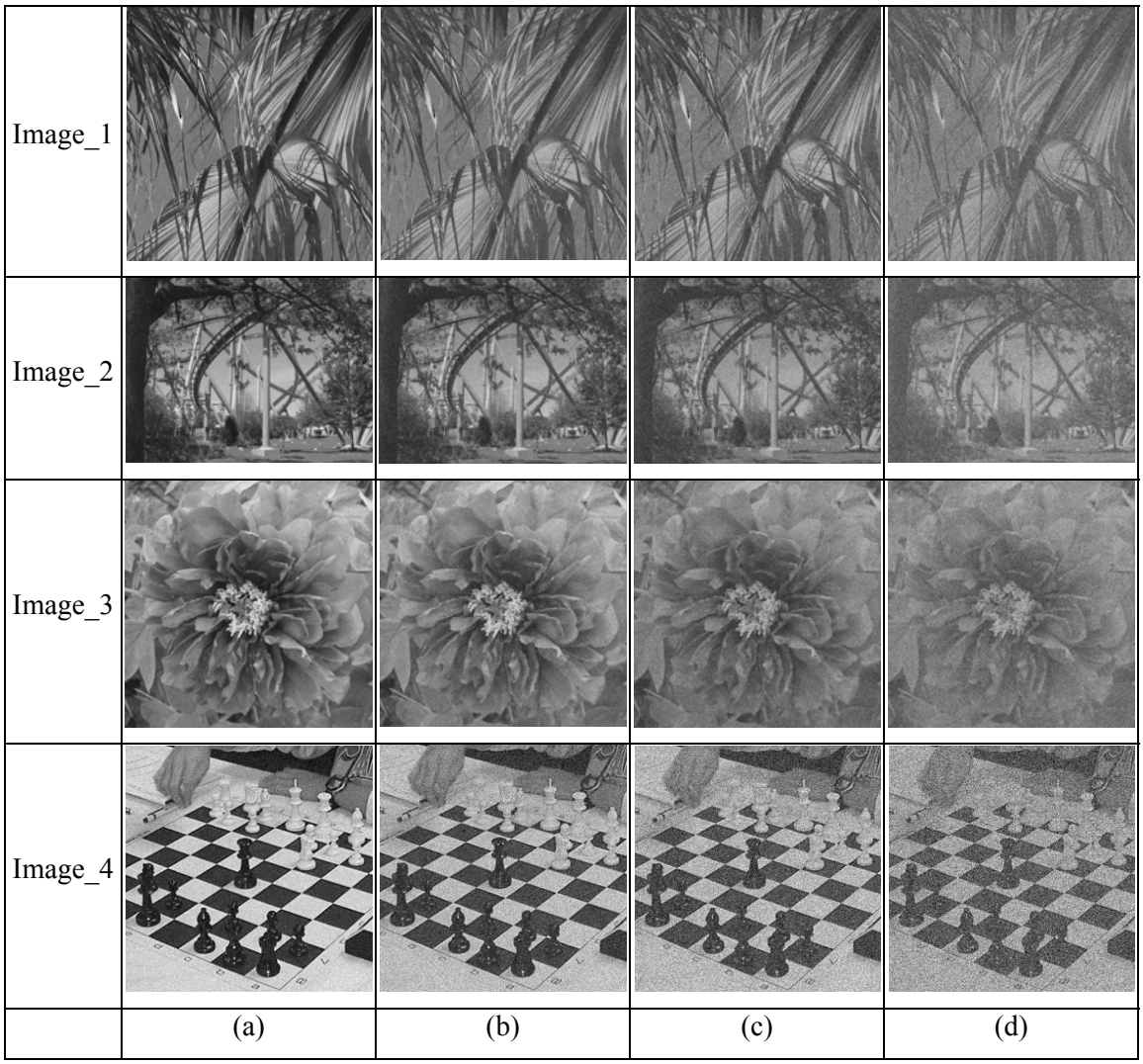


Figure 2.7: Images with different levels of Gaussian noise added.

These images with noise were measured individually by all above mentioned enhancement measures. The measure results are shown in Table 2.6 and plotted in Figure 2.8. The more Gaussian noise is added, the worse the image contrast visually will be. The

www.manaraa.com

results of SDME decrease as the level of Gaussian noise increase. This is also consistent with the visual assessment.

TABLE 2.6 MEASURE RESULTS OF IMAGES IN FIGURE 2I USING DIFFERENT ENHANCEMENT MEASURE

	EME	EMEE	AME	AMEE	logAME	logAMEE	SDME
Image_1(a)	8.1516	14.3138	9.6827	0.1213	0.0155	0.1207	23.9843
Image_1(b)	11.1389	31.6124	6.3977	-0.1497	0.0098	0.0923	20.6883
Image_1(c)	13.2356	67.5125	3.9170	-0.4788	0.0060	0.0566	18.0911
Image_1(d)	15.2586	73.2776	0.1247	-3.6137	0.0013	-0.0203	14.3536
Image_2(a)	10.2772	17.8065	7.8886	0.0509	0.0128	0.0984	22.0000
Image_2(b)	12.4190	56.3724	4.5988	-1.5568	0.0076	0.0547	18.7564
Image_2(c)	13.0054	37.2255	2.0090	-6.9031	0.0041	0.0072	16.2222
Image_2(d)	13.3541	106.0333	-1.7314	-11.4682	-0.0003	-0.0945	12.4955
Image_3(a)	3.9884	1.7298	15.0069	0.1191	0.0256	0.1402	29.9022
Image_3(b)	6.8324	6.1852	10.0712	0.0440	0.0158	0.1297	24.5424
Image_3(c)	9.6927	23.0281	6.8314	-0.1716	0.0102	0.1007	21.1741
Image_3(d)	14.2870	68.6244	2.4370	-1.4888	0.0038	0.0325	16.4915
Image_4(a)	8.3348	41.4229	12.6769	0.0892	0.0213	0.1067	26.7255
Image_4(b)	10.0902	79.0921	8.6893	-0.1807	0.0137	0.0893	22.7938
Image_4(c)	10.6306	50.2440	5.9380	-0.5848	0.0091	0.0623	20.1307
Image_4(d)	11.1258	60.5979	2.1147	-2.4057	0.0037	-0.0137	16.2023

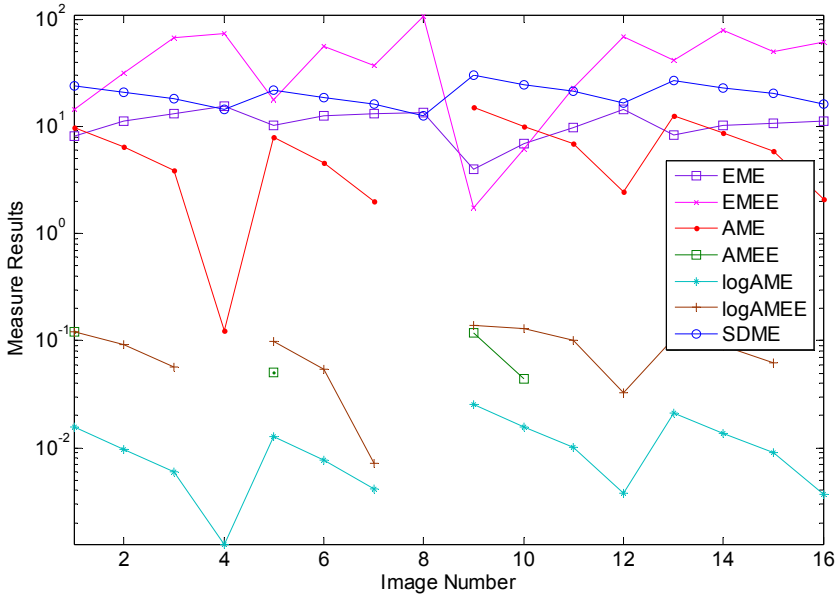


Figure 2.8: Plot measure results of images with different amount of Gaussian noise using different enhancement measures.

www.manaraa.com

2.2.3.6 Salt & Pepper Noise Effect

This simulation is to test how Salt & Pepper noise affects the measurement performance of these enhancement measures. Figure 2.9 shows 16 images embedded with different levels of Salt & Pepper noise.

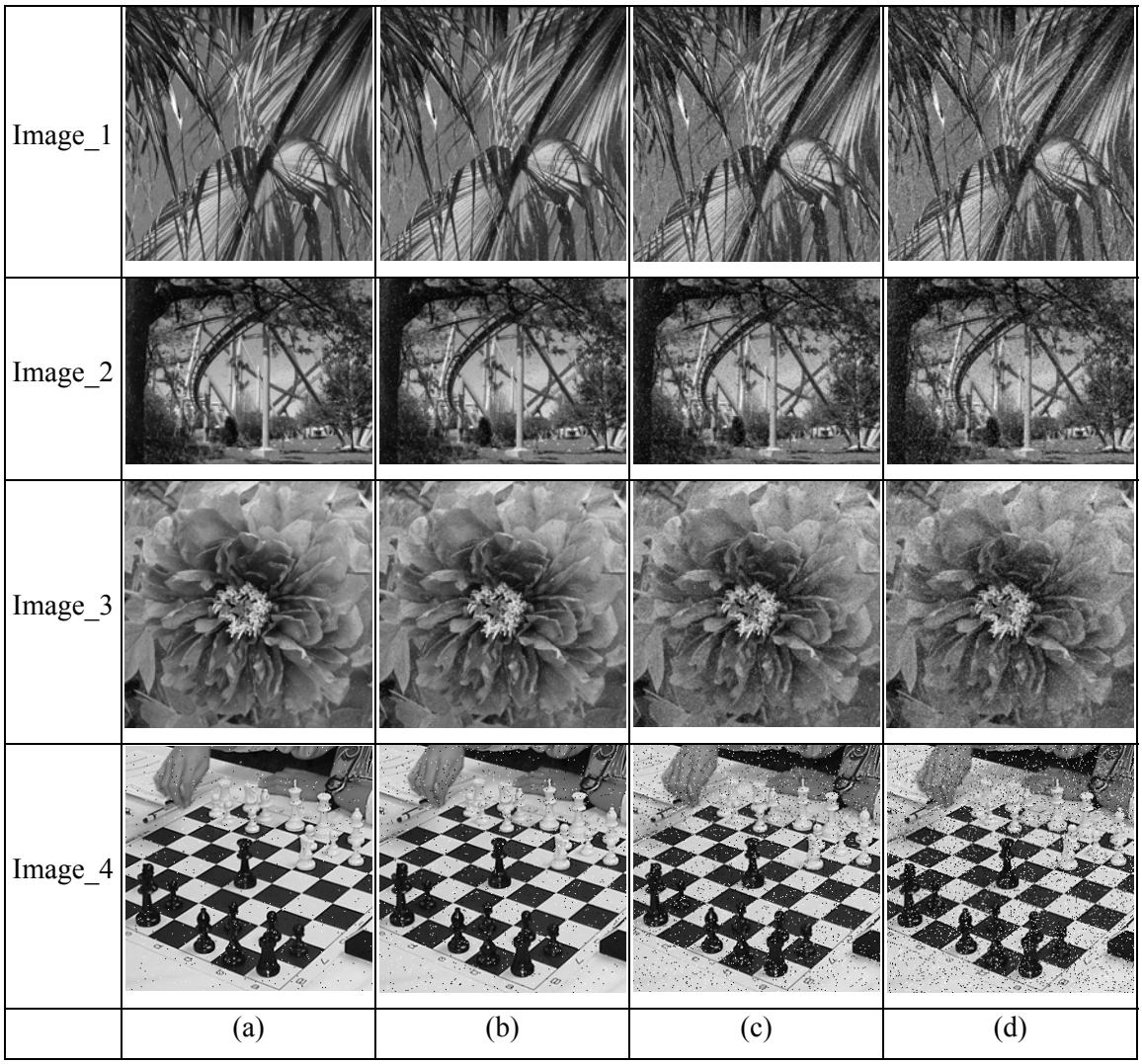


Figure 2.9: Images with different amount of Salt & Pepper noise added.

These images were measured by all enhancement measures above, individually. The measure results are shown in Table 2.7 and plotted in Figure 2.10. The results show that

www.manaraa.com

the Salt & Pepper noise does not significantly affects the SDME measure results. This demonstrates that the SDME can overcome the effect of the Salt & Pepper noise.

TABLE 2.7 MEASURE RESULTS OF IMAGES IN FIGURE 2.9 USING DIFFERENT ENHANCEMENT MEASURE

	EME	EMEE	AME	AMEE	logAME	logAMEE	SDME
Image_1(a)	6.1158	1.8539	12.8281	0.1132	0.0190	0.1033	25.9267
Image_1(b)	6.4075	2.0316	11.9228	0.1081	0.0174	0.0944	25.2521
Image_1(c)	7.2040	2.5763	9.5478	0.0942	0.0131	0.0716	23.2209
Image_1(d)	7.9108	3.0137	7.6181	0.0818	0.0098	0.0537	21.4853
Image_2(a)	7.2460	1.6201	10.8077	0.1202	0.0153	0.1050	23.7027
Image_2(b)	7.6475	2.0443	10.0273	0.1136	0.0139	0.0953	22.9607
Image_2(c)	8.4881	2.8928	8.1638	0.0972	0.0107	0.0738	21.3545
Image_2(d)	9.3620	3.7847	6.4851	0.0822	0.0079	0.0550	19.6335
Image_3(a)	2.1264	0.2843	22.0902	0.0771	0.0376	0.1015	36.8285
Image_3(b)	2.4498	0.3762	20.4982	0.0762	0.0343	0.0926	35.4825
Image_3(c)	3.2652	0.5954	16.1490	0.0721	0.0257	0.0700	31.8750
Image_3(d)	3.9543	0.7616	12.9511	0.0676	0.0195	0.0532	29.0103
Image_4(a)	5.8243	4.5907	18.7569	0.0744	0.0263	0.0886	31.3786
Image_4(b)	6.0728	4.9144	17.4180	0.0719	0.0238	0.0805	30.3944
Image_4(c)	6.6685	5.7652	14.3144	0.0642	0.0184	0.0613	28.2824
Image_4(d)	7.2770	6.0418	11.4387	0.0579	0.0134	0.0460	26.1792

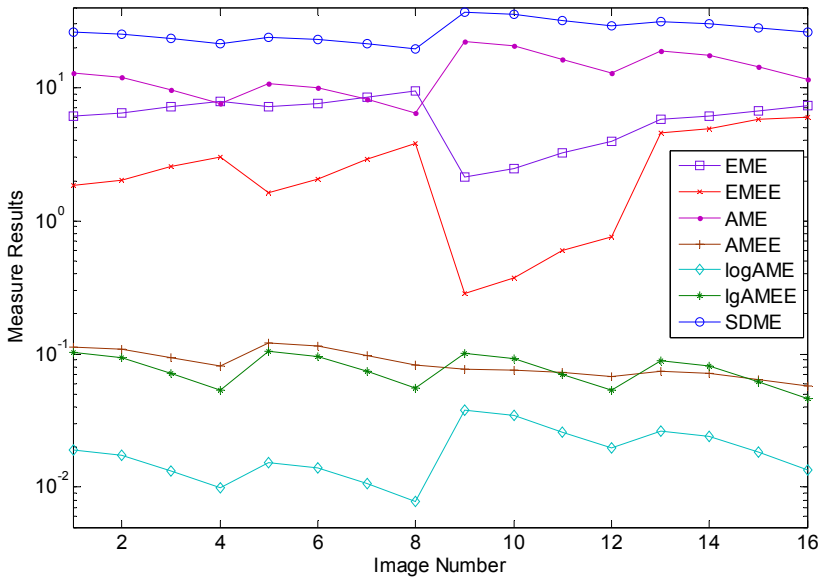


Figure 2.10: Plot measure results of images with different amount of Salt & Pepper noise using different enhancement measures.

www.manaraa.com

In summary, the SDME has been compared with six existing measure methods. Simulation results have demonstrated that the SDME's excellent measure performance. It has ability to evaluate different types of images, measure the change of the background luminance, and withstand the effect of noise. Section 2.4.2 and Chapter 3 will use the SDME for enhancement evaluation and parameter optimization.

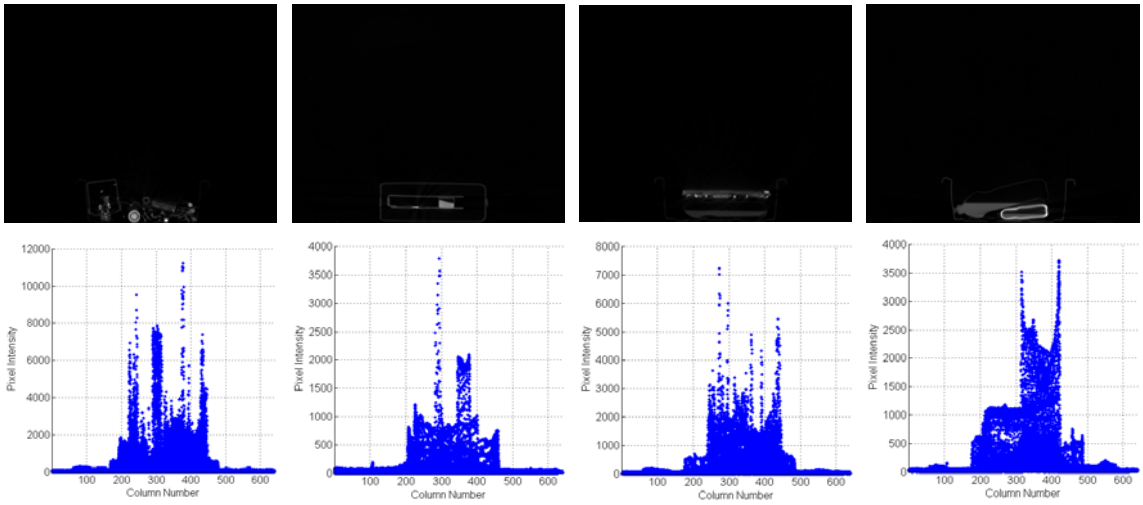
www.manaraa.com

2.3 2D CT Baggage Image Analysis and Denoising

A 3D CT baggage volume image consists of hundreds of 2D images called image slices. This section analyzes the characteristics of 2D CT baggage images. A new image denoising method is then introduced, using the alpha-weighted mean as a threshold for removing background noise from the 2D CT baggage images.

2.3.1 2D CT Baggage Image Analysis

In baggage scanning systems, the pixel values of CT baggage images are represented by 16 bits. In general, only the object skeletons with high intensity values are visually recognizable, while other regions are dark, as shown in Figure 2.11.

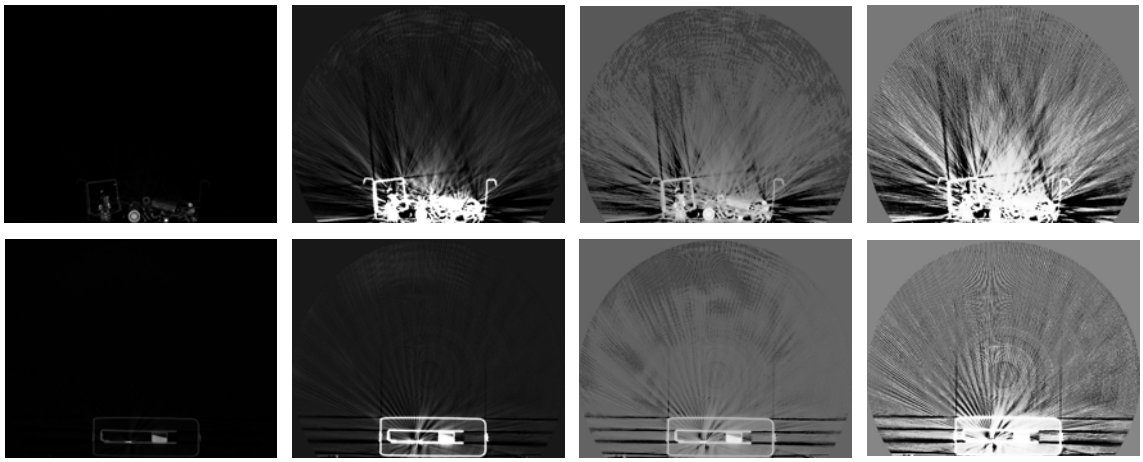


(a) (b) (c) (d)

Figure 2.11: 2D CT baggage images and their pixel intensity distribution in the column direction. The top row shows original images. The bottom row shows the pixel intensity distribution in the column direction. This demonstrates that pixel intensity values are very high in the object regions and extremely low in the dark regions.

www.manaraa.com

The bottom row in Figure 2.11 plots the pixel intensity distribution of 2D CT baggage images in the column direction. The pixels with high intensity values are concentrated in the object regions of the image. The non-object regions of the images are very dark where the pixel values are very small but not zeros. This observation shows that there is a lot of background noise in the 2D CT image. This can be verified by the results shown in Figure 2.12.



(a) (b) (c) (d)

Figure 2.12: 2D CT baggage images are processed by different nonlinear operations. (a) Original images; (b) uint8 [95]; (c) logarithmic operation [96]; (d) Histogram Equalization. This demonstrates that the CT images are subject to the presence of projection noise

In Figure 2.12, the 2D CT baggage images are processed by three different nonlinear processes, namely the uint8 format operation, the logarithmic operation and histogram equalization. The uint8 format (8-bit unsigned integer type) [95] operation converts the image intensity values to their nearest integers if they are between 0 and 255, sets them to 255 if image data values are greater than 255, and to zero if they are found to be less than zero resulting from the computational processing. The logarithmic operation processes

www.manaraa.com

images using a log function of the image intensity [96]. Histogram equalization [1] is a simple nonlinear transformation used for image enhancement. The results in Figure 2.12 demonstrate that background noise becomes visible after these nonlinear processes have been applied. Since image enhancement is also a nonlinear process, the enhancement of a 2D CT baggage image requires a preprocess to remove background noise.

2.3.2 2D CT Baggage Image Denoising

Since the intensity value of background noise in 2D CT baggage images is very small (as shown in the bottom row in Figure 2.11), background noise can be removed from the images using the image decomposition technique with a specific thresholding. In this section, an alpha-weighted mean value is used as the threshold. This is called the alpha-weighted mean separation.

For an input image, $I(m,n)$, the process separates the input image into two sub-images, $I_U(m,n)$ and $I_L(m,n)$. One sub-image, $I_L(m,n)$, contains those pixels with a value lower than the threshold. The other sub-image, $I_U(m,n)$, contains those pixels that have a value greater than the threshold. The maximum, mean and minimum values of the input images are $I_{\max}$, I_{mean}, and $I_{\min}$ respectively, while the alpha-weighted mean separation is defined by

$$\begin{cases} I_U(m,n) = I(m,n) & \text{for } I(m,n) \geq \alpha I_{mean} \\ I_L(m,n) = I(m,n) & \text{for } I(m,n) < \alpha I_{mean} \end{cases} \tag{3}$$

where αI_{mean} is the threshold value, and $I_{\min} \leq \alpha I_{mean} \leq I_{\max}$.

www.manaraa.com

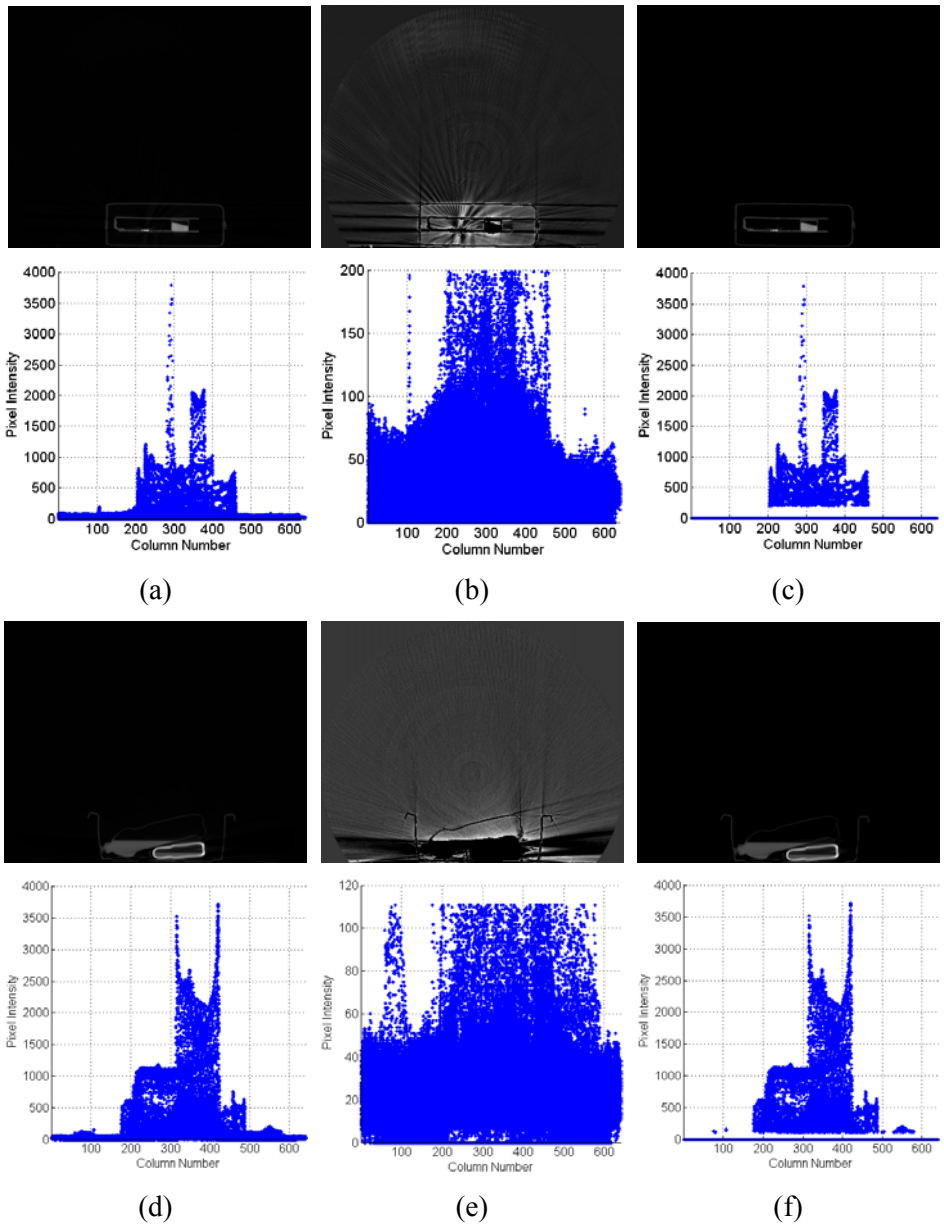


Figure 2.13: Alpha-weighted mean separation of the 2D CT baggage images. (a)-(f): the top row shows the original 2D CT baggage images and their sub-images; the second row shows their pixel intensity distributions in the column direction. (a)&(d) The original images; (b)&(e) The sub-images, $I_L(m,n)$, with pixel values less than the threshold; (c)&(f) The sub-images, $I_U(m,n)$, with pixel values greater than the threshold.

Figure 2.13 gives two examples of the alpha-weighted mean separation of the 2D CT baggage images. The sub-images with pixel values below the threshold contain the most

www.manaraa.com

background noise. The object is located in the sub-image that has a pixel value equal to or above the threshold. These are verified by their pixel intensity distributions in the column direction. The selection process of the α value will be discussed in Section 2.4.2.

www.manaraa.com

2.4 3D CT Baggage Image Enhancement Algorithm Using Alpha Weighted Mean Separation

This section introduces a new 3D CT baggage image enhancement algorithm and presents a new parameter training method using the SDME measure for optimizing the parameters and achieving the best enhancement performance. Simulation results and comparisons are given to demonstrate the enhancement performance of the presented algorithm.

2.4.1 The New Algorithm for Enhancing 3D CT Baggage Images

In general, a 3D CT baggage image is composed of hundreds of 2D images. It is also a volume image with a file size larger than 150MB. An average computer will have difficulty processing the entire 3D CT image at one time. To solve this problem, this dissertation introduces a new 3D CT baggage image enhancement algorithm that enhances the 2D images individually, and then combines the enhanced 2D images to obtain the final enhanced 3D CT image.

According to the image analysis in Section 2.3, the CT baggage images' background noise must be removed before the enhancement process is carried out. The presented enhancement algorithm uses alpha-weighted mean separation (AWMSE) for image denoising and enhancement. It enhances each 2D image using two main processes: noise removal and object image enhancement. Figure 2.14 shows the new algorithm.

www.manaraa.com

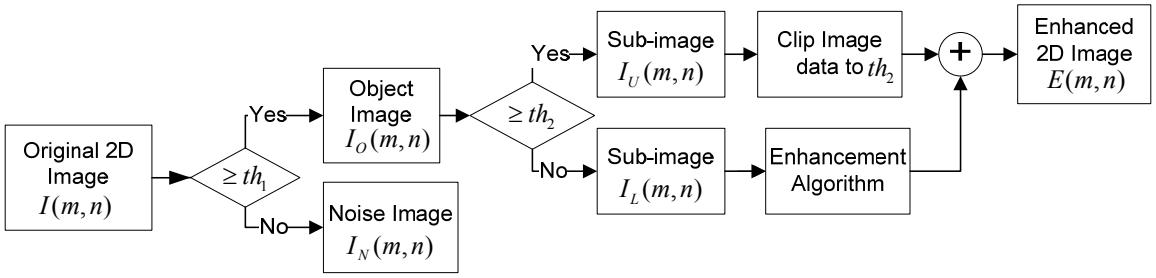


Figure 2.14: Block diagram of the AWMSE algorithm for CT baggage images.

First, the AWMSE algorithm obtains the object image by removing background noise from the original 2D CT image using the alpha-weighted mean separation as defined by,

$$\begin{cases} I_O(m,n) = I(m,n) & \text{for } I(m,n) \geq th_1 \\ I_N(m,n) = I(m,n) & \text{for } I(m,n) < th_1 \end{cases} \tag{4}$$

where $I_O(m,n)$ and $I_N(m,n)$ are the object image and the background noise image, respectively. The threshold $th_1 = \alpha_1 I_{mean}$, and I_{mean} is the mean value of the 2D CT image. The object image is then separated into two sub-images: the upper sub-image, $I_U(m,n)$, which contains those pixels that have an intensity value equal to or greater than the threshold th_2; and the lower sub-image, $I_L(m,n)$, which consists of those pixels that have an intensity value less than the threshold th_2. This separation is defined by,

$$\begin{cases} I_U(m,n) = I_O(m,n) & \text{for } I_O(m,n) \geq th_2 \\ I_L(m,n) = I_O(m,n) & \text{for } I_O(m,n) < th_2 \end{cases} \tag{5}$$

where the threshold $th_2 = \alpha_2 I_{O\_mean}$, and I_{O_mean} is the mean value of the object image $I_O(m,n)$.

www.manaraa.com

The upper sub-image includes all the bright regions of the original 2D CT image. This sub-image has a large data range despite the fact that there are a small number of pixels with adequately high intensity values. The lower sub-image, on the other hand, contains most of the informative pixels that have a lower intensity value and are in need of improvement. These pixels are what cause the CT images to be very dark even though they have a broad data range.

Users have the flexibility to use any new or existing enhancement method to enhance the lower sub-image. Histogram equalization is a well-known enhancement method and can significantly improve the contrast of and image without changing the image data range. To demonstrate the performance of the presented algorithm when considered as just one example of an existing enhancement method, histogram equalization is selected to enhance the lower sub-image.

Let $\{X_0, X_1, ..., X_{p-1}\}$, $X_0 < X_1 < ... < X_{p-1}$, denote all nonzero discrete gray levels in the lower image $I_L(m,n)$. For a given pixel value $I_L(m,n) = X_k$, $k = 0,1,...p-1$, its cumulative density function is,

$$C_{I_L(m,n)} = \sum_{i=0}^{k} \frac{q_k}{q} \tag{6}$$

where q_k is the number of times that the gray level X_k appears in the lower image $I_L(m,n)$ and q is the total number of the nonzero pixels in the lower image $I_L(m,n)$.

www.manaraa.com

The pixel intensity of the upper image can then be clipped to the maximum value of the lower image (which is also equal to the threshold th_2) in such a way that the data range of the images is significantly narrowed down without generating additional artifacts.

The final enhanced 2D CT image can be obtained by

$$E(m,n) = E_U(m,n) + E_L(m,n) \tag{7}$$

where,

$$\begin{cases} E_U(m,n) = th_2 & \text{for } I_U(m,n) \neq 0 \\ E_L(m,n) = X_0 + (X_{p-1} - X_0)C_{I_L(m,n)} \end{cases}$$

and where X_0 and $X_{p-1} = th_2$ are the minimum and maximum values in the image $I_L(m,n)$.

Note that the enhancement process in the presented algorithm reverts to the traditional histogram equalization when $th_2 = I_{\max}$. In this case, the lower sub-image is equal to the object image, namely $I_L(m,n) = I_O(m,n)$; the upper sub-image is zero, i.e. $I_U(m,n) = 0$.

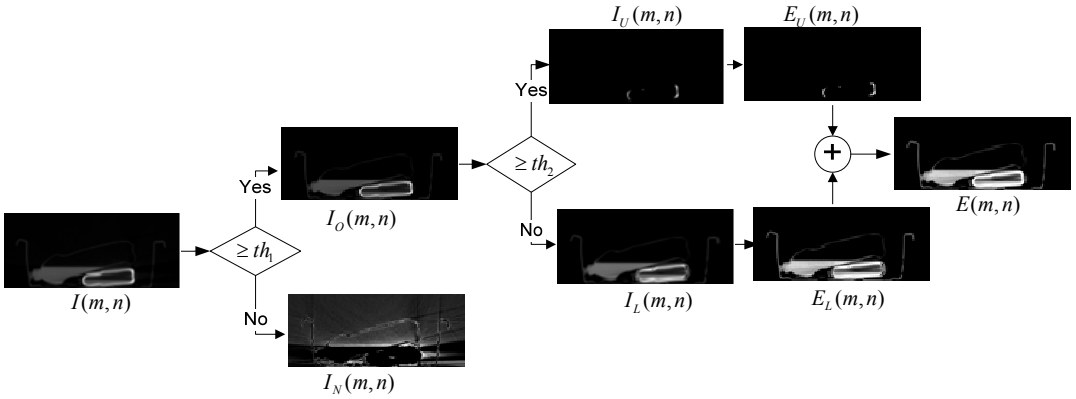


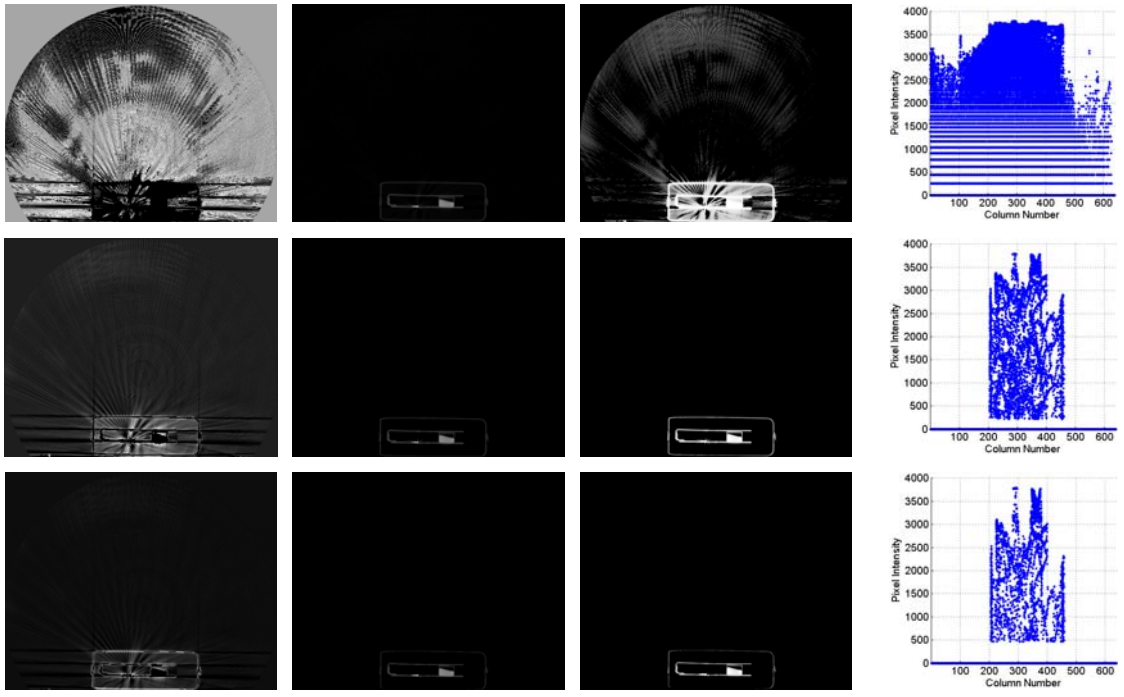
Figure 2.15: Image changes at each step of the AWMSE algorithm.

www.manaraa.com

Figure 2.15 gives an example that demonstrates how the image changes in each process in the AWMSE algorithm.

2.4.2 Train Parameters

The AWMSE algorithm has two parameters: α_1 for noise removal and α_2 for image enhancement. This section addresses how the parameters affect the enhanced results, as well as the methods used to select the parameters.



(a) Lower sub-images (b) Upper sub-images (c) Enhanced upper sub-images (d) Enhanced upper sub-images

Figure 2.16: 2D CT baggage image separation using different alpha values. Top row: α=1; Middle row: α=5.3; Bottom row: α=12. (a) The lower sub-images, namely the noise images; (b) the upper sub-images, namely the object images; (c) the enhanced upper sub-images; (d) the pixel intensity distribution of the enhanced upper images in the column direction.

www.manaraa.com

First, the parameter α_1 is trained for the noise removal process. To subtract the background noise from the original CT images, different α_1 values are used for image separation. The object images are then enhanced using the traditional histogram equalization, which is a special case of the AWMSE algorithm for $th_2 = I_{\max}$. Figure 2.16 gives a training example. If α_1 is very low, it means that there is some background noise present in the enhanced images, as is the case in the example given in the top row of Figure 2.16. The background noise can be removed when an appropriate α_1 value is used, as is the case in the middle row of Figure 2.16. However, some object information is lost if the α_1 value is very high, as is the case in the bottom row in Figure 2.16. Therefore, it can be conclude that the α_1 value of the example given in the middle row of Figure 2.16 is closest to being the best result, since it keeps the object information while removing background noise. This observation can be verified by examining the pixel intensity distributions in Figure 2.16(d).

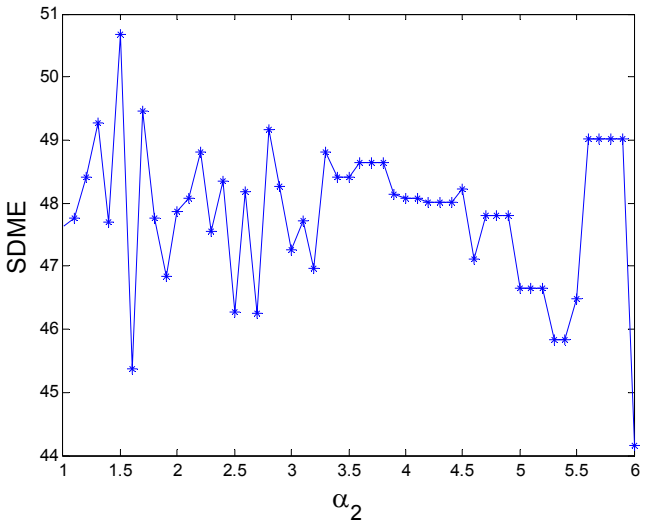
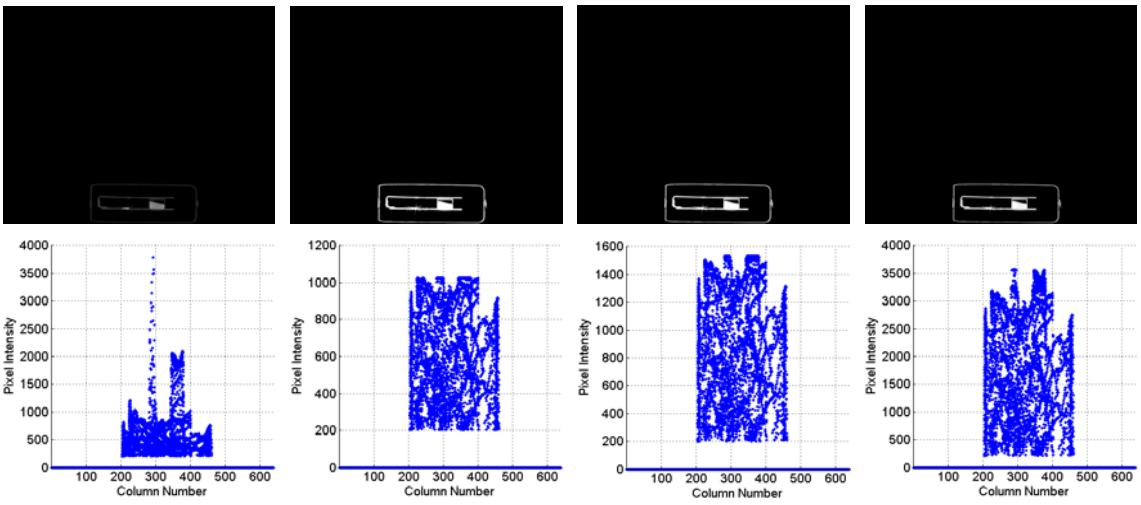


Figure 2.17: SDME measure results for 2D image enhancement using different α_2 values.

www.manaraa.com

For every α_1 value used in the noise removal process, the parameter α_2 is optimized for the image enhancement process. Based on the simulation results in Figure 2.16, the same CT baggage image is selected, whereas, for the noise removal process, α_1 is set to 5.3. Different α_2 values are applied for object image enhancement and the SDME is used to measure the enhanced images. Figure 2.17 plots the measure results. Figure 2.18 shows several enhanced images using the alpha values selected from Figure 2.17. The visual quality of the original image is significantly improved. The SDME measure results in Figure 2.18 demonstrate the improvement. The higher SDME values often results in the better enhancement performance. Thus the SDME is used to select the best α_2 value.



(a) Original 2D image SDME=44.3289 (b) α_2=1.6 SDME=45.37 (c) α_2=2.4 SDME=48.3398 (d) α_2=5.6 SDME=49.0154

Figure 2.18: 2D image enhancement using different alpha values selected from Figure 2.17. (a) shows the original object image obtained by the noise removal process, α_1=5.3; (b)-(d) shows the enhanced object images using different α_2 values.

www.manaraa.com

2.4.3 Simulation results

This section provides several simulations and measure results to demonstrate the AWMSE's enhancement performance. It then compares the presented algorithm with two existing enhancement methods for 2D CT baggage image enhancement.

2.4.3.1 CT Baggage Image Enhancement

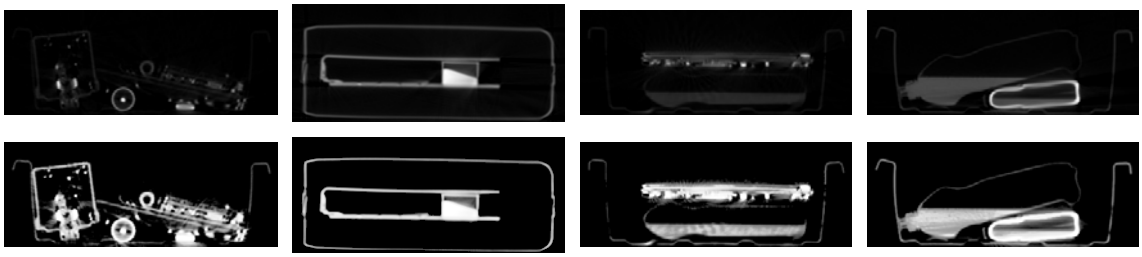
Figure 2.19 shows the enhanced results of four 2D CT baggage images. The images are enhanced by the AWMSE individually. The original images and enhanced images are measured by the SDME measure. The measure results are shown in Figure 2.19.

Figure 2.19: 2D CT baggage image enhanced by the AWMSE algorithm. The top row shows original images. The bottom row shows the enhanced images. (a) The slice image of the volume image #1; (b) The slice image of the volume image #2; (c) The slice image of the volume image #3; (d) The slice image of the volume image #4.

To show clearly the visual improvement of the enhanced images, Figure 2.20 shows object images that have been manually cropped from both the original and enhanced

www.manaraa.com

images in Figure 2.19 for visual clarity. The results show that the AWMSE significantly improves the visual quality of the 2D CT baggage images. The SDME measure results in Figure 2.19 verify this improvement.



(a) (b) (c) (d)

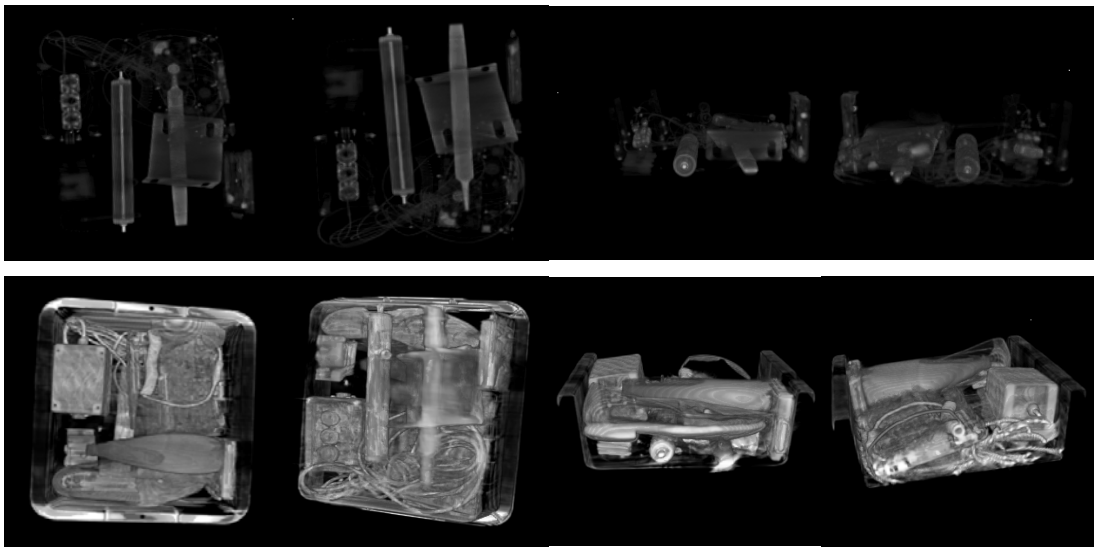
Figure 2.20: The regions cropped from the 2D CT baggage images in Figure 2.19. The top row shows the regions cropped from the original images. The bottom row shows the regions cropped from the enhanced images. (a) The object region cropped from the slice images in Fig 9(a); (b) The object region cropped from the slice images in Fig 9(b); (c) The object region cropped from the slice images in Fig 9(c); (d) The object region cropped from the slice images in Fig 9(d).

2.4.3.2 3D CT Baggage Image Enhancement

To show the performance of the AWMSE algorithm for 3D CT baggage image enhancement, this section presents several enhanced 3D CT baggage images.

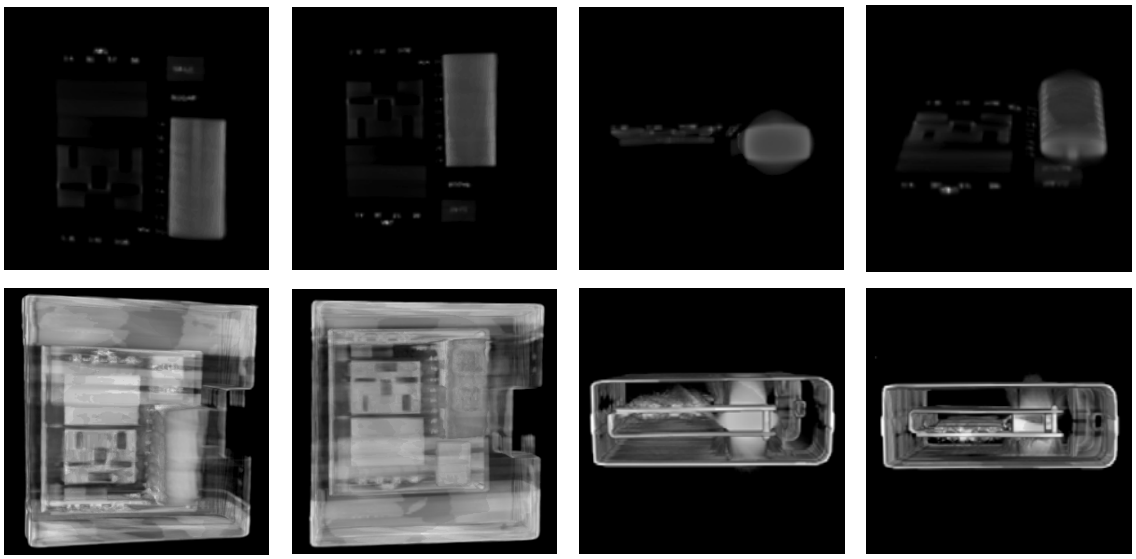
Figure 2.21-24 gives different views of the original and enhanced 3D CT baggage images. The top rows contain the original 3D CT baggage images as viewed from the top, bottom, front and back. The bottom rows show different views of the enhanced 3D CT baggage images from corresponding sides. As can be seen, the visual quality of the 3D CT baggage images is significantly improved. This demonstrates the excellent enhancement performance of the AWMSE when it comes to 3D CT baggage image enhancement.

www.manaraa.com



(a) (b) (c) (d)

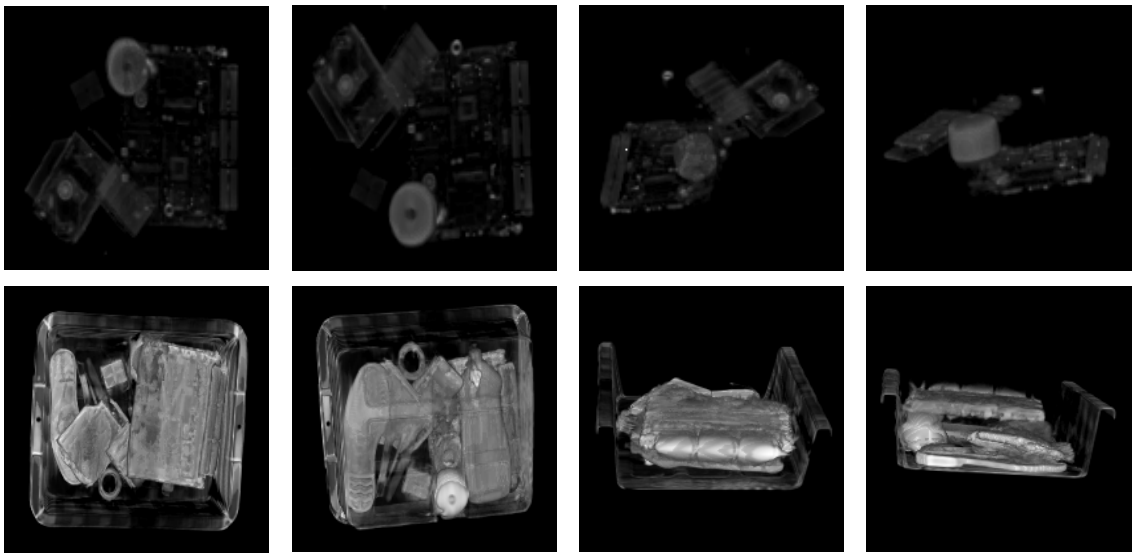
Figure 2.21: Enhanced results of 3D CT baggage image #1. The top row shows different views of the original 3D CT baggage image; the bottom row shows different views of the 3D image enhanced by the AWMSE algorithm. (a) Top view of the entire 3D image; (b) Bottom view of the entire 3D image; (c) Front side view of the 2D image slices #31-280; (d) Back side view of the 2D image slices #31-280.



(a) (b) (c) (d)

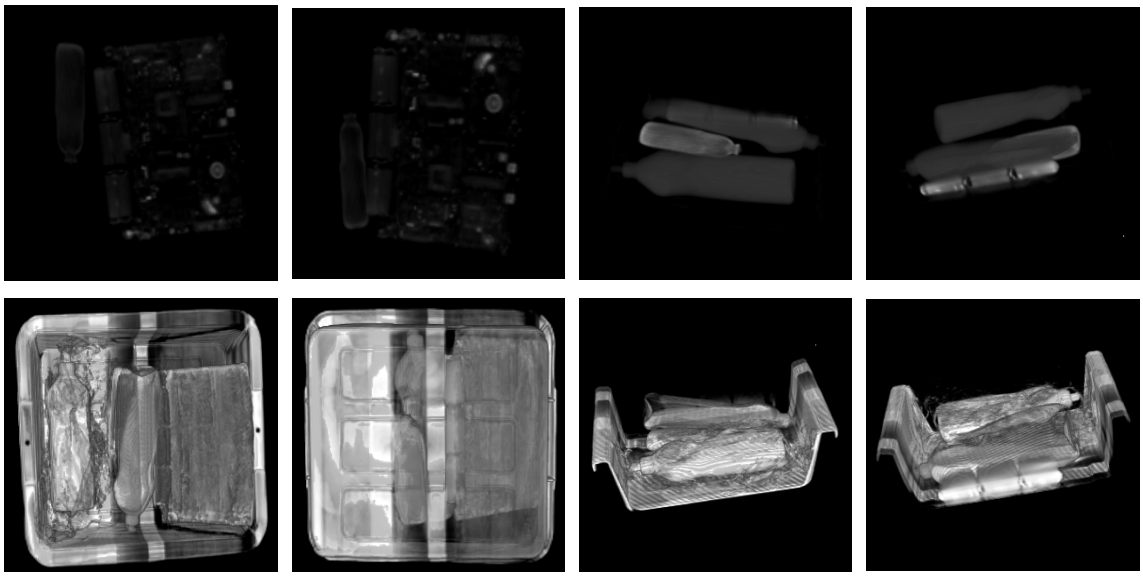
Figure 2.22: Enhanced results of 3D CT baggage image #2. The top row shows different views of the original 3D CT baggage image; the bottom row shows different views of the 3D image enhanced by the AWMSE algorithm. (a) Top view of the entire 3D image; (b) Bottom view of the entire 3D image; (c) Front side view of the 2D image slices #21-250; (d) Back side view of the 2D image slices #21-250.

www.manaraa.com



(a) (b) (c) (d)

Figure 2.23: Enhanced results of 3D CT baggage image #3. The top row shows different views of the original 3D CT baggage image; the bottom row shows different views of the 3D image enhanced by the AWMSE algorithm. (a) Top view of the entire 3D image; (b) Bottom view of the entire 3D image; (c) Front side view of the 2D image slices #34-293; (d) Back side view of the 2D image slices #34-293.



(a) (b) (c) (d)

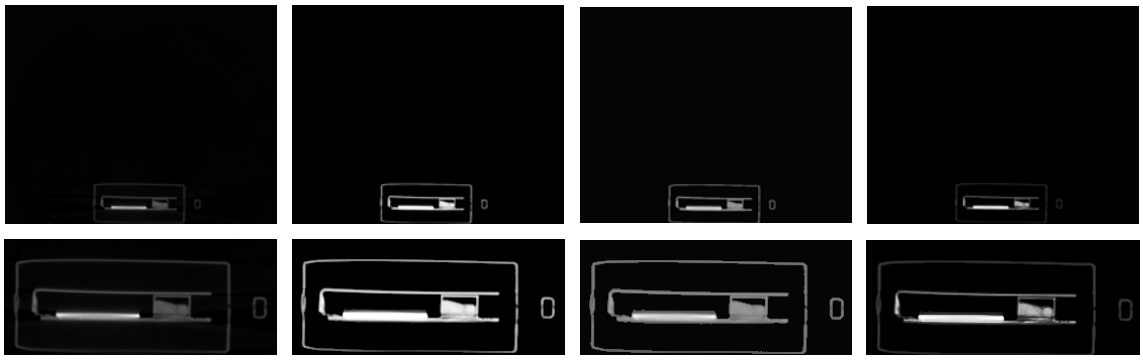
Figure 2.24: Enhanced results of 3D CT baggage image #4. The top row shows different views of the original 3D CT baggage image; the bottom row shows different views of the 3D image enhanced by the AWMSE algorithm. (a) Top view of the entire 3D image; (b) Bottom view of the entire 3D image; (c) Front side view of the 2D image slices #131-290; (d) Back side view of the 2D image slices #131-290.

www.manaraa.com

2.4.3.3 Enhancement Comparison

To demonstrate the AWMSE algorithm's enhancement performance, it can be compared with two other enhancement methods, namely, the alpha-weighted quadratic filter (AWQF) [37] (which will be introduced in Chapter 3) and bi-histogram equalization (BIHE) [97]. These are used to enhance 2D CT baggage images individually.

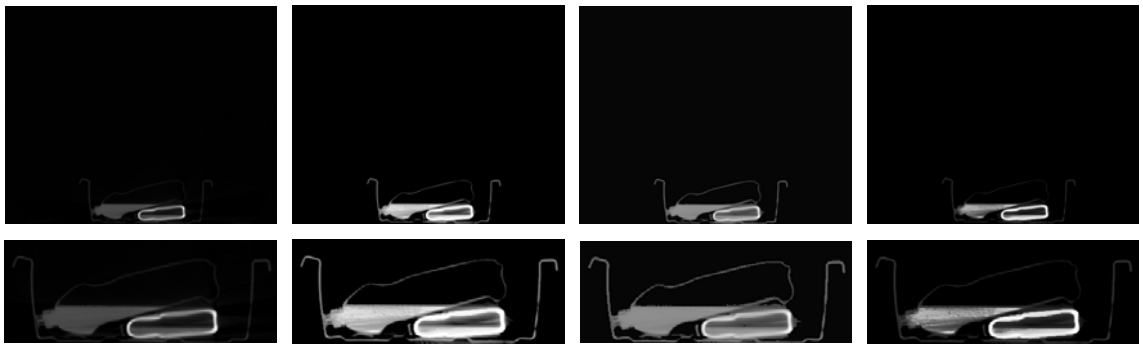
Figures 2.25 and 2.26 give the enhancement results of two 2D CT baggage images. The 2D CT baggage images are processed by the same denoising process, and then enhanced by the AWMSE, AWQF, and the BIHE, respectively. The enhanced images and cropped regions show that the images enhanced by the AWMSE have the best visual quality and the least amount of background noise. The SDME measure results demonstrate this improvement.



(a) Original	(b) AWMSE	(c) AWQF	(d) BIHE
SDME=36.124	SDME=49.5505	SDME=47.8292	SDME=48.5744

Figure 2.25: Comparison of the image enhancement using different enhancement methods. The top row shows the original and enhanced 2D CT baggage images. The bottom row shows the cropped regions from the corresponding 2D CT baggage images above. (a) The original 2D CT baggage image; (b) the image enhanced by the AWMSE; (c) the image enhanced by the AWQF; (d) the image enhanced by the BIHE. This demonstrates that the AWMSE outperforms other methods.

www.manaraa.com



(a) Original SDME=38.002 | (b) AWMSE SDME=48.2297 | (c) AWQF SDME=42.7494 | (d) BIHE SDME=45.327

Figure 2.26: Comparison of the image enhancement using different enhancement methods. The top row shows the original and enhanced 2D CT baggage images. The bottom row shows the cropped regions from the corresponding 2D CT baggage images above. (a) The original 2D CT baggage image; (b) the image enhanced by the AWMSE; (c) the image enhanced by the AWQF; (d) the image enhanced by the BIHE. This demonstrates that the AWMSE outperforms other methods.

2.4.3.4 Execution Performance

To demonstrate the execution performance of the AWMSE algorithm, it is used to enhance a 2D CT baggage image (image size of 512×640 and its file size of 627KB) and a 3D CT baggage image (image size of 512×640×317 and its file size of 198MB) as test images. The CPU time and memory usage are then measured and recorded. The results were measured by Matlab R2009a on a computer running the Windows XP operating system with 3GB memory and with a CPU using Intel Core Duo E6550 (2.60GHz, 4MB L2 cache, 1066 MHz FSB).

TABLE 2.8 THE CPU TIME AND MEMORY USAGE OF THE AWMSE ALGORITHM

Image	Image Size (pixel)	Image File Size (MB)	CPU Time (second)	Memory Usage (MB)
2D CT baggage image	512×640	0.627	1.5312	0.8216576
3D CT baggage image	512×640×317	198	1.1164×10^{3}	11.726848

www.manaraa.com

The results are shown in Table 2.2. As can be seen, the AWMSE algorithm took 1.5312 seconds to enhance the 2D CT image with the size of 512×640, and took 1.1164×10^3 seconds (about 0.31 hours) to enhance a 3D CT volume image with 317 2D image slices. Its memory usage is 0.8216576 MB for enhancing the 2D image and 11.726848 MB for enhancing the 3D image. This performance can be further improved by using the C/C++ language or a hardware implementation such as a FPGA.

www.manaraa.com

2.5 Summary and Discussion

In this chapter, a new SDME enhancement measure has been introduced to quantitatively evaluate the performance of the enhancement algorithms and to select the best parameters for the enhancement algorithms. It is based on the concept of the second derivative.

According to the analysis of the characteristics of the 2D CT baggage images, the CT images are visually very dark because they contain a number of pixels with high intensity values that greatly expand the data range of the entire image. Due to the fact that the pixels in the background regions in the image have nonzero intensity values, the CT images contain a lot of background noise. Based on the analysis results, a new image enhancement algorithm has been introduced to improve the visual quality of 3D CT baggage images and remove the background noise for homeland security applications. The performance of the presented enhancement algorithm has been demonstrated by integrating alpha-weighted mean separation with histogram equalization techniques.

The presented enhancement algorithm has been shown to have the ability to significantly improve the global contrast of the original CT images and the visual quality of objects while reducing background noise. Computer simulations and comparisons have demonstrated that the presented algorithm outperforms other enhancement methods in enhancing 3D CT baggage images. The quantitative SDME measure results have further proven the excellent enhancement performance of the presented algorithm. The presented algorithm has the potential to be used for object segmentation and recognition in homeland security and medical applications.

www.manaraa.com

Chapter 3

Nonlinear Filtering Algorithms for Medical Image Enhancement

This chapter introduces a new nonlinear filter called the Alpha-Weighted Quadratic Filter (AWQF). To enhance mammograms for breast cancer detection, the AWQF is integrated with human visual system (HVS)-based decomposition and unsharp masking techniques. To enhance prostate MR images for prostate cancer detection, the AWQF is combined with the alpha-trimmed mean separation and the logarithmic enhancement technique.

www.manaraa.com

3.1 Introduction

Cancer is a leading cause of death among human beings and is a worldwide health concern. Breast cancer, for example, is the leading cause of death in women between the ages of 35 and 55. The National Cancer Institute estimates that one out of every eight women in the United States will develop breast cancer at some point in her lifetime [98]. Statistics from the World Health Organization in 2004 showed that 13% of deaths all over the world are caused by cancer while the number of people dying of cancer is reported to rise by an estimated 12 million by 2030 [99]. Prostate cancer, on the other hand, is the single most common type of cancer in men in the United States. The latest American Cancer Society estimates that about 192,280 new cases of prostate cancer were diagnosed and 27,360 men died of prostate cancer in the United States in 2009 [100]. Currently, there are no effective ways to prevent breast cancer because its cause remains unknown [31, 101]. Early detection of cancer is an important and effective method to reduce mortality, since early stage treatments of breast cancer are most likely to succeed, while prostate cancer is curable in its early stage [82, 102, 103].

Several imaging techniques for examining the breast and prostate exist, such as magnetic resonance imaging (MRI), ultrasound imaging and X-ray imaging. Mammography (X-ray imaging) is the most common and reliable technique used by radiologists to detect and diagnose breast cancer [104, 105]. MRI is one effective method that can improve the visualization and localization of prostate cancer.

www.manaraa.com

Due to limitations in system hardware, however, medical images may present problem characteristics such as poor resolution or low contrast. The lack of good contrast between objects or regions and their local backgrounds in medical images can often make the early detection of cancer a difficult task. The features of a suspected cancer are usually minute at the earlier stage, often taking the form of microcalcifications – very small calcium deposits, appearing as granular bright spots in mammograms [106, 107] and an important early indicator of the possible presence of breast cancer [108, 109]. The distinction between malignant diseases and benign glandular tissue is also not readily discernable, making accurate diagnosis difficult. The situation is exasperated by the fact that radiologists routinely interpret large numbers of mammograms and can sometimes misdiagnose a condition [17]. Currently, the prostate boundaries have to be outlined manually in images – a tedious, time-consuming, and often irreproducible job [110].

Collecting more image data at the data acquisition stage or enhancing images during the post image processing stage are two ways to improve the visual quality of medical images in medical imaging systems. However, the former method – at the acquisition stage – significantly increases the overall acquisition time, the amount of radiation a patient is exposed to and hardware costs [111]. Image enhancement in the post image processing stage utilizes different image enhancement techniques to enhance the contrast of medical images. The goal of image enhancement is to improve the visual quality of medical images, reducing the need for tedious or subjective human interpretations and improving the accuracy of breast cancer detection and diagnosis (as well as prostate cancer in its early stage [112, 113]).

www.manaraa.com

Breast cancer appears as bright regions of mammograms, while prostate cancer presents as shadow regions of prostate MR images. Therefore, different enhancement algorithms are needed to improve the visual quality of medical images for particular real world applications. Many image algorithms for enhancing mammograms and other medical images have been developed recently. They can be classified into two basic categories: frequency domain methods and spatial domain methods. The literature review and comparison are addressed in [108, 114, 115].

Frequency domain methods: Enhancement algorithms for mammograms that use multiscale representation decompose mammograms into a multiscale subband representation in the contourlet transform [116] or Discrete Wavelet Transforms (DWTs) such as the discrete dyadic wavelet transform [26-28], Integrated Wavelets [29] or Redundant Discrete Wavelet Transform [30]. Next, technologies such as nonlinear filtering [117], regression-based extrapolation [118], adaptive unsharp masking [19], the wavelet shrinkage function [119], and direct contrast modification [120] are used to modify the transform coefficients in each subband of the multiscale representation. Finally, the enhanced mammograms are obtained from the modified coefficients. The DWT based methods include Multi-wavelet grading [121] and dynamic contrast enhancement [122] for enhancing MR images and other examples, as shown in [123-125]. However, a wavelet representation does not efficiently show the contours or the geometry of edges in images [116].

Due to the suitability of fuzzy set theory for dealing with the uncertainty associated with the definition of image edges, boundaries and contrast, it has often been used for image

www.manaraa.com

processing and pattern recognition. Algorithms based on fuzzy set theory have been developed to enhance the contrast of mammograms [31-34]. Adaptive fuzzy logic has also been used to enhance the contrast of mammography images [32] and to improve the contours and fine details of mammographic features such as microcalcifications and masses [31]. Fuzzy logic has been integrated with other techniques such as histogram equalization for medical image enhancement [33], and structure tensor for the contrast enhancement of microcalcifications in digital mammograms [34]. To enhance prostate MR images, a combination of domain knowledge-based fuzzy inference system and a set of adaptive region-based operators is used [126].

The frequency domain techniques are also based on Discrete Cosine Transform (DCT) [23-25]. Methods such as alpha-rooting, logarithmic enhancement [88] and histogram equalization [23] are used to modify the transform coefficients of the images. The advantages of the frequency domain based techniques include: (a) a low complexity of computations; (b) an important role for the orthogonal transforms in digital signal/image processing applications; and (c) they are easy to view and manipulate [127].

Spatial domain methods: Spatial domain based enhancement techniques directly manipulate an image's pixels using a variety of methods based on nonlinear filtering [7-12], histogram equalization [6, 93, 128], adaptive neighborhood [13-17] or unsharp masking [18-22].

Since nonlinear filtering is known for its ability to obtain more robust characteristics for suppressing noise and preserving edges and details, it is a technique that is particularly desirable when it comes to enhancing mammographic and other types of medical images.

www.manaraa.com

Examples include utilizing the adaptive density-weighted filter [10], the tree-structured nonlinear filters [11] and adaptive anisotropic filtering [12].

Several algorithms have been developed for mammogram enhancement using adaptive neighborhood (or region-based) contrast enhancement (ANCE) [13-17]. Operating on local region backgrounds and contrasts in mammograms, the ANCE is designed to improve the contrast of specific regions, objects and details. The region contrast is calculated and enhanced according to the region's contrast, its background, its neighborhood size and its seed pixel value [16].

Another interesting enhancement technique is unsharp masking (UM). The traditional UM performs well when it comes to enhancing the fine details of original images. However, it does also amplify noise and tends to overshoot sharp details at the same time [20, 21]. To overcome this problem, several modification schemes have been developed in which the highpass filter is replaced with the adaptive filter [20], quadratic filter [129] and its derived filtering operators known as rational unsharp masking [21] and cubic unsharp masking [22]. Algorithms using unsharp masking techniques have also been developed [18, 19].

In this chapter, a new nonlinear filter called the Alpha-Weighted Quadratic Filter (AWQF) is introduced for mammogram enhancement and the suppression of image noise in the spatial domain [37]. In order to enhance mammograms for breast cancer detection, the AWQF is integrated with human visual system (HVS)-based decomposition [38] and unsharp masking techniques [36]. In order to enhance prostate MR images for prostate

www.manaraa.com

cancer detection, the AWQF is combined with alpha-trimmed mean separation [39] and the logarithmic enhancement technique [40].

The rest of this chapter is organized as follows: Section 3.2 introduces the new alpha weighted quadratic filter and simulation results for mammogram enhancement. Section 3.3 introduces a HVS-based mammogram enhancement algorithm. In order to solve one particular problem (that traditional unsharp masking is sensitive to noise), Section 3.4 presents a new nonlinear unsharp masking scheme for mammogram enhancement. To enhance prostate MR images for prostate cancer detection, Section 3.5 combines the nonlinear filtering with the alpha-trimmed mean separation, while Section 3.6 combines the nonlinear filtering with the logarithmic enhancement technique. Finally, Section 3.7 addresses a summary discussion and indicates several future directions.

www.manaraa.com

3.2 Mammogram Enhancement Using the Alpha Weighted Quadratic Filter

Nonlinear filters demonstrate an excellent level of performance when it comes to contrast enhancement and the suppression of noise. By extending the concept of the quadratic filter, the new alpha weighted quadratic filter (AWQF) is introduced. Its application for mammogram enhancement and the increased efficiency of breast cancer detection is investigated.

The AWQF is a complex nonlinear filter and requires a large number of coefficients. This gives the AWQF more power and design flexibility to meet the specific and complex requirements of real world applications. An implementation algorithm is introduced to help users design the AWQF. Simulation results are given to show its performance for mammogram enhancement.

3.2.1 Alpha Weighted Quadratic Filter

This section reviews the definition of the quadratic filter and then introduces a new alpha weighted quadratic filter (AWQF). The AWQF's properties are also discussed.

3.2.1.1 Quadratic Filter

A quadratic filter is the second order of the polynomial (or Volterra) filter. The following equation characterizes its 1D format:

www.manaraa.com

$$y(n) = \sum_{j,k=-M}^{M} w(j,k)x(n-j)x(n-k) \tag{8}$$

where $N = 2M + 1$ is the mask size and $w(\bullet)$ is the coefficients.

Similar to the polynomial filter, the quadratic filter is known to be a complex nonlinear filter. Its implementation requires that a large number of coefficients are determined in the filter's design.

Assuming the mask size is $N \times N, N = 2M + 1$, the 2D format of the quadratic filter is defined as,

$$y(m,n) = \sum_{i,j=-M}^{M} \sum_{k,l=-M}^{M} w(i,j,k,l)x(m-i,n-j)x(m-k,n-l) \tag{9}$$

Or

$$y_n = \sum_{j,k=1}^{N^2} w_{jk} x_j x_k \tag{10}$$

A study of the quadratic filter is addressed in [130].

3.2.1.2 Alpha Weighted Quadratic Filter

The Alpha Weighted Quadratic Filter (AWQF) is an extension of the quadratic filter which is defined as follows,

$$y(n) = \sum_{i,j=-M}^{M} w(i,j)x^{\alpha(i)}(n-i)x^{\alpha(j)}(n-j) \tag{11}$$

where $w(\bullet)$ and $\alpha(\bullet)$ are coefficients.

Similarly, its 2D format is defined as follows,

www.manaraa.com

$$y(m,n) = \sum_{i,j=-M}^{M} \sum_{k,l=-M}^{M} w(i,j,k,l) x^{\alpha(i,j)}(m-i,n-j) x^{\alpha(k,l)}(m-k,n-l) \tag{12}$$

Or

$$y_n = \sum_{j,k=1}^{N^2} w_{jk} x_j^{\alpha_j} x_k^{\alpha_k} \tag{13}$$

The AWQF is also a complex nonlinear filter and requires an even larger number of coefficients compared to the quadratic filter in equation (9) or (10). Due to the fact that all its coefficients have to be determined, users may experience difficulty designing an AWQF for practical applications. However, the fact that it has a large number of coefficients means that the AWQF has more power and design flexibility to meet the specific and complex requirements of real world applications.

To make the AWQF independent of the orientation of the input image's objects or features, it is designed as an isotropic image operator, allowing the number of the AWQF's coefficients to be reduced.

For example, if the mask size is 3×3, $N = 3$ (i.e. $M = 1$), it contains nine image pixels.

$w_1 x_1^{\alpha_1}$	$w_2 x_2^{\alpha_2}$	$w_3 x_3^{\alpha_3}$
$w_4 x_4^{\alpha_4}$	$w_5 x_5^{\alpha_5}$	$w_6 x_6^{\alpha_6}$
$w_7 x_7^{\alpha_7}$	$w_8 x_8^{\alpha_8}$	$w_9 x_9^{\alpha_9}$

Based on symmetric and isotropic properties, the weight coefficient matrix of the first order terms and the alpha weight matrix can be minimized as follows:

$$W_1 = \begin{pmatrix} w_1 & w_2 & w_1 \\ w_2 & w_5 & w_2 \\ w_1 & w_2 & w_1 \end{pmatrix} \qquad \alpha = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_1 \\ \alpha_2 & \alpha_5 & \alpha_2 \\ \alpha_1 & \alpha_2 & \alpha_1 \end{pmatrix} \tag{14}$$

www.manaraa.com

Similar to the weight coefficient matrix of the second order terms,

$$W_2 = \begin{pmatrix} w_{11} & w_{12} & w_{13} & w_{12} & w_{22} & w_{12} & w_{13} & w_{12} & w_{11} \\ w_{12} & w_{15} & w_{16} & w_{24} & w_{25} & w_{24} & w_{16} & w_{15} & w_{12} \\ w_{13} & w_{16} & w_{19} & w_{16} & w_{28} & w_{16} & w_{19} & w_{16} & w_{13} \\ w_{12} & w_{24} & w_{16} & w_{15} & w_{25} & w_{15} & w_{16} & w_{24} & w_{12} \\ w_{22} & w_{25} & w_{28} & w_{25} & w_{55} & w_{25} & w_{28} & w_{25} & w_{22} \\ w_{12} & w_{24} & w_{16} & w_{15} & w_{25} & w_{15} & w_{16} & w_{24} & w_{12} \\ w_{13} & w_{16} & w_{19} & w_{16} & w_{28} & w_{16} & w_{19} & w_{16} & w_{13} \\ w_{12} & w_{15} & w_{16} & w_{24} & w_{25} & w_{24} & w_{16} & w_{15} & w_{12} \\ w_{11} & w_{12} & w_{13} & w_{12} & w_{22} & w_{12} & w_{13} & w_{12} & w_{11} \end{pmatrix} \tag{15}$$

To preserve the gray input level, the following conditions should be satisfied.

$$\begin{aligned} &1)\ 4w_1 + 4w_2 + w_5 = 1 \\ &2)\ 4\alpha_1 + 4\alpha_2 + \alpha_5 = 1 \\ &3)\ 4w_{11} + 16w_{12} + 8w_{13} + 8w_{15} + 16w_{16} + 4w_{19} + 4w_{22} + 8w_{24} + 8w_{25} + 4w_{28} + w_{55} = 0 \end{aligned} \tag{16}$$

According to the distance between the two elements of the AWQF (two pixels of the input image), the AWQF can be classified into three types:

1) Type Zero AWQF: This type of the AWQF consists of all the second order terms where the distance of two elements is zero, in other words, where two elements have the same locations. For mask size 3×3, the filter is,

$$y_n = w_{55}x_5^{2\alpha_5} + w_{11}(x_1^{2\alpha_1} + x_3^{2\alpha_1} + x_7^{2\alpha_1} + x_9^{2\alpha_1}) + w_{22}(x_2^{2\alpha_2} + x_4^{2\alpha_2} + x_6^{2\alpha_2} + x_8^{2\alpha_2}) \tag{17}$$

2) Type One AWQF: The type one AWQF includes all the second order terms where the distance of two elements is one. In other words, the two elements are two adjacent pixels. For mask size 3×3, the filter becomes,

www.manaraa.com

$$\begin{aligned} y_n = {} & w_{12}(x_1^{\alpha_1}x_2^{\alpha_2} + x_1^{\alpha_1}x_4^{\alpha_2} + x_2^{\alpha_2}x_3^{\alpha_1} + x_3^{\alpha_1}x_6^{\alpha_2} + x_4^{\alpha_2}x_7^{\alpha_1}x_6^{\alpha_2}x_9^{\alpha_1} + x_7^{\alpha_1}x_8^{\alpha_2} + x_8^{\alpha_8}x_9^{\alpha_9}) \\ & + w_{15}(x_1^{\alpha_1}x_5^{\alpha_5} + x_3^{\alpha_1}x_5^{\alpha_5} + x_5^{\alpha_5}x_7^{\alpha_1} + x_5^{\alpha_5}x_9^{\alpha_1}) + w_{25}(x_2^{\alpha_2}x_5^{\alpha_5} + x_4^{\alpha_2}x_5^{\alpha_5} + x_5^{\alpha_5}x_6^{\alpha_2} \\ & + x_5^{\alpha_5}x_8^{\alpha_2}) + w_{24}(x_2^{\alpha_2}x_4^{\alpha_2} + x_2^{\alpha_2}x_6^{\alpha_2} + x_4^{\alpha_2}x_8^{\alpha_2} + x_6^{\alpha_2}x_8^{\alpha_2}) \end{aligned} \tag{18}$$

2) Type Two AWQF: It is comprised of the second order terms where the distance of two elements is two. For mask size 3×3, the filter is,

$$\begin{aligned} y_n = {} & w_{13}(x_1^{\alpha_1}x_3^{\alpha_1} + x_1^{\alpha_1}x_7^{\alpha_1} + x_3^{\alpha_1}x_9^{\alpha_1} + x_7^{\alpha_1}x_9^{\alpha_1}) + w_{19}(x_1^{\alpha_1}x_9^{\alpha_1} + x_3^{\alpha_1}x_7^{\alpha_1}) + w_{28}(x_2^{\alpha_2}x_8^{\alpha_2} + x_4^{\alpha_2}x_6^{\alpha_2}) \\ & + w_{16}(x_1^{\alpha_1}x_6^{\alpha_2} + x_1^{\alpha_1}x_8^{\alpha_2} + x_2^{\alpha_2}x_7^{\alpha_1} + x_2^{\alpha_2}x_9^{\alpha_1} + x_3^{\alpha_1}x_4^{\alpha_2} + x_3^{\alpha_1}x_8^{\alpha_2} + x_4^{\alpha_2}x_9^{\alpha_1} + x_6^{\alpha_2}x_7^{\alpha_1}) \end{aligned} \tag{19}$$

3.2.2 The AWQF Implementation Algorithm

The fact that such a large number of coefficients exists in the AWQF means that it can be quite expensive to implement. For example, if the mask size is 3×3, there are 99 coefficients in the AWQF. Even if symmetric and isotropic properties are utilized to reduce the number of its coefficients, seventeen coefficients remain. For a larger mask size, the number of coefficients significantly increases.

This section introduces a new algorithm that simplifies the AWQF implementation when the mask size is large. The algorithm is described as follows:

- If mask size is 3×3, the input image is directly filtered by the AWQF.
- If mask size is 5×5, 9 image pixels are selected from the 5×5 mask window to generate a new 3×3 window as shown in Figure 3.1, and then filtered by the AWQF.

www.manaraa.com

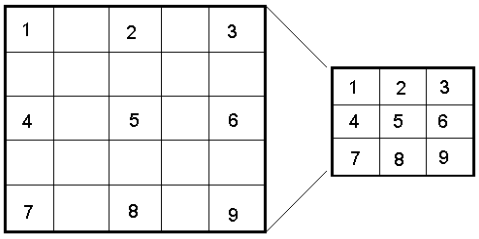


Figure 3.1: Generating a new 3×3 window.

- If the mask size is greater than 5×5, the AWQF is applied to the 3×3 sub-windows in the four corners of the mask window. The final output of the AWQF is the mean value of the results from these four sub-windows.

By using a smaller mask window in such a way that the users need only focus on designing the AWQF with a mask size 3×3, the algorithm strives to simplify the AWQF design. The number of the AWQF's coefficients is thus minimized.

3.2.3 Performance Measure and Simulation Results

To quantitatively evaluate the AWQF's enhancement performance, users have the flexibility to use any measure approach to establish a qualitative metric of mammogram enhancement. They can also optimize the AWQF's coefficients using the measure results to obtain better enhanced mammograms. In order to design the AWQF, this section utilizes the logarithmic Michelson contrast measure by entropy (LogAMEE) [93] as an example of the enhancement measure methods.

To further simplify implementation and reduce the number of the AWQF's coefficients, assume $w_1 = w_2 = h$, $\alpha_1 = \alpha_2 = h$, $w_{15} = w_{25} = w_{16} = h$, $w_{12} = 4h$, $w_{11} = w_{22} = -h$ and $-1 < h < 1$. According to constraints in the equation (16) and definition of three types of

www.manaraa.com

the AWQF, then $w_{19} = 2w_{13} = -4h$, $w_5 = \alpha_5 = 1 - 8h$, $w_{55} = 8h$ and $w_{24} = 2w_{12} = -h$. A mammogram containing breast cancer shown in Figure 3.3(a) serves as the test image. The LogAMEE of mammograms enhanced by the AWQF with different parameters is plotted in Figure 3.2. The maximum value of LogAMEE is located at $h = 0.1$. The AWQF achieves the best enhancement results for the test image at this point [93].

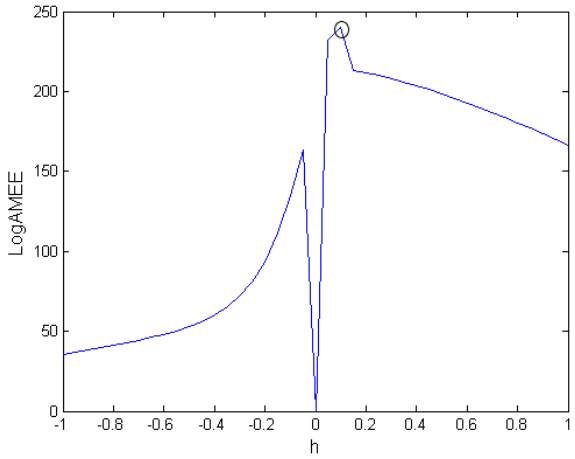
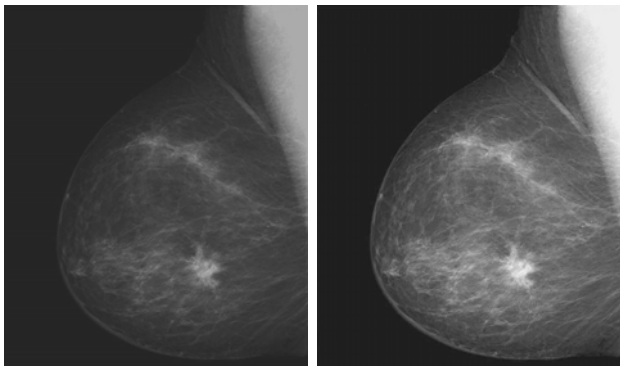


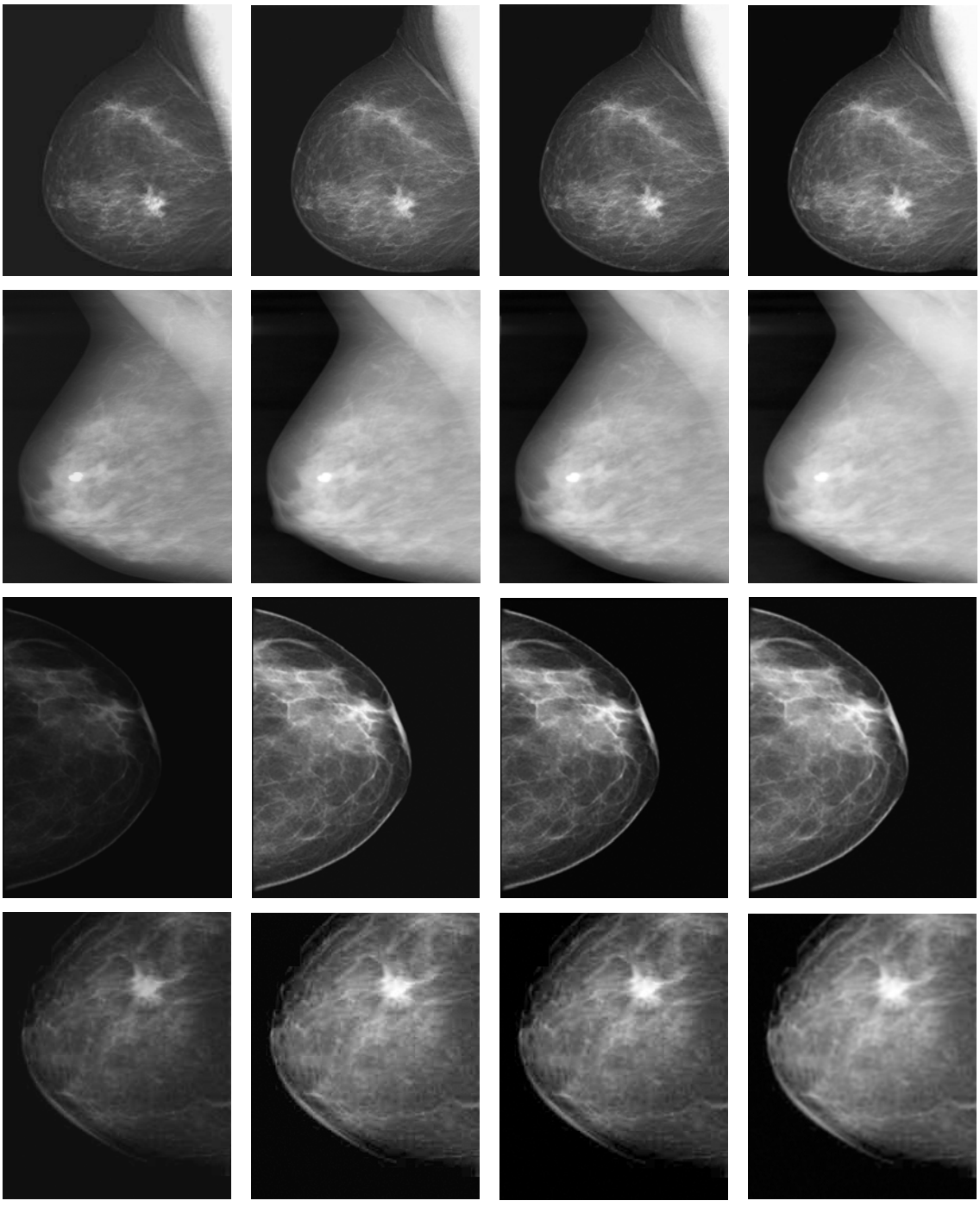
Figure 3.2: LogAMEE of the mammogram enhancement with breast cancer when parameter h changes. The maximum of the graph depicts the value of h for achieving the optimal enhanced image.



(a) (b)

Figure 3.3: Mammogram enhancement based on the LogAMEE measure result. (a) Original mammogram; (b) Enhanced mammogram with $h = 0.1$.

www.manaraa.com



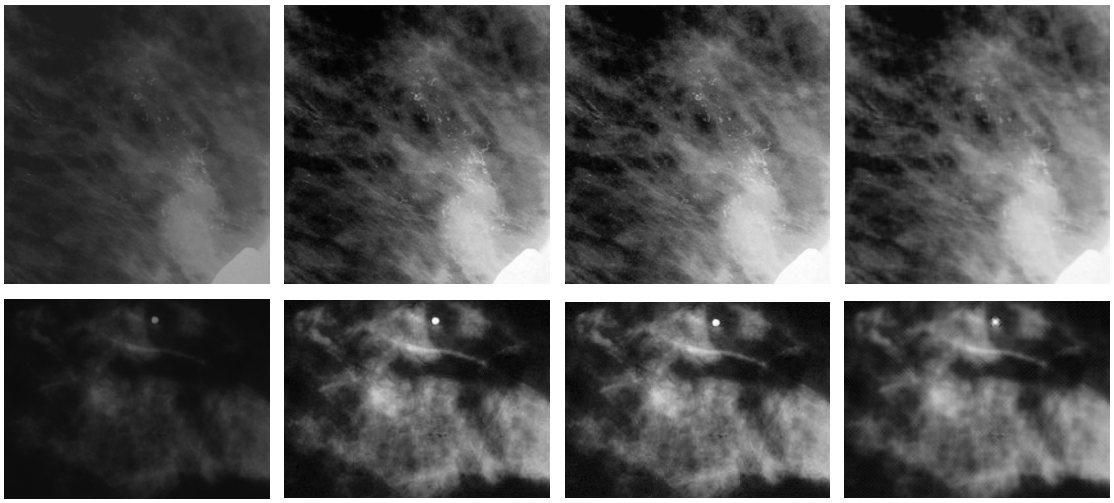
(a) (b) (c) (d)

Figure 3.4: Enhanced results of four mammograms using different types of the AWQF with different coefficients. (a) Original mammograms (b) Enhanced mammograms using the type zero AWQF; (c) Enhanced mammograms using the type one AWQF; (d) Enhanced mammograms using the type two AWQF.

www.manaraa.com

The enhanced image based on this parameter is shown in Figure 3.3(b). The global contrast of the original image is significantly improved. Users also have the flexibility to design the AWQF by manually selecting all its coefficients. By manually changing coefficients and utilizing the three types of the AWQF, 20 mammograms and 16 selected regions have been enhanced.

Figure 3.4 shows the results of four selected mammograms which were enhanced by using three types of the AWQF where the coefficients were manually selected. The visual quality of the mammograms is far superior after the contrast and fine details of the originals have been enhanced. Different types of the AWQF demonstrate different levels of performance when it comes to enhancing mammograms.



(a) (b) (c) (d)

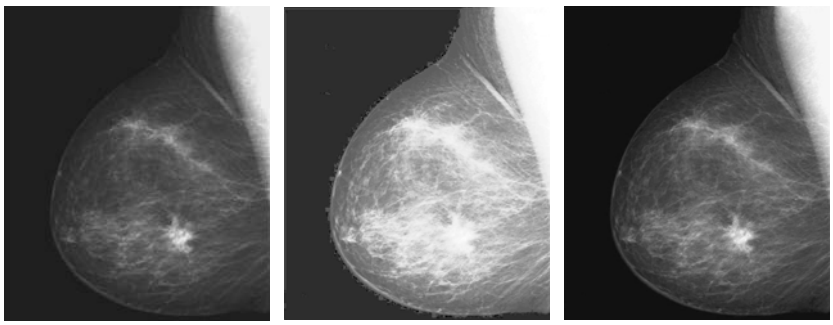
Figure 3.5: Selective region enhancement using different types of the AWQF with different coefficients and window sizes. (a) Original regions; (b) Enhanced region using the type zero AWQF; (c) Enhanced region using the type one AWQF; (d) Enhanced region using the type two AWQF.

Figure 3.5 shows the results for selected regions of four mammograms enhanced by the AWQF. As the mammograms demonstrate, the AWQF enhances not only the fine details

www.manaraa.com

and objects (breast cancer cells) but also the dark regions. These further show that the AWQF is able to enhance local contrast and fine details.

Figure 3.6 compares the enhancement performance of the AWQF and histogram equalization. The AWQF shows better enhancement performance because it enhances the contrast of mammograms and makes cancer cells and fine details more recognizable, as shown in Figure 3.6(c). However, histogram equalization spreads out the cancer cells and the boundary of the mammogram, as shown in Figure 3.6(b).



(a) (b) (c)

Figure 3.6: Comparison of the mammogram enhancement. (a) Original image; (b) Enhanced image using the histogram equalization; (c) Enhanced image using the AWQF.

www.manaraa.com

3.3 Human Visual System Based Mammogram Enhancement and Analysis

HVS-based image decomposition [131-133] is able to separate images into four sub-images using the background intensity and the rate of information change. The sub-images of regions 2 and 3 contain most of the illumination information of the original images. The less meaningful pixels are located in regions 1 and 4. These features are useful for image enhancement.

This section presents a modified version of the HVS-based image decomposition, and then introduces a new mammogram enhancement algorithm that combines the HVS-based image decomposition method with enhancement techniques such as nonlinear filtering. Simulation results and analysis demonstrate the performance of the presented algorithm for mammogram enhancement.

3.3.1 HVS-based Image Decomposition

HVS-based image decomposition separates images using the background intensity and the rate of information change. It divides an image into four sub-images based on four defined regions with different background intensities: (1) the saturation region for over-illuminated areas; (2) the Weber region for properly illuminated areas; (3) the Devries–Rose region for under-illuminated areas; (4) the fourth region for all pixels underneath

www.manaraa.com

the curve, which contains the least informative pixels [131, 132]. The four regions are shown in Figure 3.7.

The background intensity in the HVS is defined as a weighted local mean,

$$B(m,n) = a_0 X(m,n) + a_1 Y_1 + a_2 Y_2 \tag{20}$$

where, $B(m,n)$ is the background intensity at each pixel with value $X(m,n)$, and

$$Y_1 = b_{11}X(m-1,n) + b_{12}X(m+1,n) + b_{13}X(m,n-1) + b_{14}X(m,n+1)$$
$$Y_2 = b_{21}X(m-1,n-1) + b_{22}X(m+1,n-1) + b_{23}X(m-1,n+1) + b_{24}X(m+1,n+1)$$

where $a_0, a_1, a_2, b_{11}, b_{12}, b_{13}, b_{21}, b_{22}, b_{23}$ are weight coefficients.

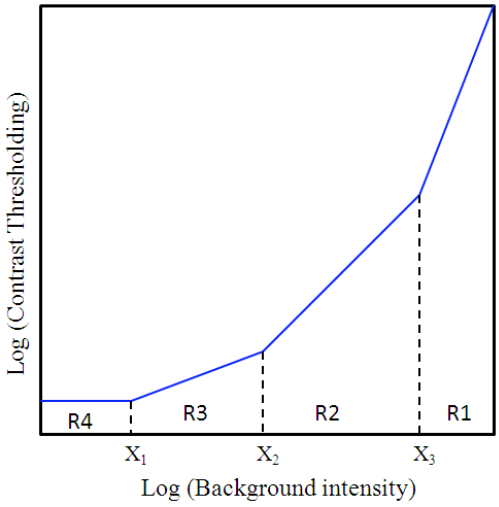


Figure 3.7: Four HVS-based regions. R1 (above X_3): Saturation region; R2 (X_2~X_3): Weber region; R3 (X_1 ~X_2): Devries-Rose region; R4 (below X_1): the fourth region [131].

For example, when $a_0 = \frac{1}{2}, a_1 = \frac{1}{16}, a_2 = \frac{1}{16\sqrt{2}}$ and $b_{11} = b_{12} = b_{13} = b_{21} = b_{22} = b_{23} = 1$, the background intensity will revert to a weighted local mean defined in [132, 133],

$$B(m,n) = \frac{1}{2}\left[\frac{1}{2}\left(\frac{Y_1}{4} + \frac{Y_2}{4\sqrt{2}}\right) + X(m,n)\right] \tag{21}$$

www.manaraa.com

and

$$Y_1 = X(m-1,n) + X(m+1,n) + X(m,n-1) + X(m,n+1)$$
$$Y_2 = X(m-1,n-1) + X(m+1,n-1) + X(m-1,n+1) + X(m+1,n+1)$$

The rate of information change is defined as a gradient, $X'(m,n)$, which is calculated by,

$$X'(m,n) = \frac{1}{2}\left(\left|X(m,n) - X(m,n+1)\right| + \left|X(m,n) - X(m+1,n)\right|\right) \tag{22}$$

Let B_1, B_2, B_3 denote the background illumination thresholds and K_1, K_2, K_3 denote the gradient thresholds at X_1, X_2, X_3. $X_{\max}$, $X_{\min}$ are the maximum and minimum values of the image respectively, then [132, 133],

$$\begin{cases} B_1 = \alpha_1 (X_{\max} - X_{\min}) \\ B_2 = \alpha_2 (X_{\max} - X_{\min}) \\ B_3 = \alpha_3 (X_{\max} - X_{\min}) \end{cases} \tag{23}$$

$$\begin{cases} K_1 = \dfrac{\beta}{100} \max\left(\dfrac{X'(m,n)}{B(m,n)}\right) \\ K_2 = K_1 \sqrt{B_2} \\ K_3 = \dfrac{K_1}{B_3} \end{cases} \tag{24}$$

where $\alpha_1, \alpha_2, \alpha_3, \beta$ are coefficients based on the response characteristics of the human eye for different regions.

The Weber's rate is $\beta\% = 0.02$, then $\beta = 2$. Since α_1 is the lower saturation level, it is usually set $\alpha_1 = 0$. α_2 and α_3 have to be determined by experimental results. It was found

www.manaraa.com

that the best results obtained when $\alpha_2 = 0.1$ and $\alpha_2 = 0.9$ [132]. Finally, the four sub-images for each HVS-based region can be defined by,

$$\begin{cases} R_1 = X(m,n) & \text{for } B(m,n) \geq B_3 \;\&\; \dfrac{X^{'}(m,n)}{B^2(m,n)} \geq K_3 \\ R_2 = X(m,n) & \text{for } B_3 \geq B(m,n) \geq B_2 \;\&\; \dfrac{X^{'}(m,n)}{B(m,n)} \geq K_2 \\ R_3 = X(m,n) & \text{for } B_2 \geq B(m,n) \geq B_1 \;\&\; \dfrac{X^{'}(m,n)}{\sqrt{B(m,n)}} \geq K_1 \\ R_4 = X(m,n) & \textit{Otherwise} \end{cases} \tag{25}$$

where R_1, R_2, R_3, and R_4 are four sub-images for the four regions, respectively. For example, R_1 is the sub-image of the first region.

The four sub-images contain different intensity information. Regions 2 and 3 contain the most illumination information in the original images. The less meaningful pixels are located in regions 1 and 4. These features are useful for image enhancement. In this section, their applications are extended to mammogram visualization for breast cancer detection.

3.3.2 The New mammogram Enhancement Algorithm

Since the four sub-images obtained by the HVS-based image decomposition contain different intensity information, users can selectively enhance only sub-images of regions 2 and 3 while the sub-images of regions 1 and 4 remain unchangeable. As a result, it is mostly only the illumination information in the original images that is enhanced. This is accomplished without affecting other less meaningful information in the original image, thus minimizing the creation of artifacts in the enhanced images. Alternatively, all four

www.manaraa.com

sub-images can be enhanced individually and recombined to form a more visually pleasing output image.

Based on this concept, a new algorithm is introduced for mammogram enhancement combining HVS-based image decomposition with the enhancement operation. It is called HVS-based Enhancement (HVSE). The algorithm is shown in Figure 3.8.

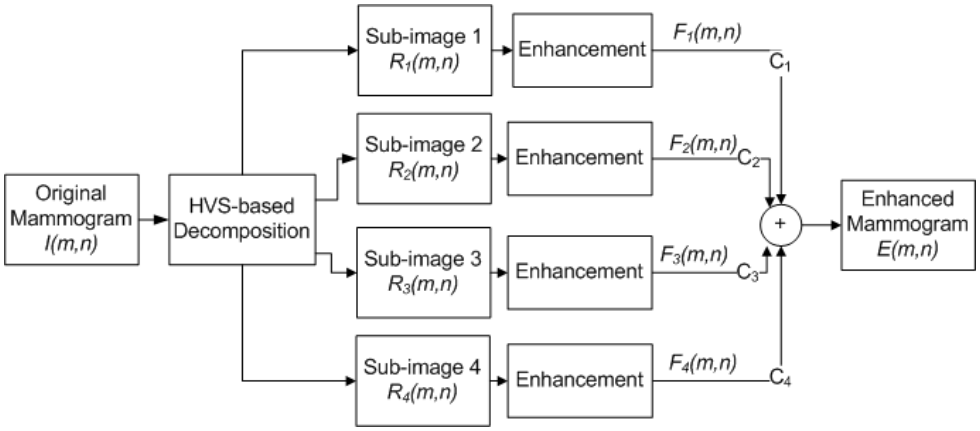


Figure 3.8: The block diagram of the HVSE algorithm.

The HVSE separates the original mammogram into four sub-images, R_1, R_2, R_3, R_4 using the HVS-based image decomposition defined in equation (25). An enhancement process is used to enhance each sub-image respectively. This enhancement process can be a filtering operator or any other enhancement algorithm. In this section, as an example of the enhancement process, a nonlinear filtering method is proposed. Finally, the resulting enhanced mammogram is obtained by combining all enhanced sub-images.

The enhanced sub-images F_1, F_2, F_3, F_4 are obtained by the following filtering operation,

$$F(m,n) = w_0 S_0 + w_1 S_1 + w_2 S_2 \tag{26}$$

www.manaraa.com

where

$$\begin{aligned} S_0 &= R^{2\alpha_0}(m,n) \\ S_1 &= R^{2\alpha_1}(m-1,n) + R^{2\alpha_1}(m+1,n) + R^{2\alpha_1}(m,n-1) + R^{2\alpha_1}(m,n+1) \\ S_2 &= R^{2\alpha_2}(m-1,n-1) + R^{2\alpha_2}(m+1,n-1) + R^{2\alpha_2}(m+1,n-1) + R^{2\alpha_2}(m+1,n+1) \end{aligned} \quad (27)$$

where constants w_0, w_1, w_2 are weight coefficients and $\alpha_0, \alpha_1, \alpha_2$ are exponential coefficients. The output enhanced mammogram is a combination of all enhanced sub-images as defined by,

$$E(m,n) = C_1F_1(m,n) + C_2F_2(m,n) + C_3F_3(m,n) + C_4F_4(m,n) \quad (28)$$

where constants $C_1,\ C_2,\ C_3,\ C_4$ are weight coefficients.

The nonlinear filter in equation (26) is a type zero of the Alpha Weighted Quadratic Filter (AWQF) [37]. This type of the AWQF contains only the square term of each element. This is why the power of all elements in the equation (27) is $2\alpha_i,\ i = 0,1,2$. The AWQF has been shown to have the ability to enhance images while suppressing noise. One novelty of the HVSE is that the nonlinear filtering operator can be designed as a combination of two different types of filters. For example, the coefficients w_0, w_1, w_2 can be designed as a highpass filter and $\alpha_0, \alpha_1, \alpha_2$ can be chosen as a center weighted mean filter. In this case, the HVSE algorithm can suppress noise and keep sharp details unchanged while enhancing the fine details of mammograms. This gives the HVSE algorithm more robust characteristics for different applications.

www.manaraa.com

For practical applications, there are ten coefficients to be specified in the HVSE algorithm. However, a large number of coefficients gives the presented HVSE the design flexibility to meet the more specific and complex requirements of real world applications.

To simplify the HVSE design and reduce the number of its coefficients, the HVSE coefficients can be optimized using an enhancement measure approach, obtaining the best enhanced result. In an alternative way, the HVSE can be designed by manually selecting its coefficients. However, this is a time-consuming process. If there is a lack of quantitative evaluation criterion, the best enhancement results might be extremely difficult to achieve.

3.3.3 Simulation Results and Analysis

The original mammograms in this section were obtained from the mini-MIAS database of mammograms [134]. All mammograms are cropped into smaller-sized images in such a way that the resulting cropped image contains a minimum of background. Each mammogram is denoted by the same name as the one in the database.

3.3.3.1 Parameter design

The HVS-based decomposition process groups pixels into four sub-images based on different thresholdings. This decomposition may change the surrounding pixel values of a specific pixel. The filtered result for a filter applied to all sub-images in the presented algorithm is different than that of the same filter directly applied to the original image. Therefore, for simplicity, the same filter is used for all sub-images throughout this section.

www.manaraa.com

To find the parameters for achieving a better enhanced image, assume: $C_1 = C_2 = C_3 = C_4 = 1, \alpha_1 = \alpha_2 = h, \alpha_0 = 8h, w_1 = w_2 = -w, w_0 = 8w$ and $0 < h, w \le 1$. The mammogram referred to as mdb206 in the database is enhanced by the HVSE and measured by the SDME when the parameters h and w change. Of course, users have the flexibility to choose other assumptions and images to design parameters.

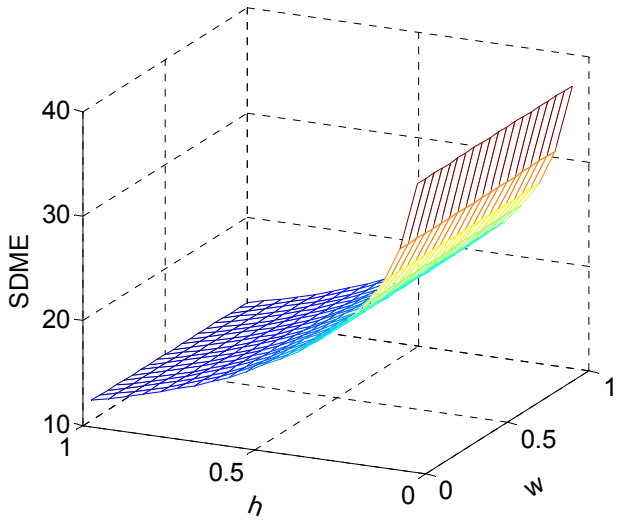
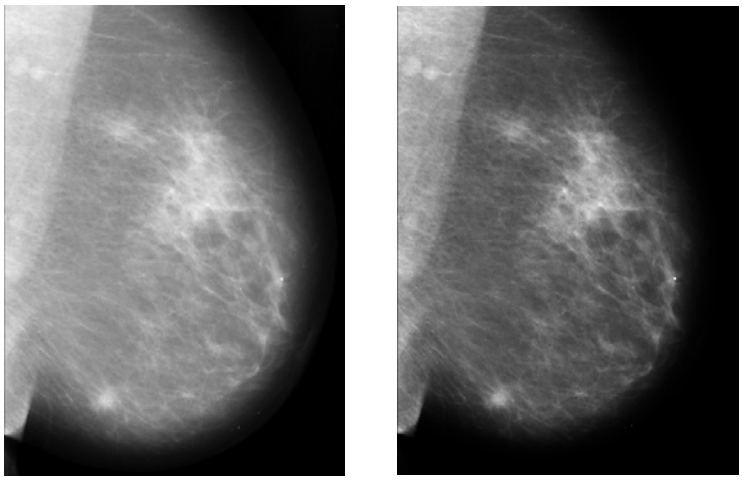


Figure 3.9: Parameter optimization: SDME measure using the presented HVSE with different parameters



(a) (b)

Figure 3.10: Mammogram enhancement using parameters from Figure 3.9. (a) Original mammogram, mdb206; (b) Enhanced mdb206.

www.manaraa.com

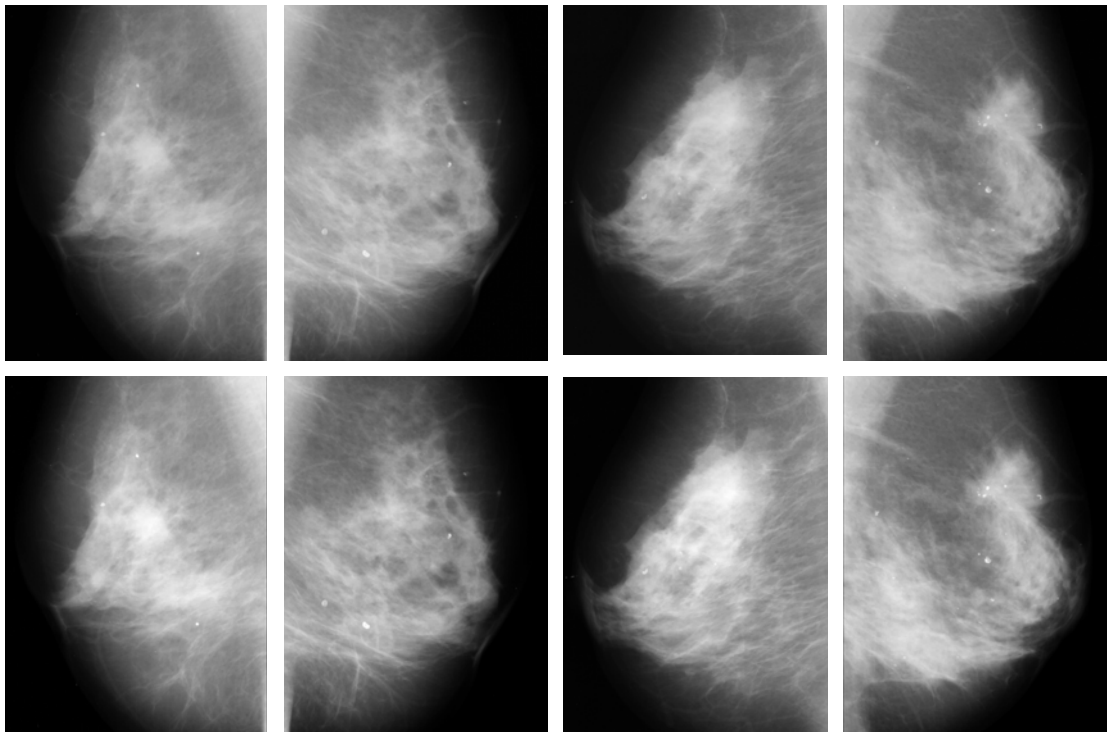
Figure 3.9 plots the SDME measure results. The parameters h and w for the best enhanced result can be located at the points where the SDME curve reaches the local extrema. The enhanced images are then inspected by human eye so that a decision can be made as to the best enhancement results and parameters. In this manner, the SDME significantly narrows the selection range of parameters and helps users to reach the best enhancement results quickly. Figure 3.10 shows the best enhancement results based on the measure results in Figure 3.9.

3.3.3.2 Performance Measure

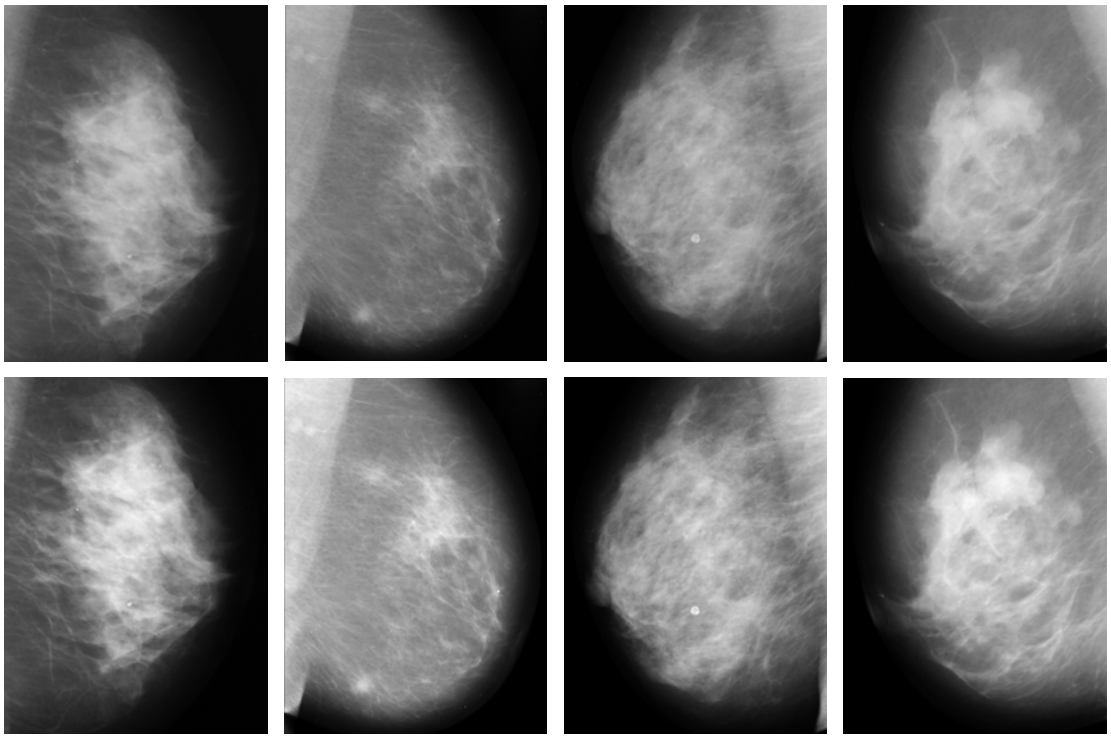
The HVSE has been applied to more than 44 mammograms from the mini-MIAS database. Figure 3.11 gives several examples of mammograms enhanced by the HVSE. The first row in Figure 3.11(a)-(h) shows the original mammograms. The second row shows the enhanced mammograms. These enhanced results demonstrate that the HVSE significantly improves the contrast of the original mammograms, especially in the case of abnormal regions, which are the potentially tumorous or cancerous regions.

To provide better focus for the specific regions in the mammograms, the regions of interest are cropped from the original mammograms and their enhanced results in Figure 3.11. The cropped regions are shown in Figure 3.12. Similar to Figure 3.11, the first and second rows in Figure 3.12(a)-(h) show regions that have been cropped from the original and enhanced mammograms, respectively. The visual quality and contrast of specific objects in the regions are greatly improved.

www.manaraa.com



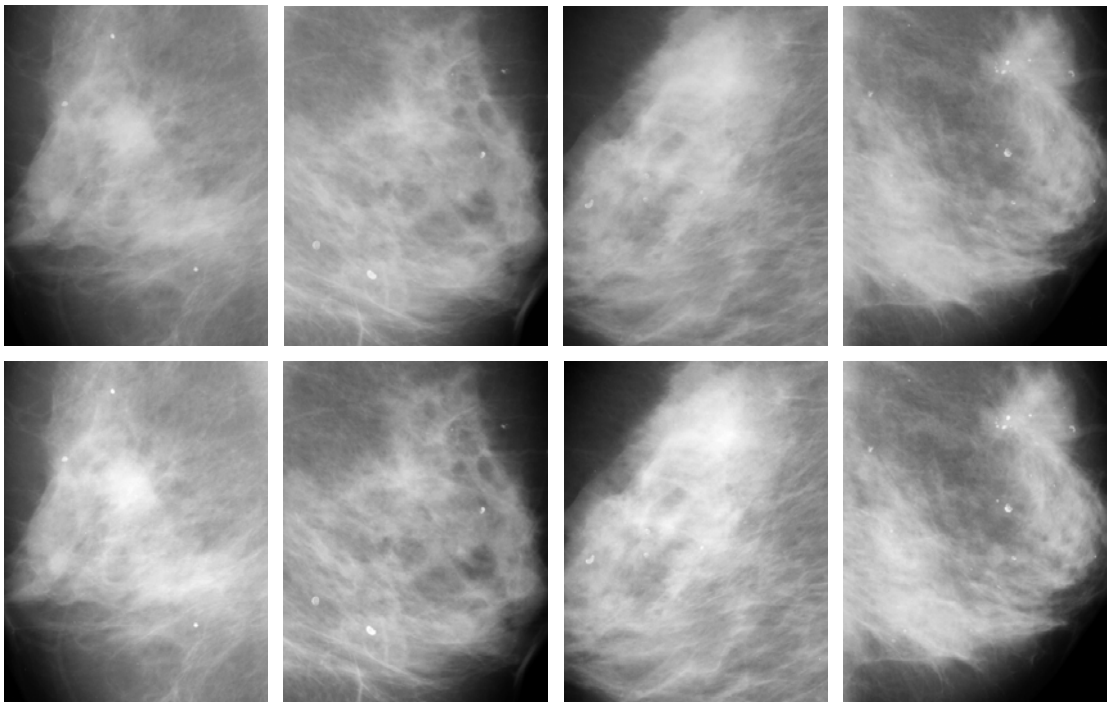
(a) mdb063 (b) mdb064 (c) mdb121 (d) mdb170



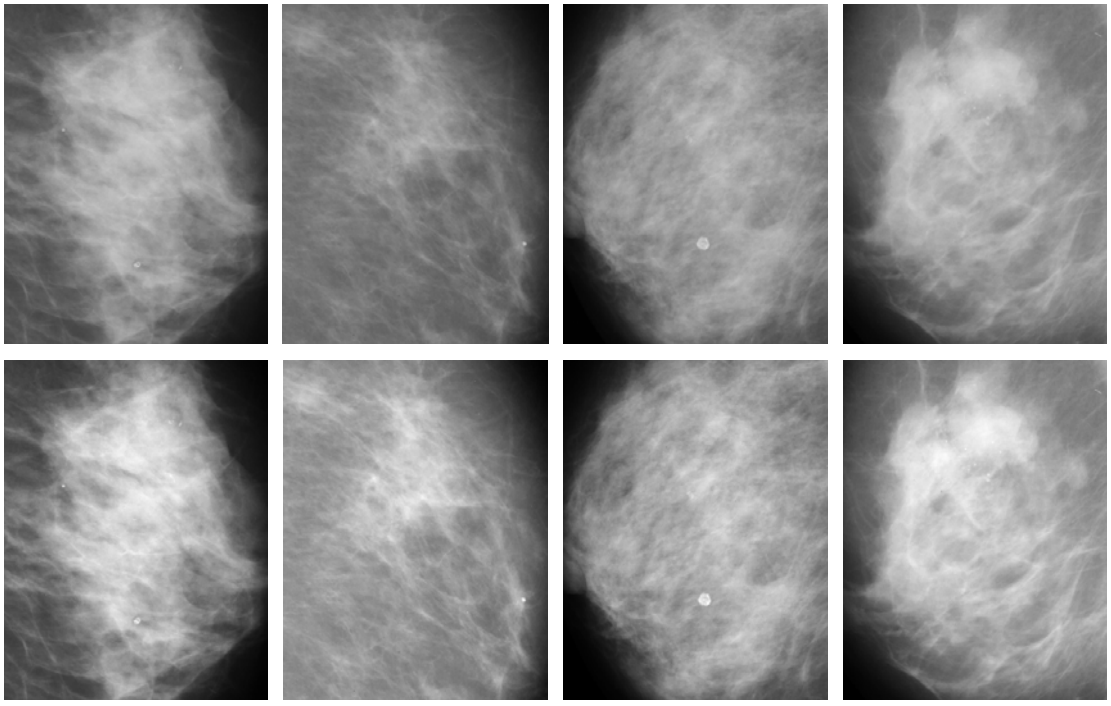
(e) mdb188 (f) mdb206 (g) mdb227 (h) mdb265

Figure 3.11: Eight cases of Mammogram enhancement. (a)-(h) Top row: The original mammograms; Bottom row: The enhanced mammograms.

www.manaraa.com



(a) mdb063 (b) mdb064 (c) mdb121 (d) mdb170



(e) mdb188 (f) mdb206 (g) mdb227 (h) mdb265

Figure 3.12: Regions cropped from the mammograms in Figure 3.11. (a)-(h) Top row: The regions cropped from the original mammograms; Bottom row: The regions cropped from the enhanced mammograms.

www.manaraa.com

TABLE 3.1 SDME MEASURE RESULTS FOR MAMMOGRAM ENHANCEMENT SHOWN IN FIGURE 3.11 AND FIGURE 3.12.

Mammogram #	Name in database	original	enhanced
1	mdb063	38.3146	44.6766
2	mdb064	38.6223	40.1847
3	mdb121	41.2823	49.3953
4	mdb170	38.0557	41.3682
5	mdb188	39.7389	43.2786
6	mdb206	38.6094	45.0378
7	mdb227	37.2989	39.1545
8	mdb265	38.8355	42.8653

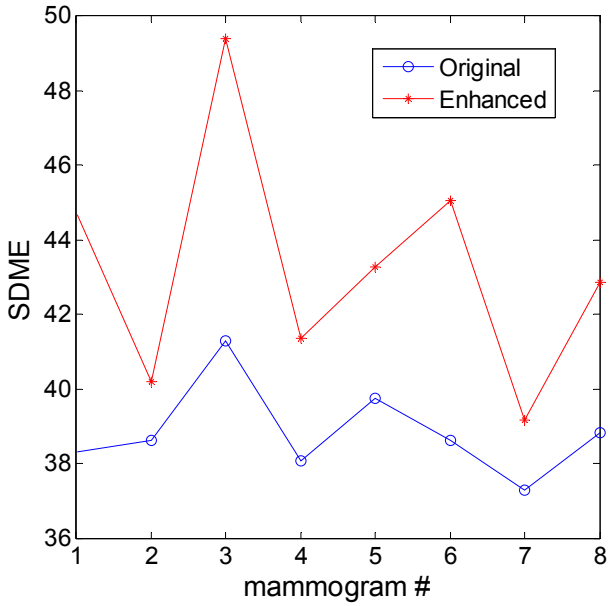


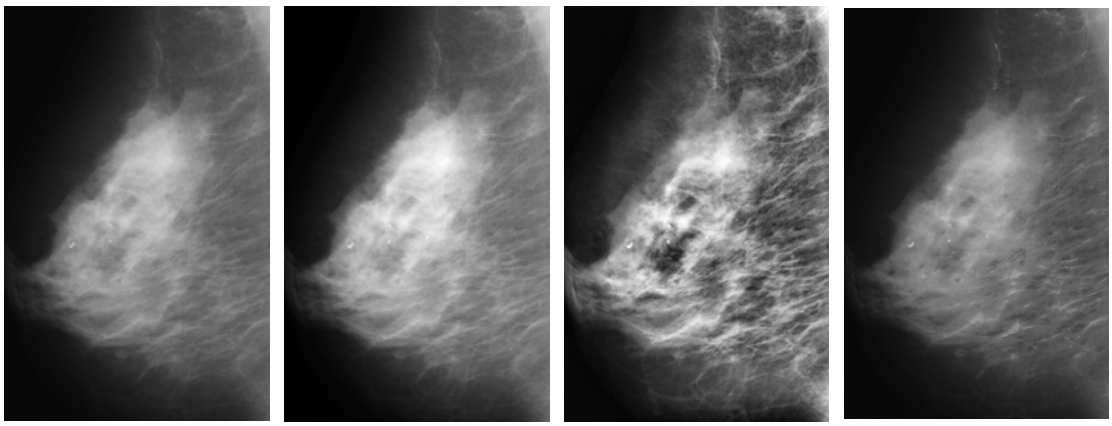
Figure 3.13: Plot of the SDME measure results.

The SDME measure results shown in Table 3.1 and the plotted curve shown in Figure 3.13 verifies the improvement of the contrast and visual quality of specific regions and objects. These enhancement results are useful for computer-aided diagnosis systems to automatically segment the abnormal regions in mammograms with breast cancer.

www.manaraa.com

3.3.3.3 Performance Comparison

The enhancement performance of the HVSE can be compared to other well-known methods such as the CLAHE [135] and the ANCE [16]. Figure 3.14 gives an example of this. The image enhanced by the HVSE in Figure 3.14(b) has the better visual quality. The contrast of the microcalcifications and abnormal regions is significantly improved. The CLAHE, on the other hand, over-enhances the abnormal regions in the mammogram, as shown in Figure 3.14(c). In the ANCE result shown in Figure 3.14(d), there are many residual artifacts. Furthermore, due to the fact that higher SDME values indicate a better enhancement performance, the SDME measure results at the bottom of each image verify that the HVSE outperforms the other two methods.



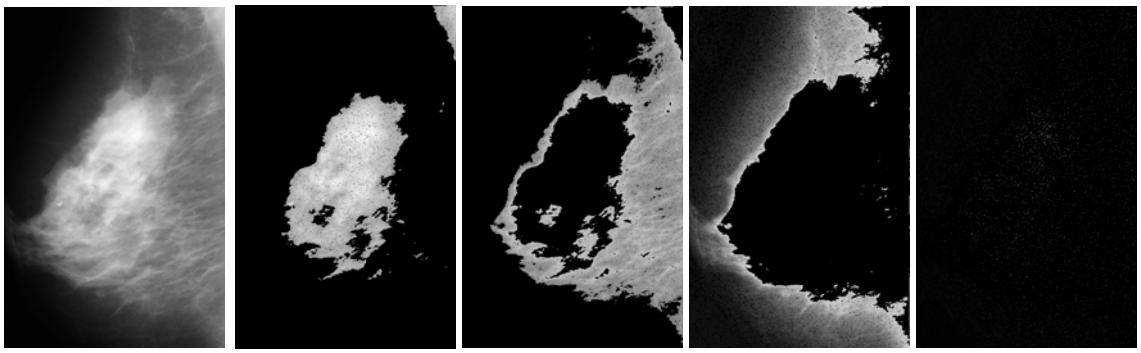
(a) SDME=40.1437 (b) SDME=48.114 (c) SDME=34.326 (d) SDME=38.0198

Figure 3.14: Performance comparison. (a) The original mammogram, mdb121; (b) The mammogram enhanced by the HVSE; (c) The mammogram enhanced by the CLAHE; (d) The mammogram enhanced by the ANCE.

3.3.3.4 Mammogram Visualization and Analysis

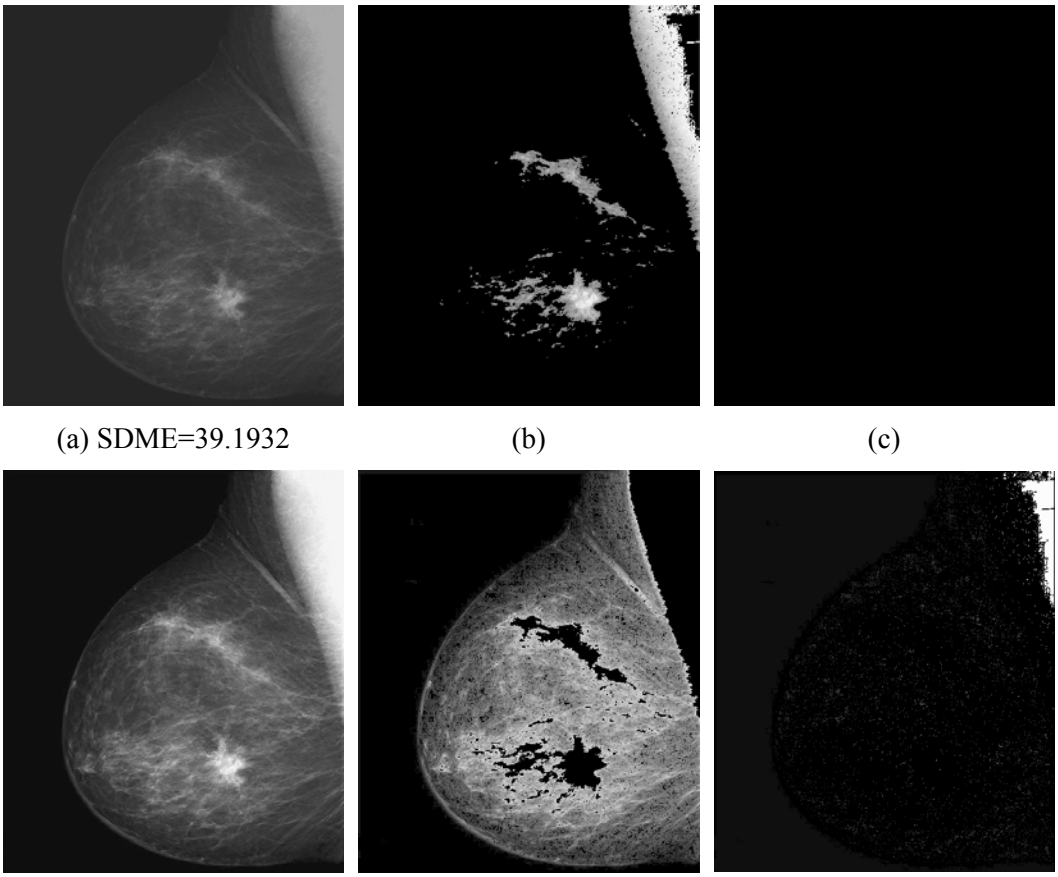
Since the HVS-based image decomposition separates images based on the background intensity and the rate of information change, its application can be extended to analyze the enhancement performance.

www.manaraa.com



(a) (b) (c) (d) (e)

Figure 3.15: HVS-based mammogram decomposition. (a) The enhanced mammogram in Figure 3.14(b); (b) The first sub-image; (c) The second sub-image; (d) The third sub-image; (e) The fourth sub-image.



(a) SDME=39.1932 (b) (c)

(d) SDME=43.8149 (e) (f)

Figure 3.16: HVS-based mammogram decomposition. (a) The original mammogram; (b) The first sub-image; (c) The second sub-image; (d) The mammogram enhanced by the presented HVSE; (e) The third sub-image; (f) The fourth sub-image.

www.manaraa.com

Figure 3.15 shows the enhanced mammogram from Figure 3.14(b) after it has been separated by the HVS-based image decomposition. The most interesting feature is that all the abnormal regions are located in the decomposed sub-image shown in Figure 3.15(b). This representation provides a good visualization for the human eye. It is a very useful tool for radiologists to analyze and diagnose breast cancer in mammograms.

Figure 3.16 gives another example of the HVS-based mammogram decomposition. The results show that the abnormal regions are more visible in the enhanced mammogram of Figure 3.16(d) compared to the original mammogram in Figure 3.16(a). The enhancement process also helps the HVS-based decomposition to separate the abnormal regions or objects from the mammograms.

www.manaraa.com

3.4 Nonlinear Unsharp Masking for Mammogram Enhancement

The unsharp masking technique shows excellent performance for enhancing edges or fine details in images, but it is, however, sensitive to noise. Benefiting from the nonlinear filter's ability to suppress noise while enhancing images, this section introduces a new nonlinear unsharp masking (NLUM) scheme that integrates the nonlinear filtering and the unsharp masking technique. Simulation results and comparisons are given to demonstrate that the presented scheme shows excellent performance for mammogram enhancement.

3.4.1 Background

This section reviews the traditional unsharp masking technique in order to provide some background to what follows. Three existing enhancement algorithms are discussed here and then compared with the new NLUM scheme. These algorithms include rational unsharp masking (RUM) [21], adaptive neighborhood contrast enhancement (ANCE) [16] and contrast-limited adaptive histogram equalization (CLAHE) [135]. The arithmetic operations of the Parameterized Logarithmic Image Processing (PLIP) are also presented here, since the PLIP will be used as an operator in the new NLUM scheme.

3.4.1.1 Traditional Unsharp Masking

The foundation of the traditional unsharp masking (UM) technique is to subtract a lowpass filtered signal from its original. The same results can be achieved by adding a

www.manaraa.com

scaled high-frequency part of the signal to its original. This is equivalent to adding the scaled gradient magnitude back to the original signal [129].

The unsharp masking is used to improve the visual quality of images by emphasizing their high frequency contents in such a way that the edges and details of images will be enhanced. The scheme for image enhancement is shown in Figure 3.17.

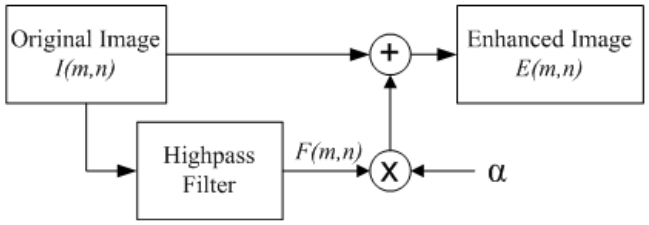


Figure 3.17: The block diagram of the traditional unsharp masking.

The output enhanced image $E(m,n)$ is defined by,

$$E(m,n) = I(m,n) + \alpha F(m,n) \tag{29}$$

where the constant α is a scaling factor, and $F(m,n)$ is a highpass filtered image obtained from the original image $I(m,n)$.

The highpass filter and scaling process in the traditional UM amplify those high frequency portions of original images that contain fine details as well as noise and sharp details. Therefore, due to the fact that the traditional UM enhances fine details in images, it also amplifies noise while over-enhancing the steep edges.

3.4.1.2 The RUM Algorithm

In the traditional unsharp masking scheme in Figure 3.17, the rational unsharp masking (RUM) [21] uses a rational function operator to replace the highpass filter. The rational

www.manaraa.com

function is the ratio of two polynomials of the input variables. This scheme is intended to enhance the details in images that contain low and medium sharpness without significantly amplifying noise or affecting the steep edges. The enhanced image is defined by,

$$E(m,n) = I(m,n) + \lambda[C_x(m,n)F_x(m,n) + C_x(m,n)F_x(m,n)] \tag{30}$$

where λ is scaling factor, and

$$C_x(m,n) = \frac{\left[I(m,n+1) - I(m,n-1)\right]^2}{k\left[I(m,n+1) - I(m,n-1)\right]^4 + h} \tag{31}$$

$$C_y(m,n) = \frac{\left[I(m+1,n) - I(m-1,n)\right]^2}{k\left[I(m+1,n) - I(m-1,n)\right]^4 + h} \tag{32}$$

$$F_x(m,n) = 2I(m,n) - I(m,n-1) - I(m,n+1) \tag{33}$$

$$F_y(m,n) = 2I(m,n) - I(m-1,n) - I(m+1,n) \tag{34}$$

where k and h are proper positive factors,

3.4.1.3 The ANCE Algorithm

The adaptive neighborhood contrast enhancement (ANCE) method [16] was developed to improve the contrast of objects and features with varying sizes and shapes. In this algorithm, each pixel in an image is considered a seed pixel for a region-growing process. Including those neighboring pixels whose gray values are within a specified gray-level deviation (known as the growth tolerance, k) from the seed, a local region – called the

www.manaraa.com

foreground – is the generated around the seed pixel. Another region – called the background – consists of those neighboring pixels that are outside the range of a specified gray-level deviation. The background, which surrounds the foreground, contains nearly the same number of pixels as the foreground. The region contrast is defined by,

$$C = \frac{f - b}{f + b} \tag{35}$$

where f and b are the mean gray-level values of the foreground and background, respectively.

The contrast equation above is similar to Weber's ratio [136], $W = \Delta L / L$,where ΔL is the luminance difference between the central region and the overall image luminance L. The minimum contrast of the region is $C_{\min} = k / 2$ and k is the growth tolerance. The Weber's rate of approximately 0.02 for a just-noticeable object under standard light conditions indicates that the growth tolerance should be at the most 0.04 if regions or objects are to be distinguishable from their background.

The region's contrast is enhanced by increasing its foreground value when the following conditions are satisfied:

- The region's contrast is low, i.e. $0.02 \le C \le 0.4$;
- The pixels in the region's background have a standard deviation normalized by their mean values less than 0.1.

The background in the second condition is defined as a region three pixels thick, molded to the original region in shape. The new foreground value is defined by,

www.manaraa.com

$$f' = b\frac{1+C'}{1-C'} \tag{36}$$

where C' is the increased contrast based on an empirical look-up table described in [16]. Therefore, only regions with low contrast are enhanced while the high-contrast regions such as steep edges remain unaffected. In order to save computational costs, the redundant pixels in the foreground regions, which have the same values as the seed pixels, are changed to the same new values.

3.4.1.4 The CLAHE Algorithm

The contrast-limited adaptive histogram equalization (CLAHE) [135] is a well-known technique of adaptive contrast enhancement. The normal and adaptive histogram equalizations enhance images using the integration operation. This operation yields large values in the enhanced image if the histogram of the nearly uniform regions of the original image contains several high peaks. As a result, those enhancement methods may over-enhance noise and sharp regions in the original images. To solve this problem, the CLAHE uses a clip level to limit the local histogram in such a way that the amount of contrast enhancement for each pixel can be limited. This clip level is a maximum value of the local histogram specified by users. An interactive binary search process is used to redistribute those pixels that are beyond the clip level. The CLAHE algorithm has the following steps:

1) Divide the original image into contextual regions;

2) Obtain a local histogram for each pixel;

www.manaraa.com

3) Clip this histogram based on the clip level;

4) Redistribute the histogram using binary search;

5) Obtain the enhanced pixel value by histogram integration.

3.4.1.5 The PLIP Model

The Parameterized Logarithmic Image Processing (PLIP) model was introduced to provide a non-linear framework for image processing [137]. The PLIP model can process images as absorption filters using the gray tone function of images. From the point of view of the human visual system, this is a more precise approach.

TABLE 3.2 PLIP MODEL ARITHMETIC OPERATIONS

PLIP Operation	Definition
Addition	$g_1 \oplus g_2 = g_1 + g_2 - \frac{g_1 g_2}{\gamma(M)}$
Subtraction	$g_1 \Theta g_2 = k(M)\frac{g_1 - g_2}{k(M) - g_2}$
Scalar Multiplication	$c \otimes g = \gamma(M) - \gamma(M)\left(1 - \frac{g}{\gamma(M)}\right)^c$
Image Multiplication	$g_1 * g_2 = \varphi^{-1}\left(\varphi(g_1)\cdot\varphi(g_2)\right)$ $\varphi(g) = -\lambda(M)\cdot\ln^{\beta}\left(1 - \frac{g}{\lambda(M)}\right)$ $\varphi^{-1}(g) = \lambda(M)\cdot\left(1 - \exp\left(\frac{-g}{\lambda(M)}\right)^{1/\beta}\right)$

c and β are constants. $\gamma(M)$, $k(M)$ and $\lambda(M)$ are arbitrary functions. g is the gray tone. g_1 and g_2 are two gray tone pixel values with the same location in two different images.

www.manaraa.com

The gray tone function is defined as follows,

$$g(i,j) = \mu(M) - f(i,j) \tag{37}$$

where $f(i,j)$ is the original image, $\mu(M)$ is a function of the maximum value, M, of the original image, and $g(i,j)$ is the gray tone function, which is likely to be a negative photo of the original image. The arithmetic operations of the PLIP model are listed in Table 3.2.

3.4.2 The New Nonlinear Unsharp Masking

Integrating the nonlinear filtering operation with unsharp masking technique, this section introduces a new unsharp masking scheme called nonlinear unsharp masking (NLUM) for mammogram enhancement. The NLUM can be used to enhance the contrast of mammograms and can also be applied to other type of medical images such as CT or MRI images.

3.4.2.1 The New NLUM Scheme

The block diagram of the NLUM scheme is shown in Figure 3.18. The original mammogram $I(m,n)$ is filtered by a nonlinear filter. The filtered mammogram $F(m,n)$ is then normalized and combined with the original mammogram using the fusion #1 and #2 in Figure 3.18.

Depending on the different applications, the fusion operators use arithmetic addition, PLIP addition or even nonlinear operation such as mean square root or logic operation.

www.manaraa.com

This offers the NLUM scheme more general property to meet more complicated requirements for different objects, operations and applications.

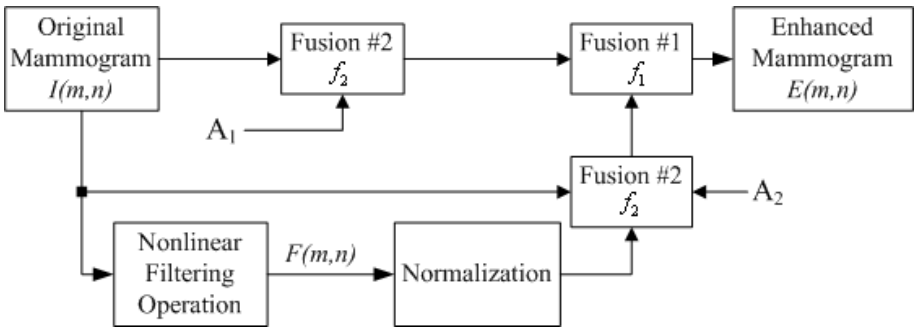


Figure 3.18: The block diagram of the new NLUM scheme.

For instance, if the fusion #1 and #2 in Figure 3.18 are selected as

1) arithmetic operations, the output enhanced mammogram is defined by,

$$E(m,n)=\left(A_1+A_2\frac{F(m,n)}{|F|_{\max}}\right)I(m,n) \tag{38}$$

where the constants A_1 and A_2 are the scaling factors, and $|F|_{\max}$ is the maximum absolute value of the filtered mammogram $F(m,n)$ which is defined by,

$$F(m,n)=w_0I_0-w_1I_1-w_2I_2 \tag{39}$$

where constants $w_0,w_1,w_2\geq 0$ are weight coefficients, and

$$\begin{aligned} I_0&=I^{2\alpha_0}(m,n)\\ I_1&=I^{2\alpha_1}(m-1,n)+I^{2\alpha_1}(m+1,n)+I^{2\alpha_1}(m,n-1)+I^{2\alpha_1}(m,n+1)\\ I_2&=I^{2\alpha_2}(m-1,n-1)+I^{2\alpha_2}(m+1,n-1)+I^{2\alpha_2}(m+1,n-1)+I^{2\alpha_2}(m+1,n+1) \end{aligned} \tag{40}$$

where the coefficients $\alpha_0,\alpha_1,\alpha_2$ are constants.

www.manaraa.com

2) PLIP operations, the output definition will change to,

$$E(m,n) = A_1 \otimes I(m,n) \oplus A_2 \otimes \left(\frac{F(m,n)}{|F|_{\max}} * I(m,n) \right) \tag{41}$$

where the filtered mammogram $F(m,n)$ is defined as,

$$F(m,n) = w_0 \otimes I_0 \Theta w_1 \otimes I_1 \Theta w_2 \otimes I_2 \tag{42}$$

and

$$\begin{aligned} I_0 &= I^{2\alpha_0}(m,n) \\ I_1 &= I^{2\alpha_1}(m-1,n) \oplus I^{2\alpha_1}(m+1,n) \oplus I^{2\alpha_1}(m,n-1) \oplus I^{2\alpha_1}(m,n+1) \\ I_2 &= I^{2\alpha_2}(m-1,n-1) \oplus I^{2\alpha_2}(m+1,n-1) \oplus I^{2\alpha_2}(m+1,n-1) \oplus I^{2\alpha_2}(m+1,n+1) \end{aligned} \tag{43}$$

where $\oplus, \Theta, \otimes, *$ are PLIP addition, subtraction, scalar multiplication and image multiplication, respectively, and the coefficients $A_1, A_2, w_0, w_1, w_2, \alpha_0, \alpha_1, \alpha_2$ are constants. Interestingly, the nonlinear filtering operator in the NLUM can be designed as a combination of two different types of filters. This offers the presented NLUM more robust characteristics for different applications. For example, the coefficients w_0, w_1, w_2 can be designed as a highpass filter and $\alpha_0, \alpha_1, \alpha_2$ can be chosen as a center weighted mean filter. In this case, the NLUM can suppress noise and keep sharp details unchanged while enhancing fine details in mammograms.

3.4.2.2 Discussion

Due to the fact that there are eight coefficients to be specified for practical applications, the NLUM is a complex unsharp masking scheme. However, more coefficients offer the

www.manaraa.com

NLUM more power and design flexibility to meet the specific and complex requirements of real world applications.

To simplify the NLUM design and reduce the number of its coefficients in practical applications, the NLUM's coefficients can be represented by one or two variables based on reasonable assumptions. An enhancement measure approach can then be used to optimize the coefficients and obtain the best enhanced result.

An alternative method is available, whereby users can manually select all the NLUM's coefficients. However, this is a time-consuming method and it is hard to attain the best enhancement results due to the lack of a criterion for quantitative evaluation.

In summary, the presented NLUM scheme has at least the three following impressive features:

- Fusion #1 and #2 in Figure 3.18 can be defined as linear or nonlinear operations
- The nonlinear filtering operator can be designed as a combination of different types of filters.
- The coefficients allow users to change the NLUM's properties to meet the specific requirements of application more effectively.

All these features offer users more design flexibility to adapt the scheme to meet the specific and complicated requirements of real world applications.

www.manaraa.com

3.4.3 Results and Analysis

In this section, one mammogram from the internet is used as an example to demonstrate how the NLUM parameters can be designed and automatically optimized using the presented SDME. The HVS-based image decomposition is then used for the visualization and analysis of the enhanced results. In the coming Section 3.4.4, the SDME is also used to measure and evaluate the performance of the NLUM scheme for mammogram enhancement.

3.4.3.1 Parameter Optimization

To assess the enhancement performance of the presented NLUM scheme, the users have the flexibility to adopt any existing measure approach for establishing a qualitative metric of mammogram enhancement. The enhancement measure can also be used to optimize all the NLUM coefficients to achieve the best enhanced results. In this section, the SDME is selected to measure and evaluate the performance of the NLUM for mammogram enhancement.

To reduce the number of the NLUM's coefficients, the users can make assumptions. For example, (1) $A_2 = 1/A_1, w_0 = 2$, $\alpha_0 = 8h$, $\alpha_1 = \alpha_2 = h$, and $w_1 = w_2 = -0.125$; or (2) $A_2 = 20A_1$, $w_0 = 8h$, $\alpha_0 = 12h$, $\alpha_1 = h$, $\alpha_2 = 2h$, and $w_1 = w_2 = -h$. Of course, users can make other assumptions. Therefore, all the NLUM's coefficients change according to the different values of the parameters A_1 and h after the above assumptions. This section selects the assumption (1) to show how to design the new NLUM automatically.

www.manaraa.com

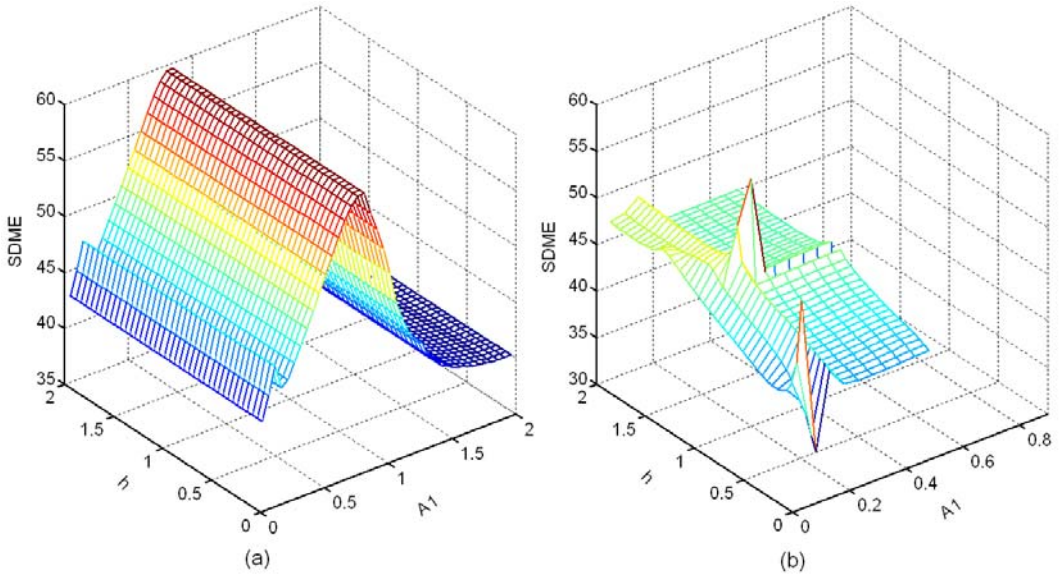
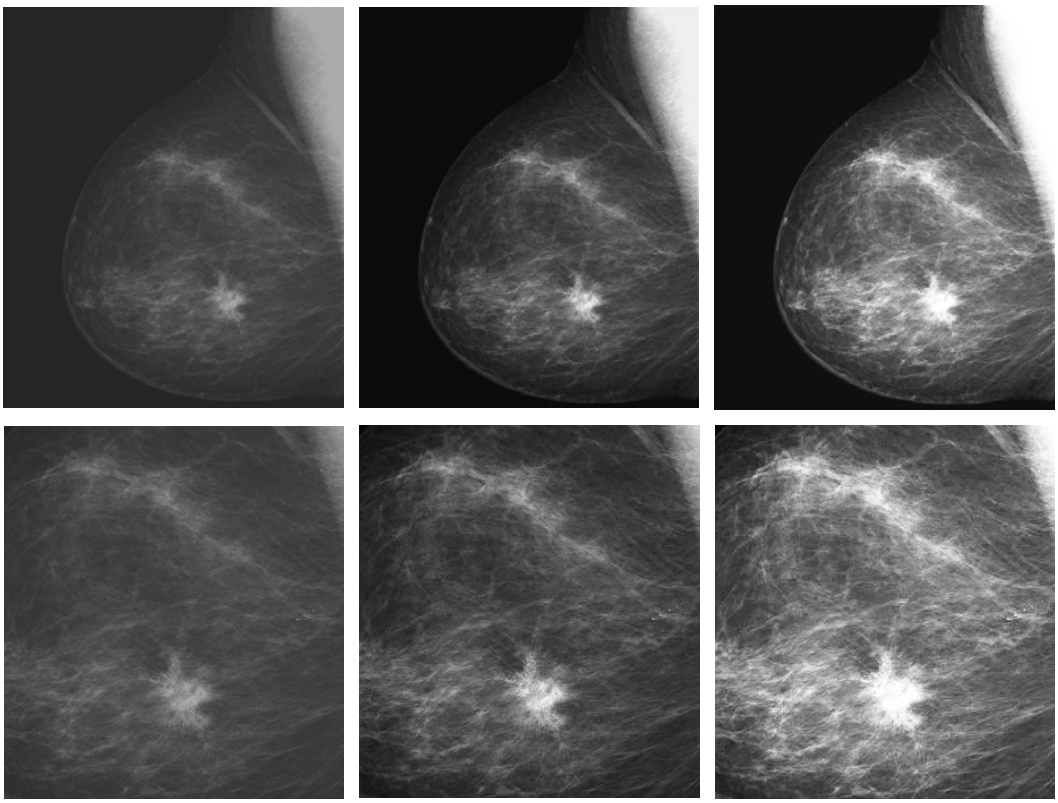


Figure 3.19: The SDME measure plots of mammogram enhancement based on different parameters A_1 and h. (a) SDME measure graph by arithmetic addition; (b) SDME measure graph by PLIP addition. In (b), easily discernable peaks denote optimal parameters that yield the best visual image enhancement.

The presented NLUM is applied to the mammograms after different designs are obtained through changing the parameters A_1 and h. The SDME is then used to measure the enhanced mammograms. The measure results are plotted as a graph. The parameters A_1 and h for the best enhanced results can be located at the points where the SDME curve reaches the first local extrema. Users apply the parameters in these points to enhance the original image. They are then inspected by human eyes to decide the best enhanced results and parameters.

The mammogram in Figure 3.20(a) is used as a test image for the NLUM design and the enhancement measure. Figure 3.19 plots the SDME measure results of the enhanced mammograms. From the measure results, parameters A_1 and h are located for achieving the best enhanced result.

www.manaraa.com



(a) (b) (c)

Figure 3.20: Mammogram enhancement using the presented NLUM. (a) The original mammogram and its cropped region; (b) The mammogram and its cropped region after they have been enhanced by the NLUM with arithmetic addition; (c) The mammogram and its cropped region after they have been enhanced by the NLUM with PLIP addition.

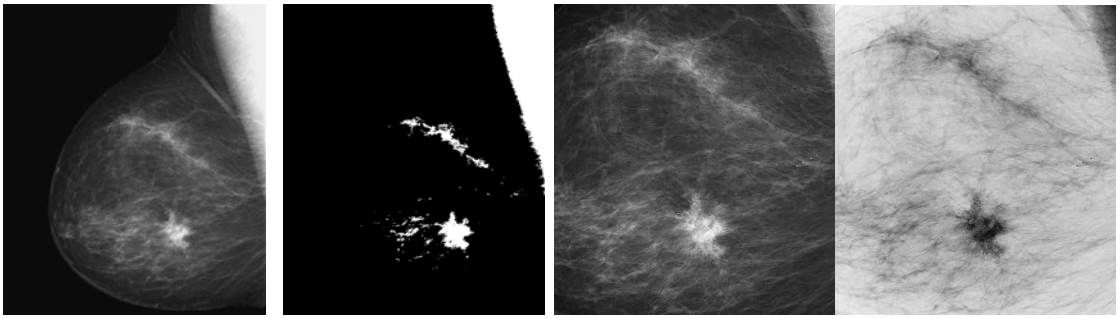
Using the parameters obtained from the measure in Figure 3.19, the NLUM enhances the original mammogram with arithmetic addition and PLIP addition, respectively. The enhanced mammograms and their cropped abnormal regions are shown in Figure 3.20. As can be seen from the images, both the visual quality and local contrast of the enhanced mammograms are far superior to those of the originals. The fine details of the cancer cells and masses that appear in the original mammogram are significantly improved. Not only are the cancer cells more recognizable in the enhanced mammograms, the masses are too.

www.manaraa.com

Compared to the enhanced results obtained by using two types of fusion operators in Figure 3.20, the arithmetic addition shows better performance than the NLUM based on PLIP addition because the latter slightly over-enhances the cancer cells and mass regions shown in Figure 3.20(c). Therefore, the rest of this section chooses the arithmetic addition as the default fusion operator for the presented NLUM for mammogram enhancement.

3.4.3.2 Enhancement Analysis

Figure 3.21 shows different ways to analyze the enhanced images, including thresholding, zoom view and negative photo projection of specific regions of interest. They demonstrate that the NLUM provides excellent performance for improving the contrast of specific regions, objects and details in mammograms.



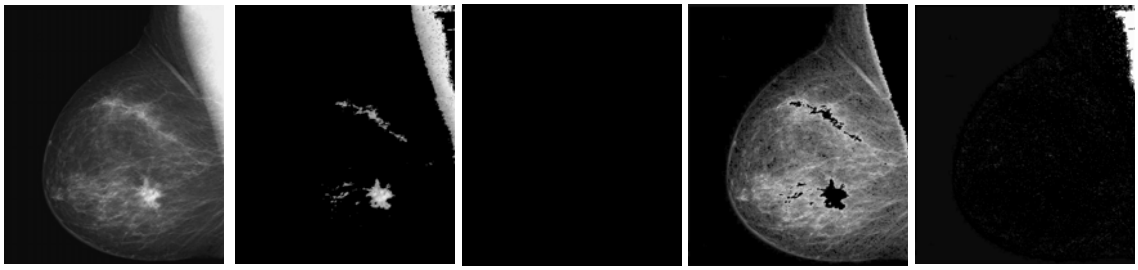
(a) (b) (c) (d)

Figure 3.21: Enhancement analysis. (a) The enhanced mammogram; (b) the threshold image of (a); (c) Region cropped from (a); (d) the negative photo of (c).

www.manaraa.com

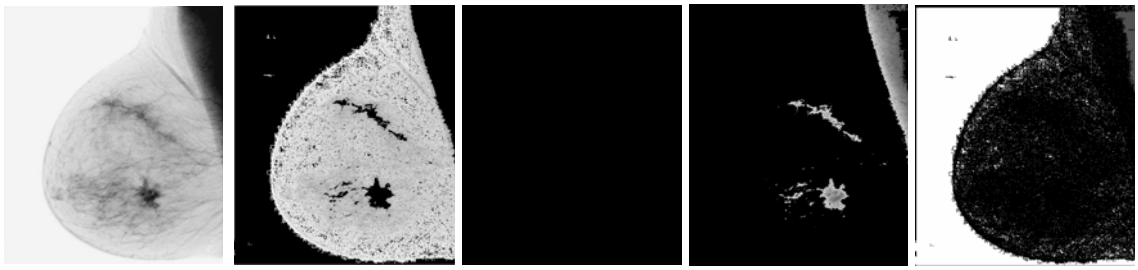
3.4.3.3 HVS-based Analysis and Visualization

Since the HVS-based image decomposition method separates images based on the background intensity and the rate of information change, its application is extended to enhancement analysis and visualization.



(a) (b) (c) (d) (e)

Figure 3.22: HVS-based decomposition of the enhanced mammogram. (a) The enhanced mammogram; (b) The first sub-image; (c) The second sub-image; (d) The third sub-image; (e) The fourth sub-image.



(a) (b) (c) (d) (e)

Figure 3.23: HVS-based decomposition of the visualized mammogram. (a) The negative of the image of the enhanced mammogram; (b) The first sub-image; (c) The second sub-image; (d) The third sub-image; (e) The fourth sub-image.

Figures 3.22 and 3.23 show the HVS-based decomposition results of the enhanced mammogram and its negative (tonal inversion), respectively. Interestingly one characteristic of the results is that the cancer cells and mass regions are automatically segmented by HVS-based decomposition in the sub-image without any thresholding or segmentation process being involved. The results are shown in Figures 3.22(b) and

www.manaraa.com

3.23(d). Therefore, HVS-based image decomposition can be used for segmentation and classification of pathological cases in the computer-aided detection (CAD) system.

3.4.4 Performance Comparison

The objective of this section is to compare the performance of four image enhancement algorithms on secondarily digitized (i.e., digitized from film) mammograms using the presented NLUM scheme and three other well-known enhancement algorithms: adaptive neighborhood contrast enhancement algorithm (ANCE) [16], Rational Unsharp Masking (RUM) [21], and Contrast-limited adaptive histogram equalization (CLAHE) [135]. Those three algorithms are standard enhancement methods with high citations. The algorithms' implementation codes were provided by the authors. Without any modification, these codes were directly used to enhance the original images. The authors confirmed all the enhanced results. In this manner, the comparison results are accurate and convincing. The SDME measure and several existing measures will be used to judge the enhancement results of these algorithms in order to compare their performance. The results show that all algorithms change the image appearance drastically. In most cases, the best enhancement results are obtained by the presented NLUM.

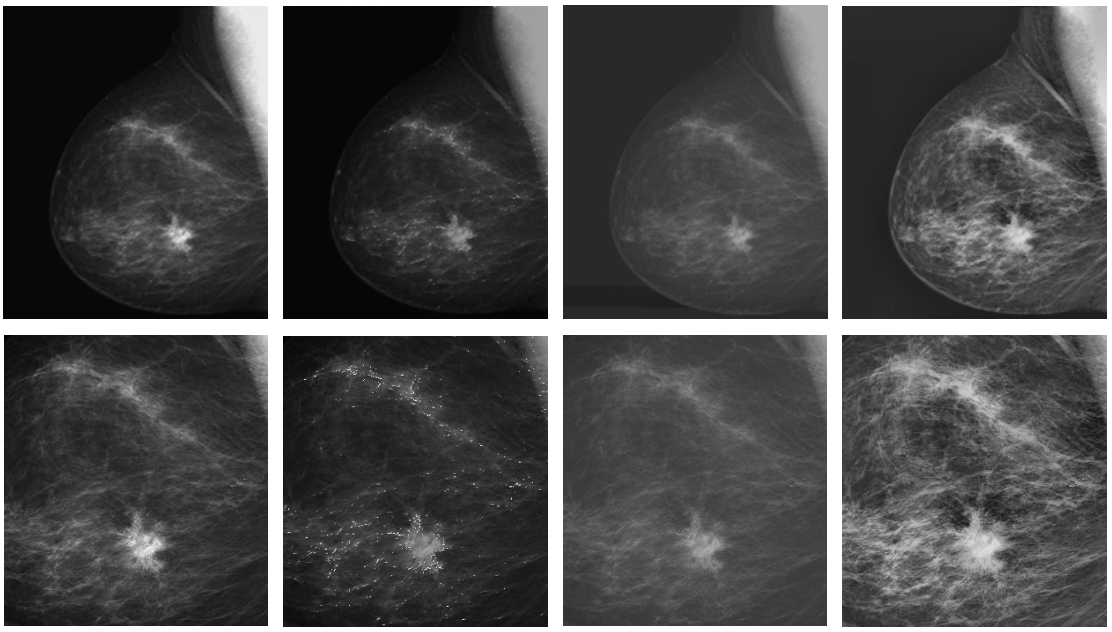
3.4.4.1 Comparison of Measure Performance

The above mentioned algorithms are used to enhance the mammogram in Figure 3.20(a). Figure 3.24 shows the enhanced mammograms and their cropped regions.

Figure 3.24(b) shows the enhanced mammogram by the RUM. The RUM generated a lot of artifacts in the enhanced image such as noise spots. The ANCE didn't enhance the

www.manaraa.com

mammogram since its enhanced result in Figure 3.24(c) is visually the same as the original mammogram in Figure 3.20(a). The CLAHE over-enhanced the brightest regions. However, the presented NLUM shows an excellent performance when it comes to enhancing the mammograms. As can be seen in Figure 3.24(a), the NLUM significantly improves the mammograms' visual quality without generating artifacts or over-enhancing the images.



(a) (b) (c) (d)

Figure 3.24: Enhanced results of the mammogram in Figure 3.20(a) by different algorithms. (a) The mammogram enhanced by the NLUM and its cropped region; (b) The mammogram enhanced by RUM and its cropped region; (c) The mammogram enhanced by ANCE and its cropped region; (d) The mammogram enhanced by CLAHE and its cropped region.

The original and enhanced mammograms are then measured by the new SDME and several existing measures. The measure results are shown in Table 3.3. The higher the measure results the better the enhancement performance.

www.manaraa.com

Comparing the visual quality of mammograms in Figure 3.24 to their corresponding measure results in Table 3.3, the new SDME measure shows the best overall measure performance. Therefore, in the rest of this section, the SDME is selected to measure and assess the enhancement results of different algorithms.

TABLE 3.3 MEASURE RESULTS OF THE ENHANCEMENT IN FIGURE 3.24

	Original	NLUM	RUM	ANCE	CLAHE
EME	0.8717	1.0287	1.0978	0.8223	2.2345
EMEE	0.0531	0.0651	0.0899	0.0497	0.1857
AME	23.3439	22.6722	22.7153	24.0022	17.7211
AMEE	0.0781	0.0851	0.0806	0.0748	0.1135
logAME	0.0454	0.0435	0.0441	0.0469	0.0329
logAMEE	0.1084	0.1156	0.1078	0.1047	0.1319
SDME	38.9001	43.2643	38.0607	39.3719	33.0089

Note: A higher score indicates the better enhancement performance.

3.4.4.2 Comparison of Enhancement Performance

All original mammograms appearing in this section were obtained from the mini-MIAS database of mammograms [134]. The database consists of 322 mammograms. The cases range from fairly dense to extraordinarily dense breast parenchyma. Some cases are completely fatty. Most masses have ill-defined, indistinct, or speculated borders. All mammograms are cropped into images with smaller sizes for analysis so that the resulting cropped mammographic images have limited black background, which contains non-object regions and background project noise.

The presented NLUM scheme and three existing enhancement algorithms have been applied to more than 76 mammographic images. This section selects 6 mammograms from the mini-MIAS database and two others obtained from the internet and shown in

www.manaraa.com

Figure 3.25. The description of the medical record attached to each mammogram is provided in Table 3.4.

TABLE 3.4 MEDICAL DESCRIPTION OF MAMMOGRAMS IN FIGURE 3.25

		Resource	Ref. #	Background Tissue	Severity of Abnormality
(A)	Mammogrma #1	mini-MIAS	mdb010	Fatty	Benign
(B)	Mammogrma #2	mini-MIAS	mdb058	Dense-glandular	Malignant
(C)	Mammogrma #3	mini-MIAS	mdb121	Fatty-glandular	Benign
(D)	Mammogrma #4	Internet			
(E)	Mammogrma #5	mini-MIAS	mdb091	Fatty	Benign
(F)	Mammogrma #6	Internet			
(G)	Mammogrma #7	mini-MIAS	mdb063	Dense-glandular	Benign
(H)	Mammogrma #8	mini-MIAS	mdb064	Dense-glandular	None

Reference: http://peipa.essex.ac.uk/info/mias.html.

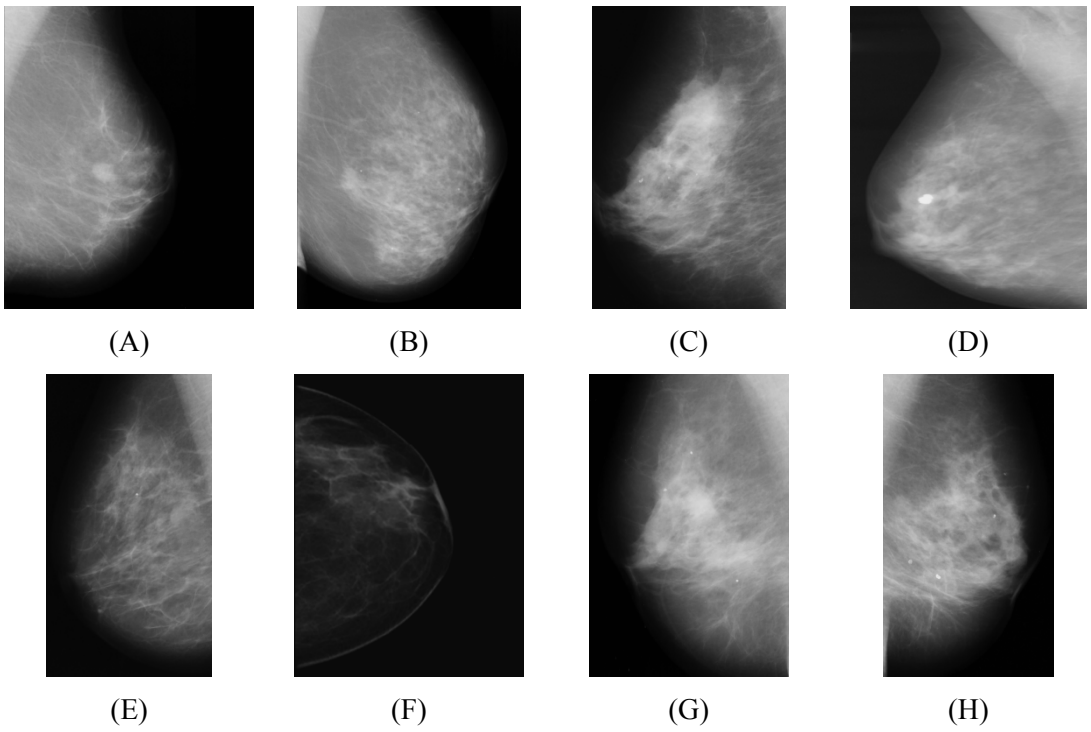
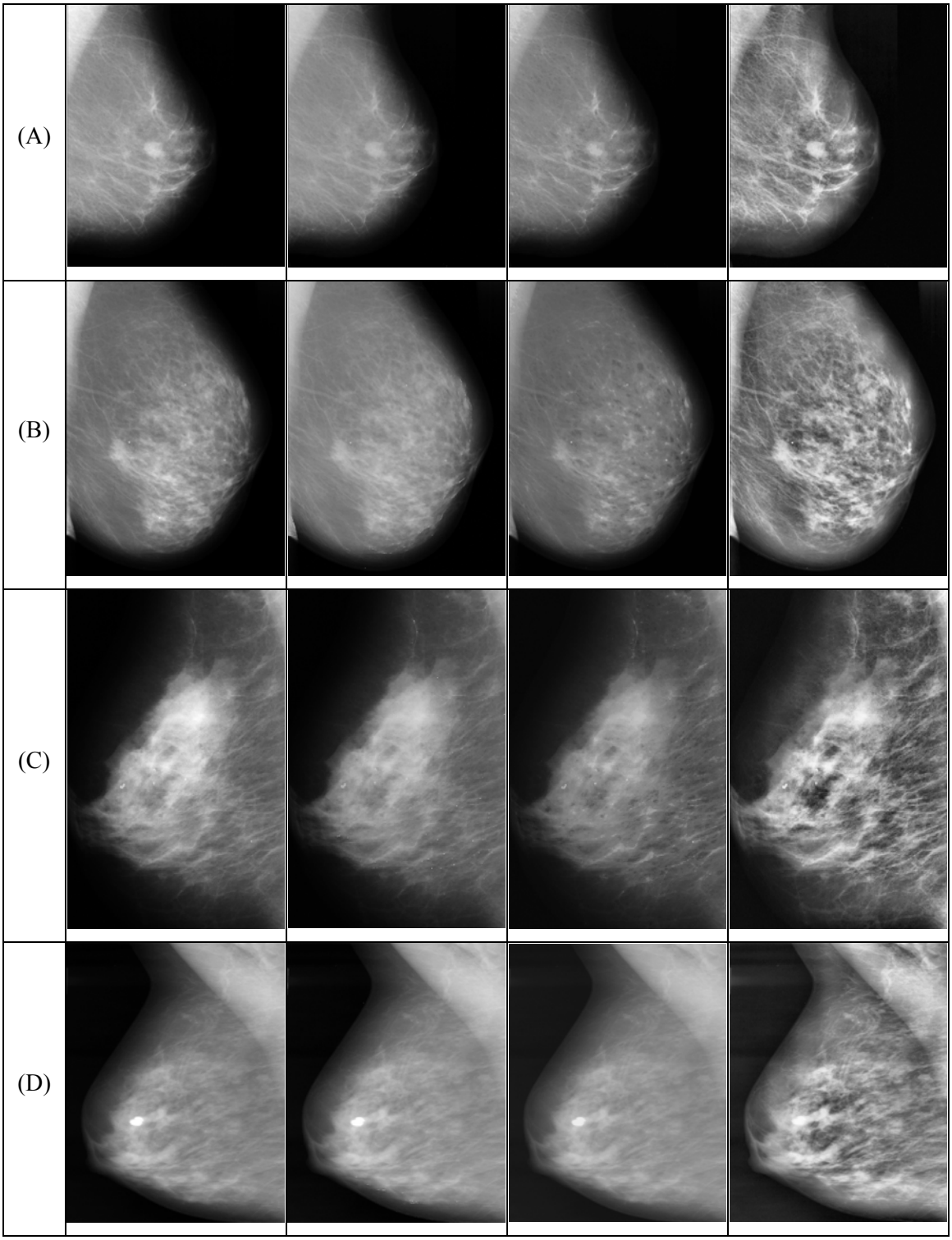
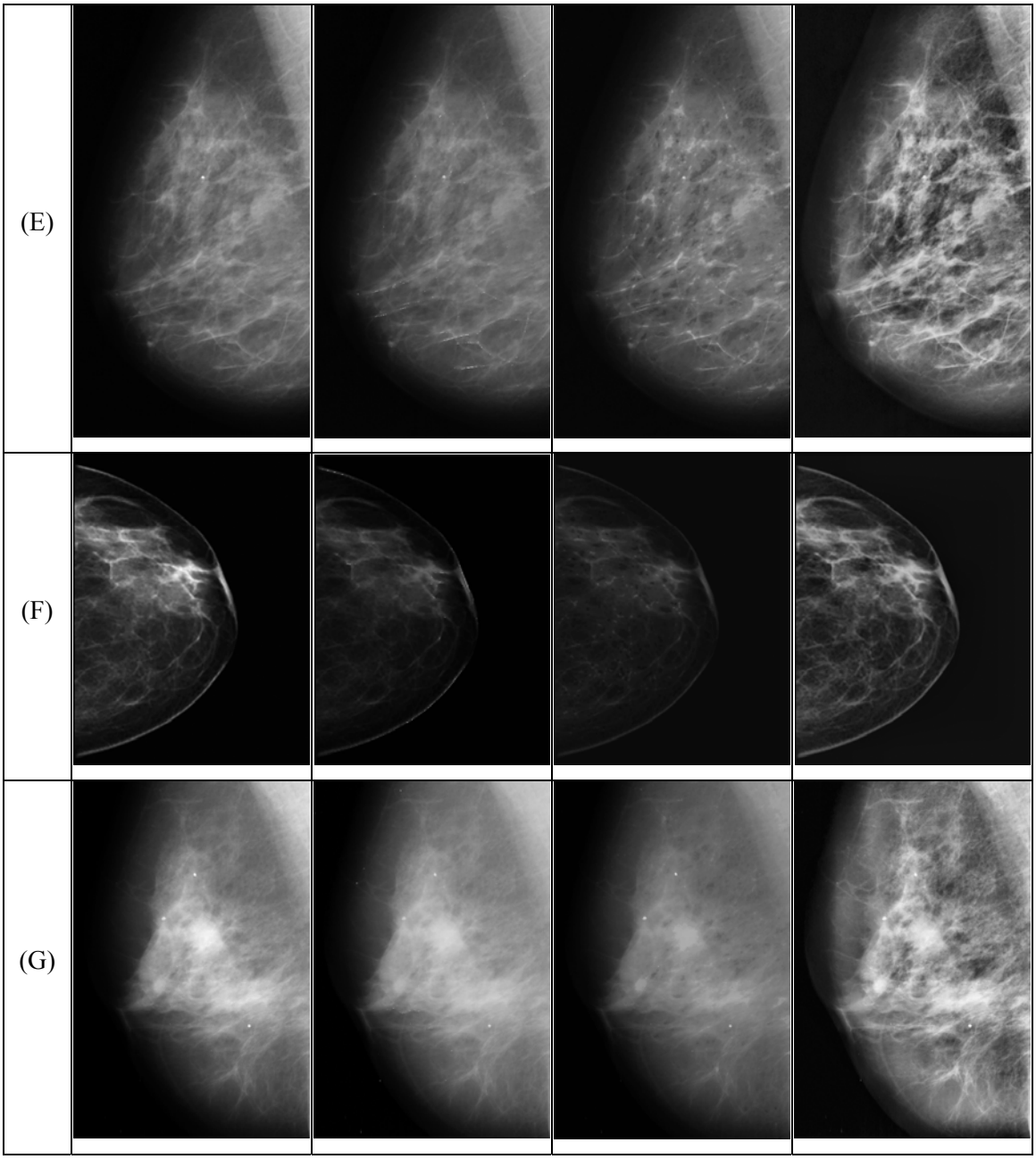


Figure 3.25: Original mammograms. (A) mammogram #1; (B) mammogram #2; (C) mammogram #3; (D) mammogram #4; (E) mammogram #5; (F) mammogram #6; (G) mammogram #7; (H) mammogram #8.

www.manaraa.com



www.manaraa.com



www.manaraa.com

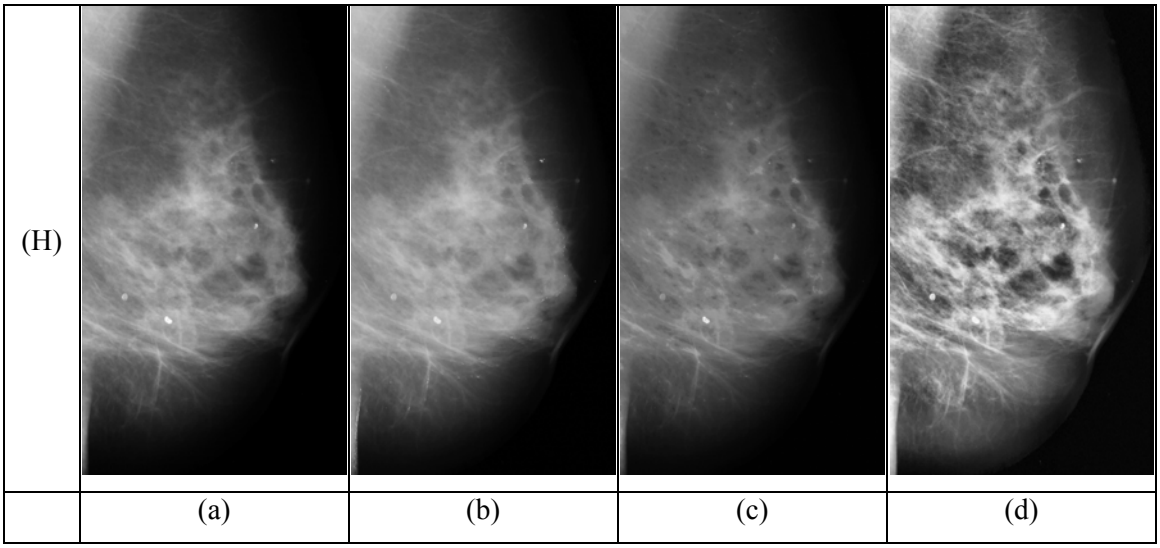


Figure 3.26: Mammograms enhanced by different algorithms. (a) The mammograms enhanced by the NLUM; (b) The mammograms enhanced by RUM; (c) The mammograms enhanced by ANCE; (d) The mammograms enhanced by CLAHE.

TABLE 3.5 SDME RESULTS OF MAMMOGRAMS ENHANCED BY DIFFERENT ALGORITHMS

		Original	NLUM	RUM	ANCE	CLAHE
(A)	Mammogrma #1	45.324	51.4999	45.2696	45.324	38.3484
(B)	Mammogrma #2	37.1411	43.4236	36.9899	39.8874	32.4629
(C)	Mammogrma #3	37.7296	44.2589	37.5586	35.0562	32.7181
(D)	Mammogrma #4	39.7331	44.1372	39.6407	37.6267	33.9583
(E)	Mammogrma #5	30.4969	37.6857	30.453	36.9915	29.0275
(F)	Mammogrma #6	34.204	50.7331	34.0114	32.8442	30.3406
(G)	Mammogrma #7	37.9647	46.0087	37.9444	40.3314	33.8075
(H)	Mammogrma #8	37.2825	43.4025	37.1356	35.7032	33.1566

Note: A higher score indicates the better enhancement performance.

All mammograms in Figure 3.25 are enhanced by the NLUM and the three existing enhancement algorithms individually. The enhanced results are shown in Figure 3.26. The results show that the NLUM shows a high quality of performance when it comes to improving the contrast of specific regions and objects. These regions or objects may

www.manaraa.com

contain cancer cells and abnormal diseases that are extremely important to find if the right clinical treatment is to be offered.

The SDME measure results for all enhanced mammograms are shown in Table 3.5 and plotted in Figure 3.27. The measure results also verify that the NLUM shows better enhancement performance.

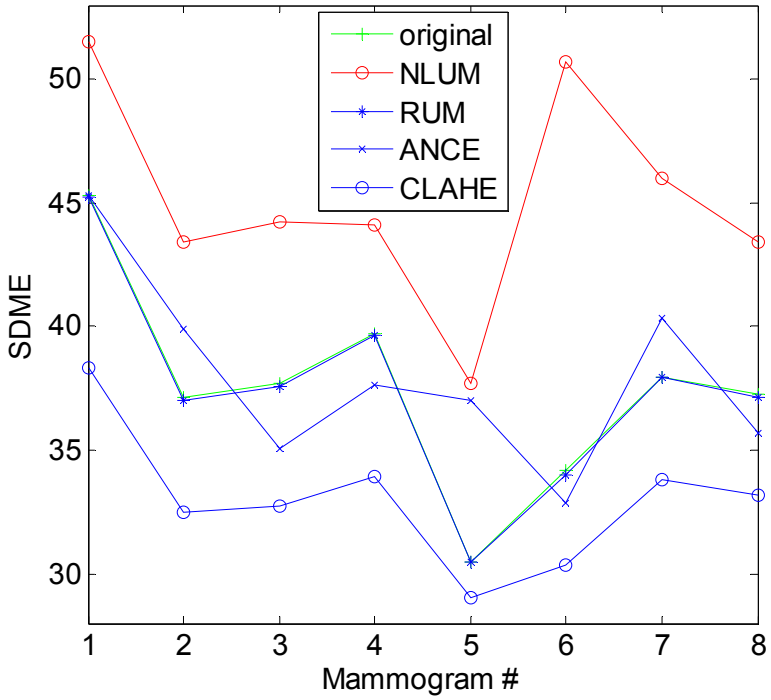
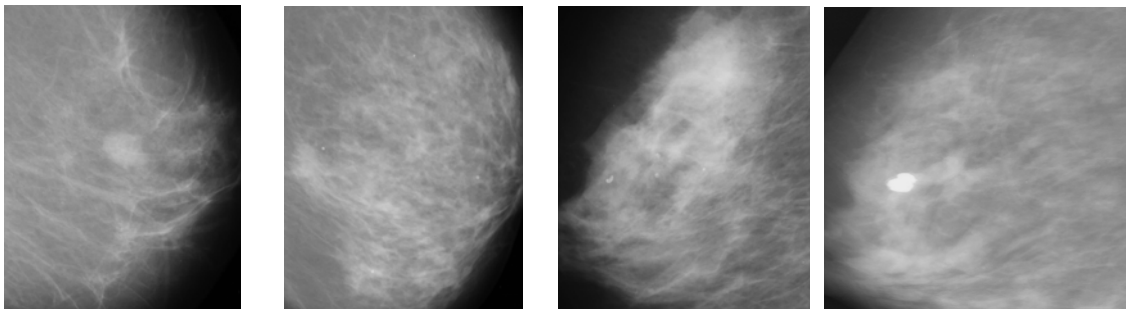


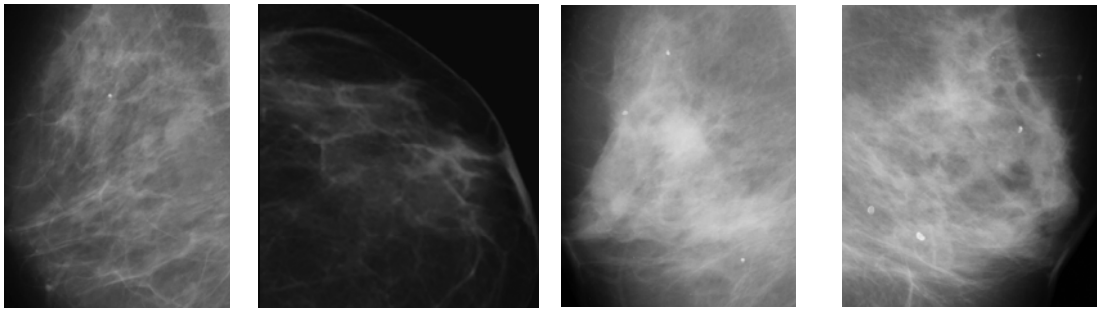
Figure 3.27: SDME measure results of mammograms enhanced by different algorithms in Figure 3.26.

The SDME measure results for all enhanced mammograms are shown in Table 3.5 and plotted in Figure 3.27. The measure results also verify that the NLUM shows better enhancement performance.

www.manaraa.com

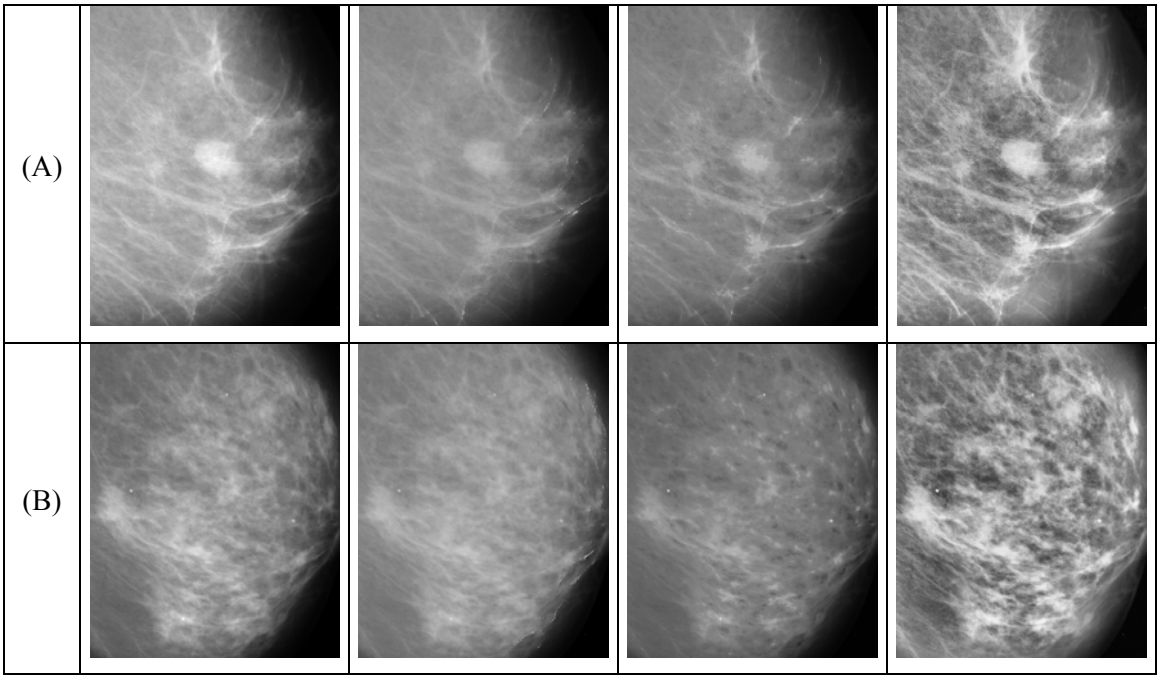


(A) (B) (C) (D)

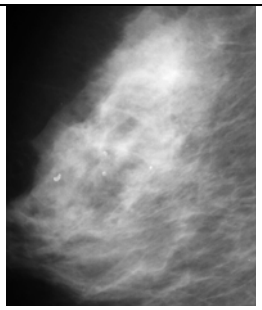
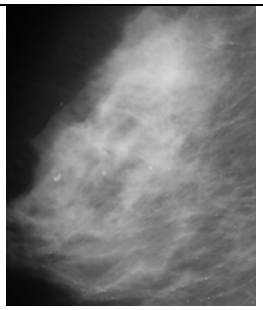
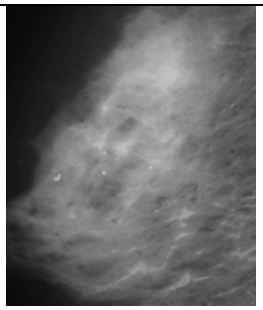
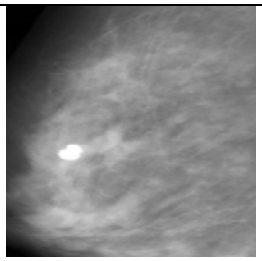
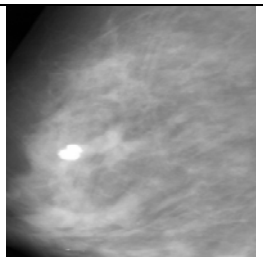
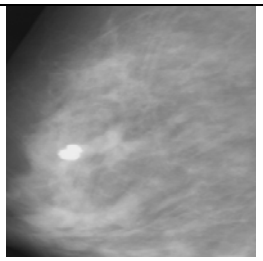
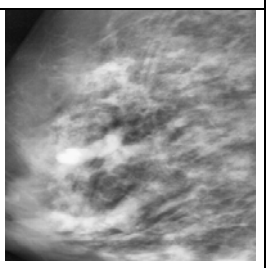
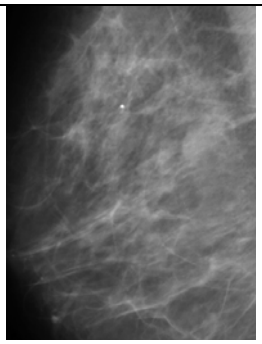
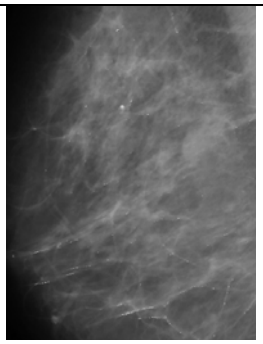
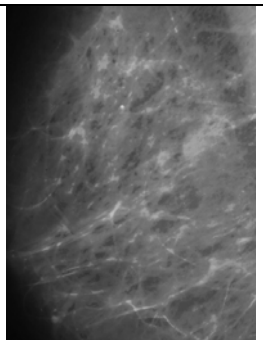
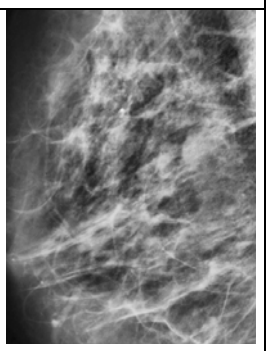
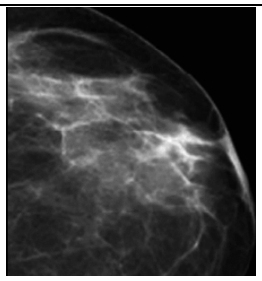
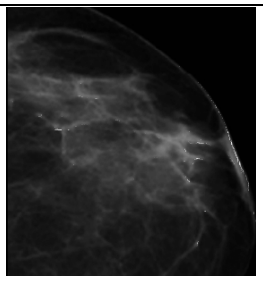
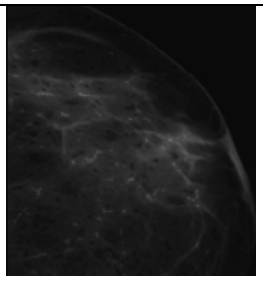
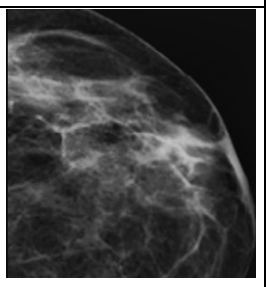
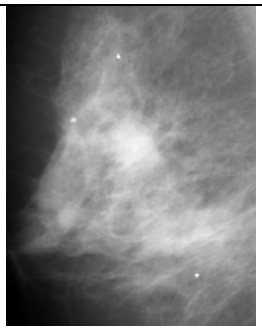
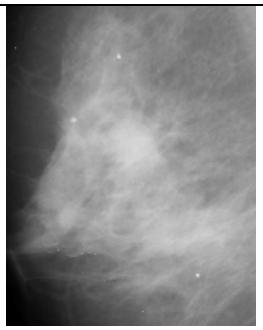
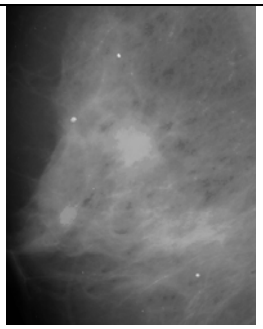
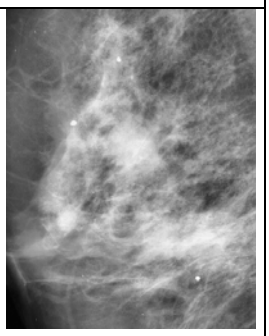


(E) (F) (G) (H)

Figure 3.28: Regions cropped from original mammograms in Figure 3.25. (A) region from mammogram #1; (B) region from mammogram #2; (C) region from mammogram #3; (D) region from mammogram #4; (E) region from mammogram #5; (F) region from mammogram #6; (G) region from mammogram #7; (H) region from mammogram #8.



www.manaraa.com

(C)				
(D)				
(E)				
(F)				
(G)				

www.manaraa.com

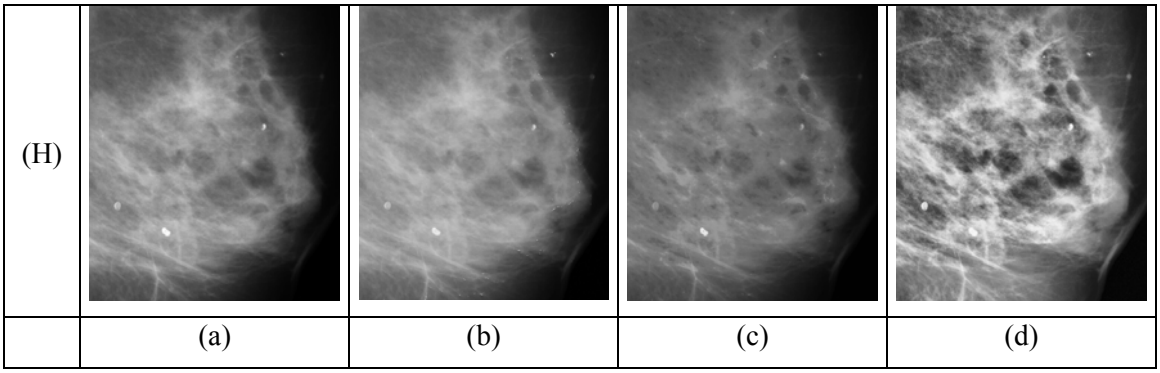
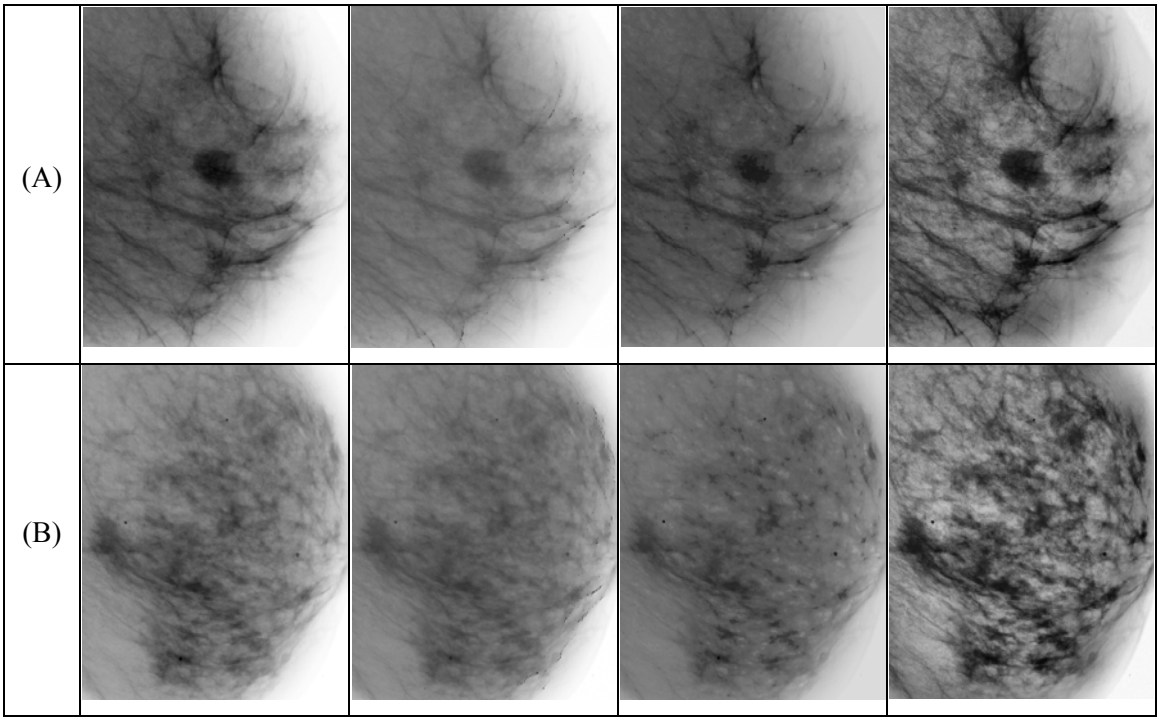
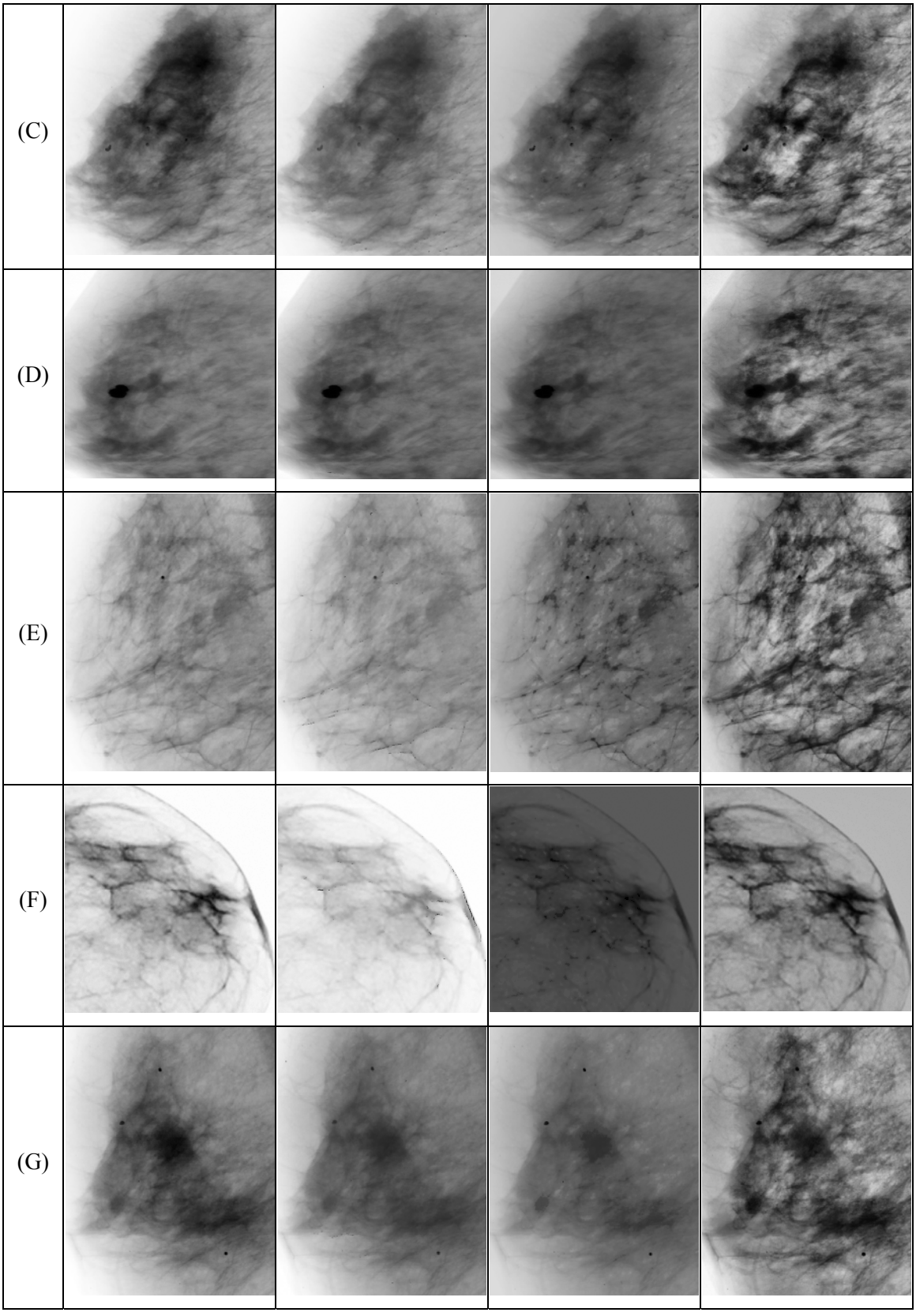


Figure 3.29: Regions enhanced by different algorithms. (a) The regions enhanced by the NLUM; (b) The regions enhanced by RUM; (c) The regions enhanced by ANCE; (d) The regions enhanced by CLAHE.

Figure 3.28 shows the cropped regions from each original mammogram in Figure 3.25. These regions contain the specific objects and details that may be of interest to radiologists for clinical purposes. The enhanced results for each mammogram are shown in Figure 3.29. The negative photo projections of the enhanced regions are provided in Figure 3.30.



www.manaraa.com



www.manaraa.com

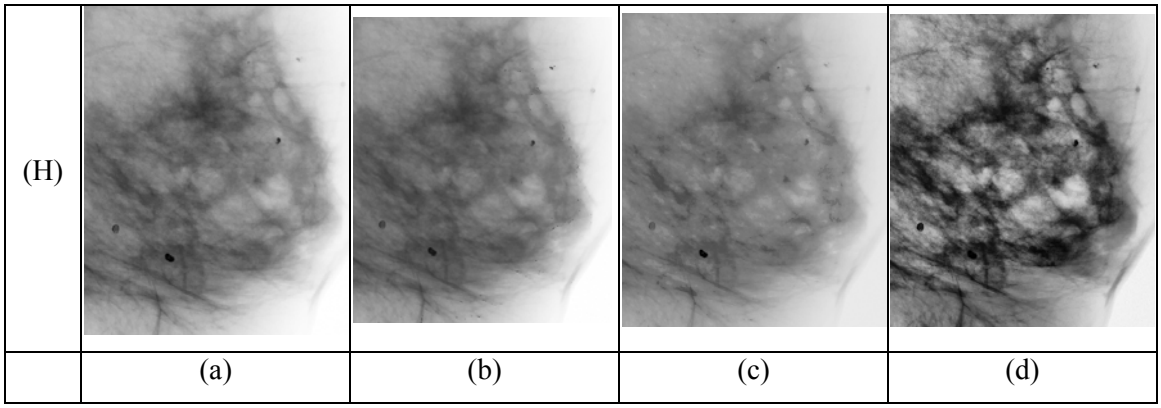
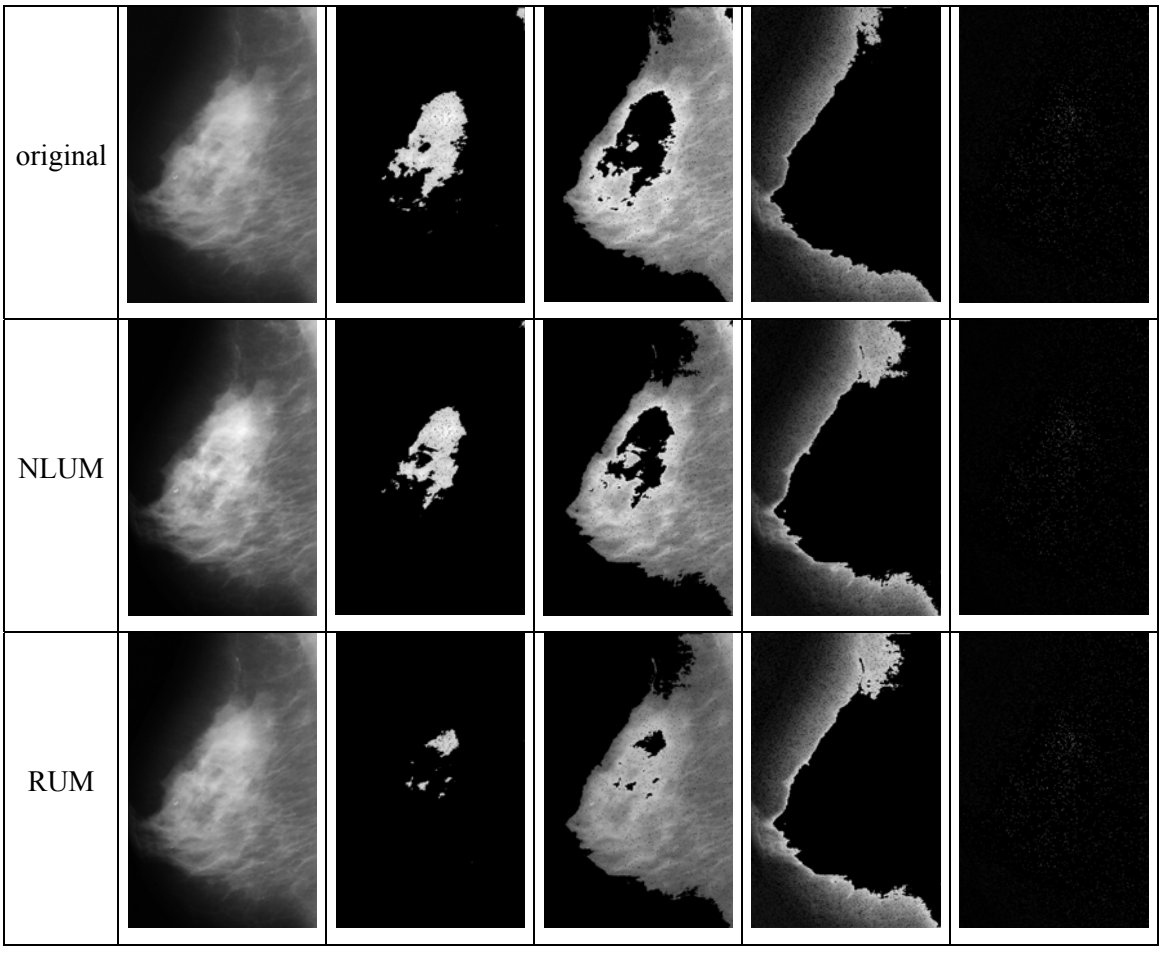


Figure 3.30: Negative photos of regions enhanced by different algorithms. (a) Negative photos of regions enhanced by the NLUM; (b) Negative photos of regions enhanced by RUM; (c) Negative photos of regions enhanced by ANCE; (d) Negative photos of regions enhanced by CLAHE.



www.manaraa.com

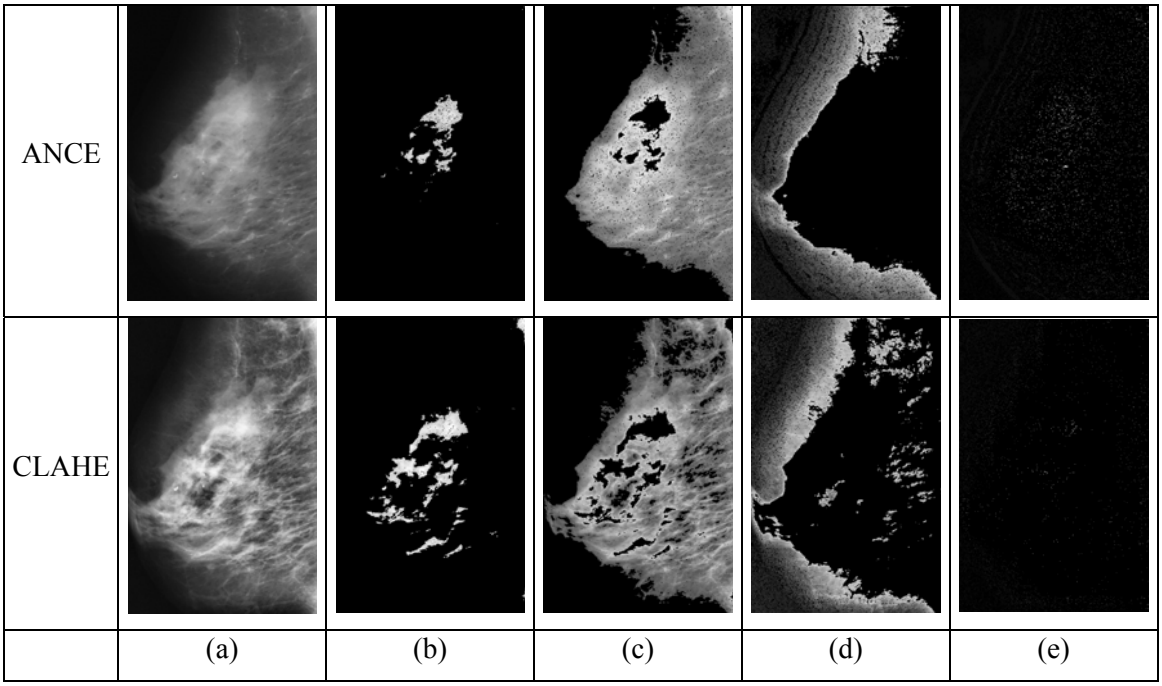


Figure 3.31: HVS-based decomposition (HVSD) of the original mammogram and its enhanced results by different algorithms. (a) The original mammogram and the enhanced mammograms; (b) The first HVSD sub-images of the original mammogram and the enhanced mammograms; (c) The second HVSD sub-images of the original mammogram and the enhanced mammograms; (d) The third HVSD sub-images of the original and enhanced mammograms.

Figure 3.31 shows the HVS-based decomposition (HVSD) results for the original mammogram and the mammograms enhanced by different algorithms. The results demonstrate that HVS-based decomposition can separate abnormal regions, which may contain the breast cancer cells, from the mammograms without using any thresholding or segmentation algorithm.

www.manaraa.com

3.5 Nonlinear Filtering for Enhancing Prostate MR Images via Alpha-Trimmed Mean Separation

Mean separation for image enhancement offers users the flexibility to enhance images with different intensity ranges. This section combines the AWQF with a parametric mean separation, alpha-trimmed mean separation, for enhancing prostate MR images.

3.5.1 The New Enhancement Algorithm

This section introduces a new enhancement algorithm for prostate MR images, integrating the nonlinear filtering with image decomposition, which uses the alpha-trimmed mean as the threshold.

3.5.1.1 Alpha-Trimmed Mean

The alpha-trimmed mean filter is widely used for image processing such as image denoising [138] and restoration [139, 140]. Here, the alpha-trimmed mean is used for image decomposition.

For an image with a size of $M \times N$, let $K = M \times N$ and a single index $x_1, x_2, ...x_K$ indicate the sorted values of all pixels of the image such that $x_1 \le x_2 \le ... \le x_K$. Let $T_\alpha = \lceil \alpha K \rceil$ (the nearest integer greater than or equal to αK) be the number of the smallest and largest pixel samples to be trimmed or discarded from the sorted sequence. The alpha-trimmed mean of the image is defined by,

www.manaraa.com

$$X_\alpha = \frac{1}{K - 2T_\alpha} \sum_{i=T_\alpha+1}^{K-T_\alpha} x_i \tag{44}$$

where $0 \le \alpha < 0.5$ is the percentage of the trimmed samples.

The alpha-trimmed mean will be different when the parameter α changes. For example, for $\alpha = 0$, it will be the mean value of the image, whereas if α is close to 0.5, it will be the median value of the image. Taking this advantage, the alpha-trimmed mean is used as the threshold for image decomposition.

3.5.1.2 The New Enhancement Algorithm

To improve the visual quality of prostate MR images for prostate cancer detection, the nonlinear filter is integrated with the image decomposition technique described above. A new algorithm for enhancing prostate MR images is then introduced. The algorithm is shown in Figure 3.32.

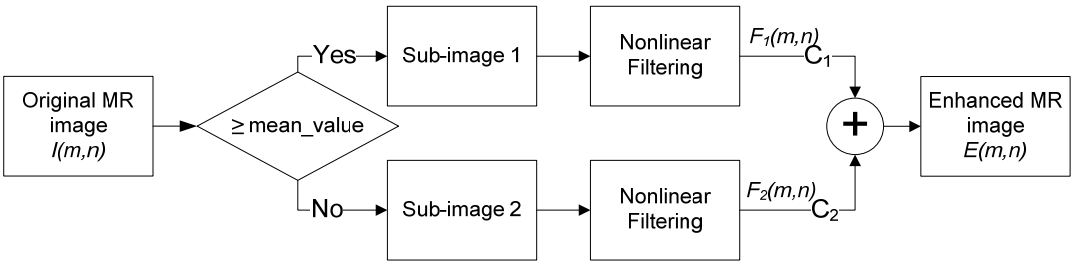


Figure 3.32: Block diagram of the MSNLF scheme

The algorithm first separates the original MR image $I(m,n)$ into two sub-images. The threshold value of the image decomposition is the alpha-trimmed mean of the input MR image defined in equation (44). The two sub images are then individually filtered by a

www.manaraa.com

nonlinear filtering operation to obtain the filtered images $F_1(m,n)$ and $F_2(m,n)$. The filtering operation is defined by,

$$F(m,n) = w_0 Y_0 + w_1 Y_1 + w_2 Y_2 \tag{45}$$

where

$$\begin{aligned} Y_0 &= I^{2\alpha_0}(m,n) \\ Y_1 &= I^{2\alpha_1}(m-1,n) + I^{2\alpha_1}(m+1,n) + I^{2\alpha_1}(m,n-1) + I^{2\alpha_1}(m,n+1) \\ Y_2 &= I^{2\alpha_2}(m-1,n-1) + I^{2\alpha_2}(m+1,n-1) + I^{2\alpha_2}(m+1,n-1) + I^{2\alpha_2}(m+1,n+1) \end{aligned}$$

and constants w_i, α_i are weight coefficients, $i = 0,1,2$.

Finally, the output enhanced image is defined by,

$$E(m,n) = C_1 F_1(m,n) + C_2 F_2(m,n) \tag{46}$$

where constants C_1, C_2 are the scaling factors.

Since the alpha-trimmed mean value is dependent on alpha, the decomposed sub-images contain different background intensities when the alpha value changes. The nonlinear filter then enhances sub-images with different intensity values. Therefore, the presented algorithm enhances images while preserving the background intensity at different levels.

The nonlinear filter is embedded in two filters specified by w_0, w_1, w_2 and $\alpha_0, \alpha_1, \alpha_2$ separately. These two filters can be designed as two different types of linear or nonlinear filters. For example, the coefficients w_0, w_1, w_2 can be designed as a highpass filter and $\alpha_0, \alpha_1, \alpha_2$ can be chosen as a weighted mean filter. The nonlinear filtering

www.manaraa.com

process can suppress noise and keep sharp details unchangeable while enhancing the contrast of fine details in prostate MR images. All these capabilities give the presented algorithm robust characteristics for a variety of applications.

3.5.2 Enhancement Results and Analysis

The original prostate MR images were obtained from the Department of Radiology at Memorial Sloan-Kettering Cancer Center in New York, NY. In order to minimize the dark background and also remove the text records of patients' information, these images are cropped into images with smaller sizes. The presented algorithm is then used to enhance the images.

The presented algorithm has been successfully applied to more than 30 different MR images with prostate cancer. This section provides several enhanced results to demonstrate the presented algorithm's enhancement performance and then compares this performance with that of several existing enhancement methods.

3.5.2.1 Parameter Selection

To find those parameters of the coefficients in the nonlinear filtering operator that will give the best enhancement results, assume: $\alpha_1 = \alpha_2 = h, w_1 = w_2 = -w,\ \alpha_0 = 4h,$ $w_0 = 4w,\ C_1 = C_2 = 1$ and $0 < h, w \le 1$. The prostate MR image in Figure 3.34(a) has been enhanced by the presented algorithm when the coefficients change as different h, w values within $(0,1]$. The enhanced images are then measured by the SDME respectively.

www.manaraa.com

The measure results are plotted in Figure 3.33. The parameters to achieve the best enhanced image are located at the local extrema in the SDME curve.

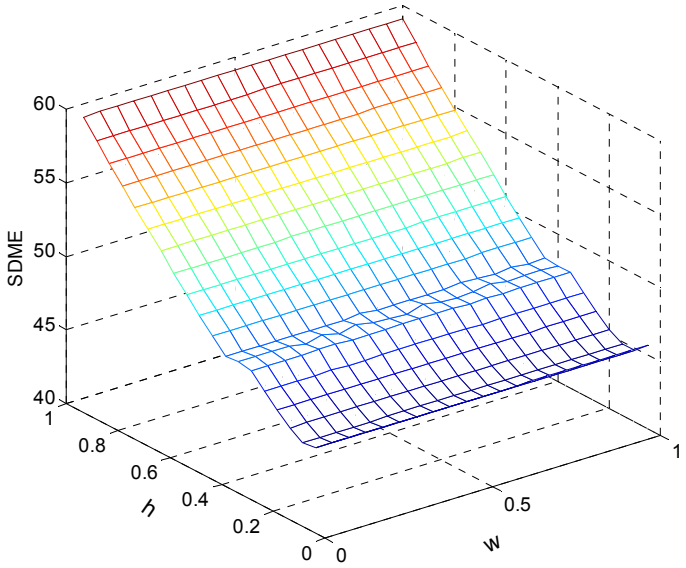
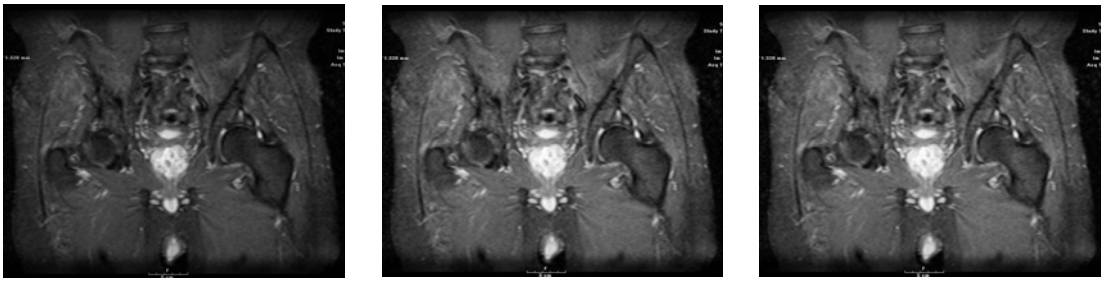


Figure 3.33: SDME results of the enhanced MR images for parameter optimization.

3.5.2.2 Enhancement Analysis

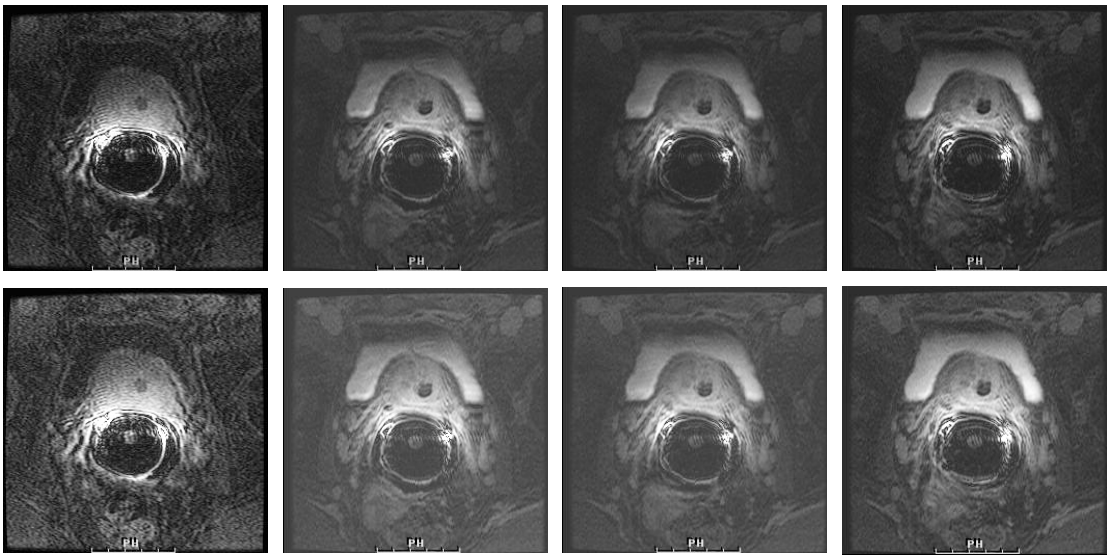
Figure 3.34 shows the images enhanced using this parameter. The contrast of the original MR image and the visual quality of its fine details are both significantly improved.



(a) (b) (c)

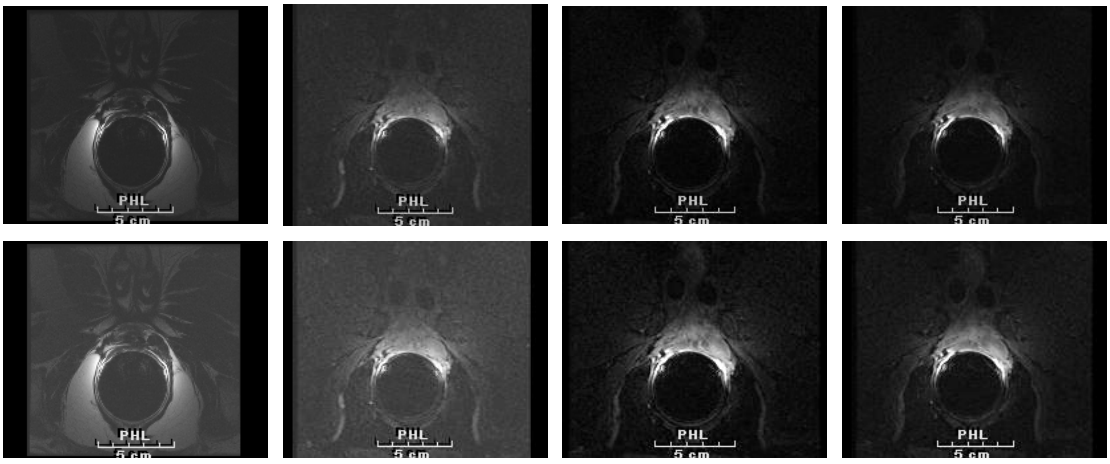
Figure 3.34: Prostate MR image enhancement. (a) The original prostate MR image; (b) The image enhanced by the presented algorithm, alpha=0; (c) The image enhanced by the presented algorithm, alpha=0.5.

www.manaraa.com



(a) (b) (c) (d)

Figure 3.35: Prostate MR images enhanced by the presented algorithm. (a)-(d): The top row shows the original prostate MR images; the bottom row shows the enhanced prostate MR images, alpha=0.



(a) (b) (c) (d)

Figure 3.36: Prostate MR images enhanced by the presented algorithm. (a)-(d): The top row shows the original prostate MR images; the bottom row shows the enhanced prostate MR images, alpha=0.49.

More enhanced examples are shown in Figures 3.35 and 3.36. The first row shows the original prostate MR images. The second row of each figure shows the MR images after

www.manaraa.com

they have been enhanced by the presented algorithm. The SDME is used to measure all the enhanced images. The measure results are plotted in Figure 3.37. The larger SDME values often indicate the better enhancement performance. These SDME results quantitatively demonstrate that the presented algorithm shows excellent enhancement performance when applied to prostate MR images.

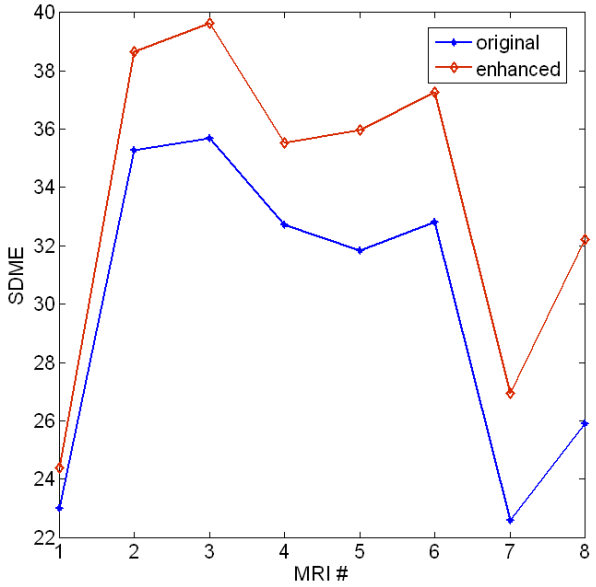
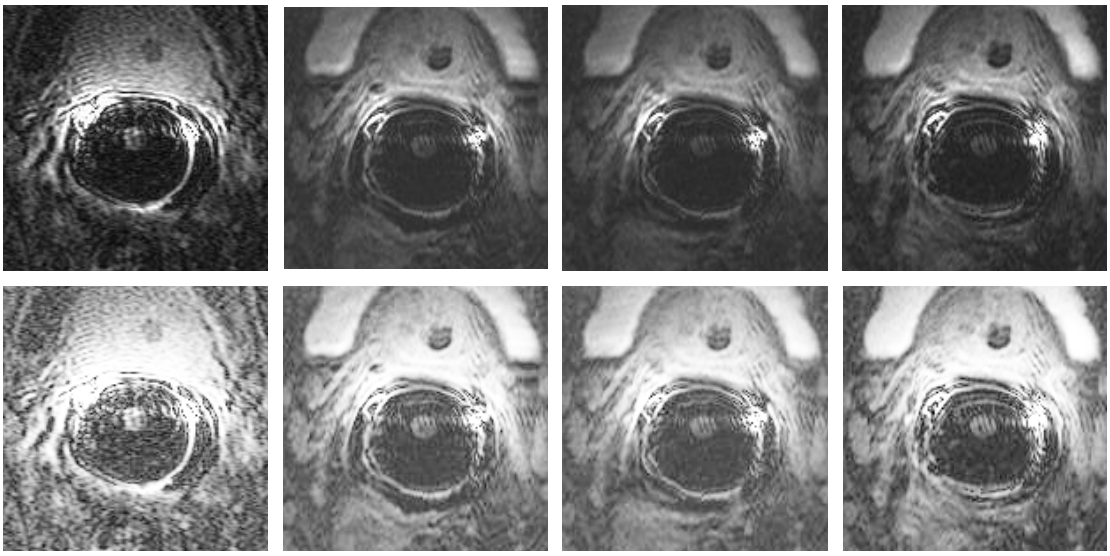


Figure 3.37: SDME plot of the prostate MR image enhancement in Figures 3.35-36.

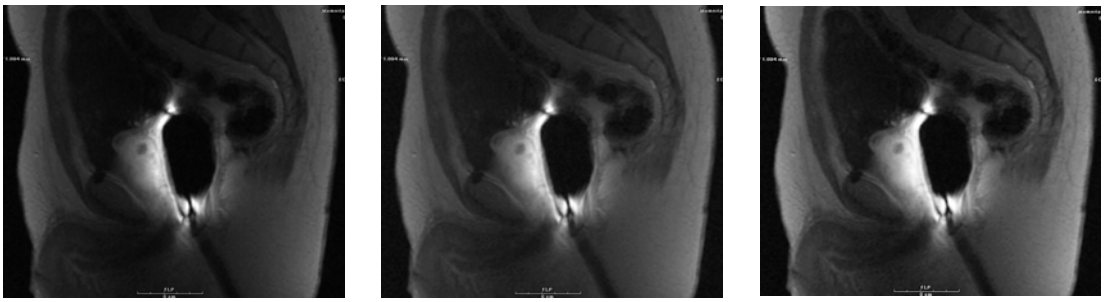
Figure 3.38 gives some examples of regional enhancement. The regions shown in the top row in Figure 3.38 are cropped from the original prostate MR images. They have been enhanced by the presented algorithm individually. The enhancement results are shown in the bottom row in Figure 3.38. The region contrast is greatly improved. This shows that the presented algorithm has potential applications for enhancing fine details or specific regions of images.

www.manaraa.com



(a) (b) (c) (d)

Figure 3.38: Prostate regions enhanced by the presented algorithm. Top row: The regions cropped from the original prostate MR images; Bottom row: The corresponding enhanced regions.



(a) (b) (c)

Figure 3.39: Comparison of prostate MR image enhancement. (a) The original prostate MR image; (b) The image enhanced by the presented algorithm; (d) The image enhanced by the rational unsharp masking.

3.5.2.3 Performance Comparison

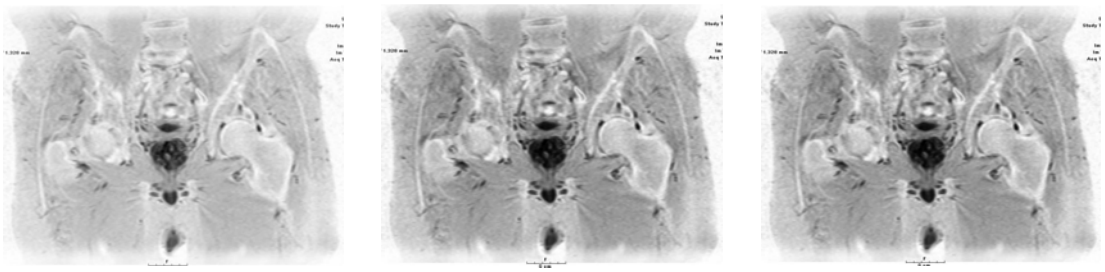
When the algorithm's enhancement of several prostate MR images is compared to the results of the rational unsharp masking method [21], the algorithm demonstrates superior enhancement performance. It not only enhances the contrast of prostate cancer regions

www.manaraa.com

but also improves the visual quality of the image in general. An example is given in Figure 3.39.

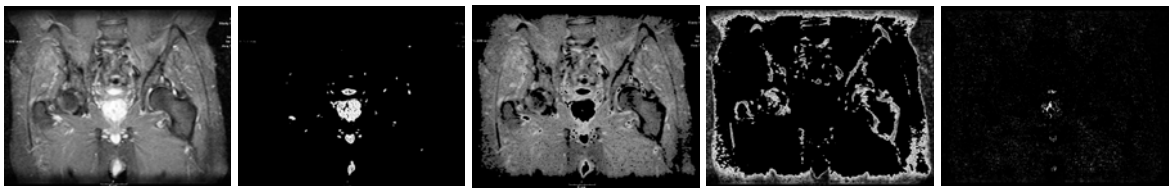
3.5.2.4 Visualization

Figure 3.40 gives an example of the negative representation of the prostate MR images. This provides an alternative method for radiologists to diagnose and determine prostate cancer.



(a) (b) (c)

Figure 3.40: Negative representation of prostate MR image enhancement. (a) The negative photo of the original prostate MR image; (b) The negative photo of the image enhanced by the presented algorithm, alpha=0; (c) The negative photo of the image enhanced by the presented algorithm, alpha=0.49.



(a) (b) (c) (d) (e)

Figure 3.41: HVS-based decomposition of the enhanced prostate MR image. (a) The prostate MR image enhanced by the presented algorithm, alpha=0; (b) The first sub-image; (c) The second sub-image; (d) The third sub-image; (e) The fourth sub-image.

Human visual system (HVS)-based image decomposition has been employed for edge detection [133] and image enhancement [93]. Since the HVS-based image decomposition

www.manaraa.com

separates images based on background intensity and the rate of information change, its application is extended to image visualization. Figure 3.41 shows the HVS-based decomposition results for a prostate MR image. The observation shows that some specific regions in the prostate MR image are contained within a decomposed sub-image.

www.manaraa.com

3.6 Logarithmic Enhancement for Prostate MR Images Using Nonlinear Filtering

Medical images such as MRIs, ultrasound images and CT images are generally very dark. Logarithmic enhancement is able to enhance dark regions where pixels with very low intensity values are located. Nonlinear filtering can enhance fine details while suppressing noise. In order to benefit from the advantages of these two methods, a presented enhancement algorithm is introduced using a combination of the nonlinear filtering and logarithmic enhancement to enhance prostate MR images for prostate cancer detection.

3.6.1 Transform Based Logarithmic Enhancement

This section reviews the existing transform based logarithmic enhancement method, which will be used as a comparison for the image enhancement performance.

Figure 3.42 shows a block diagram of the transform based logarithmic enhancement algorithm.

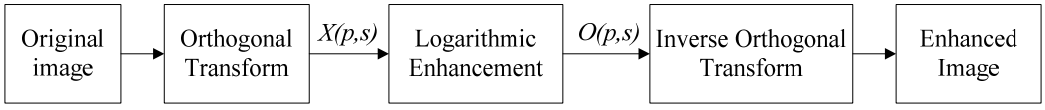


Figure 3.42: The transform based logarithmic enhancement algorithm.

The algorithm first converts the image into a frequency domain using an orthogonal transform such as Fast Fourier Transform (FFT), modifies then magnitude of the

www.manaraa.com

transform coefficients using logarithmic enhancement in equation (47), and then performs the inverse transform to obtain an enhanced image [141]. This section selects Fast Fourier Transform (FFT).

$$O(p,s) = \log^{\beta}\left(\left|X(p,s)\right|^{\lambda} + 1\right) \bullet X(p,s) \tag{47}$$

where $O(p,s)$ and $X(p,s)$ are the FFT results of the output image and input image, respectively, β and λ are operating parameters.

3.6.2 The New Enhancement Algorithm

This section introduces the new algorithm for enhancing prostate MR images, integrating the logarithmic enhancement and the nonlinear filtering technique.

3.6.2.1 The New Enhancement Algorithm

MR images of prostate cancer are generally dark images. Logarithmic enhancement has the ability to improve the visual quality of dark regions or objects in images. Nonlinear filtering is known for its ability to suppress noise and preserve edges and details. Taking advantages of both capabilities, a new algorithm combining those two approaches is introduced to enhance prostate MR images. The presented enhancement algorithm is called the Logarithmic Nonlinear Filtering (LogNLF) and is shown in Figure 3.43.

In the original MR images, background noise composed of pixels with very low intensity values can be detected in the regions around the objects. Image enhancement is generally a nonlinear process that enhances images while making noise more visually recognizable.

www.manaraa.com

Therefore, a denoising process must be carried out before the LogNLF algorithm can perform enhancement. This process is able to remove noise from the original MR image, *I(m,n)*, by discarding pixels with values lower than a small threshold. The output image of the denoising process is the object image with background noise reduced, *X(m,n)*.

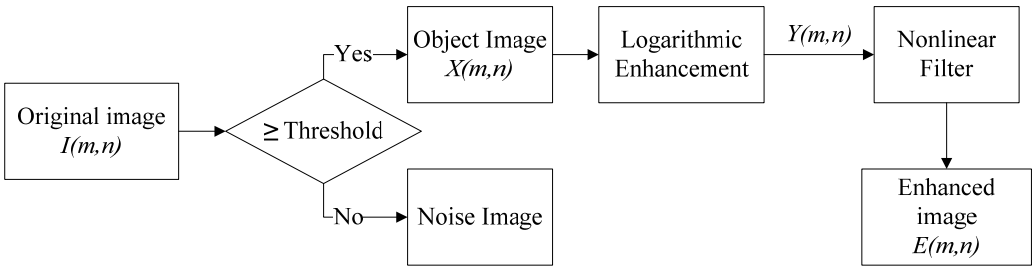


Figure 3.43: The block diagram of the LogNLF algorithm.

Then, the LogNLF applies a logarithmic operation to enhance the object image, *X(m,n)*, using the following equation (48),

$$Y(m,n) = \log^{\beta}(|X(m,n)|^{\lambda} + 1) \tag{48}$$

where β and λ are constants, and $\beta, \lambda > 0$

The output image, *Y(m,n)*, is then filtered by a nonlinear filter defined by equation (49) to obtain the final enhanced image.

$$E(m,m) = w_0 Y_0 + w_1 Y_1 + w_2 Y_2 \tag{49}$$

where

$$Y_0 = Y^{2\alpha_0}(m,n)$$
$$Y_1 = Y^{2\alpha_1}(m-1,n-1) + Y^{2\alpha_1}(m+1,n-1) + Y^{2\alpha_1}(m+1,n-1) + Y^{2\alpha_1}(m+1,n+1)$$
$$Y_2 = Y^{2\alpha_2}(m-1,n) + Y^{2\alpha_2}(m+1,n) + Y^{2\alpha_2}(m,n-1) + Y^{2\alpha_2}(m,n+1)$$

and the coefficients w_0, w_1, w_2, α_0, α_1, α_2 are constants.

www.manaraa.com

According to the definition in equation (49), the nonlinear filter is a special case of the type zero of the alpha weighted quadratic filter [37] with a mask window size of 3×3. Its weight coefficients, w_0, w_1, w_2, can be considered as a 3×3 filter. Its exponential coefficients, α_0, α_1, α_2, consist of another 3×3 filter. They can be written in the matrix format as shown in equation (50).

$$W = \begin{bmatrix} w_1 & w_2 & w_1 \\ w_2 & w_0 & w_2 \\ w_1 & w_2 & w_1 \end{bmatrix} \qquad \alpha = \begin{bmatrix} \alpha_1 & \alpha_2 & \alpha_1 \\ \alpha_2 & \alpha_0 & \alpha_2 \\ \alpha_1 & \alpha_2 & \alpha_1 \end{bmatrix} \tag{50}$$

Interestingly, this nonlinear filter is a nonlinear combination of two filters W and α. This gives the LogNLF more robust characteristics for a variety of applications. For example, the weight coefficient W could be designed as a high-pass filter and exponential coefficient α could be chosen as a center weighted mean filter. In this case, the nonlinear filter is able to suppress noise and keep sharp details unchanged while enhancing the fine details of images.

3.6.2.2 Discussion

Background noise in the MR images is useless for disease diagnosis and significantly affects both the enhancement measure results and the visual quality of the enhanced images. The denoising process is thus very important for MR image enhancement.

The LogNLF has two steps: logarithmic enhancement and nonlinear filtering. The logarithmic enhancement process is intended to enhance the dark regions of the MR images while the nonlinear filtering is used to improve the visual quality of small objects

www.manaraa.com

and fine details (as well as suppressing noise within an object image). This type of noise is different from the background noise. For example, it may be visible to the human eye, such as Gaussian noise or Salt & Pepper noise.

There are eight coefficients in the LogNLF. Two of them, β and λ, affect the performance of the logarithmic enhancement. Six other parameters determine the characteristics of the nonlinear filter. Those eight coefficients have to be specified for practical applications. Therefore, the implementation of the LogNLF is complex. However, the fact that more parameters are involved offers the LogNLF more power and design flexibility when it comes to meeting the specific and complex requirements of real world applications.

In real world applications, users can manually select the coefficients of the logarithmic enhancement process and design the nonlinear filter as a combination of two existing filters. This, however, is a time-consuming process and it can be difficult to achieve the best enhancement results due to a lack of quantitative evaluation.

Alternatively, users can utilize a train system to optimize the LogNLF's coefficients, thereby obtaining better enhancement results. This issue will be discussed in detail in Section 3.6.3.

In summary, there are at least three following features for the LogNLF:

- By removing background noise, the denoising process can improve the accuracy of the enhancement measure results and the visual quality of the enhanced images.

www.manaraa.com

- Making the most of the advantages of the logarithmic enhancement and nonlinear filtering, the LogNLF can enhance fine details and the dark regions/objects while suppressing noise.

- The nonlinear filter can be designed as the nonlinear combination of different types of filters.

- The coefficients offer users more design flexibility to adapt the scheme to the specific and complicated requirements of real world applications.

3.6.3 Methods to Train Coefficients

This section presents the training system that can be used to select the best values for the LogNLF's eight coefficients. This can be accomplished by choosing the local extrema from the plot of the SDME versus the coefficients. These coefficients are then used to obtain the best enhanced images. The enhancement results are verified by the SDME values and visual evaluation.

First, the training system individually trains the best coefficients for the two steps in the LogNLF: the logarithmic enhancement and nonlinear filtering. Based on these results, the system then trains all coefficients by combining the two steps in order to enhance prostate MR images. This study was performed for more than twenty MR images. This section presents the training results for one image.

www.manaraa.com

3.6.3.1 Individual Training

First, the logarithmic enhancement is trained on its own by removing the nonlinear filter from the LogNLF. After the removal of the nonlinear filter, only two coefficients, β and λ, remain in the LogNLF. The LogNLF enhances the original images using different values for the coefficients, β and λ. Figure 3.44 plots the SDME measure results for one MR image with prostate cancer, which can be seen in Figure 3.45(a).

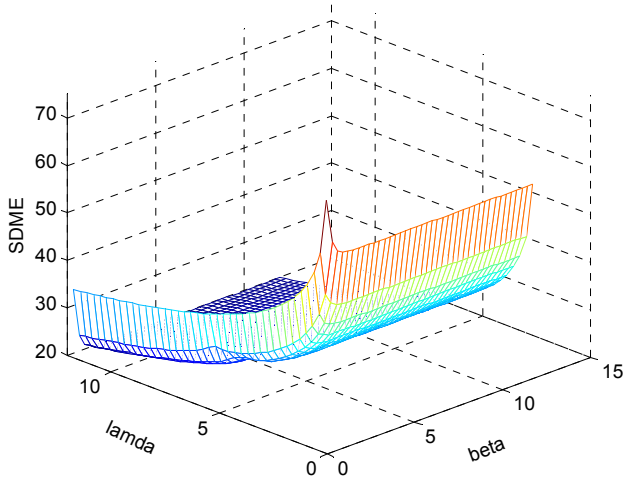
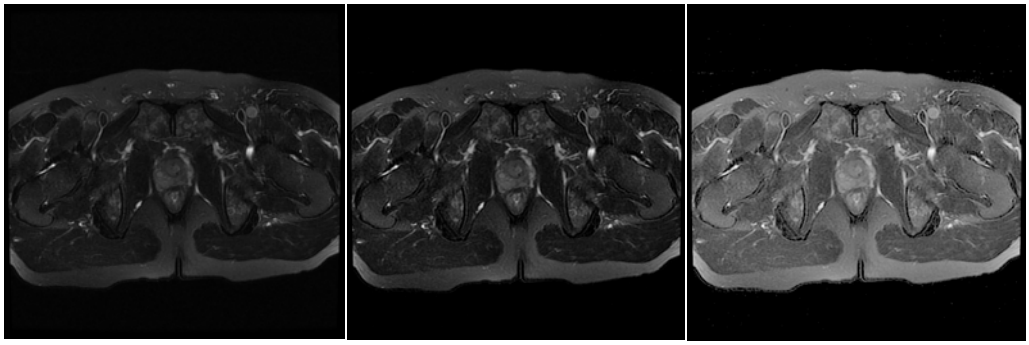


Figure 3.44: SDME measure results of the logarithmic enhancement using different coefficients.



(a) SDME=26.2759 (b) SDME=31.1605 (c) SDME=36.1192

Figure 3.45: MR images enhanced by logarithm enhancement using coefficients selected from the SDME plot in Figure 3.44. (a) Original MR image; (b) Enhanced image, β=4 and λ=3; (c) Enhanced image, β=2 and λ=1. Higher SDME scores indicate better visual quality.

www.manaraa.com

Figure 3.45 shows images enhanced by logarithmic enhancement using coefficients selected from the SDME plot in Figure 3.44. The best enhanced image in Figure 3.45(c) is obtained at β=2 and λ=1. It shows better contrast and visual improvement. The SDME values confirm this enhancement.

In order to train the nonlinear filter for image enhancement, the logarithmic enhancement step is removed from the LogNLF algorithm. In this case, the LogNLF has six coefficients, w_0, w_1, w_2, α_0, α_1, α_2. As mentioned previously, the six coefficients can be designed as two 3×3 filters, W and α. The LogNLF is a nonlinear combination of them. There are two problems associated with this: (1) what types of filters should the W and α be; and (2) how can their coefficients be optimized?

To solve those problems, the W and α are designed using different existing low-pass and high-pass filters. Table 3.6 lists several low-pass and high-pass filters. The LogNLF is then utilized to enhance the different MR images.

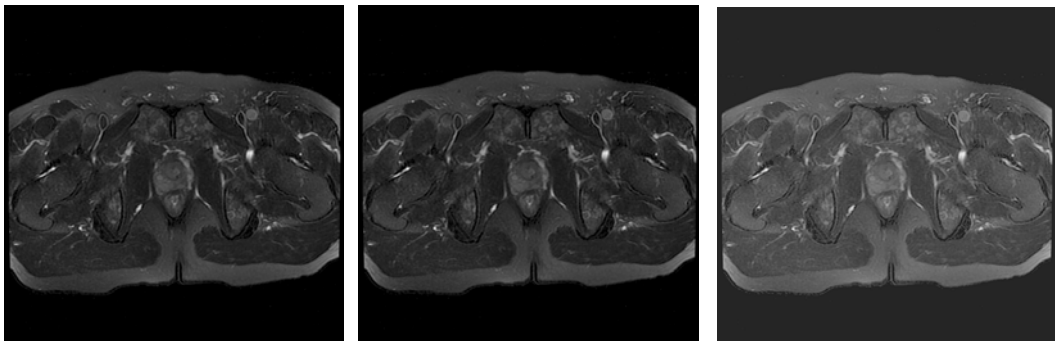
TABLE 3.6 LOW-PASS AND HIGH-PASS FILTERS

$H_1 = \frac{1}{7}\begin{bmatrix} 0 & 1 & 0 \\ 1 & 3 & 1 \\ 0 & 1 & 0 \end{bmatrix}$	$H_2 = \frac{1}{17}\begin{bmatrix} 1 & 2 & 1 \\ 2 & 5 & 2 \\ 1 & 2 & 1 \end{bmatrix}$	$H_3 = \begin{bmatrix} 1 & -2 & 1 \\ -2 & 4 & -2 \\ 1 & -2 & 1 \end{bmatrix}$
Low-pass filter	Low-pass filter	High-pass filter

Figure 3.46 shows several enhanced versions of the MR image that appears in Figure 3.45(a). These results were obtained by using different combinations of the filters that appear in Table 3.6. Figure 3.46(a) and (b) are MR images obtained using two different low-pass filters. Figure 3.46(c) shows the image after it has been enhanced by the

www.manaraa.com

combination of a low-pass filter and a high-pass filter. The resulting images have a better contrast and a higher SDME value than the original MR image in Figure 3.45(a). This verifies that the combination of the low-pass filter and the high-pass filter gives the best enhancement performance. The SDME values also confirm this.



(a) SDME=33.5849 (b) SDME=33.7376 (c) SDME=37.6977

Figure 3.46: MR images enhanced by the different combinations of existing filters. (a) Enhanced image, $W = \alpha = H_1$; (b) Original MR image, $W = H_2, \alpha = H_1$; (c) Enhanced image, $W = H_3, \alpha = H_2$.

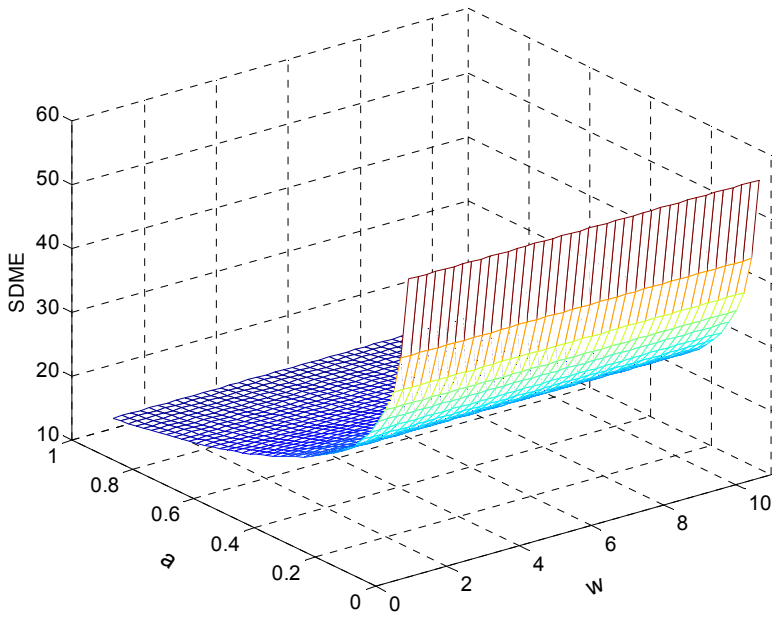
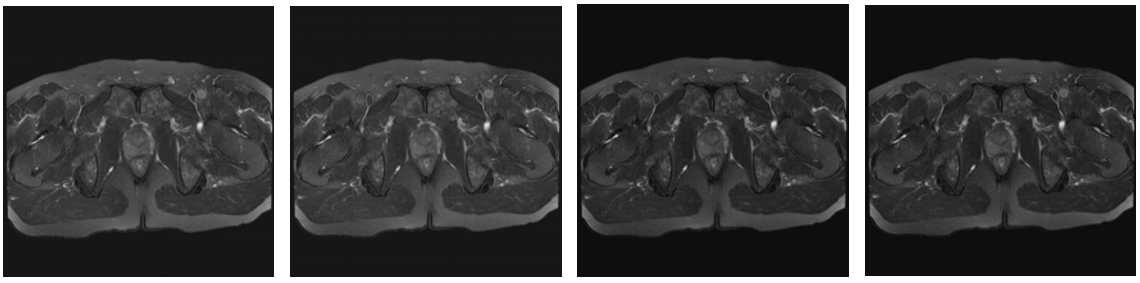


Figure 3.47: SDME measure results of the images enhanced by the nonlinear filter using different coefficients.

www.manaraa.com

Based on the enhancement results in Figure 3.46, the coefficients for the nonlinear filter are optimized by designing W as a high-pass filter and α as a low-pass filter. To reduce the number of coefficients, each filter is represented by one variable based on reasonable assumptions. The SDME is utilized as a quantitative assessment to optimize the coefficients, thereby achieving the best enhancement result. For example, set $\alpha_1 = a$, $\alpha_2 = 2a$, $\alpha_0 = 5a$ and $w_2 = -2w$, $w_0 = 4w$, $w_1 = w$. The MR image in Figure 3.45(a) is used as the test image. The SDME measure results are plotted in Figure 3.47.

Figure 3.48 gives several examples enhanced using the nonlinear filter. The coefficients are selected from the SDME plot in Figure 3.47. The SDME plot and the enhanced images demonstrate that the coefficient change of low-pass filter α can significantly affect the performance of the nonlinear filter when it comes to image enhancement, whereas the coefficient change of the high-pass filter W does not. The SDME values in Figure 3.48 prove this. The results at $a = 0.7$ in Figure 3.48 demonstrate better contrast and a higher SDME score.



(a) SDME=35.9037 (b) SDME=35.9037 (c) SDME=34.6562 (d) SDME=34.6562

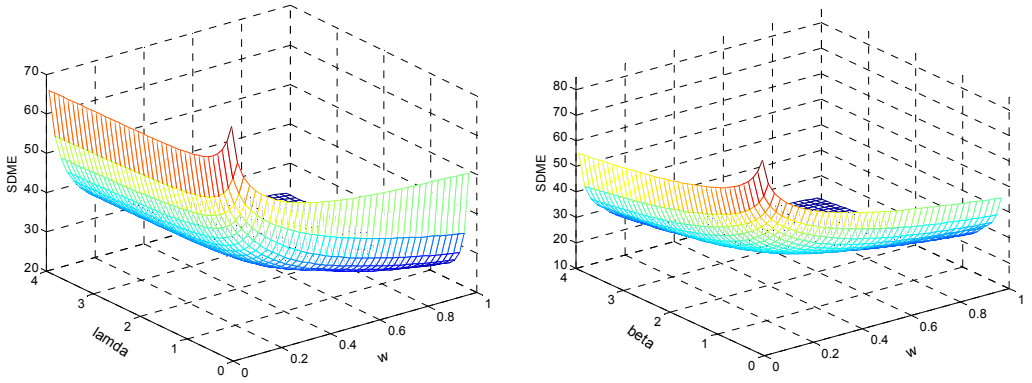
Figure 3.48: MR images enhanced by the nonlinear filter using coefficients selected from the SDME plot in Figure 3.47. (a) Enhanced image, $w = 1, a = 0.07$; (b) Enhanced image, $w = 10, a = 0.07$; (c) Enhanced image, $w = 1, a = 0.15$; (d) Enhanced image, $w = 5, a = 0.15$.

www.manaraa.com

3.6.3.2 Combined Training

The above training results for each step of the LogNLF algorithm have demonstrated the exact nature of the enhancement performance of both logarithmic enhancement and nonlinear filtering. This section combines them and trains the LogNLF algorithm.

Assume $\alpha_1 = w,\ \alpha_2 = 2w,\ \alpha_0 = 5w,\ w_1 = 5w, w_2 = -10w,\ w_0 = 20w$ for the nonlinear filter. In order to individually train β and λ values for logarithmic enhancement, one of them is set to one and the other is varying for training. For example, set β=1 for training λ values (as shown in Figure 3.49(a)), and vice versa (as shown in Figure 3.49(b)). The test image is the MR image in Figure 3.45(a). The training results are plotted in Figure 3.49.



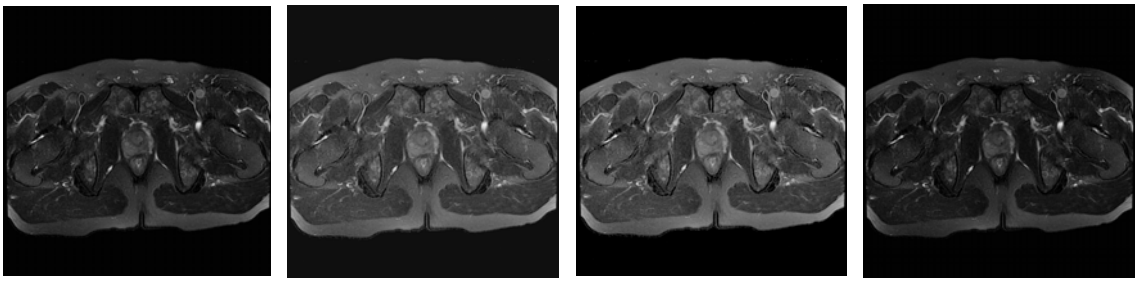
(a) (b)

Figure 3.49: SDME measure results of the images enhanced by the LogNLF using different coefficients. (a) $\beta = 1$; (b) $\lambda = 1$.

Figure 3.50 gives the results after the original MR image in Figure 3.45(a) has been enhanced using different LogNLF's coefficients. The image in Figure 3.50(b) shows the best enhancement performance due to excellence of contrast. Its highest SDME value confirms this. The observation proves that parameter λ does not play a large role in image enhancement. However, the changes of parameter β and of coefficients in the nonlinear

www.manaraa.com

filter will significantly affect the enhancement results. Increasing the values of parameter β and coefficients in the nonlinear filter will make the enhanced images darker and more recognizable.



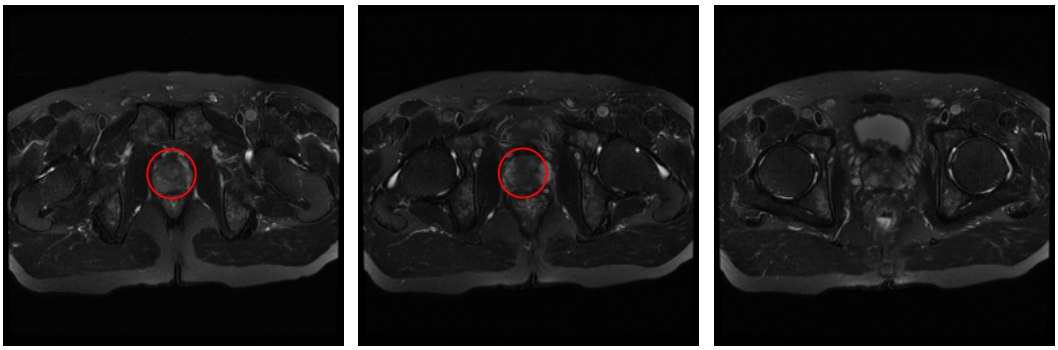
(a) SDME=31.5917 (b) SDME=34.5268 (c) SDME=33.8345 (d) SDME=31.2231

Figure 3.50: MR images enhanced by the LogNLF using coefficients selected from the SDME plot in Figure 3.49. (a) Enhanced image, $\beta = \lambda = 1, w = 0.4$; (b) Enhanced image, $\beta = \lambda = 1, w = 0.25$; (c) Enhanced image, $\beta = 1, \lambda = 9, w = 0.27$; (d) Enhanced image, $\beta = 1.7, \lambda = 1, w = 0.25$.

3.6.4 Enhancement Comparison and Evaluation

To show the enhancement performance of the presented LogNLF, it is compared with two existing enhancement approaches: FFT based logarithmic enhancement (LogFFT) and contrast-limited adaptive histogram equalization (CLAHE). These methods were applied to more than thirty (30) prostate MR images. This section presents the enhanced results of six of them. Figure 3.51 shows the six original prostate MR images. The shadow regions inside the red circles are prostate cancer regions, as indicated by the doctor who provided the original MR images.

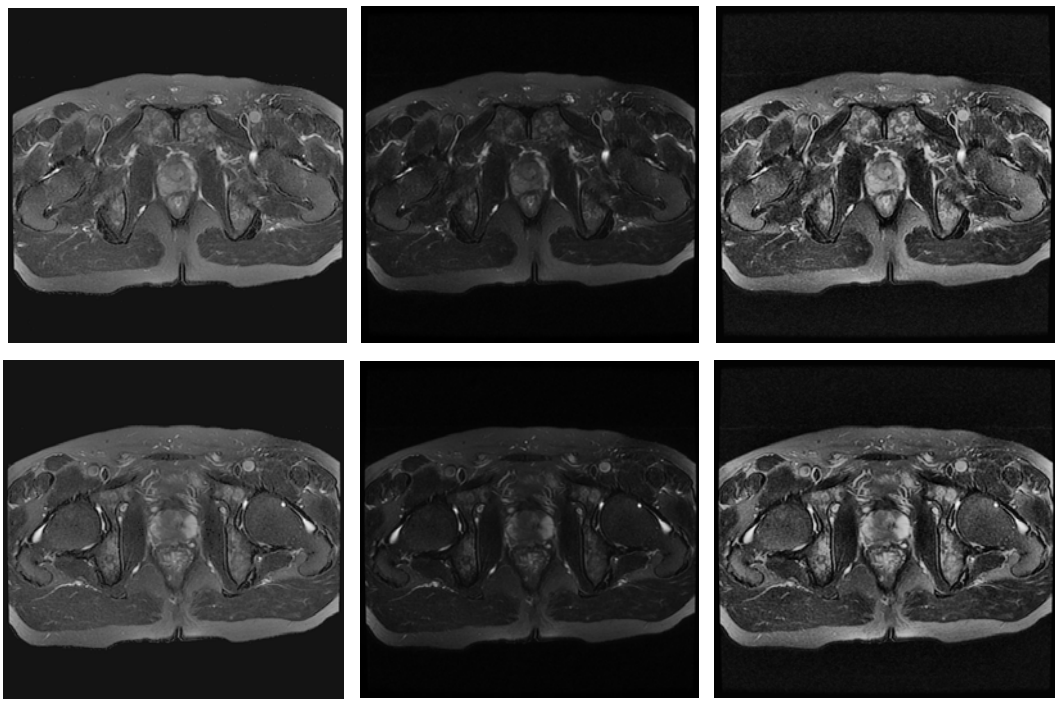
www.manaraa.com



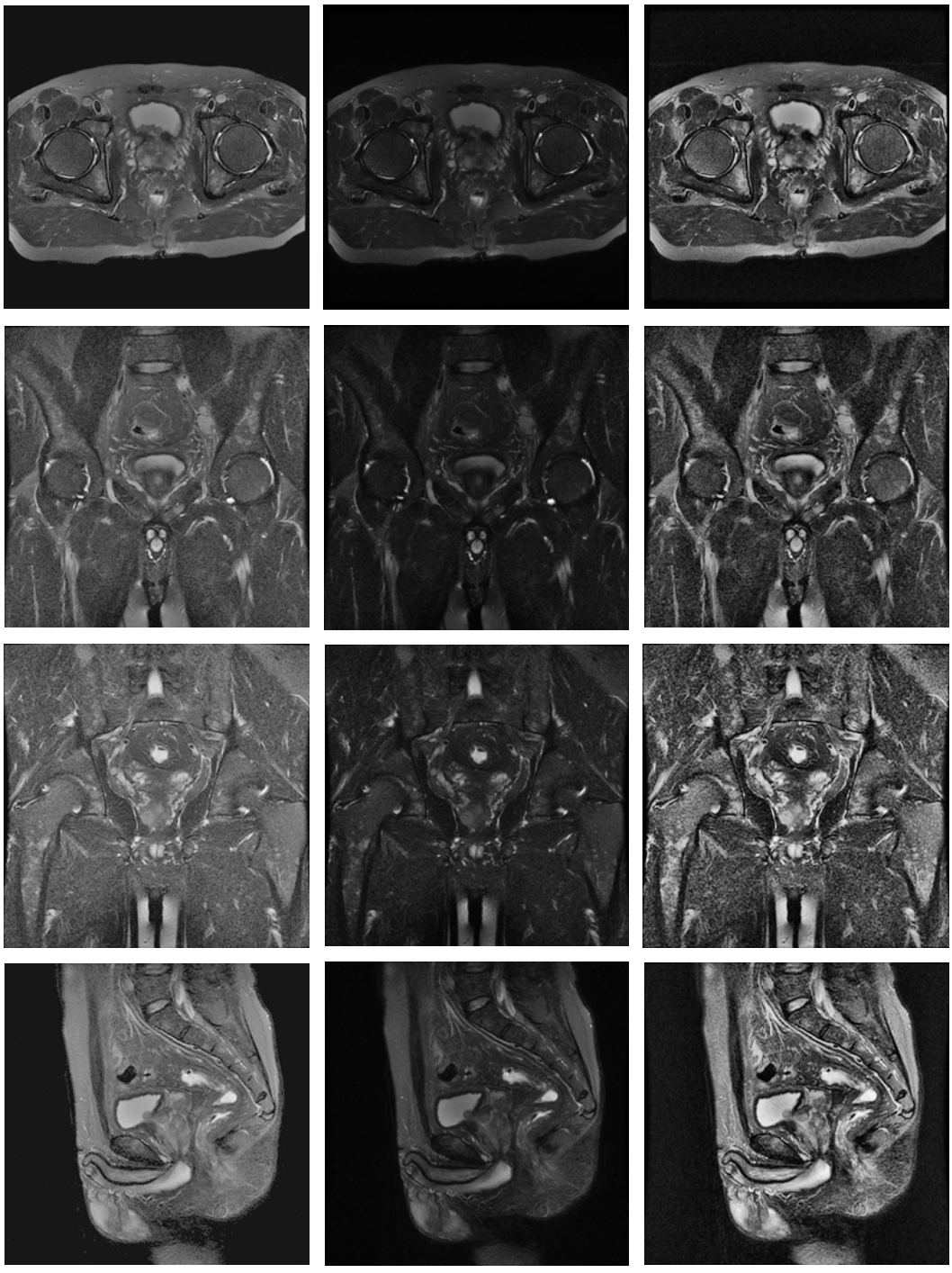
(a) MRI #1 (a) MRI #2 (a) MRI #3

(a) MRI #4 (a) MRI #5 (a) MRI #5

Figure 3.51: Original prostate MR images.



www.manaraa.com



(a) (b) (c)

Figure 3.52: Comparison of MR image enhancement. (a) MR image enhanced by the LogNLF; (b) MR image enhanced by the LogFFT; (c) MR image enhanced by the CLAHE.

www.manaraa.com

The images in each row of Figure 3.52 gives the results after the original images in Figure 3.51 have been enhanced using different algorithms. For example, the images in the second row of Figure 3.52 are the enhanced results of the MRI #2 in Figure 3.51(b).

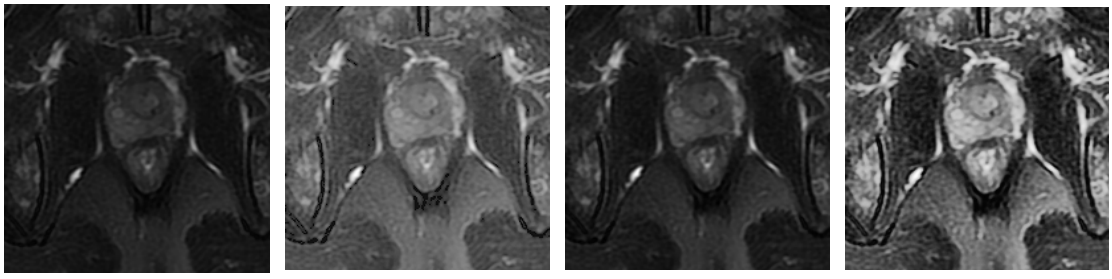
Table 3.7 gives the SDME measure results of the images in Figure 3.51-52. The enhanced images and the results of SDME quantitative evaluation demonstrate that the LogNLF gives better enhancement performance than other two enhancement methods.

The six original prostate MR images found in Figure 3.51 contain prostate cancers that appear as drop shadow regions in the images. Figure 3.53 shows these regions cropped from the original images, alongside their enhanced versions. The results of the presented LogNLF show prostate cancer in the best visual quality. This is consistent with the SDME measure results in Table 3.7.

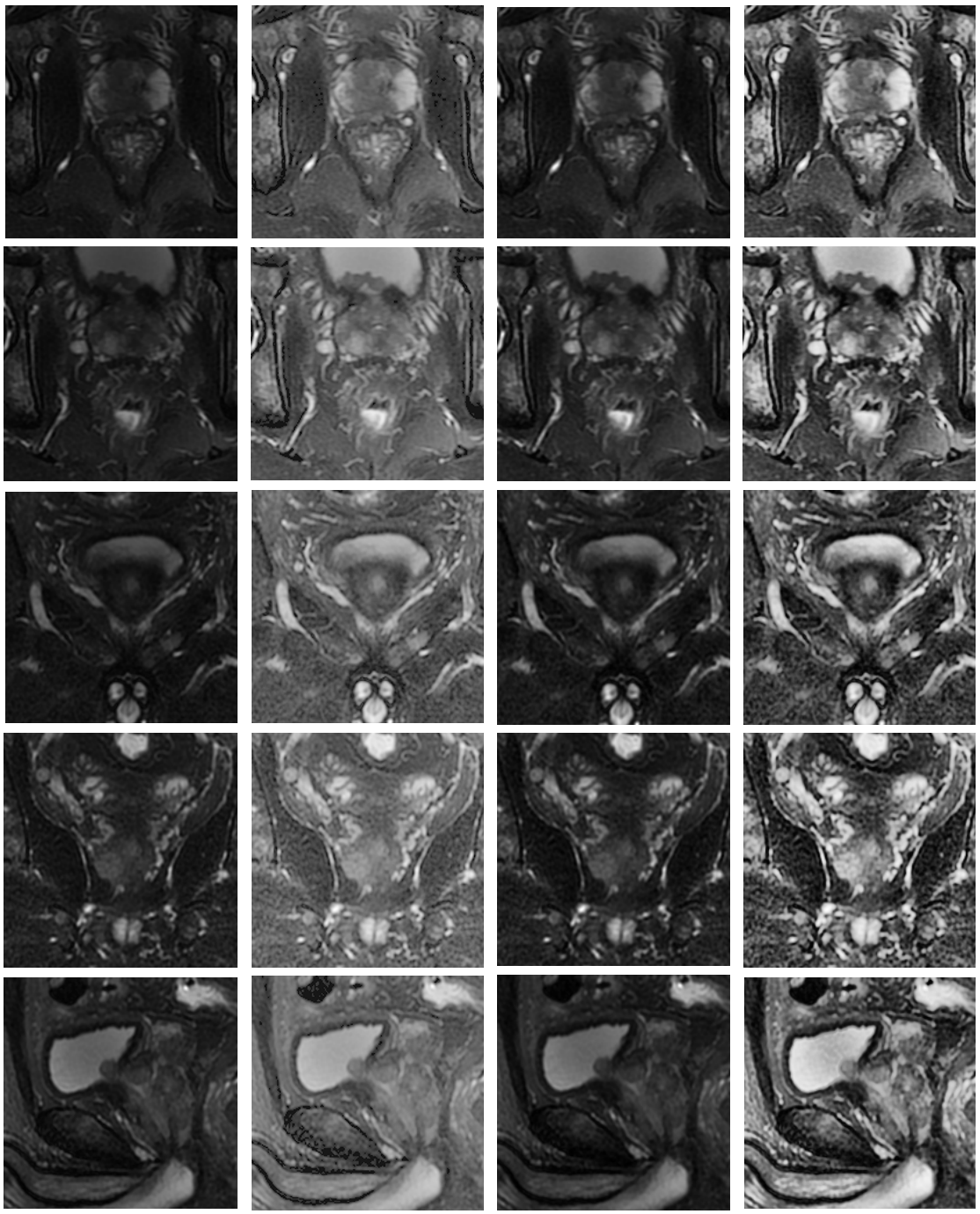
TABLE 3.7 SDME ASSESSMENT OF ENHANCEMENT RESULTS

	Original	LogNLF	LogFFT	CLAHE
MRI #1	26.2759	35.2359	32.8927	26.712
MRI #2	25.8493	35.2157	33.0147	26.9453
MRI #3	25.9825	35.2608	33.1492	27.0172
MRI #4	28.299	34.0891	32.6198	27.0686
MRI #5	28.8411	34.5906	32.2785	26.5684
MRI #6	27.6713	35.6682	33.5823	27.3713

The evaluation results show that LogNLF outperforms other methods numerically.



www.manaraa.com



(a) (b) (c) (d)

Figure 3.53: Comparison of enhancing regions of interest. (a) Region cropped from the original MR image; (b) Region enhanced by the LogNLF; (c) Region enhanced by LogFFT; (d) Region enhanced by the CLAHE.

www.manaraa.com

3.7 Summary and Discussion

This chapter has investigated the applications of the nonlinear filtering technique for enhancing medical images such as mammograms and prostate MR images.

A new type of nonlinear filter called the alpha weighted quadratic filter (AWQF) has been introduced. It was shown that this filter effectively enhances the overall contrast of mammograms and also improves local fine details.

The AWQF can be designed as the nonlinear combination of different types of filters. This offers users greater design flexibility to accomplish the more specific and complicated requirements of real world applications. Its coefficients can be optimized by means of the measure approaches in order to obtain a better enhanced mammogram.

A new HVS-based algorithm has also been introduced for mammogram enhancement. The nonlinear filter has been selected as an example of the presented algorithm's enhancement methods. The SDME measure results and comparisons demonstrated that the HVS-based algorithm shows better overall enhancement performance for improving the contrast of specific regions, objects and fine details in mammograms, without generating artifacts or over-enhancing high illuminated regions.

The HVS-based image decomposition has been demonstrated to have the capability to be used for mammogram visualization and analysis. It can separate the abnormal regions such as cancer cells from the original mammogram and represent them in a single sub-

www.manaraa.com

image without using any thresholding or segmentation algorithm. This feature is useful for automatically detecting and diagnosing breast cancer in the CAD systems.

To solve the problem that traditional unsharp masking is sensitive to noise, a new nonlinear unsharp masking scheme (NLUM) has been introduced. The presented scheme was shown to provide users with more design flexibility to meet the specific and complex requirements of real world applications. Computer simulations have demonstrated that the NLUM scheme possesses superior performance for mammogram enhancement, especially when it comes to improving the local contrast of specific regions and fine details of mammograms.

To improve the visual quality of prostate MR images for the sake of cancer detection, a new enhancement algorithm has been introduced using the alpha-trimmed mean separation and nonlinear filtering. Simulation results and comparisons demonstrated that the algorithm significantly improves the visual quality of prostate MR images.

By combining the logarithmic enhancement technique with nonlinear filtering, another new algorithm has been introduced for enhancing prostate MR images, called the LogNLF algorithm. The LogNLF combines the advantages of both methods and has the ability to enhance dark regions and fine details while suppressing noise.

A train system was introduced to design the LogNLF and optimize its coefficients. Firstly, the system trained the two enhancement steps individually, and then designed the LogNLF by combining the two steps together. The training results show that the best enhancement results for a specific image can be obtained.

www.manaraa.com

The enhancement results and comparisons demonstrated that the presented LogNLF has superior overall enhancement performance for prostate MR images.

Different types of cancers, when viewed in medical images, display different characteristics. For example, breast cancer appears as bright regions of mammograms, while prostate cancer appears as shadow regions of prostate MR images. Therefore, different enhancement algorithms are needed to improve the visual quality of medical images, depending on the particular applications, such as algorithms concentrating on the bright regions of mammograms and the shadow regions of prostate MR images, as presented in this dissertation. All enhancement algorithms introduced here contain several characteristic parameters/coefficients. This provides users with the design flexibility to not only specify the enhancement algorithms for different medical images, but also meet the specific requirements of real world applications.

www.manaraa.com

Part III

Multimedia Encryption for Security and Medical Applications

www.manaraa.com

Thus far, this dissertation has focused on image enhancement for security and medical applications. As described in Part I, a parallel goal of the presented multimedia security system is to provide protection for information, as shown in Figure III-1. Part III of this dissertation presents robust algorithms for ensuring the protection and privacy of multimedia information.

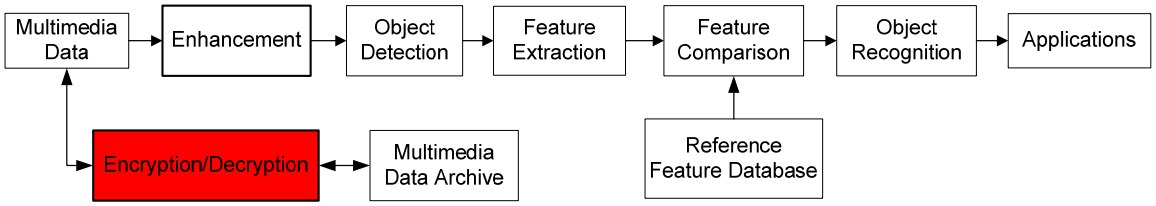


Figure III-1: Block diagram of the presented multimedia security system

Providing security for multimedia data is extremely important for individuals, businesses and governments. Multimedia encryption is an effective method to protect multimedia data by transferring it into an unrecognizable format so that unauthorized users will have difficulty decoding the encrypted multimedia data. However, traditional encryption methods either require high computational costs or have a low level of security due to a lack of security keys or a small key space.

To enhance efficiency while providing a higher level of security, Chapter 4 introduces five new recursive sequences and their corresponding transforms [63-68, 74]. These sequences include the truncated P-Fibonacci sequence [74], P-Lucas sequence [63], P-recursive sequence [65], *(n, k, p)*-Gray code [64], and Parametric M-sequence [66]. A universal 2D P-recursive transform adaptive to all these recursive sequences is then introduced to efficiently scramble/encrypt the 2D and 3D multimedia data. Based on this,

www.manaraa.com

two new multimedia encryption algorithms are introduced to scramble or encrypt the 2D multimedia data by means of a simple one-step using the new 2D P-recursive transform.

The permutation based encryption algorithms are known to be vulnerable to plaintext attacks [69, 70]. To achieve higher security levels, an effective solution is to change image pixel values while scrambling image pixels or blocks using different techniques. Image bit-plane decomposition is an interesting method for changing image pixel data. However, several existing bit-plane decomposition based encryption schemes have security weaknesses due to the fact that their decomposed results are predictable.

To address this problem, Chapter 5 introduces two parameter-dependent bit-plane decomposition methods, namely, the truncated Fibonacci p-code bit-plane decomposition (truncated to reduce the redundancy of the Fibonacci p-code bit-plane decomposition) [74], and the *(n, k, p)*-Gray code bit-plane decomposition, which extends the concept of the image bit-plane decomposition from base 2 (binary bit string) into an arbitrary base [75, 76]. By integrating these parameter-dependent decomposition methods with the P-recursive transforms developed in Chapter 4, three new image encryption algorithms are then introduced [74, 76, 77].

In addition, Chapter 5 applies the Discrete Parametric Cosine Transform for image encryption according to the concept of using one set of security keys to encrypt the original data and a different set of security keys to reconstruct the data to obtain the final encrypted data [78].

www.manaraa.com

The edge map, a binary image containing all edge information, is traditionally used for image processing such as image enhancement, denoising, compression, segmentation and recognition, but it is never used for image encryption. Chapter 6 presents inventive work using the edge map for image encryption. The edge map is first combined with the newly introduced 3D Cat Map for image encryption [79]. The edge map is then found to have the capability to be used as a binary security key image to encrypt the bit-planes of an image. It is then integrated with the chaotic logistic map to encrypt medical images for privacy protection [80]. This concept is further extended to a binary "key-image", which is either a bit-plane or an edge map obtained from any another image. Using this binary key-image, a new image encryption algorithm is developed [81].

This part consists of Chapter 4, Chapter 5 and Chapter 6. It is organized as follows.

Chapter 4 introduces:

- Five new recursive sequences and their corresponding transforms [63-68, 74]
  - The truncated P-Fibonacci sequence and its transform [74]
  - The P-Lucas sequence and its transform [63]
  - The P-recursive sequence and its transform [65]
  - The *(n, k, p)*-Gray code and its transform [64]
  - The Parametric M-sequence and its transform [66]
- The 2D P-recursive transform [63-68, 74]

www.manaraa.com

- Two P-recursive transform based multimedia encryption algorithms [63-68, 74]

Chapter 5 introduces:

- Two bit-plane decomposition methods:
  - The truncated Fibonacci p-code bit-plane decomposition [74]
  - The *(n, k, p)*-Gray code bit-plane decomposition [75, 76]
- Image encryption using P-Fibonacci transform and decomposition [77]
- Selective object encryption using truncated Fibonacci p-code bit-plane decomposition [74]
- Image encryption using *(n, k, p)*-Gray code transform and decomposition [76]
- Image encryption using the Discrete Parametric Cosine Transform [78]

Chapter 6 introduces:

- Image encryption using edge map and 3D Cat map [79]
- Medical image encryption using edge map and chaotic logistic map [80]
- Image encryption using binary key-images [81]

www.manaraa.com

Chapter 4

Recursive Sequences and Transforms for Multimedia Encryption

This chapter introduces five new recursive sequences and their corresponding transforms to encrypt 1D multimedia data. These sequences include the P-Lucas sequence, P-recursive sequence, *(n, k, p)*-Gray code, Parametric M-sequence and truncated P-Fibonacci sequence. Due to the fact that these sequences can be specified to different subsequences using different combinations of their parameters, they show more comprehensive properties. A universal 2D P-recursive transform adaptive to all recursive sequences is then introduced to encrypt the 2D multimedia data efficiently. Following this, two multimedia encryption algorithms are introduced using the simple one-step process of applying the new 2D P-recursive transform. Simulation results and comparisons show the excellent encryption performance of the presented algorithms.

www.manaraa.com

4.1 Introduction

With the explosive growth in wired and wireless digital communication and ubiquitous internet multimedia services, enormous and diverse technologies are available to individuals all over the world to create, distribute, and access images and videos. In this climate, providing security for images and videos that contain proprietary or private information becomes an important issue for individuals, businesses and governments. Multimedia encryption is an effective way to protect multimedia data by transferring it into an unrecognizable format so that unauthorized users will have difficulty decoding the encrypted multimedia data. Examples of the many applications that require robust security methods include the need to preserve the privacy of medical images in clinical applications, to enforce copyright protection for design graphs, images and videos for commercial purposes, and to provide security for personal identification via fingerprinting or iris matching and for video monitoring in homeland security applications.

Images or videos can be fully or partially encrypted using different technologies in the spatial domain or the frequency domain.

Images or videos are frequently compressed into JPEG or JPEG2000 formats to meet the requirements of network distribution in real time applications. Image/video encryption in the frequency domain is often embedded in the compression process, which is based mainly on the Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT). Selective encryption is a common encryption method to encrypt only important parts or

www.manaraa.com

regions of interest (ROI) in image/videos in the frequency domain [142-146]. As a result, users have the flexibility to choose a tradeoff among security levels, computation complexity and the leakage of image/video content [147, 148].

The DCT based image/video encryption algorithms attempt to scramble or encrypt the DCT coefficients or blocks [41, 42, 149, 150], the quantization table [43, 44], Huffman table [45, 46], or after Huffman coding stage [151]. On the other hand, the image encryption algorithms based on the DWT shuffle or encrypt DWT coefficients [47, 53], or wavelet embedded zerotree [48], or quadtree [49]. However, image encryption algorithms in the frequency domain can neither control compression pixelwise errors [152] nor preserve the high quality of images.

Image/video encryption in the spatial domain can protect images or videos with a desired level of security while providing a high level of quality. Encryption algorithms in the spatial domain are based on scrambling image/video pixels or blocks using different technologies. One straightforward method is the naïve encryption algorithm [153]. This scheme considers the image or video as a data sequence or stream. It scrambles or encrypts part of or the entirety of a sequence or data stream using different techniques. Data Encryption Standard (DES) [50] and Advanced Encryption Standard (AES) [51, 52] are two examples of this method. Nevertheless, this method requires significant computational resources [53] and has the worst error resilience performance [148].

Security is important not only for the encrypted objectives but also for the encryption algorithms themselves. The larger the key space the algorithm has, the more difficulty an

www.manaraa.com

unauthorized user will face when attempting to decode the encrypted images. As a result, a higher level of security for encrypted images will be achieved.

Many encryption schemes are based on chaos theory since the chaotic maps or systems can generate random noise-like sequences iteratively for given initial conditions and parameters [54-58]. However, their resulting sequences are real numbers that need transforming into integer or binary sequences according to additional conditions or thresholds for data encryption purposes, thereby requiring extra computation costs.

Recently, recursive sequences have been applied to image encryption due to the fact that they directly generate integer sequences for specific parameters or keys. These recursive sequences include the Fibonacci numbers [59, 154], Gray code [60, 61] and cellular automata [62, 155]. However, due to the lack of security keys or the small key space associated with these approaches, they provide a low level of security.

This chapter introduces five new recursive sequences: the P-Lucas sequence [63], P-recursive sequence [65], *(n, k, p)*-Gray code [64], Parametric M-sequence [66] and the truncated P-Fibonacci sequence [74]. Their corresponding transforms are also presented here [67, 68]. These sequences and their corresponding transforms can be used to encrypt 1D multimedia data such as data string, text, passwords and speech/audio streams. Although they are also able to scramble 2D or 3D multimedia data line by line – such as images, biometrics and videos – their computational cost will be extremely high. A universal 2D P-recursive transform adaptive to all recursive sequences is introduced to efficiently scramble the 2D and 3D multimedia data in a simple one-step. Two P-

www.manaraa.com

recursive transform based multimedia encryption algorithms are introduced to overcome the limitations of the existing encryption methods in the issue of efficiency and security.

The rest of this chapter is organized as follows. Section 4.2 presents five new recursive sequences and their transforms. Section 4.3 introduces two new recursive sequence based multimedia encryption algorithms. Section 4.4 provides computer simulation results and analysis. Section 4.5 offers an analysis and comparison of the security issues. Section 4.6 reaches a conclusion.

www.manaraa.com

4.2 Recursive Sequences and Transforms

This section introduces five new recursive sequences and their corresponding transforms [67, 68]. The sequences are the truncated P-Fibonacci sequence [74], P-Lucas sequence [63], P-recursive sequence [65], *(n, k, p)*-Gray code [64], and the Parametric M-sequence [66]. These sequences bear more comprehensive properties because they can be specified to different subsequences by changing the combinations of their parameters. These sequences can directly encrypt 1D multimedia data such as data string, text, passwords and speech/audio streams. They can also encrypt 2D or 3D multimedia data such as images and videos line by line. To efficiently encrypt 2D and 3D multimedia data, a universal 2D transform called the 2D P-recursive transform is introduced. It can encrypt the 2D multimedia data by a simple one-step process.

4.2.1 Truncated P-Fibonacci Sequence

This section reviews the Fibonacci number and P-Fibonacci sequence. A truncated P-Fibonacci sequence is then introduced. This sequence can be used for image decomposition and encryption.

4.2.1.1 Fibonacci Number

The classical Fibonacci numbers are a recursive integer sequence of numbers named after Leonardo of Pisa and known as Fibonacci. The Fibonacci number is defined as [156]:

www.manaraa.com

$$F(i)=\begin{cases}0 & i=0\\ 1 & i=1\\ F(i-1)+F(i-2) & i>1\end{cases} \tag{51}$$

From the definition above, each number in the sequence is the sum of the two consecutive previous numbers after the two initial values. The sequence can be listed in the following way: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181...

4.2.1.2 P-Fibonacci Sequence

The P-Fibonacci sequence is a sequence defined by [157, 158],

$$F_p(i)=\begin{cases}0 & i<1\\ 1 & i=1\\ F(i-1)+F(i-p-1) & i>1\end{cases} \tag{52}$$

where i is a position index of the sequence and a non-negative integer p is a distance parameter.

Based on the definition in equation (52), the P-Fibonacci sequence changes as the value of p changes.

- Power of two series: p=0, the sequence is geometric progression increasing by two, 1, 2, 4, 8, 16…;
- Traditional Fibonacci number: p=1, the sequence is 1, 1, 2, 3, 5, 8, 13, 21…;
- For the large values of p, the sequence starts with p consecutive 1's and immediately after that 1, 2, 3, 4…p…

www.manaraa.com

Several examples of P-Fibonacci sequences are shown in Table 4.1.

TABLE 4.1 P-FIBONACCI SEQUENCES WITH DIFFERENT P VALUES

P \ n	1	2	3	4	5	6	7	8	9	10	11	…
0	1	2	4	8	16	32	64	128	256	512	1024	…
1	1	1	2	3	5	8	13	21	34	55	89	…
2	1	1	1	2	3	4	6	9	13	19	28	…
3	1	1	1	1	2	3	4	5	7	10	14	…
4	1	1	1	1	1	2	3	4	5	6	8	…
…	…											
∞	1	1	1	1	1	1	1	1	1	1	1	…

The P-Fibonacci has following properties [157, 158]:

$$\sum_{i=0}^{n-1} F_p(i) = F_p(n+p) - 1 \tag{53}$$

$$\sum_{i=n-p}^{n-1} F_p(i) = F_p(n+p), \qquad n \geq p \tag{54}$$

$$F_p(n) = \binom{p}{0} + \binom{n-p}{1} + \binom{n-2p}{2} + \ldots + \binom{m+r}{m} \tag{55}$$

4.2.1.3 Truncated P-Fibonacci Sequence

The truncated P-Fibonacci sequence (TPFS) is defined as [74],

$$T_p(i) = \begin{cases} 0 & i < 0 \\ 1 & i = 0 \\ F_p(i+p) & i > 0 \end{cases} \tag{56}$$

where $F_p(i+p)$ is the P-Fibonacci sequence defined in equation (52).

www.manaraa.com

TABLE 4.2 TRUNCATED P-FIBONACCI SEQUENCES WITH DIFFERENT P VALUES

P \ n	0	1	2	3	4	5	6	7	8	…
0	1	2	4	8	16	32	64	128	256	…
1	1	2	3	5	8	13	21	34	55	…
2	1	2	3	4	6	9	13	19	28	…
3	1	2	3	4	5	7	10	14	19	…
4	1	2	3	4	5	6	8	11	15	…
…	…									
∞	1	2	3	4	5	6	7	8	9	…

The truncated P-Fibonacci sequence also changes with different p values. For example,

- $p=0$, the truncated P-Fibonacci sequence is geometric progression increasing by two, 1, 2, 4, 8, 16…;
- $p=1$, the truncated P-Fibonacci sequence is the truncated classical Fibonacci sequence 1, 2, 3, 5, 8, 13, 21…;
- $p=\infty$, the truncated P-Fibonacci sequence is an integer sequence, 1, 2, 3, 4, 5, 6 …

Some TPFS examples are given in Table 4.2.

4.2.2 P-Lucas Sequence

Similarly, the P-Lucas sequence is introduced after reviewing the classical Lucas number in this section. It can be used for image decomposition and encryption.

4.2.2.1 Lucas Number

The Lucas numbers are a recursive integer sequence named after the mathematician François Édouard Anatole Lucas. The Lucas number is defined as [156],

www.manaraa.com

$$L(i)=\begin{cases}2 & i=0\\ 1 & i=1\\ L(i-1)+L(i-2) & i>1\end{cases} \tag{57}$$

In a manner similar to the Fibonacci number, each Lucas number is the sum of the two immediate previous numbers in the sequence. The sequence is listed as follows: 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, 9349, 15127, 24476 …

4.2.2.2 P-Lucas Sequence

The P-Lucas sequence is defined as [63],

$$L_p(i)=\begin{cases}0 & i<1\\ 2 & i=1\\ 1 & i=2\\ L(i-1)+L(i-p-1) & i>2\end{cases} \tag{58}$$

where p is a nonnegative integer.

TABLE 4.3 P-LUCAS SEQUENCE WITH DIFFERENT P VALUES

P \ n	1	2	3	4	5	6	7	8	9	10	11	…
0	2	2	4	8	16	32	64	128	256	512	1024	…
1	2	1	2	3	5	8	13	21	34	55	89	…
2	2	1	1	2	3	4	6	9	13	19	28	…
3	2	1	1	1	2	3	4	5	7	10	14	…
4	2	1	1	1	1	2	3	4	5	6	8	…
…	…											
∞	2	1	1	1	1	1	1	1	1	1	1	…

The P-Lucas sequence will be different according to the p value.

www.manaraa.com

- Power of two series: p=0, the sequence is geometric progression increasing by two, 2, 1, 2, 4, 8, 16…;
- Classical Lucas number: p=1, the sequence is 2, 1, 2, 3, 5, 8, 13, 21…;
- For the large values of p the sequence starts with 2 and consecutive 1's.

The detail results are shown in Table 4.3.

4.2.3 P-recursive Sequence and Transform

Here, another new recursive sequence called P-recursive sequence and its corresponding transform are also introduced for 1D multimedia encryption.

4.2.3.1 P-recursive sequence

The P-recursive sequence is defined as [65],

$$R(i) = \begin{cases} B(i) & i \le p+1 \\ B(i-1) * B(i-p-1) & i > p+1 \end{cases} \quad (59)$$

where p is a nonnegative integer, and

$$* = \begin{cases} + & \text{B(i) is integer} \\ \oplus & \text{B(i) is binary} \end{cases}$$

From the definition, the P-recursive sequences differ based on changes in the $B(i)$ and p values.

When $B(i)$ is integer, the "*" is the arithmetic addition operation.

www.manaraa.com

$$R(i)=\begin{cases}B(i) & i\le p+1\\ B(i-1)+B(i-p-1) & i>p+1\end{cases} \tag{60}$$

- If $B(0)=0$ and $B(1)=1$ for $0\le i\le p+1$, the P-recursive sequence is the P-Fibonacci sequence.

$$R(i)=\begin{cases}0 & i=0\\ 1 & 0<i\le p+1\\ R(i-1)+R(i-p-1) & i>p+1\end{cases} \tag{61}$$

- If $B(0)=0$, $B(1)=2$ and $B(i)=1$ for $0\le i\le p+1$, the P-recursive sequence is the P-Lucas sequence.

$$R(i)=\begin{cases}0 & i\le 0\\ 2 & i=1\\ 1 & 1<i\le p+1\\ R(i-1)+R(i-p-1) & i>p+1\end{cases} \tag{62}$$

- If $B(0)=0$, $B(1)=3$ and $B(i)=2$ for $0\le i\le p+1$, the P-recursive sequence is another new P-Fibonacci sequence.

$$R(i)=\begin{cases}0 & i\le 0\\ 3 & i=1\\ 2 & 1<i\le p+1\\ R(i-1)+R(i-p-1) & i>p+1\end{cases} \tag{63}$$

When $B(i)$ is binary, the "*" is the mod 2 operation (XOR).

$$R(i)=\begin{cases}B(i) & i\le p+1\\ B(i-1)\oplus B(i-p-1) & i>p+1\end{cases} \tag{64}$$

www.manaraa.com

- If $B(i)$ is a binary sequence, the P-recursive sequence $R(i)$ is the P-Gray code representation of the binary sequence $B(i)$.

Furthermore, many of the classical sequences can be derived from the functions (61), (62), (63) and (64) based on specific p values. For example, the power of two series and the classical Fibonacci number can be derived from the equation (61), P-Fibonacci sequence, when p=1.

4.2.3.2 P-recursive Sequence Transform

Definition 4.1: Let $R(i)$ and $R(i+1)$ be two consecutive elements in the P-Fibonacci, truncated P-Fibonacci, P-Lucas, or P-recursive sequence. The following transformation is called the P-recursive sequence transform [65].

$$\begin{pmatrix} T_1 \\ T_2 \\ \cdots \\ T_N \end{pmatrix} = \left(R(i)+\varepsilon\right)\begin{pmatrix} 1 \\ 2 \\ \cdots \\ N \end{pmatrix} \bmod R(i+1) \tag{65}$$

where $R(i)+\varepsilon < R(i+1)$, $N = R(i+1)-1$, the non-negative integer i is the index location of the P-recursive sequence. The constant ε is a minimal integer offset such that the greatest common divisor of $R(i)+\varepsilon$ and $R(i+1)$ is one.

The two constraints are important for this transform. The first constraint $R(i)+\varepsilon < R(i+1)$ is a limitation for choosing the minimal offset ε. The second constraint $N = R(i+1)-1$ specifies the maximum value of the input sequence. Otherwise, the input sequence has to be resized to meet this condition. For example, if the input

www.manaraa.com

sequence is $(1,2,3,4,5,6,7,8,9,10)$ and the recursive sequence is the P-Fibonacci sequence with $p=2$, the P-Fibonacci sequence is $1,1,1,2,3,4,6,9,13,19...$, then $R(i+1)=13$ and $R(i)=9$. To meet the second constraint in the equation (65), the input sequence should be resized to $(1,2,3,4,5,6,7,8,9,10,11,12)$. The output will be $(9,5,1,10,6,2,11,7,3,12,8,4)$.

For the changing $R(i)$ and p values in the transformation above, the output sequence $(T_1,T_2,T_3,...,T_N)$ should be the permutation of an input sequence $(0,1,...,N)$. For example, if the input sequence is $(1,2,3,4,5,6,7,8,9,10,11,12)$, the output sequence of the P-recursive transform will be $(9,5,1,10,6,2,11,7,3,12,8,4)$ when choosing the P-Fibonacci sequence with $p=2$, or $(12,7,2,14,9,4,16,11,6,1,13,8,3,15,10,5)$ when choosing the P-Lucas sequence with $p=2$, or $(1,3,2,6,7,5,4,12,13,15,14,10,11,9,8)$ when choosing the P-Gray code with $p=0$.

4.2.4 *(n, k, p)*-Gray code and its Transform

In this section, the classical Gray code is reviewed and a new *(n, k, p)*-Gray code is introduced called the Generalized P-Gray code, another new recursive sequence that can be used for multimedia encryption.

4.2.4.1 Gray code

The Gray code named after Frank Gray, is the Binary-reflected Gray code (BRGC). It is a binary code sequence in which two successive values differ in only one digital. The Gray code is widely used in digital communication systems for error correction.

www.manaraa.com

Definition 4.2: If the n-bit binary representations of the non-negative integer B and G are $A=(a_{n-1}\cdots a_1a_0)_2$ and $G=(g_{k-1}\cdots g_1g_0)_2$, A is the Gray code of B if they are satisfied with [159, 160],

$$g_i=\begin{cases} a_{k-1} & i=k-1 \\ a_i\oplus a_{i+1} & 0\le i<k-2 \end{cases} \tag{66}$$

Where $\oplus$ is the exclusive-OR operation.

Table 4.4 gives some examples of the Gray code.

TABLE 4.4 EXAMPLES OF THE GRAY CODE

A	Binary Code	Gray code
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010
4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

4.2.4.2 (n, k)-Gray code

The n-ary Gray code is a non-Boolean Gray code in which the base is greater than two. The *(n, k)*-Gray code is an n-ary Gray code in which *n* is the value of the base and *k* is the code length. It is also called the Generalized Gray code.

www.manaraa.com

Definition 4.3: If $(a_{k-1}\cdots a_1 a_0)_n$ is the *k*-digit base-*n* representation of a non-negative integer A (i.e., $A=\sum_{i=0}^{k-1} a_i n^i$), and a sequence $(g_{k-1}\cdots g_1 g_0)_n$, which is a k-digit base-n representation of G (i.e., $G=\sum_{i=0}^{k-1} g_i n^i$), is satisfied with

$$g_i=\begin{cases} a_i & i>k-2 \\ (a_i+a_{i+1}) \bmod n & 0\le i\le k-2 \end{cases} \tag{67}$$

where $0\le i\le k-1$, $n\ge 2$, G is called the *(n, k)*-Gray code of A.

Notice that when the base n of the *(n, k)*-Gray code is greater than 2, the condition of a single bit change from one code in the sequence to the next is no longer required as it is in the definition of the binary-reflected Gray code. Formally, such a code will not satisfy either the unit distance property or the adjacency property of two adjacent code words that differ by exactly one element [161].

4.2.4.3 (n, k, p)-Gray code

Here, the concept of the *(n, k)*-Gray code is extended with an additional distance parameter *p* and then a new type of Gray code, called the *(n, k, p)*-Gray code, is introduced. This presented Gray code is a new type of non-Boolean Gray code when its base is greater than 2. In the *(n, k, p)*-Gray code scheme presented here, the code changes as the values of the base *n* and the distance parameter *p* vary. By applying its specific transform, another new recursive sequence is introduced for multimedia encryption.

www.manaraa.com

Definition 4.4: If $(a_{k-1}\cdots a_1 a_0)_n$ is the k-digit base-n representation of a non-negative integer A, i.e., $A=\sum_{i=0}^{k-1} a_i n^i$, and a sequence $(g_{k-1}\cdots g_1 g_0)_n$, which is a k-digit base-n representation of G, i.e. $G=\sum_{i=0}^{k-1} g_i n^i$, is satisfied with

$$g_i=\begin{cases} a_i & i>k-p-2 \\ (a_i+a_{i+p+1}) \bmod n & 0\le i\le k-p-2 \end{cases} \tag{68}$$

where $0\le i\le k-1$, $n\ge 2$ and $0\le p\le k-1$, G is called the *(n, k, p)*-Gray code of A.

The definition of the *(n, k, p)*-Gray code in equation (68) can be represented in the matrix format. For example, if $p=0$, it can be written as,

$$\begin{pmatrix} g_0 \\ g_1 \\ g_2 \\ \dots \\ g_{k-2} \\ g_{k-1} \end{pmatrix} = \left(\begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 1 & 1 \\ 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \dots \\ a_{k-2} \\ a_{k-1} \end{pmatrix} \right) \bmod n \tag{69}$$

And if $p=2$, it will be,

$$\begin{pmatrix} g_0 \\ g_1 \\ g_2 \\ \dots \\ g_{k-3} \\ g_{k-2} \\ g_{k-1} \end{pmatrix} = \left(\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \dots \\ a_{k-3} \\ a_{k-2} \\ a_{k-1} \end{pmatrix} \right) \bmod n \tag{70}$$

www.manaraa.com

From equation (68), the *(n, k, p)*-Gray code will be different based on the *n* and *p* values. For example,

- When n=2, the *(n, k, p)*-Gray code is the binary P-Gray code, also called *(2, k, p)*-Gray code.

$$g_i = \begin{cases} a_i & i > k-p-2 \\ (a_i + a_{i+p+1}) \bmod 2 & 0 \le i \le k-p-2 \end{cases} \tag{71}$$

- When n=3, the (n, k, p)-Gray code is the ternary P-Gray code, also called *(3, k, p)*-Gray code.

$$g_i = \begin{cases} a_i & i > k-p-2 \\ (a_i + a_{i+p+1}) \bmod 3 & 0 \le i \le k-p-2 \end{cases} \tag{72}$$

- When p=0, the *(n, k, p)*-Gray code in equation (68) reverts to the classical gray code of base n.

$$g_i = \begin{cases} a_i & i > k-2 \\ (a_i + a_{i+1}) \bmod n & 0 \le i \le k-2 \end{cases} \tag{73}$$

- The *(n, k, p)*-Gray code is the classical Gray code when p=0 and n=2.

$$g_i = \begin{cases} a_i & i > k-2 \\ (a_i + a_{i+1}) \bmod 2 & 0 \le i \le k-2 \end{cases} \tag{74}$$

Table 4.5 gives some examples for the *(n, k, p)*-Gray code of the integer values from 0 to 20 with different n and p. Notice that for $n = 2$ and $p = 0$, the code degrades back to the BRGC. It can also be observed in Table 4.5 that the *(n, k, p)*-Gray code with a base equal to 3 demonstrates that the presented Gray code differs from the BRGC in that it does not

www.manaraa.com

satisfy either the unit distance property or the adjacency property of two adjacent code words that differs by exactly one element, as is the case in the BRGC [161].

TABLE 4.5 EXAMPLES OF *(N, K, P)*-GRAY CODES FOR BINARY AND NON-BINARY BASES FOR INTEGER VALUES 0 TO 20

A	(n, k, p)-Gray code of A			
	$n=2, p=0$	$n=2, p=2$	$n=3, p=0$	$n=3, p=1$
1	00001	00001	001	001
2	00011	00010	002	002
3	00010	00011	011	010
4	00110	00100	012	011
5	00111	00101	010	012
6	00101	00110	022	020
7	00100	00111	020	021
8	01100	01001	021	022
9	01101	01000	110	101
10	01111	01011	111	102
11	01110	01010	112	100
12	01010	01101	121	111
13	01011	01100	122	112
14	01001	01111	120	110
15	01000	01110	102	121
16	11000	10010	100	122
17	11001	10011	101	120
18	11011	10000	220	202
19	11010	10001	221	200
20	11110	10110	222	201

4.2.4.4 (n, k, p)-Gray code transform

Definition 4.5: Two non-negative integer sequences $(A_1, A_2, ..., A_m)$ and $(G_1, G_2, ..., G_m)$ can be represented in the k-digital n-base matrices respectively. Namely [64, 75, 76]

www.manaraa.com

$$(A_1, A_2, ..., A_m) = \begin{pmatrix} a_{11} & a_{21} & ... & a_{m1} \\ a_{12} & a_{22} & ... & a_{m2} \\ ... & ... & ... & ... \\ a_{1k} & a_{2k} & ... & a_{mk} \end{pmatrix} \text{ and } (G_1, G_2, ..., G_m) = \begin{pmatrix} g_{11} & g_{21} & ... & g_{m1} \\ g_{12} & g_{22} & ... & g_{m2} \\ ... & ... & ... & ... \\ g_{1k} & g_{2k} & ... & g_{mk} \end{pmatrix},$$

where $A_i = \sum_{j=1}^{k} a_{ij} n^{j-1}$ $G_i = \sum_{j=1}^{k} g_{ij} n^{j-1}$ and $1 \le i \le m$, the following transformation is called the *(n, k, p)*-Gray code Transform.

$$\begin{pmatrix} g_{11} & g_{21} & ... & g_{m1} \\ g_{12} & g_{22} & ... & g_{m2} \\ ... & ... & ... & ... \\ g_{1k} & g_{2k} & ... & g_{mk} \end{pmatrix} = (C_p \begin{pmatrix} a_{11} & a_{21} & ... & a_{m1} \\ a_{12} & a_{22} & ... & a_{m2} \\ ... & ... & ... & ... \\ a_{1k} & a_{2k} & ... & a_{mk} \end{pmatrix}) \bmod n \qquad (75)$$

where the coefficient matrix

$$C_p = \begin{pmatrix} c_{11} & c_{12} & ... & c_{1k} \\ c_{21} & c_{22} & ... & c_{2k} \\ ... & ... & ... & ... \\ c_{k1} & c_{k2} & ... & c_{kk} \end{pmatrix} \quad \text{where } c_{xy} = \begin{cases} 1 & x = y \\ 1 & y = x + p + 1 \le k \\ 0 & otherwise \end{cases}$$

m, k, i, j, p, x, y are integers and $1 \le x, y \le k$, $0 \le p \le k$.

From the definition above, the *k*-digital *n*-base representation matrices of the input sequence $(A_1, A_2, ..., A_m)$ and the output sequence $(G_1, G_2, ..., G_m)$ change with different base *n* values. The $k \times k$ coefficient matrix C_p changes with different values of base *n* and parameter *p*. For example, if $p = 0$, the *(n, k, p)*-Gray code transform is,

www.manaraa.com

$$\begin{pmatrix} g_{11} & g_{21} & \cdots & g_{m1} \\ g_{12} & g_{22} & \cdots & g_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ g_{1k} & g_{2k} & \cdots & g_{mk} \end{pmatrix} = \left(\begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1k} & a_{2k} & \cdots & a_{mk} \end{pmatrix} \right) \bmod n$$

If $p = 1$, the *(n, k, p)*-Gray code transform will change to,

$$\begin{pmatrix} g_{11} & g_{21} & \cdots & g_{m1} \\ g_{12} & g_{22} & \cdots & g_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ g_{1k} & g_{2k} & \cdots & g_{mk} \end{pmatrix} = \left(\begin{pmatrix} 1 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 1 & 0 & 1 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1k} & a_{2k} & \cdots & a_{mk} \end{pmatrix} \right) \bmod n$$

The output integer sequence $(G_1, G_2, ..., G_m)$ in the *(n, k, p)*-Gray code transform is the permutation of the input sequence $(A_1, A_2, ..., A_m)$. It changes with alterations in the base n and parameter p values. For example, if the input sequence of the *(n, k, p)*-Gray code Transform is $(1,2,3,4,5,6,7,8)$, its output sequence will be $(1,2,4,5,3,8,6,7)$ for $n = 3, p = 0$. The output sequence will be $(1,2,3,5,4,7,6,8)$ when $n = 2$, $p = 1$. In this way, various permutations of the input sequence are obtained. For a given permutated sequence, its inverse transform is defined in Definition 4.6.

Definition 4.6: If a non-negative integer sequence $(G_1, G_2, ..., G_m)$ is the *(n, k, p)*-Gray code representation of a non-negative integer sequence $(A_1, A_2, ..., A_m)$, the following transformation is called the inverse *(n, k, p)*-Gray code transform.

www.manaraa.com

$$\begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \dots & \dots & \dots & \dots \\ a_{1k} & a_{2k} & \dots & a_{mk} \end{pmatrix} = (C_p^{-1} \begin{pmatrix} g_{11} & g_{21} & \dots & g_{m1} \\ g_{12} & g_{22} & \dots & g_{m2} \\ \dots & \dots & \dots & \dots \\ g_{1k} & g_{2k} & \dots & g_{mk} \end{pmatrix}) \bmod n \qquad (76)$$

where the matrices and m, n, p, k are given by definition 4.5, C_p^{-1} is the inverse matrix of C_p.

4.2.5 Parametric M-sequence and its Transform

This section introduces a new sequence called the Parametric M-sequence. Changing the parameter yields a different sequence. Its transform is also introduced for multimedia encryption.

4.2.5.1 M-sequence

Definition 4.7: The classical binary M-sequence $(m_1, m_2, ..., m_k)$ is satisfied as the following operation [162, 163]

$$m_k = \sum_{i=1}^{n} a_i m_{k-i} (\bmod 2) \qquad (77)$$

where n is the number of the shift registers, $m_k = 0,1$, and $a_i = 0,1$ is the coefficient of the i^{th} shift register. The circuit implementing the operation above is called the M-sequence generator.

The output of the M-sequence generator depends on the coefficient and the initial value of the registers. The output M-sequence is a binary sequence with a maximum length

www.manaraa.com

period of $T = 2^n - 1$. Let the output M-sequence be $(m_1, m_2, ..., m_k) = (m_1, m_2, ..., m_T)$, then $m_k = m_{k+T} = m_{k+2T} = ...$

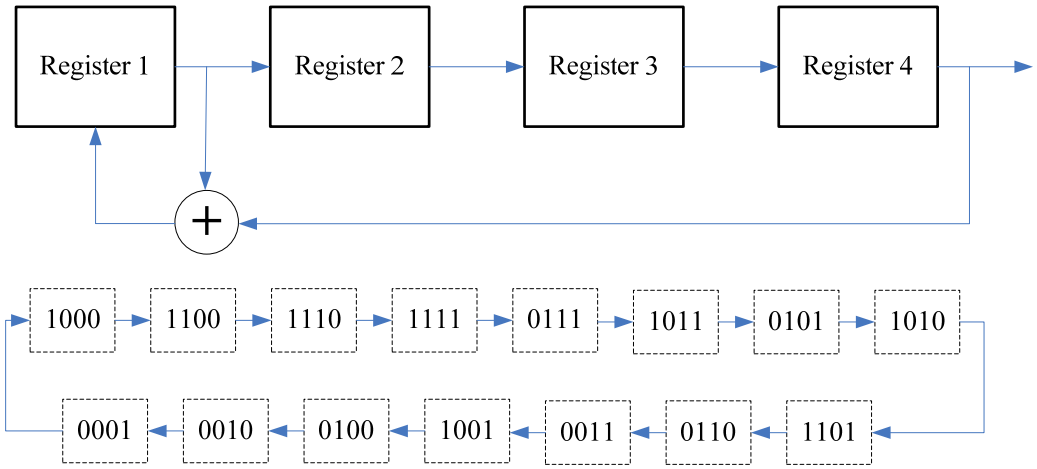


Figure 4.1: The block diagram of a 4-stage M-sequence generator and its state cycles.

For example, an M-sequence generator has 4 registers and the initial values of the shift registers are 1000. A block diagram of the generator is shown in Figure 4.1.

From the Figure 4.1, the output M-sequence is 000111101011001…, and its period is $T = 2^4 - 1 = 15$.

4.2.5.2 Parametric M-sequence

Definition 4.8: Let the binary sequence $(s_1, s_2, ..., s_n)$ be the initial value of the n-stage shift registers in the M-sequence generator, and the output M-sequence be $(b_{r1}, b_{r2}, ..., b_{rT})$ after the registers are shifted *r* times. The binary sequence $(c_{r1}, c_{r2}, ..., c_{rn})$, which is called the parametric M-sequence (PMS), is defined by [66]

$$c_{ri} = b_{r(i+p)} \tag{78}$$

www.manaraa.com

$(c_{r1}, c_{r2}, ..., c_{rn})$ is also called the PMS representation of $(s_1, s_2, ..., s_n)$ where i, r, p, T are integers, and $1 \le i \le n$, $T = 2^n - 1$, $1 \le r \le T$, $0 \le p \le T - n$.

From the example in Figure 4.1, the PMS of 1000 is 0001 if $p = 0$ and $r = 1$, or 0111 if $p = 2$ and $r = 1$.

4.2.5.3 Parametric M-sequence Transform

Based on the definition 4.8, a decimal number with binary representation of $S = (s_1, s_2, ..., s_n)_2$ can be transformed into its PMS representation $C_r = (c_{r1}, c_{r2}, ..., c_{rn})_2$, where C_r is another decimal number. Similarly, a decimal sequence $(1, 2, 3, ..., N)$ can also be transformed to its PMS representation $(C_{r1}, C_{r2}, C_{r3}, ..., C_{rN})$, which is the permutation sequence of $(1, 2, 3, ..., N)$. Furthermore, the permutation sequence $(C_{r1}, C_{r2}, C_{r3}, ..., C_{rN})$ will differ when the shift parameter r and the distance parameter p have different values.

This transformation can be applied to 1D multimedia encryption since it can shuffle the position of the multimedia data. The shift parameter r and the distance parameter p will act as the security keys to generate the different sequences $(C_{r1}, C_{r2}, C_{r3}, ..., C_{rN})$.

For the given value of r and p, the PMS representation of $(1, 2, 3, ..., N)$ can be defined by

$$C_r = (C_{r1}, C_{r2}, C_{r3}, ..., C_{rN}) \tag{79}$$

www.manaraa.com

4.2.6 2D P-recursive Transforms

The above transforms are based on different recursive sequences, including the original or truncated P-Fibonacci sequence, P-Lucas sequence, P-recursive sequence, *(n, k, p)*-Gray code and the parametric M-sequence. They are generally named as the 1D P-recursive transforms and are able to generate a permutation sequence $(R_1, R_2, R_3, ..., R_N)_p$ of the input sequence $(1, 2, 3, ..., N)$. The 1D P-recursive transform can be used to encrypt one dimensional media data such as a string, password, audio or speech signals. Thus, the 1D P-recursive transform can be represented as another general format, namely,

$$(R_1, R_2, ..., R_N) = f_T\left((1, 2, 3, .., N)\right) \tag{80}$$

where $f_T(.)$ is a transform function determined by the specific P-recursive sequence. For example, if the P-recursive sequence is selected to be the P-Lucas sequence, $f_T(.)$ is the P-Lucas transform defined in equation (65).

The 2D multimedia data are 2D data matrices such as signatures, fingerprints, binary images and grayscale images, as well as 3D multimedia data containing several 2D data matrices such as color images and 3D medical images. Although the 1D P-recursive transforms work optimally for 1D data, the same transforms can be used to encrypt 2D multimedia data line by line, even though the computational costs of this are extremely high. To overcome the high overhead of using the 1D P-recursive transforms for 2D cases, an efficient 2D P-recursive transform is introduced to create the permutations for the 2D case.

www.manaraa.com

The 2D P-recursive transform is a general 2D transform for all the recursive sequences presented above. It is a more efficient process than the 1D P-recursive transform because it is able to encrypt 2D multimedia by applying the transform just one time. Furthermore, to reconstruct the original multimedia data, the inverse 2D P-recursive transform is simply used just once. 3D multimedia data encryption is accomplished by encrypting its 2D matrices individually using the 2D P-recursive transform.

Definition 4.9: Let D be an $M \times N$ multimedia data matrix and let T_r and T_c be the row and column coefficient matrices respectively. The 2D P-recursive Transform is defined as [63-68, 76, 77],

$$E = T_r D T_c \tag{81}$$

where E is the encrypted multimedia data, and

$$T_r(m,n) = \begin{cases} 1 & \text{for } (m, R_m) \\ 0 & otherwise \end{cases} \text{ and } T_c(i,j) = \begin{cases} 1 & \text{for } (R_j, j) \\ 0 & otherwise \end{cases}$$

where $1 \le m, n \le M$, $1 \le i, j \le N$, R_m and R_j can be generated from equation (80).

To give an example, Table 4.6 lists row and column coefficient matrices of an 8x10 image according to different parameters when the *(n, k, p)*-Gray code is used in the transform above.

Definition 4.10: Let S be an encrypted $M \times N$ multimedia data matrix, T_r^{-1} and T_c^{-1} be the inverse matrices of the row and column coefficient matrices defined in definition 4.9, while the inverse 2D P-recursive transform is defined as [63-68, 76, 77],

$$R = T_r^{-1} E T_c^{-1} \tag{82}$$

www.manaraa.com

where R is the reconstructed 2D multimedia data matrix.

TABLE 4.6 ROW AND COLUMN COEFFICIENT MATRICES WITH DIFFERENT PARAMETERS FOR AN 8X12 GRAYSCALE IMAGE

(n, p)	Row coefficient matrix	Column coefficient matrix
(3,0)	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$
(2,1)	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

www.manaraa.com

4.3 P-recursive Transform Based Multimedia Encryption Algorithms

To encrypt 2D and 3D multimedia data in the different domains, this section introduces two P-recursive transform-based multimedia encryption algorithms. They are suitable for different recursive sequences. One encrypts the 2D or 3D multimedia data in the spatial domain. The other works in the frequency domain. Both can be also used for video encryption.

4.3.1 Multimedia Encryption Algorithm in the Spatial Domain

2D multimedia data such as electronic signatures, binary images, fingerprints, medical images, and grayscale images are 2D data matrices. The 2D P-recursive transform can encrypt 2D multimedia data based on different recursive sequences.

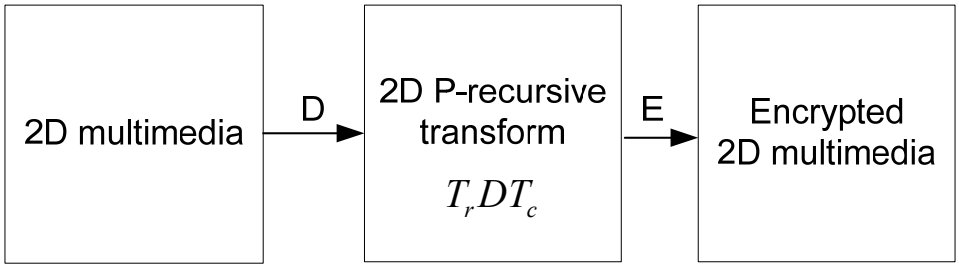


Figure 4.2: The PRTME_SD algorithm.

The P-recursive transform based multimedia encryption algorithm in spatial domain (PRTME_SD) is introduced as shown in Figure 4.2. It requires a simple one-step process to encrypt 2D multimedia data. The row and column coefficient matrices of the 2D P-

www.manaraa.com

recursive transform can be calculated using the definition 4.9 and the selected security keys. The 2D multimedia data can be encrypted in just one step by applying the row and column coefficient matrices simultaneously. This algorithm can also be applied to black video in real-time applications [64, 65].

Recovering the original multimedia data is also a one-step process. The authorized users should be provided the correct security keys. The row and column coefficient matrices can be obtained using security keys based on the definition 4.10, while their inverse matrices can be calculated. By applying the inverse 2D P-recursive transform, the original multimedia data can be reconstructed.

4.3.2 Multimedia Encryption Algorithm in the Frequency Domain

By applying the Discrete Cosine Transform (DCT), the 2D multimedia data can be converted to the frequency domain. The P-recursive transform based multimedia encryption algorithm in the frequency domain (PRTME_FD) is introduced using the 2D P-recursive transform. It is shown in Figure 4.3

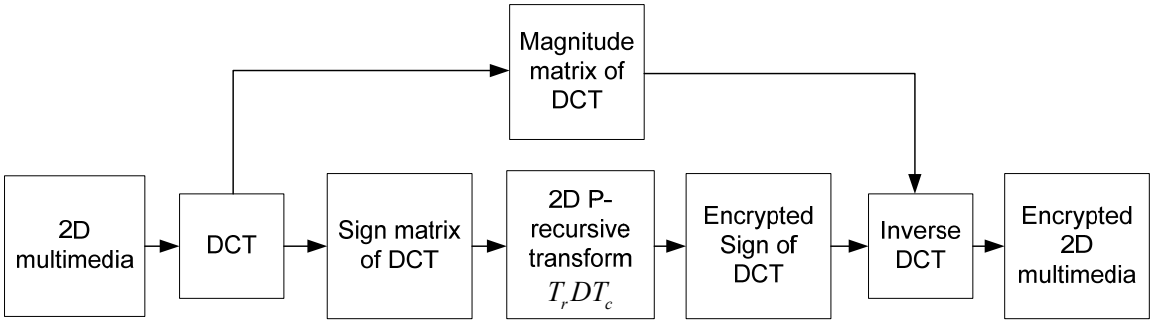


Figure 4.3: The PRTME_FD algorithm.

www.manaraa.com

The PRTME_FD algorithm first transforms the original 2D multimedia data into the frequency domain by means of the 2D DCT. The DCT result is separated into the magnitude and sign matrices. The 2D P-recursive transform is used to encrypt its sign matrix. By applying the inverse 2D DCT to the combination of the encrypted sign of DCT result and their original magnitude matrix, the encrypted 2D multimedia is obtained.

To recover the original multimedia data, the user separates the encrypted multimedia data into magnitude and sign matrix, decodes the sign matrix using the inverse 2D P-recursive transform, and combines the magnitude and decoded sign matrix to yield the recovered DCT matrix. By applying the inverse DCT to the recovered DCT matrix, the reconstructed multimedia data can be obtained.

4.3.3 3D Multimedia Encryption

3D multimedia data has several 2D data matrices called 2D multimedia components in the spatial domain. For example, a color image has three individual color planes. Each color plane is a 2D data matrix.

3D multimedia data can be encrypted using the PRTME_SD or PRTME_FD algorithms to encrypt each component individually in either the spatial domain or the frequency domain. By combining all encrypted 2D components, the encrypted 3D multimedia data can be obtained. Users have the flexibility to choose the same security keys for all 2D components or select different security keys for each of them.

www.manaraa.com

4.4 Simulation Results

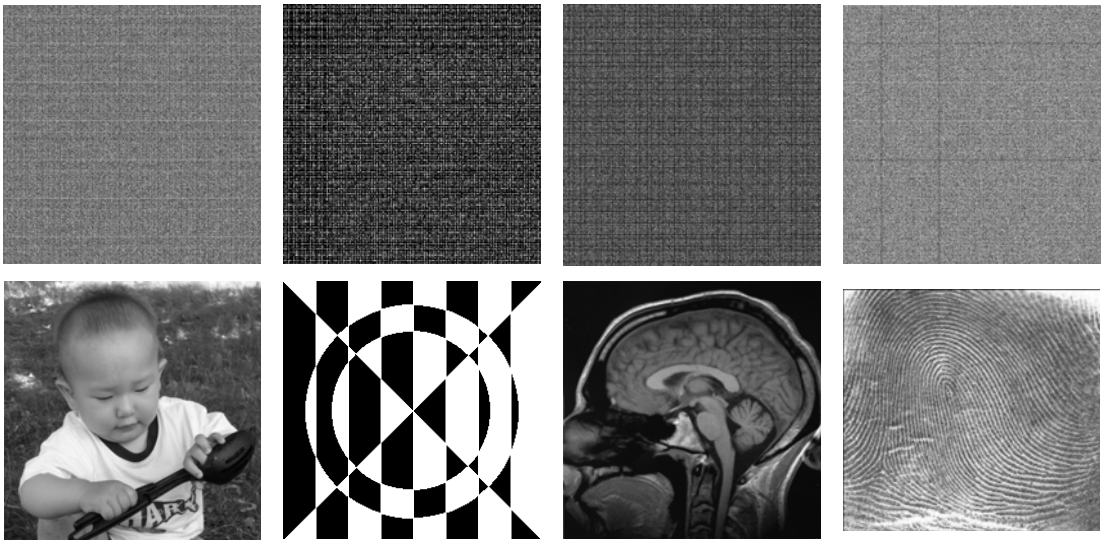
In this section, several simulation results of the 2D and 3D multimedia encryption are given using the PRTME_SD and PRTME_FD algorithms with different recursive sequences in both the spatial domain and the frequency domain.

4.4.1 Multimedia Encryption in the Spatial Domain

Multimedia encryption in the spatial domain is accomplished by applying the 2D P-recursive transform to the 2D multimedia data or 2D components of the 3D multimedia data. Users have the flexibility to choose different recursive sequences for the 2D P-recursive transform.

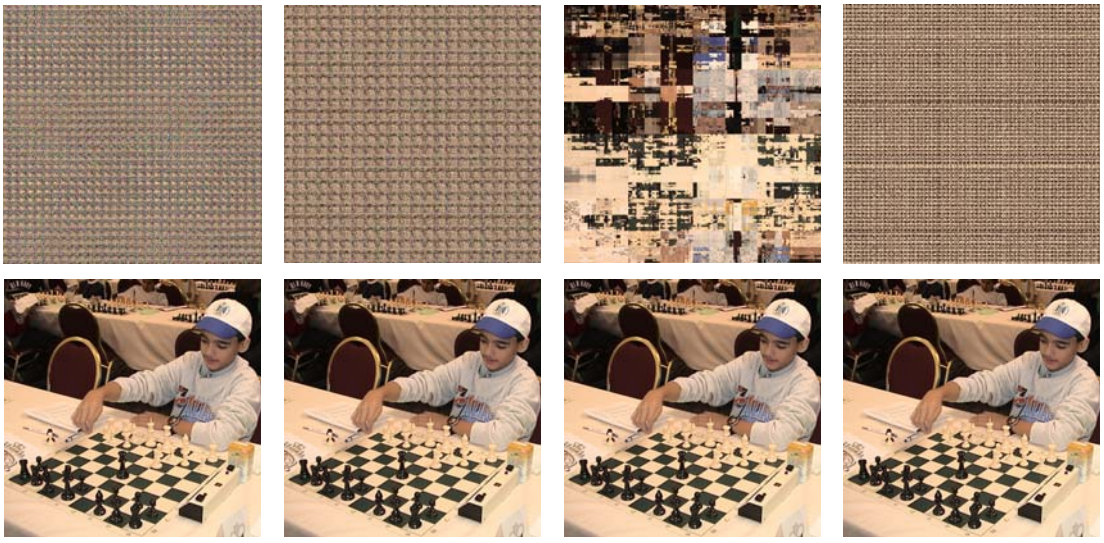
Figures 4.4 and 4.5 present the encrypted and reconstructed results of the PRTME_SD algorithm. Figure 4.4 shows the 2D multimedia encryption results for different types of multimedia data. Figure 4.5 demonstrates the 3D multimedia encryption using different recursive sequences. The results show that the PRTME_SD algorithm has the ability to encrypt different types of multimedia data such as grayscale images, binary images, medical images, fingerprints and color images. The encrypted images look like texture images and are completely different from the original ones, as shown in the top row in Figures 4.4 and 4.5. As shown in the bottom row of these two figures, the original images are perfectly reconstructed. Figure 4.5 (c) shows that the (n, k, p)-Gray code can partially encrypt images.

www.manaraa.com



(a) Grayscale image (b) Binary image (c) Medical image (d) Fingerprint

Figure 4.4: Multimedia encryption using the PRTME_SD algorithm with the P-Fibonacci sequence, p=3. The top row shows the encrypted images. The bottom row shows the reconstructed images. This demonstrates that the PRTME_SD algorithm has the ability to encrypt different types of multimedia data and that the original multimedia data can be completely reconstructed.



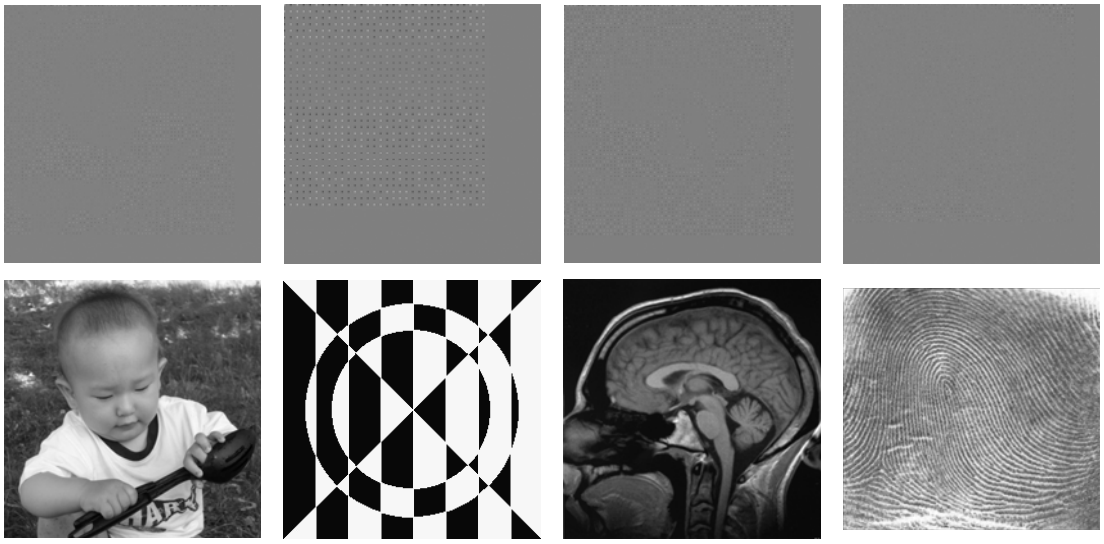
(a) (b) (c) (d)

Figure 4.5: Color image encryption by the PRTME_SD algorithm using different recursive sequences. The top row shows the encrypted images. The bottom row shows the reconstructed images. This demonstrates that the PRTME_SD algorithm can encrypt color images and that the original color image is completely reconstructed. (a) P-Fibonacci sequence, p=2; (b) P-Lucas sequence, p=2; (c) (n, k, p)-Gray code, n=2, p=2; (d) Parametric M-sequence, r=9, p=2.

www.manaraa.com

4.4.2 Multimedia Encryption in the Frequency Domain

Similarly, several simulation results using different recursive sequences in the frequency domain are given to demonstrate the encryption performance of the presented PRTME_FD algorithm.



(a) Grayscale image (b) Binary image (c) Medical image (d) Fingerprint

Figure 4.6: Multimedia encryption using the PRTME_FD algorithm with the P-Fibonacci sequence, p=3. The top row shows the encrypted images. The bottom row shows the reconstructed images. This demonstrates that the PRTME_FD algorithm has the ability to encrypt different types of multimedia data and that the original multimedia data can be completely reconstructed.

Figure 4.6 demonstrates the 2D multimedia encryption for different multimedia data. Figure 4.7 shows the results of 3D multimedia encryption using different recursive sequences. The security keys in these two figures are the same as they are for the results of the 2D multimedia cases in Figures 4.4 and 4.5. The encrypted images in the top row of two figures demonstrate that the PRTME_FD algorithm can fully encrypt the 2D and 3D multimedia data. The original images are also completely reconstructed, as shown in the bottom row of Figures 4.6 and 4.7. Note that the original images should be resized

www.manaraa.com

before encryption in order to meet the size of the Fibonacci sequence transform. As a result, the size of the encrypted image is bigger than that of the original. Examples include the encrypted images in the top row of Figures 4.6 and Figures 4.7(a) and (b).

(a) (b) (c) (d)

Figure 4.7: Color image encryption by the PRTME_FD algorithm using different recursive sequences. The top row shows the encrypted images. The bottom row shows the reconstructed images. This demonstrates that the PRTME_FD algorithm can encrypt color images and that the original color image is completely reconstructed. (a) P-Fibonacci sequence, p=2; (b) P-Lucas sequence, p=2; (c) (n, k, p)-Gray code, n=2, p=0; (d) Parametric M-sequence, r=9, p=2.

www.manaraa.com

4.5 Security Analysis and Comparison

Security is important not only for the encrypted objectives but also for the encryption algorithms themselves. This section gives several analysis approaches to evaluate the characteristics and performance of the PRTME_SD and PRTME_FD algorithms, and discusses specific properties of the encryption algorithms such as security key space, different types of attacks and execution time.

4.5.1 Security Keys and Key Space

The security keys and key space are important specifications for all multimedia encryption algorithms. If there is no security key in the encryption algorithm (i.e. the key space of the encryption algorithm is zero), the encrypted multimedia data is easy to decode. If the algorithm has a larger number of security keys (i.e. if it has a larger key space), it will be more difficult for an unauthorized user to decrypt the encrypted multimedia data even if the individual knows the encryption algorithm.

The experimental results of the PRTME_SD algorithm in Figure 4.8 demonstrate the importance of the security keys in multimedia encryption. The Lena grayscale image was encrypted by the PRTME_SD algorithm using different recursive sequences including the P-Fibonacci sequence, P-Lucas sequence, *(n, k, p)*-Gray code and the parametric M-sequence.

www.manaraa.com

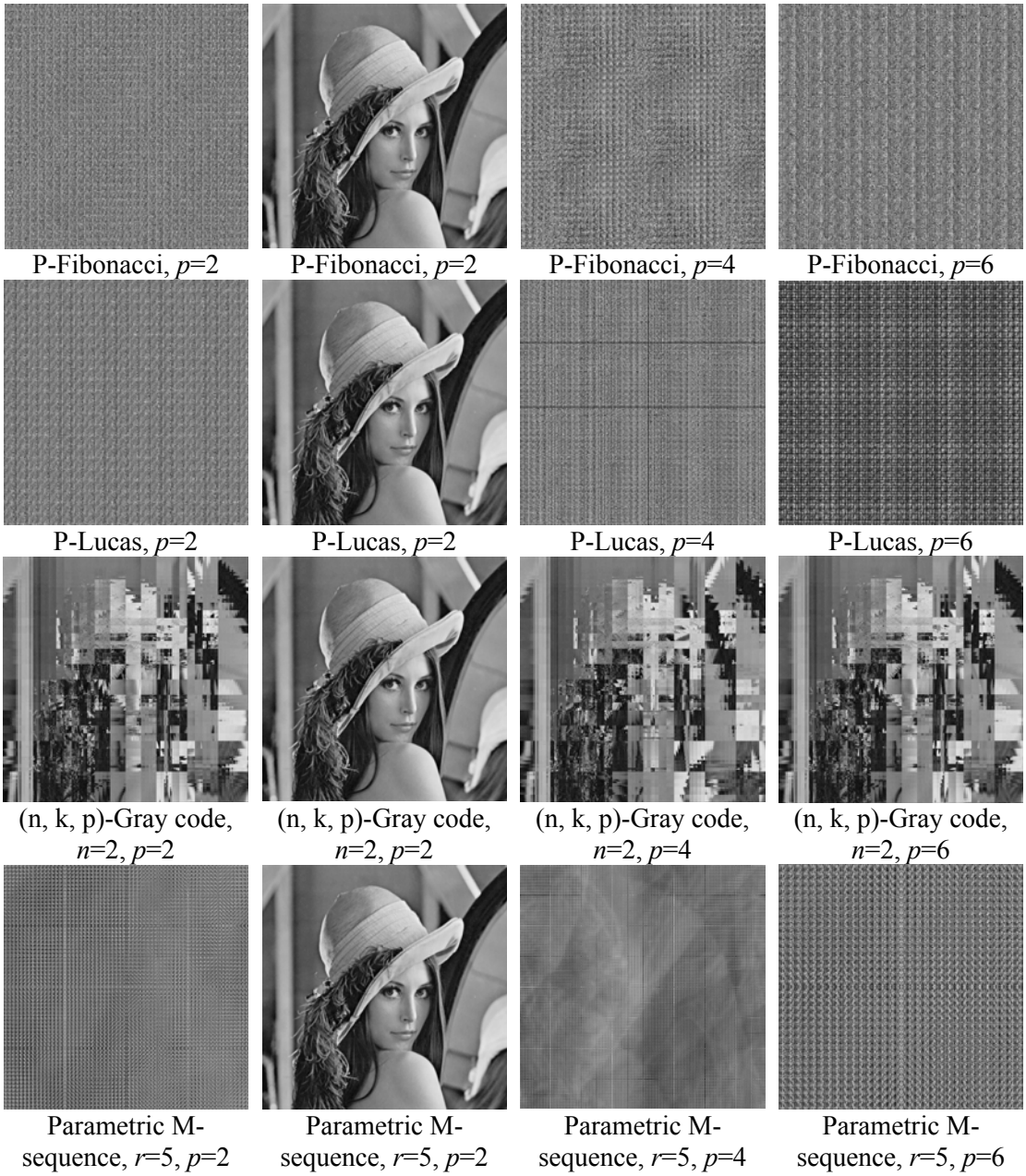


Figure 4.8: Image reconstruction using different parameters. The first column shows the images encrypted by different recursive sequences. The 2nd-4th columns show the images reconstructed using different p values. This demonstrates that the original image can only be reconstructed completely when the correct security keys are utilized.

Here, an attempt is made to use the same sequence, but to employ different security keys to decode the encrypted color images. The encrypted images are decrypted using the

www.manaraa.com

same recursive sequence but with different p values. The original image can be reconstructed perfectly only when the correct security keys are used, as shown in the reconstructed images in the second column in Figure 4.8. However, the original image cannot be recovered with the wrong security keys, even when the same sequence is being utilized. The reconstructed images in the third and fourth columns of Figure 4.8 verify this.

TABLE 4.7 THE SECURITY KEYS OF THE ENCRYPTION ALGORITHMS

Encryption algorithms using	**Security key(s)**	**Possible choices of the security key(s)**
Gray code	none	none
Fibonacci number	none	none
Generalized Fibonacci number	Initial value a and b, the parameter in transform r	Less than 315
Generalized Gray code	The base q	Less than 16
(n, k, p)-Gray code	Base n, the distance parameter p	272
P-Fibonacci sequence	The distance parameter p and the parameter in transform ε	$(256!)^2$
P-Lucas sequence	The distance parameter p and the parameter in transform ε	$(256!)^2$
Parametric M-sequence	Shifting times r, the distance parameter p	62985
P-recursive sequence	$B(n)$, the distance parameter p	$(256!)^2$

The calculation results are based on a 256x256 grayscale image

www.manaraa.com

Furthermore, the more choices of the security keys there are in the multimedia encryption algorithms, the higher the resulting security level of the encrypted multimedia. Here, the PRTME_SD and PRTME_FD algorithms are compared with several existing encryption algorithms using different recursive sequences such as Fibonacci number in [59], Gray code in [60, 164], and Generalized Gray code in [61]. A 256x256 grayscale image was used as an example to calculate the number of possible choices of the security key(s) as shown in Table 4.7. The results show the level of security achieved by each algorithm.

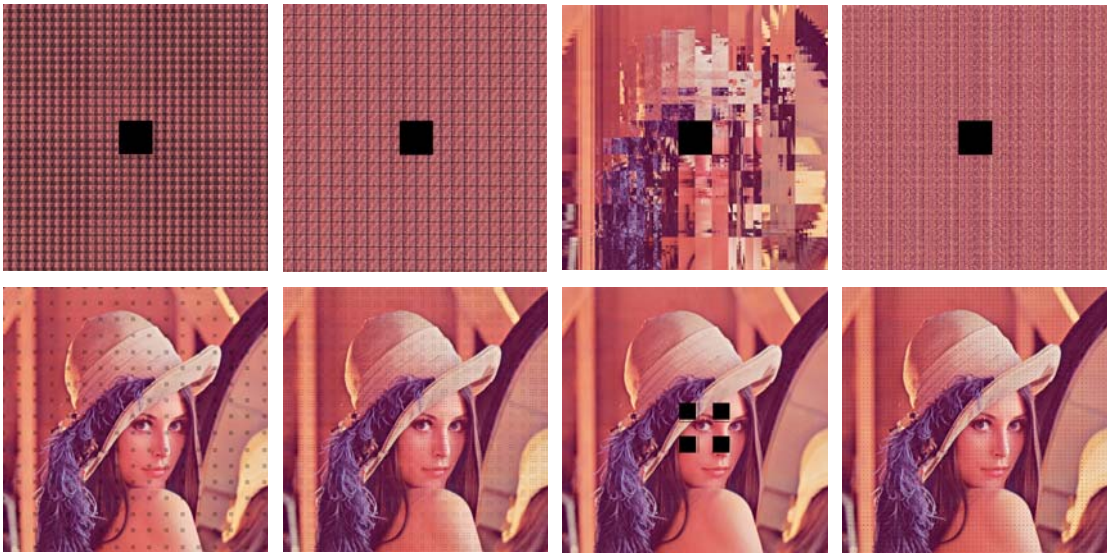
When it comes to the encryption algorithms that use the Fibonacci number in [59] and the Gray code in [60, 164], the above-mentioned security issue is not a concern, since they don't have any security key. The parameter q can act as a security key for the encryption algorithm based on the Generalized Gray code in [61]. However, due to the limited amount of possible security key combinations, the security level of this algorithm is still relatively low.

The security issue has been carefully taken into account in the PRTME_SD and PRTME_FD algorithms based on the P-Fibonacci sequence, P-Lucas sequence, P-recursive sequence and the Parametric M-sequence. Higher security levels of the encrypted multimedia can be achieved because these algorithms have at least two security keys and all the security keys have a sufficient number of possible combinations. In practical applications, users should select these three recursive sequences for encryption if security is a more important issue than others.

www.manaraa.com

4.5.2 Data Loss Attacks

Data loss attacks such as data cutting and filtering are common ways of image attacks. Applying these attacks deliberately helps to verify the ability of the encrypted multimedia data to tolerate possible distortions that may occur in public media transmission channels.



(a) (b) (c) (d)

Figure 4.9: Images reconstructed by the PRTME_SD algorithm using different recursive sequences after a 64x64 center cutting attack. The top row shows the encrypted images after a 64x64 center cutting attack. The bottom row shows the images reconstructed by different recursive sequences. (a) P-Fibonacci sequence; (b) P-Lucas sequence; (c) (n, k, p)-Gray code; (d) Parametric M-sequence. This demonstrates that the PRTME_SD algorithm can withstand data cutting attacks.

Figure 4.9 gives an example of cutting attacks. The PRTME_SD algorithm encrypted a 512x512 Lena image using the P-Fibonacci sequence, P-Lucas sequence, *(n, k, p)*-Gray code and the Parametric M-sequence respectively. A 64x64 center cutting attack was applied to these encrypted images, as shown in the top row of Figure 4.9. The reconstructed images shown in the bottom row of Figure 4.9 are the results obtained from

www.manaraa.com

these encrypted images after a cutting attack. Since they contain most of the original images' visual information, these reconstructed images are visually acceptable, even though some distortions are apparent.

(a) (b) (c) (d)

Figure 4.10: Images reconstructed by the PRTME_SD algorithm using different recursive sequences after a 3x3 Gaussian low pass filter. The top row shows the encrypted images after a 3x3 Gaussian low pass filter has been applied. The bottom row shows the reconstructed images. (a) P-Fibonacci sequence; (b) P-Lucas sequence; (c) (n, k, p)-Gray code; (d) Parametric M-sequence. This demonstrates that the PRTME_SD algorithm can withstand filtering attacks.

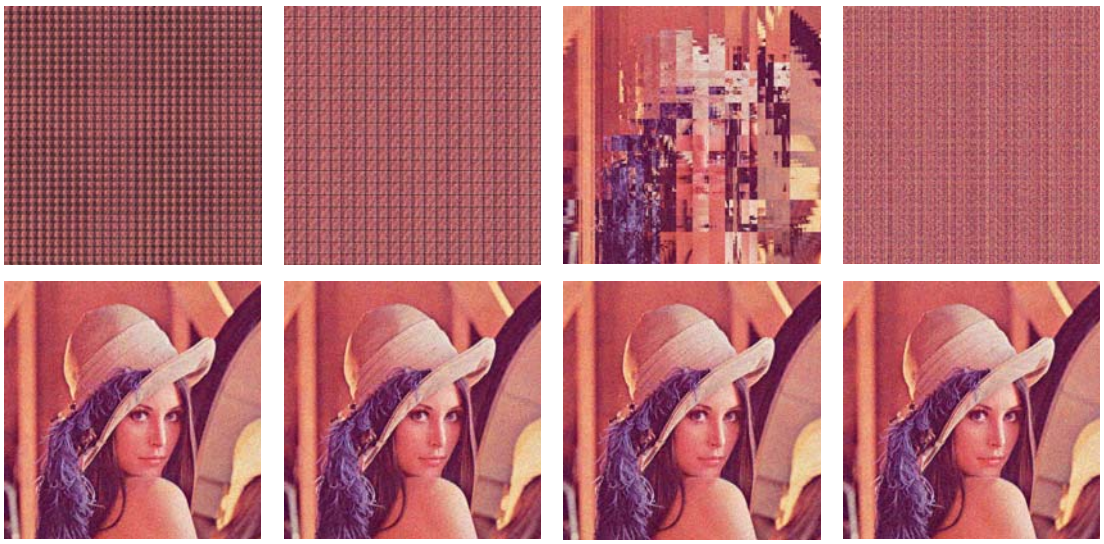
Figure 4.10 gives examples of low pass filter attacks. The Lena image was encrypted by the PRTME_SD algorithm using the same sequences as those in Figure 4.9. These encrypted images, shown in the top row of Figure 4.10, were filtered by a 3x3 digital low pass filter called the Gaussian low pass filter. The images shown in the bottom row of Figure 4.10 were reconstructed from these filtered images. These reconstructed images are obviously recognizable.

www.manaraa.com

The encryption algorithms based on other sequences show similar results as those in Figures 4.9 and 4.10. These experimental results demonstrate that the PRTME_SD algorithm retains its excellent performance in the face of data loss attacks. Therefore, they can withstand the distortions of public multimedia channels.

4.5.3 Noise Attacks

Many different types of noise exist in public multimedia channels such as internet and wireless communication networks. Gaussian noise and Salt and pepper noise are different kinds of image noise. Employing noise attacks demonstrates the ability of the encrypted multimedia to withstand the contamination of different noises. This demonstrates another advantage of the PRTME_SD algorithm.

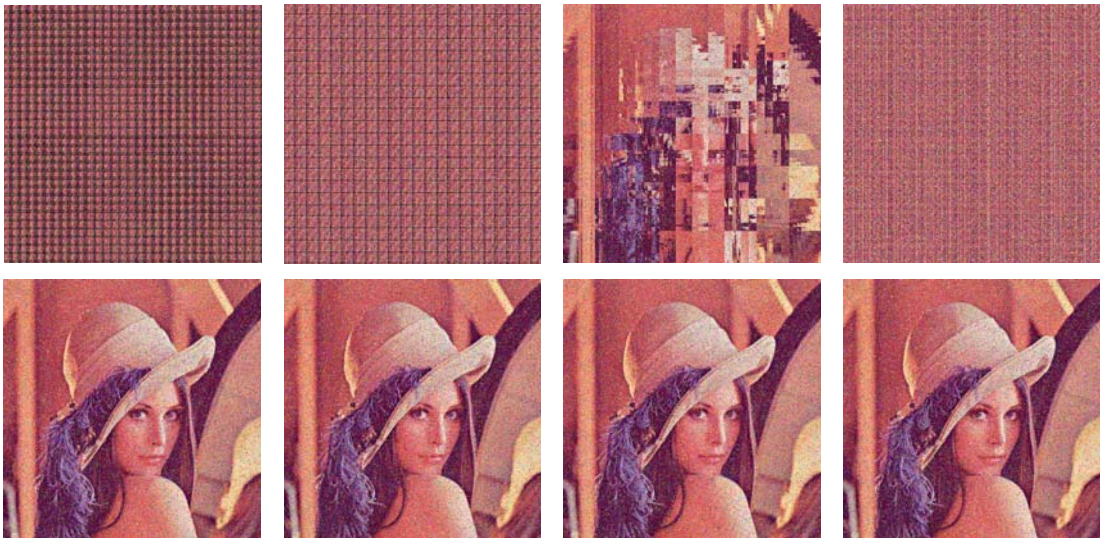


(a) (b) (c) (d)

Figure 4.11: Images reconstructed by the PRTME_SD algorithm using different recursive sequences with 10% Gaussian noise attack. The top row shows the encrypted images with 10% Gaussian noise. The bottom row shows the reconstructed images. (a) P-Fibonacci sequence; (b) P-Lucas sequence; (c) (n, k, p)-Gray code; (d) Parametric M-sequence. This demonstrates that the PRTME_SD algorithm can withstand the Gaussian noise attack.

www.manaraa.com

The experimental results in Figures 4.11 and 4.12 show the performance of the PRTME_SD algorithm after it has been subjected to noise attack. A Lena image was encrypted using the same sequences as those in Figures 4.9 and 4.10. An additional 10% Gaussian noise was added to the encrypted images, as shown in the top row of Figure 4.11. The images shown in the bottom row of Figure 4.11 were recovered from the encrypted images that featured noise. The reconstructed images shown in the bottom row of Figure 4.12 were obtained from the encrypted images with 10% Salt & Pepper noise in the top row of Figure 4.12.



(a) (b) (c) (d)

Figure 4.12: Images reconstructed by the PRTME_SD algorithm using different recursive sequences with 10% Salt Pepper noise attack. The top row shows the encrypted images with 10% Salt Pepper noise. The bottom row shows the reconstructed images. (a) P-Fibonacci sequence; (b) P-Lucas sequence; (c) (n, k, p)-Gray code; (d) Parametric M-sequence. This demonstrates that the PRTME_SD algorithm can withstand the Salt & Pepper noise attack.

Despite being affected by noise, these reconstructed images contain most of the original images' visual information. These experimental results demonstrate that the PRTME_SD

www.manaraa.com

algorithm demonstrates a good performance against noise attacks as well. The original images can be completely reconstructed even though they are subject to a noisy environment.

4.5.4 Execution Time Analysis

The execution time can demonstrate how efficiently the encryption algorithms encrypt multimedia data. This feature is designed to show whether the encryption algorithm can meet the requirements of low computation and high processing speed in real-time applications.

TABLE 4.8 EXECUTION TIME OF THE ENCRYPTION ALGORITHMS

Encryption algorithms based on	**Encryption time (second)**	**Decryption time (second)**
Fibonacci number	0.0173	0.0246
Generalized Fibonacci number	0.0207	0.025
Gray code	2.4121	2.4131
Generalized Gray code	2.2769	2.2765
P-Fibonacci sequence	0.1665	0.3624
P-Lucas sequence	0.125	0.2701
(n, k, p)-Gray code	2.5522	2.6841
P-recursive sequence	0.9479	1.1055
Parametric M-sequence	7.4808	7.6158

The measurement is based on a 512x512 grayscale image

Table 4.8 gives the execution time using the PRTME_SD algorithm with different recursive sequences. The results were measured on a computer running the Windows XP

www.manaraa.com

operating system with 3GB memory and with a CPU using Intel Core Duo E6550 (2.60GHz, 4MB L2 cache, 1066 MHz FSB).

The time of encryption process was measured when different sequences were applied individually to encrypt a 512x512 grayscale image. By applying a one-time decryption process to the encrypted images using the same sequences, the time of decryption process was also measured. Since the PRTME_SD algorithm encrypts images by changing pixel location, its encryption/decryption time is dependent on the image size, not the image data. Therefore, the measure results in Table 8 can prove the encryption performance of the PRTME_SD algorithm even if they are only obtained from one grayscale image.

The results shown in Table 4.8 demonstrate that the encryption algorithm based on the Fibonacci number has the shortest execution time when it comes to both the encryption and the decryption processes. The algorithms based on the Generalized Fibonacci number, P-Fibonacci and the P-Lucas sequences can also encrypt images more efficiently. The encryption algorithm using the Parametric M-sequence takes the longest time to perform one encryption/decryption process. This is because it takes the majority of the process time for the serial shift registers to generate the M-sequence. This can be improved by using parallel shift registers to generate M-sequence instead of the serial shift registers.

According to the results in Tables 4.7 and 4.8, users can select the P-Fibonacci and the P-Lucas sequences for encryption if both efficiency and security are important.

www.manaraa.com

4.6 Summary and Discussion

Five different recursive sequences and their corresponding transforms have been presented in this chapter including the P-Lucas sequence, P-recursive sequence, *(n, k, p)*-Gray code, Parametric M-sequence and the truncated P-Fibonacci sequence. All these recursive sequences and transforms can be implemented successfully for the 2D and 3D multimedia encryption.

The presented recursive sequences demonstrated comprehensive properties that can be specified to new recursive sequences by changing the parameters. For example, the *(n, k, p)*-Gray code can derive the classical Gray code, classical ternary Gray code, P-Gray code, and the ternary P-Gray code. Under different conditions, the P-recursive sequence can generate the P-Fibonacci sequence, P-Lucas sequence and the P-Gray code. All parameters in different recursive sequences can act as the security keys in the 2D P-recursive transform based multimedia encryption algorithms.

The 2D P-recursive transform has been introduced to efficiently encrypt 2D and 3D multimedia data. It is suitable for all above mentioned recursive sequences. It not only makes the 2D multimedia encryption a straightforward one-step process, but also provides an open platform that allows users to input new recursive sequences into the multimedia encryption system without requiring any changes to the system architecture.

Two multimedia encryption algorithms called the PRTME_SD and PRTME_FD algorithms were introduced that can encrypt multimedia data in the spatial and frequency

www.manaraa.com

domains, respectively. Simulation results and comparisons demonstrated their encryption performance. Security analysis has demonstrated that the PRTME_SD and PRTME_FD are able to withstand common attacks such as data loss attacks and noise attacks. In the PRTME_SD algorithm, the original image can be completely reconstructed. However, for the PRTME_FD algorithm, the reconstructed images are slightly different from the original image due to the data loss during the DCT transformation.

However, the PRTME_SD algorithm encrypts multimedia data only by changing the data locations in the spatial domain, whereas the PRTME_FD algorithm scrambles the DCT coefficients in the frequency domain. These permutation-only based encryption methods are known to be vulnerable to plaintext attacks [69, 70]. To overcome this problem and achieve higher levels of security, one effective solution is to change multimedia data values while also changing the locations of data or the transform coefficients using different techniques. In the following two chapters, several new encryption algorithms will be introduced according to this scheme.

www.manaraa.com

Chapter 5

Decompositions and Transforms for Image Encryption

This chapter introduces two new bit-plane decomposition methods, namely the truncated Fibonacci p-code bit-plane decomposition and the *(n, k, p)*-Gray code bit-plane decomposition. Their decomposition results and the number of decomposed bit-planes changes as the parameter values are altered. Integrating these two parameter-dependent decomposition methods with recursive sequence based encryption techniques, three new image encryption algorithms are introduced to improve the security level of several existing bit-plane decomposition based encryption approaches. In addition, a new image encryption algorithm is introduced using the Discrete Parametric Cosine Transform. Simulation results, comparisons and security analysis are then given to demonstrate the encryption performance of the algorithms and their ability to encrypt images, videos and selective objects.

www.manaraa.com

5.1 Introduction

The algorithms presented in Chapter 4 encrypt multimedia data by changing the data locations. These permutation-only based encryption methods are known to be vulnerable to several plaintext attacks [69, 70]. To overcome this problem, one solution is to simultaneously change multimedia data values and locations using different techniques.

There are many ways to change multimedia data values. Image bit-plane decomposition is one possible option. This encryption method first decomposes images into their binary bit-planes. It then encrypts bit-planes using different technologies, and combines all the encrypted bit-planes in order to obtain the encrypted images. Recently, a bit-plane encryption algorithm using exclusive-OR operations (BPE-XOR) was presented for an optical system [71]. Later, a selective bit-plane encryption scheme using the AES algorithm (SBE-AES) was developed for image encryption in mobile environments [72]. To reduce the computational workload, another selective bit-plane encryption algorithm using the least significant bit-plane of images (SBE-LBP) was proposed to encrypt images [73].

These bit-plane decomposition based encryption schemes have been able to contribute to their specific applications. However, due to the fact that they are based on traditional image bit-plane decomposition, they do have some security weaknesses: (1) from a cryptanalysis point of view, this decomposition method has a low level of security because, for each specific image, the number of its decomposed bit-planes and the content of each bit-plane are fixed. For example, a grayscale image with gray levels 0-

www.manaraa.com

255 can only be decomposed into eight bit-planes. The contents in each bit-plane are fixed for the same image. As a result, it can be easy for the attacker to predict the decomposition results. (2) The XOR operation and selective bit-plane encryption schemes have been shown to be vulnerable to a low computational cost attack [165].

This chapter introduces the truncated Fibonacci p-code bit-plane decomposition (to reduce redundancy of the Fibonacci p-code bit-plane decomposition) [74], and the *(n, k, p)*-Gray code bit-plane decomposition (which extends the concept of the image bit-plane decomposition from base 2 (binary bit string) into arbitrary base) [75, 76]. The decomposition results and the number of the decomposed bit-planes of these decomposition methods are parameter-dependent. This particular property is very useful and makes the methods suitable for multimedia encryption.

To enhance the security of the bit-plane decomposition based encryption approaches, three new image encryption algorithms are introduced combining image bit-plane decomposition with recursive sequence based encryption methods.

Based on the concept of using one set of security keys to encrypt the original data and a different set of security keys to reconstruct it to obtain the final encrypted data, a new image encryption algorithm is introduced using the Discrete Parametric Cosine Transform. Simulation results, comparisons and security analysis are also provided.

The rest of this chapter is organized as follows: after reviewing several existing decomposition methods, Section 5.2 introduces the truncated Fibonacci p-code bit-plane decomposition and the *(n, k, p)*-Gray code bit-plane decomposition. Section 5.3

www.manaraa.com

introduces a new image encryption algorithm combining the P-Fibonacci transform and the Fibonacci p-code bit-plane decomposition. Section 5.4 presents a selective object encryption scheme using the truncated Fibonacci p-code. Section 5.5 introduces another new image encryption algorithm using the *(n, k, p)*-Gray code and its decomposition. Section 5.6 introduces an image encryption algorithm using the Discrete Parametric Cosine Transform. Section 5.7 reaches a conclusion.

www.manaraa.com

5.2 Image Bit-plane Decomposition Methods

This section reviews three existing methods for image bit-plane decomposition, namely binary bit-plane decomposition, Gray code decomposition [136] and Fibonacci p-code bit-plane decomposition [157]. These methods are intended for images that are decomposed into binary bit-planes. They are frequently used for image compression, enhancement and encryption. To reduce the redundancy of the Fibonacci p-code bit-plane decomposition, the truncated Fibonacci p-code bit-plane decomposition is introduced for selective image encryption [74]. By extending the concept of the image bit-plane decomposition from base 2 (binary bit string) into arbitrary base, the *(n, k, p)*-Gray code bit-plane decomposition is then introduced [75, 76]. These decomposition methods will be used for image encryption.

5.2.1 Binary and Gray code Bit-plane Decompositions

Definition 5.1: The non-negative decimal number D can be represented by the following form of the base-2 polynomial.

$$D = \sum_{i=0}^{n-1} a_i 2^i = a_0 2^0 + a_1 2^1 + \ldots + a_{n-1} 2^{n-1} \tag{83}$$

The binary code $(a_{n-1}, \ldots, a_1, a_0)$ is the binary representation of the non-negative decimal number D.

The pixel values of the grayscale images are non-negative integers. Each of them can be represented by a binary code according to the equation (83). Therefore, a grayscale image

www.manaraa.com

can be decomposed into n binary bit-planes. The i^{th} bit-plane contains the coefficient a_i bits of all image pixels. This image decomposition method is called binary bit-plane decomposition.

Figure 5.1 gives an example of the binary bit-plane decomposition. Bit-plane 7 consists of all the most significant bits of each image pixel, and bit-plane 0 collects all the least significant bits of image pixels.

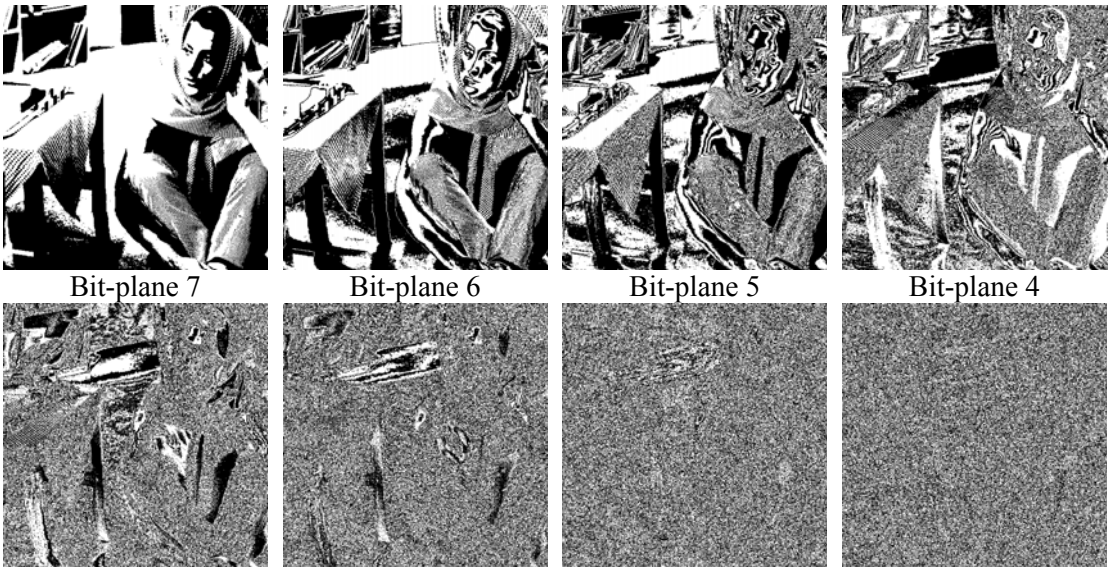


Figure 5.1: Binary bit-plane decomposition of a grayscale image.

Definition 5.2: A non-negative integer can be represented by an *n*-bit Gray code $(g_{n-1},...,g_1,g_0)$, which can be calculated from the binary code in definition 5.1 using the following operation,

$$g_i = \begin{cases} a_{n-1} & i = n-1 \\ a_i \oplus a_{i+1} & 0 \le i < n-2 \end{cases} \tag{84}$$

where $\oplus$ is the exclusive-OR operation.

www.manaraa.com

In this manner, a grayscale image can be decomposed into n gray code bit-planes. Figure 5.2 gives an example of this. This alternative image decomposition method can reduce the effect of small gray-level changes due to the fact that the successive Gray codes differ in only one bit position. For example, the Gray codes corresponding to the decimal number 127 and 128 are 01000000 and 11000000, respectively.

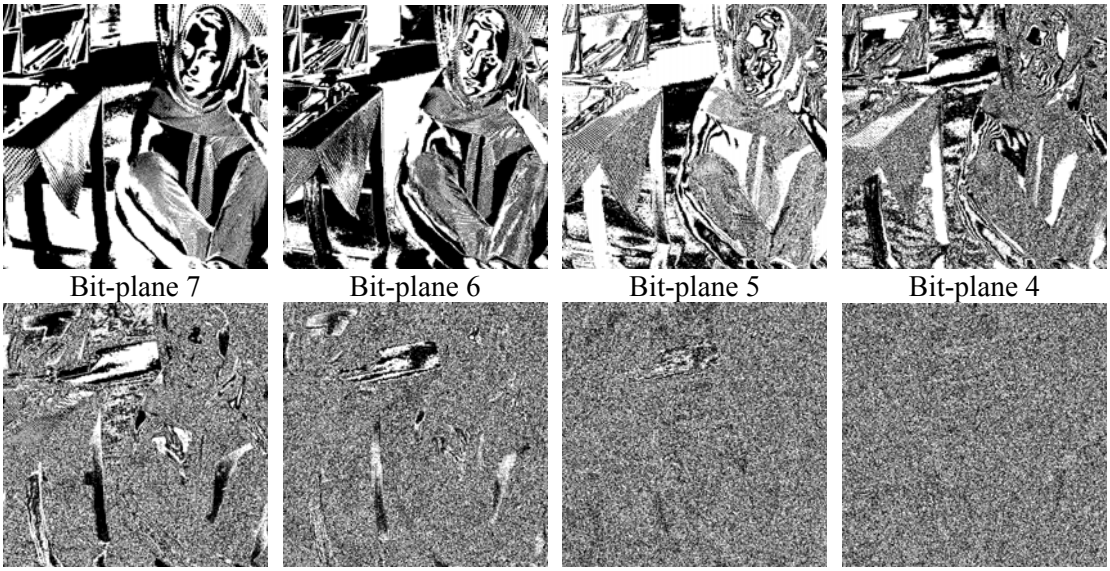


Figure 5.2: Gray code bit-plane decomposition of a grayscale image.

In the decomposed results of these two traditional methods, the higher-order bit-planes contain almost all the significantly visual data, especially the top four bit-planes. The other lower-order bit-planes describe more of the image's details. This advantage is useful for image compression. However, from a cryptanalysis point of view, these two traditional decomposition approaches may not be suitable for image encryption because:

A grayscale image can be decomposed into only a specific number of binary bit-planes via these two decomposition methods, since they are based on the binary representation

www.manaraa.com

of the image. For example, a grayscale image with gray levels within 0-255 can be decomposed only into eight bit-planes.

For a specific grayscale image, the user can easily predict any bit value of each image pixel in any bit-plane since their decomposition process is not parameter-dependent.

Because of the fixed number of bit-planes, the encryption result can be broken easily.

5.2.2 Fibonacci P-code Bit-plane Decomposition

This section reviews the definition of the Fibonacci p-code and Fibonacci p-code bit-plane decomposition.

5.2.2.1 Fibonacci P-code

A non-negative decimal number can be represented using a binary code sequence based on equation (83). This concept can be extended to the Fibonacci p-code since the power of two series is a special case of the P-Fibonacci sequence. Therefore, the definition of Fibonacci p-code is given below.

Definition 5.3: A non-negative decimal number D can be represented by the following format:

$$D = \sum_{i=0}^{n-1} c_i f_p(i) = c_0 f_p(0) + c_1 f_p(1) + \ldots + c_{n-1} f_p(n-1) \tag{85}$$

where n and p are nonnegative integers, $i = 0,1,\ldots,n-1$, $c_i \in (0,1)$, the weight $f_p(i)$ is the i^{th} element of the P-Fibonacci sequence with a specific p value in equation (52) in

www.manaraa.com

Chapter 4. The coefficient sequence $(c_{n-1},...,c_1,c_0)$ is called the Fibonacci p-code of D, namely,

$$D=(c_{n-1},...,c_1,c_0)_p \tag{86}$$

where p is the distance parameter of the P-Fibonacci sequence, and the largest value $f_p(n-1)$ in equation (85) corresponds to the most significant bit in the Fibonacci p-code in equation (86).

The Fibonacci p-code of a specific decimal number will change as the p value changes. However, for a given p value, the Fibonacci p-code of a specific decimal number is not unique either.

TABLE 5.1. DIFFERENT FIBONACCI P-CODES OF 30 FOR P=3

$f_3(i)$	26	19	14	10	7	5	4	3	2	1	1	1
Fibonacci p-codes	1	0	0	0	0	0	1	0	0	0	0	0
	1	0	0	0	0	0	0	1	0	1	0	0
	0	1	0	1	0	0	0	0	0	1	0	0
	0	1	0	0	1	0	1	0	0	0	0	0
	…											

For example, if $D=30$ and $p=3$, the P-Fibonacci sequence would yield a sequence with 12 elements as shown in Table 5.1. Each element serves as a weight in the Fibonacci p-code. The decimal number 30 can be represented by different Fibonacci p-codes with 12 bits. Several examples of the Fibonacci p-code of 30 are given in Table 5.1.

In order to obtain a unique Fibonacci p-code for each non-negative decimal number, several different rules or constraints are presented [158, 166, 167]. Users have the flexibility to choose one of them. This section selects the constraints presented in [158].

www.manaraa.com

If the following constraints are satisfied, a non-negative decimal number has a unique Fibonacci p-code [158]:

$$D = f_p(i) + s \tag{87}$$

where the $f_p(i)$ is the i^{th} element of the P-Fibonacci sequence with a specific p value, $0 \le i < n$, and a non-negative decimal number s is a reminder, $0 \le s < f_p(i-p)$.

Based on the constraints in equation (87), for $D = 30$ and $p = 3$, its Fibonacci p-code is $30 = (1,0,0,0,0,0,1,0,0,0,0,0)_3$. Note that, after applying the constraints in equation (87), there are at least p 0's between two consecutive 1's in the Fibonacci p-code of any non-negative decimal number.

5.2.2.2 Fibonacci P-code Bit-plane Decomposition

The decomposition results of the traditional binary and Gray code bit-plane decompositions and the number of bit-planes are unchangeable for a specific grayscale image. They are easy to predict and, therefore, are not conducive to image encryption.

For a given p value, each non-negative decimal number has a unique Fibonacci p-code. With the same concept of the traditional bit-plane decomposition, an image can be decomposed into several Fibonacci p-codes. Moreover, due to the fact that the P-Fibonacci sequence becomes the power of two series when $p = 0$, the traditional bit-plane decomposition is a special case of the Fibonacci p-code bit-plane decomposition.

The number of the Fibonacci p-code bit-planes n_B depends on the maximum value of images $I_{\max}$. In order to make the decomposition method work over all p values, the

www.manaraa.com

following rules are introduced: If $p \le I_{\max}$, n_B is calculated from $I_{\max}$; otherwise, if $p > I_{\max}$, n_B is calculated by p values. For the latter case, this means that the number of Fibonacci p-code bit-planes is only determined by the p value. Figure 5.3 describes the algorithm of the Fibonacci p-code bit-plane decomposition for a 2D image with a size of $M \times N$.

```
/* generate the P-Fibonacci sequence */
 if p > I_max then I_max = p
f_p(0) = 1, i = 1;
while f_p(i-1) < I_max then
      if i - p < 1 then f_p(i) = f_p(i-1);
      else f_p(i) = f_p(i-1) + f_p(i-p-1);
      i = i + 1; end
n_B = i - 1; f_p = f_p(i-1:-1:1);
/* Decompose Image into the Fibonacci P-code bit-planes */
for m = 1 to M ; n = 1 to N ; s = I(m,n);
for i = n_B to 0
    if s ≥ f_p(i) then s = s - f_p(i); B(m,n,i) = 1 ;
   else B(m,n,i) = 0;
end
```

Figure 5.3: The algorithm of the Fibonacci p-code bit-plane decomposition

For a specific grayscale image, the results of the Fibonacci p-code bit-plane decomposition are parameter-dependent. The number of the Fibonacci p-code bit-planes n_B changes as the parameter p values change. For instance, for a grayscale image,

www.manaraa.com

$I_{\max} = 255$; for $p = 2$, $n_B = 15$; and for $p = 3$, $n_B = 19$. Figure 5.4 gives an example of a grayscale image decomposed using the Fibonacci P-code bit-plane decomposition with $p = 2$.

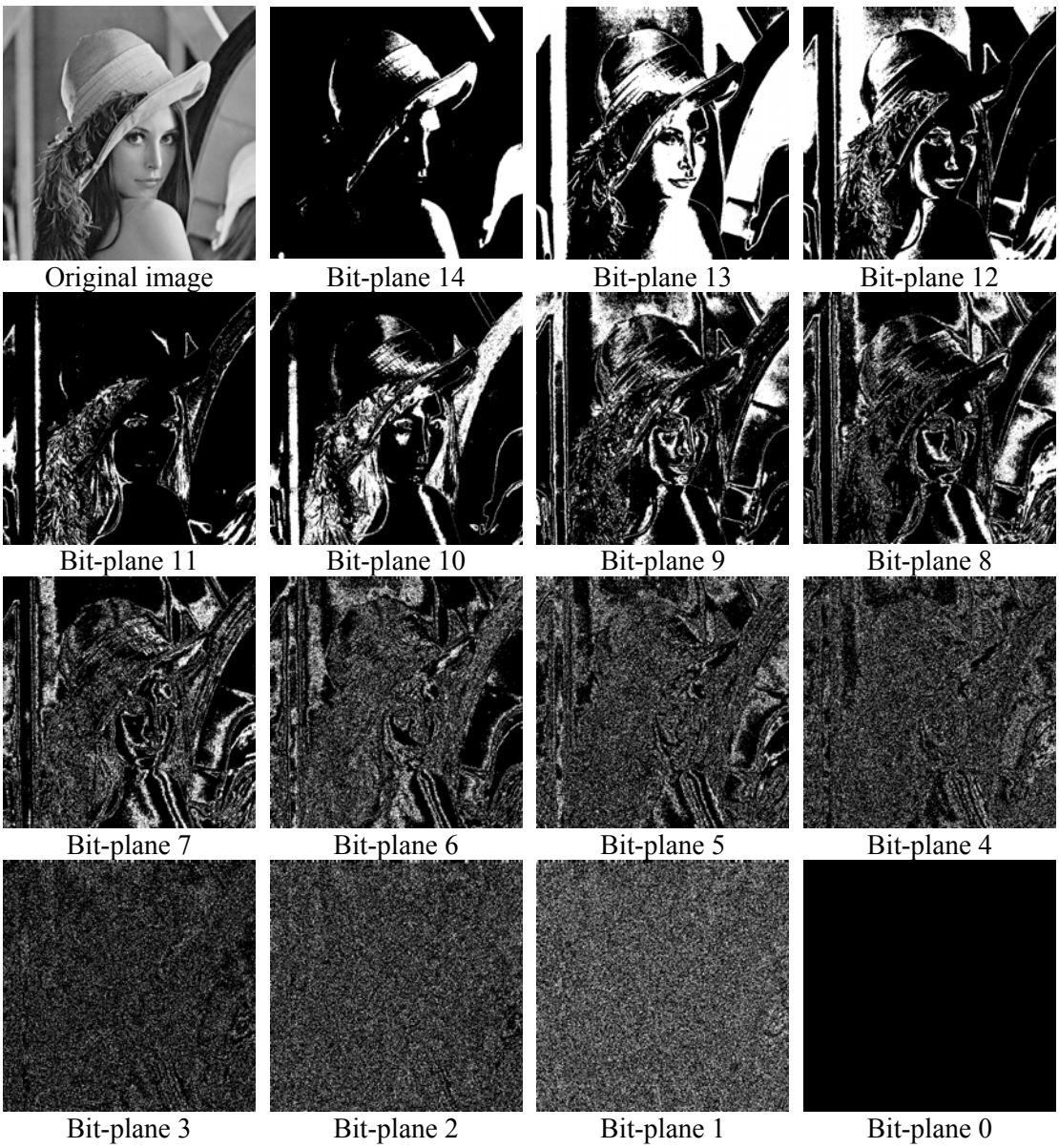
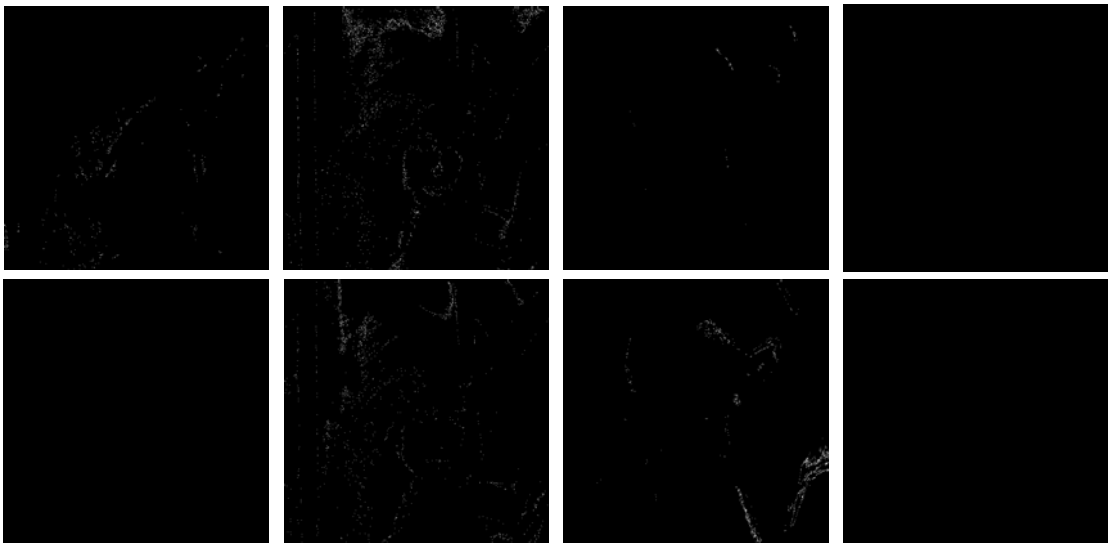


Figure 5.4: Fibonacci p-code bit-plane decomposition of the grayscale Lena image, p=2

www.manaraa.com

When p is greater than the maximum value of the image, the P-Fibonacci sequence will contain p 1's immediately after decimal numbers 1, 2, 3, 4,..., p . Therefore, the Fibonacci p-code bit-planes of an image have the property that each nonzero image pixel has only a one stored in a bit-plane and a zero stored in all other bit-planes. Moreover, the number of the Fibonacci p-code bit-planes changes with different p values.



Bit-plane 290 Bit-plane 380 Bit-plane 480 Bit-plane 510

Figure 5.5: Selected Fibonacci p-code bit-planes of the grayscale Lena image using different p values. The top row shows the selected Fibonacci p-code bit-planes, $p = 256$; The bottom row shows the selected Fibonacci p-code bit-planes, $p = 270$.

For example, when $p = 256$, which is greater than $I_{\max} = 255$ of the grayscale image, then $n_B = 511$ and the Fibonacci p-code of 255 has only a one stored in the 510^{th} bit-plane and a zero stored in other bit-planes. Likewise, when $p = 270$, then $n_B = 539$ and the Fibonacci p-code of 255 has only a one stored in the 524^{th} bit-plane and zeros for other bit-planes. Since the number of the Fibonacci p-code bit-planes changes, the Fibonacci p-code of a specific pixel value will be different as the value of the parameter p

www.manaraa.com

changes. Figure 5.5 gives several Fibonacci p-code bit-planes selected from the decomposed results using $p = 256$ and $p = 270$.

In the image encryption algorithm presented in Section 5.3, a shuffling process will be used to change the positions of each Fibonacci p-code bit-plane. As a result, the shuffled results will change as the p values change as well as in the image decomposition process.

Moreover, the contents of the Fibonacci p-code bit-planes differ based on changes in the p value. These advantages make the Fibonacci p-code bit-plane decomposition well suited to image encryption. Note that the maximum value of medical images can be greater than 255 (for example, 16-bit medical images) so the presented decomposition approach will work also for other types of images.

5.2.3 The New Truncated Fibonacci P-code Bit-plane Decomposition

To reduce the redundancy of the Fibonacci p-code bit-plane decomposition and thereby generate the Fibonacci p-code more efficiently, the truncated Fibonacci p-code and its bit-plane decomposition are introduced for selective object encryption [74].

5.2.3.1 The New Truncated Fibonacci P-code

Definition 5.4: A non-negative decimal number can be represented by the following format,

$$A = c_0 T_p(0) + c_1 T_p(1) + \ldots + c_{n-1} T_p(n-1) \tag{88}$$

www.manaraa.com

where n and p are nonnegative integers, $i = 0,1,...,n-1$, $c_i \in (0,1)$ and $T_p(i)$ is the TPFS defined in equation (56) in Chapter 4. The binary coefficient sequence $(c_{n-1},...,c_1,c_0)$ is called the truncated Fibonacci p-code (TFPC) of A, namely,

$$A = (c_{n-1},...,c_1,c_0)_p \tag{89}$$

For a certain p value, the TFPC of a specific decimal number is shorter than the Fibonacci p-code in equation (86) [157, 158]. This allows the TFPC to be generated more efficiently. In a manner similar to the Fibonacci p-code, the TFPC is not unique. For example, if $A = 35$, $p = 4$, the TFPC of A will be,

$$\begin{aligned} 35 &= (1,0,0,0,0,0,0,0,0,0,0,1)_4 = (0,1,0,0,0,1,0,0,0,0,0,1)_4 \\ &= (0,1,0,0,0,0,1,0,0,1,0,0)_4 = ... \end{aligned}$$

To obtain a unique TFPC of a non-negative decimal number for specific parameter p, the following condition should be satisfied,

$$A = T_p(n) + s \tag{90}$$

where $0 \le s < T_p(n-p)$.

The above condition is the same as the constraint of the Fibonacci p-code in [157, 158]. There are at least p 0's between two consecutive 1's in the unique TFPC of any non-negative decimal number. The unique TFPC is $35 = (1,0,0,0,0,0,0,0,0,0,0,1)_4$ for the example above.

www.manaraa.com

5.2.3.2 The New Truncated Fibonacci P-code Bit-plane Decomposition

For a specific p value, each non-negative decimal number has a unique TFPC representation as long as the condition in equation (90) is satisfied. Its TFPC will differ based only on different p values due to the fact that the TFPS is specified by the parameter p values.

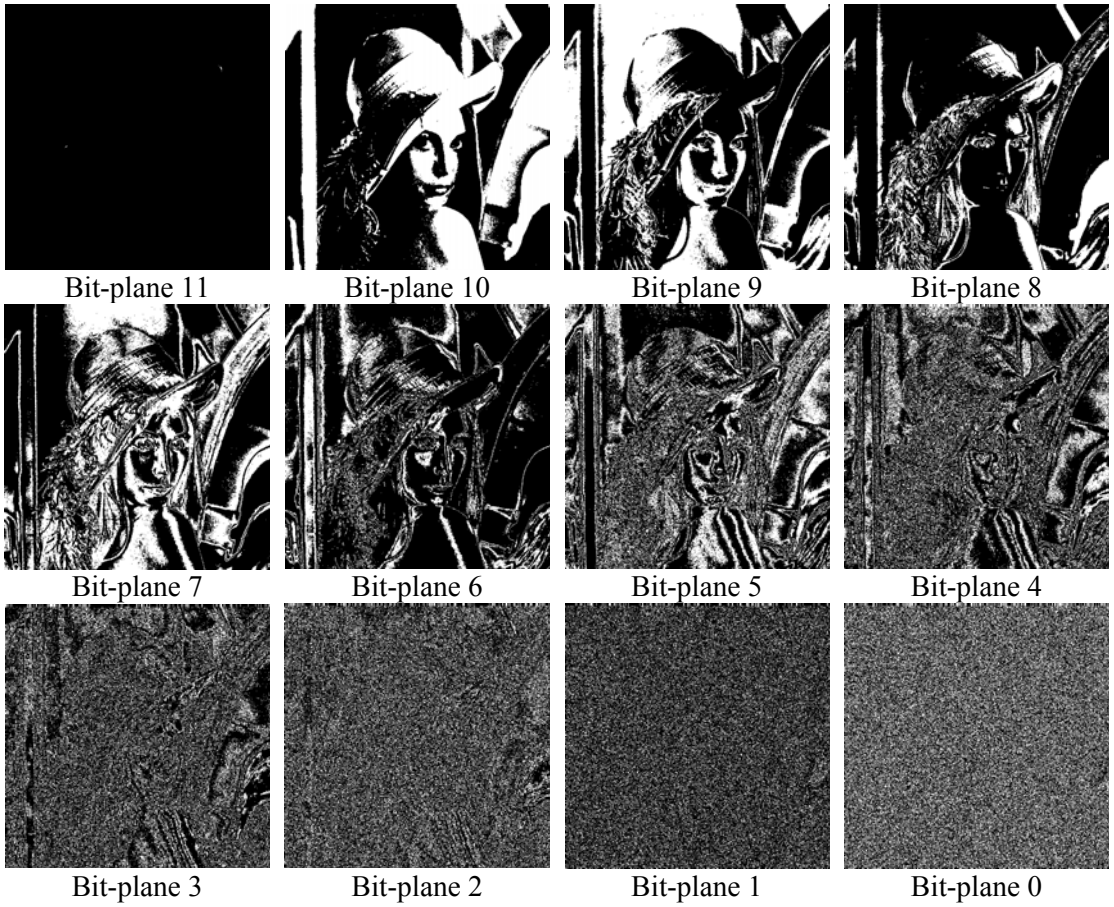


Figure 5.6: Truncated Fibonacci p-code bit-plane decomposition of the grayscale Lena image, p=1.

Based on the definition 5.4, a grayscale image can also be decomposed into the TFPC bit-planes, a process called the Truncated Fibonacci p-code bit-plane decomposition. The

www.manaraa.com

traditional binary bit-plane decomposition is a special case of the TFPC bit-plane decomposition when $p = 0$.

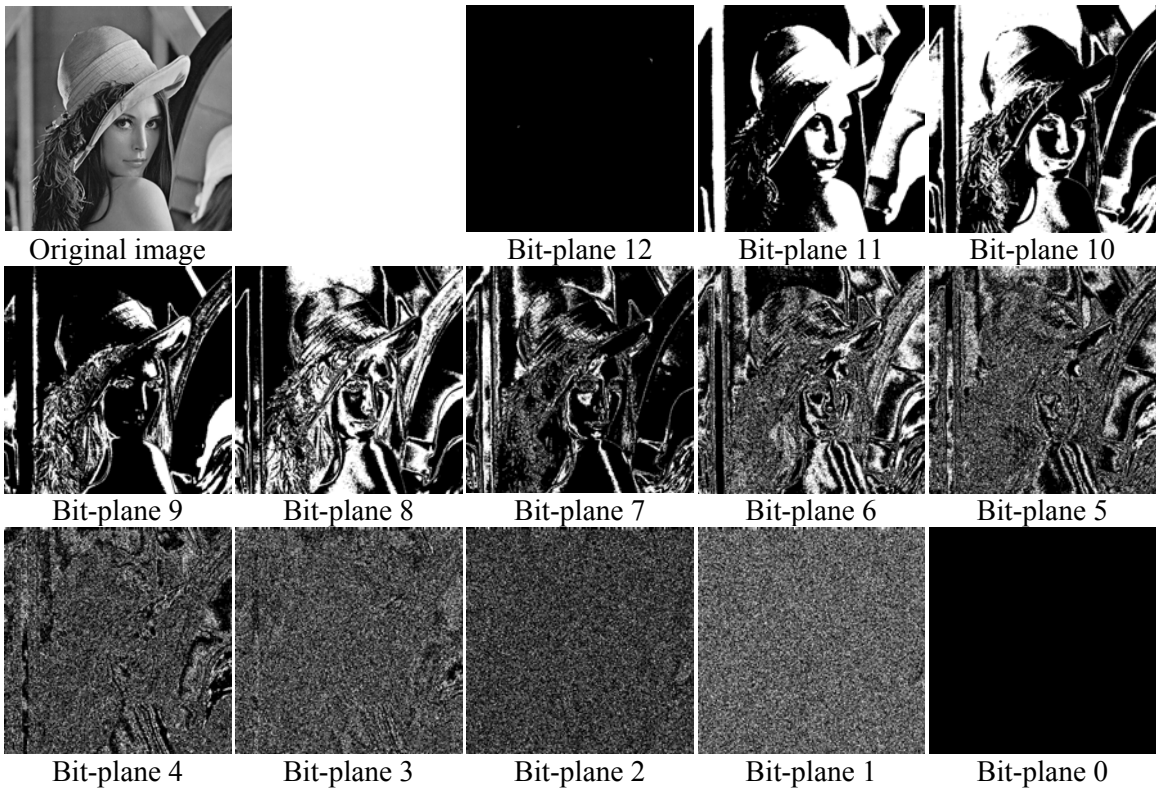


Figure 5.7: Fibonacci P-code bit-plane decomposition of the grayscale Lena image, p=1.

A grayscale image with gray levels within 0-255 is decomposed into 12 TFPC bit-planes when $p = 1$. A TFPC decomposition example is given in Figure 5.6. For a specific grayscale image, the number of its TFPC bit-planes changes as the value of parameter p changes. For instance, the number of its TFPC bit-plane is 17 for $p = 3$, and 21 for $p = 5$, respectively. Moreover, the contents of the TFPC decomposition results are different based on changes in the value of p. This makes the TFPC decomposition a suitable method for image encryption. To demonstrate the difference between the TFPC

www.manaraa.com

decomposition and the Fibonacci p-code bit-plane decomposition, Figure 5.7 gives the decomposition results of the same grayscale image using the Fibonacci p-code with $p=1$.

5.2.4 The New *(n, k, p)*-Gray Code Bit-plane Decomposition

By extending the concept of the image bit-plane decomposition from base 2 (binary bit string) into an arbitrary base, this section introduces a new image decomposition method that makes use of the *(n, k, p)*-Gray code [75, 76].

From definition 4.4 in Chapter 4, the grayscale image can be decomposed into *k (n, k, p)*-Gray code bit-planes, where the pixel values in the i^{th} bit-plane are the i^{th} bit g_i of those pixels that have the same location in the grayscale image. This method is called the *(n, k, p)*-Gray code bit-plane decomposition.

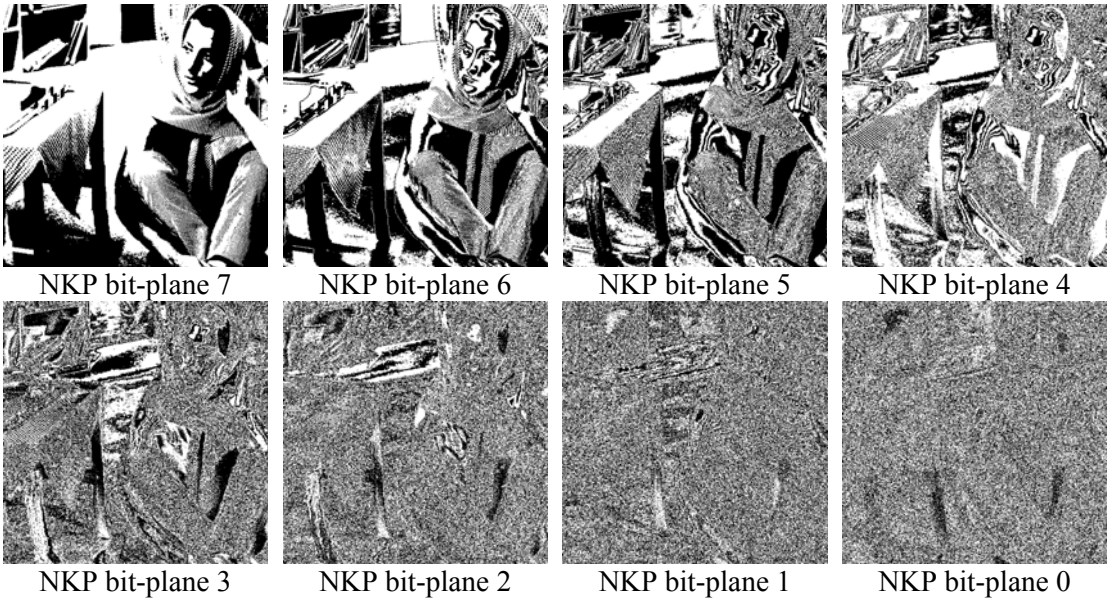


Figure 5.8: *(n, k, p)*-Gray code bit-plane decomposition of a grayscale image, n=2, p=2.

www.manaraa.com

When the base n is greater than 2, the values in the *(n, k, p)*-Gray code bit-planes are no longer binary. For example, the *(3, 6, 1)*–Gray code for a pixel with decimal value 10 is 000102. The least significant bit-plane for a pixel of this value will have a "2" stored in the respective bit-plane.

The novelty of this decomposition method is that it can decompose an image not only into binary bit-planes (for base $n=2$) but also into non-binary bit-planes (for base $n>2$). The *(n, k, p)*-Gray code bit-planes will change as the values of base n and distance parameter p change. For a specific image, the number of bit-planes, k, is determined by the base n value. For example, a grayscale image with gray levels between 0 and 255 can be decomposed to 8 ($k=\lceil \log_2 255 \rceil = 8$) binary bit-planes for $n=2$. Figure 5.8 gives an example of this.

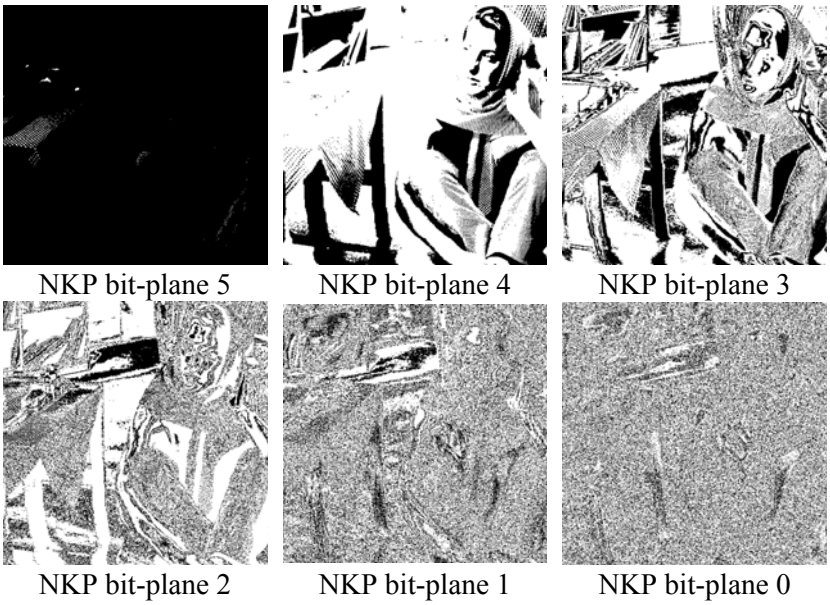


Figure 5.9: *(n, k, p)*-Gray code bit-plane decomposition of a grayscale image, n=3, p=0. This is also an example of the *(n, k)*-Gray code.

www.manaraa.com

When the base n is greater than 2, the decomposed bit-planes of a grayscale image that has gray levels between 0 and 255 will no longer be binary and the number of decomposed bit-planes will be less than 8. The *(n, k)*-Gray code can also achieve this since it is a special case of the *(n, k, p)*-Gray code. Figure 5.9 gives an example of this where $n = 3, p = 0$. However, for a given base n, the content of the decomposition results of an image that uses the *(n, k)*-Gray code will always be the same, whereas the content of the *(n, k, p)*-Gray code bit-planes will change with the value of p. This is one of the advantages of the presented decomposition method that uses the *(n, k, p)*-Gray code. Figure 5.10 gives another example with $n = 3, p = 4$.

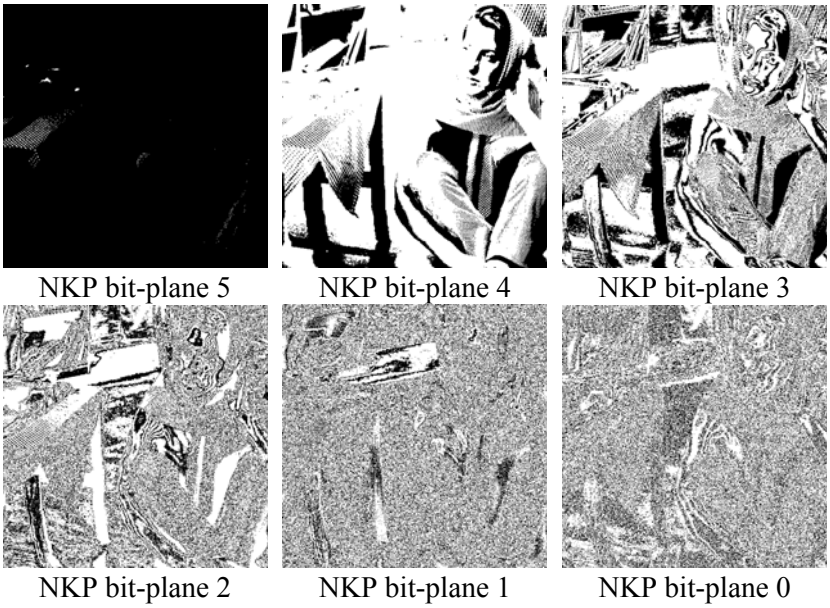


Figure 5.10: *(n, k, p)*-Gray code bit-plane decomposition of a grayscale image, n=3, p=4.

Analysis of Figures 5.9 and 5.10 demonstrates that the most significant bit-plane doesn't change while the content of several of the least significant bit-planes differs as the p

www.manaraa.com

values change. This is because, according to its definition 4.4 in Chapter 4, the *(n, k, p)*-Gray code keeps the most significant bit unchangeable.

In summary, both the decomposed results and the number of the *(n, k, p)*-Gray code bit-planes are parameter-dependent. This feature makes the *(n, k, p)*-Gray code bit-plane decomposition a more desirable method for applying to image encryption.

Given three image bit-plane decomposition approaches, the following sections will make use of them for three new image encryption algorithms.

www.manaraa.com

5.3 Image Encryption Using P-Fibonacci Transform and Decomposition

This section introduces a new image encryption algorithm that integrates the P-Fibonacci Transform and Fibonacci p-code bit-plane decomposition [77]. To demonstrate the algorithm's performance when it comes to encrypting grayscale images, biometrics, medical images and color images, simulation results and a comparison will be given. Security analysis will demonstrate that the algorithm has the ability to withstand several attacks such as brute force, statistics, data loss, noise and plaintext attacks.

5.3.1 The New Image Encryption Algorithm

This section introduces a new image encryption algorithm using the P-Fibonacci transforms and Fibonacci p-code bit-plane decomposition, called the P-Fibonacci Encryption (PFE) algorithm. It can be used to encrypt images, biometrics, and videos.

The new PFE algorithm shown in Figure 5.11 contains five processes: image decomposition, bit-plane shuffling, bit-plane resizing, bit-plane encryption and data mapping. The algorithm decomposes the original image into its Fibonacci p-code bit-planes, shuffles the order of all bit-planes, resizes bit-planes based on the size of the 2D P-Fibonacci transform, performs the 2D P-Fibonacci transform to encrypt the bit-planes individually, combines all encrypted bit-planes using binary code definition in equation

www.manaraa.com

(83) and then maps the image data back into the original image data range to generate the final resulting encrypted image.

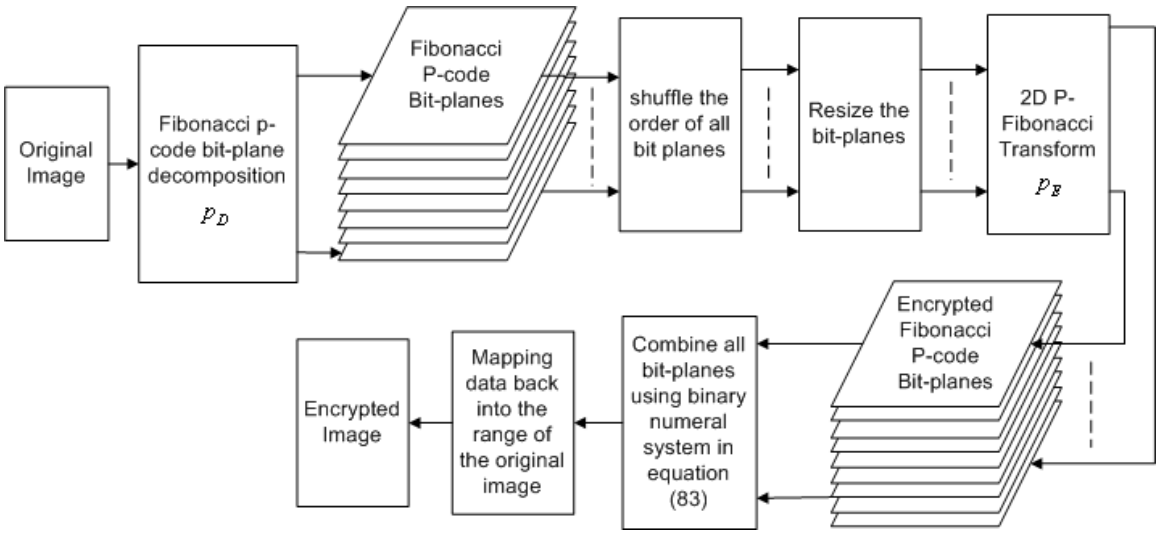


Figure 5.11: The block diagram of the new PFE algorithm

Let $\{X_0, X_1, ..., X_{L-1}\}$, $X_0 < X_1 < ... < X_{L-1}$ denote all discrete intensity levels in an input image $I(m,n)$, and let the data mapping function be defined by,

$$E(m,n) = k \quad \text{for } I(m,n) = X_k \tag{91}$$

where $E(m,n)$ is the output encrypted image, $k = 0,1,...,L-1$. Note that this is a nonlinear data mapping process.

The Fibonacci p-code and P-Fibonacci transform will be different as the value of parameter p changes. Both image decomposition and encryption processes are parameter-dependent. The parameter p for both the decomposition process (called P_D) and the encryption process (called P_E) can act as security keys for the presented PFE algorithm. Users have the flexibility to choose the same p value for both processes, i.e. $P_D = P_E$, or

www.manaraa.com

select different p values for each process, namely $P_D \neq P_E$. They may also select different P_E values for each bit-plane, thereby helping to achieve a higher level of security but increasing computational complexity.

The image resizing process helps to improve the security level of the PFE algorithm because it makes it difficult for an attacker to decode the encrypted images. Users have the flexibility to choose any existing method to perform the shuffling process. While keeping the encrypted images within the same data range as those of the original images, the data mapping process changes and shrinks the image data.

Except for the image resizing process, the other four processes in the presented PFE algorithm are parameter-dependent. Its security keys consist of the parameters in these four processes, namely (1) P_D for image decomposition, (2) security key for bit-plane shuffling, (3) P_E for bit-plane encryption, and (4) the pixel value array for data mapping.

To recover the original image from the encrypted image, the authorized users will have to be given security keys. The decryption process of the PFE algorithm works in the following order: it maps encrypted image data back into the original range, decomposes the image into its binary bit-planes (the Fibonacci p-code bit-planes generated in the encryption process), reverts the order of all bit-planes back to their original order, decrypts all bit-planes individually using the 2D Fibonacci transform, resizes all bit-planes back to their original condition and, finally, combines all decrypted bit-planes to obtain the reconstructed image.

www.manaraa.com

5.3.2 Simulation Results

The PFE algorithm has been successfully applied to more than fifty images, including grayscale images, biometrics, color images, and medical images such as Magnetic Resonance Images (MRIs) and Computer Tomography (CT) images. To demonstrate the encryption performance of the PFE algorithm, this section will give several illustrative examples of image encryption.

In all simulation results obtained by the PFE algorithm in the rest of this section, the same security key P_E is used for all bit-planes, while the order of the Fibonacci p-code bit-planes is reversed in the shuffling process. The random numbers are added in the padding region in the image resize process. Of course, users have the flexibility to use any other method to shuffle the order of the bit-planes and to resize the original images.

The structural similarity (SSIM) index is a quantitative assessment method for measuring the similarity between two images [168]. The SSIM is used to quantitatively evaluate the similarity between the reconstructed and original images to demonstrate whether the original images are completely reconstructed or not. A value 1 of the SSIM index indicates that two measured images are identical. The Matlab code of the SSIM was obtained from the author's webpage [169]. Its default settings for the image measure are utilized in this section.

Figure 5.12 gives an illustrative example of a grayscale image that has been encrypted by the PFE algorithm after its security keys have been set to high values, $P_D = 32$ and $P_E = 300$. The results demonstrate that the image changes according to different

www.manaraa.com

stages of encryption and decryption. The encrypted image shown in Figure 5.12(d) is visually different from the original image shown in Figure 5.12(a). The fact that the reconstructed image shown in Figure 5.12 (f) is visually the same as the original image and that the SSIM value 1 confirms that the two are identical, means that the original images have been completely reconstructed.

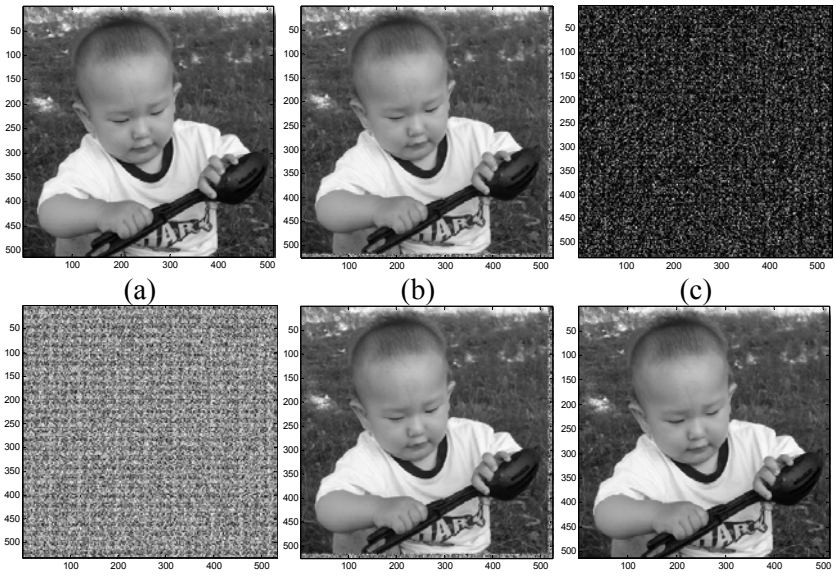
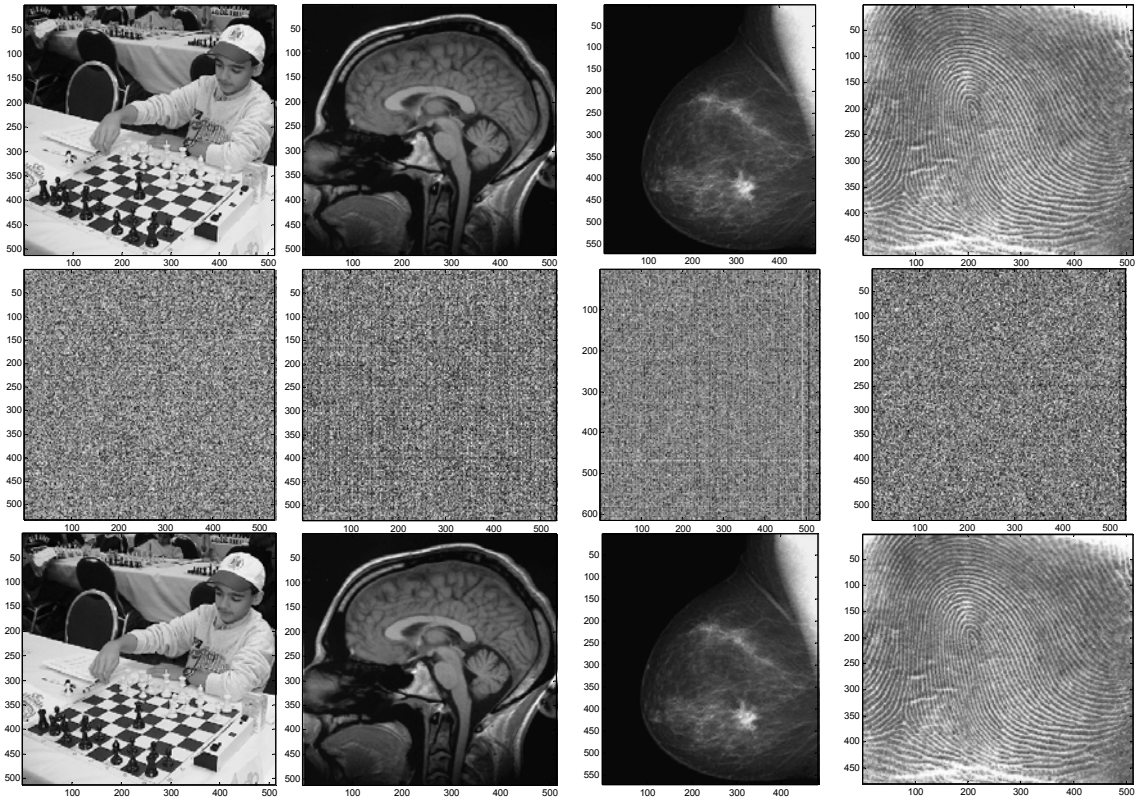


Figure 5.12: Grayscale image encryption using the PFE algorithm, $P_D = 32$ and $P_E = 300$. (a) The original image; (b) The resized image; (c) The encrypted image before data mapping; (d) The final encrypted image; (e) The reconstructed image without image resizing; (f) The final reconstructed image.

Figure 5.13 gives four encryption results to show that the presented PFE algorithm has the ability to protect different types of images, including grayscale images, MR images, CT images and fingerprints. The PFE algorithm has encrypted all these images with values $P_D = 10$ and $P_E = 15$. Visually, the encrypted images are close to noise images. They show the excellent encryption performance of the presented PFE algorithm. All the

www.manaraa.com

reconstructed images and their SSIM values demonstrate that the original images have been perfectly reconstructed.



(a) SSIM=1 (b) SSIM=1 (c) SSIM=1 (d) SSIM=1

Figure 5.13: Encryption for different types of images, $P_D = 10$, and $P_E = 15$. The first row shows the original images; the second row shows the encrypted images; the third row shows the reconstructed images. (a) The grayscale image case; (b) The MRI case; (c) The CT image case; (d) The biometrics case. This demonstrates that the presented PFE algorithm has the ability to encrypt different types of images and that the original images can be reconstructed completely.

3D images, such as color images and 3D medical images, contain several 2D data matrices called 2D components. Color images, for example, contain three color planes. Each color plane is a 2D component. In this manner, the 3D images can be considered as combinations of several 2D images. The 3D image encryption can be accomplished by encrypting all its 2D components individually. Users have the flexibility to choose the

www.manaraa.com

same security keys for all 2D components or to choose different security keys for each of them.

Figure 5.14 gives a descriptive example of color image encryption using the PFE algorithm with the security keys $P_D = 10$ and $P_E = 20$. Visually, the encrypted image in Figure 5.14(d) looks like a noise image. The results also demonstrate the PFE algorithm's ability to encrypt 3D images. The reconstructed image shown in Figure 5.14(f) and its SSIM value further verify that the original image has been reconstructed completely.

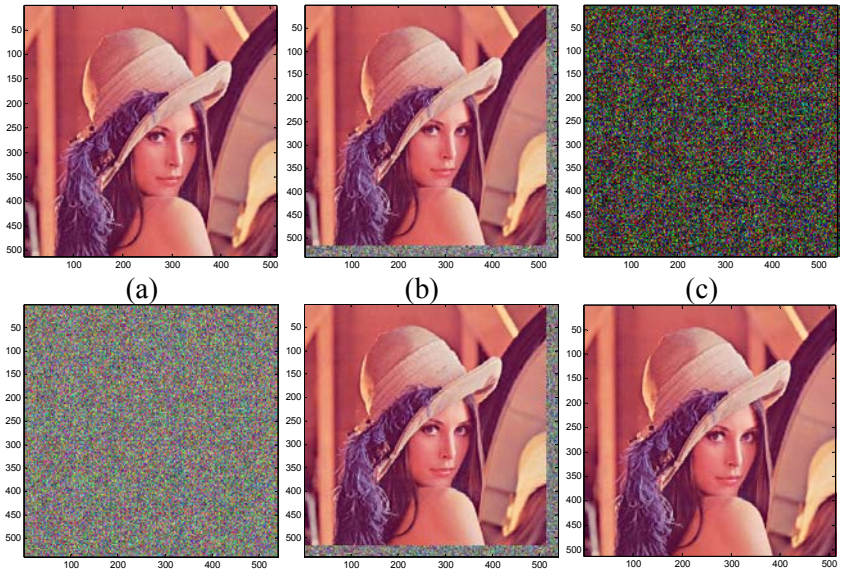


Figure 5.14: Color image encryption using the PFE algorithm, $P_D = 10$ and $P_E = 20$. (a) The original color image; (b) The resized color image; (c) The processed image before the data mapping process; (d) The encrypted image; (e) The reconstructed image without image resizing; (f) The final reconstructed image.

5.3.3 Performance Analysis

The efficiency of the encryption algorithm translates into faster encryption and decryption, and lower computational costs. Efficiency, moreover, is an important

www.manaraa.com

property when it comes to evaluating the suitability of an encryption algorithm for real time applications. The efficiency of this particular algorithm can be verified clearly by analyzing the time it takes to execute its encryption and decryption of images.

5.3.3.1 Performance Analysis

In this experiment, the presented PFE algorithm encrypts a 256×256 grayscale Lena image with different security keys, P_D and P_E. The execution time of the encryption and decryption processes is measured and recorded when the security keys change. The encryption time is given in Table 5.2, and the decryption time is given in Table 5.3.

TABLE 5.2. ENCRYPTION TIME OF A 256×256 GRAYSCALE IMAGE USING THE PRESENTED PFE ALGORITHM WITH DIFFERENT P_D AND P_E VALUES

P_E \ P_D	1	2	5	10	20	30
1	2.3351	1.0805	1.1295	1.4178	1.3794	1.5504
3	0.8913	0.9074	0.9568	1.2268	1.1403	1.3083
10	0.6138	0.5952	0.6266	0.8093	0.7693	0.8640
50	0.4960	0.5009	0.5254	0.6563	0.6370	0.7077
200	0.5285	0.5231	0.5487	0.6866	0.6625	0.7387
300	0.5026	0.4998	0.5377	0.6761	0.6776	0.7525

TABLE 5.3. DECRYPTION TIME OF A 256×256 GRAYSCALE IMAGE USING THE PRESENTED PFE ALGORITHM WITH DIFFERENT P_D AND P_E VALUES

P_E \ P_D	1	2	5	10	20	30
1	1.3452	1.3153	1.3667	1.6534	1.6370	1.7899
3	1.1072	1.0907	1.1630	1.3939	1.3577	1.4847
10	0.7082	0.7037	0.7316	0.8914	0.8924	0.9595
50	0.5892	0.5859	0.6048	0.7403	0.7226	0.7979
200	0.6179	0.6152	0.6421	0.7733	0.7618	0.8276
300	0.5779	0.5804	0.6174	0.7567	0.7589	0.8375

The results in Tables 5.2 and 5.3 demonstrate that both the encryption and decryption processes have low execution times. This means that their computational costs are very

www.manaraa.com

low. Furthermore, changes in the combination of security keys do not significantly affect the execution time of the encryption and decryption processes. This indicates that the encryption or decryption time of the PFE encryption algorithm for any given image is almost independent of changes in the security keys.

5.3.3.2 Performance Comparison

To further verify the efficiency of the presented PFE algorithm, its image encryption execution time is compared with those of the previously mentioned algorithms such as the bit-plane encryption algorithm using exclusive-OR operations (BPE-XOR) [71], the selective bit-plane encryption algorithm using the AES algorithm (SBE-AES) [72], and the selective bit-plane encryption algorithm using the least significant bit-plane of images (SBE-LBP) [73].

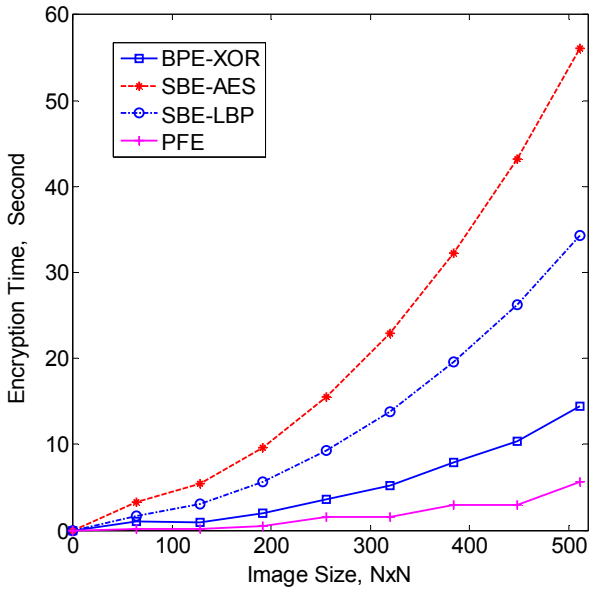


Figure 5.15: Performance comparison of different encryption algorithms. PFE indicates the presented PFE algorithm. This demonstrates the efficiency of the PFE algorithm for image encryption.

www.manaraa.com

A 512×512 grayscale Lena image is cropped into different images of varying sizes from 64×64 to 512×512. The images are then encrypted by the presented PFE, the BPE-XOR, the SBE-AES and the SBE-LBP algorithms, respectively. The encryption time is measured and plotted in Figure 5.15. The results are measured in a computer running the Windows XP operating system with 3GB memory and a CPU using Intel Core2 Quad Q6700 (2.66GHz/1066MHz/2X4MB L2).

In this example, the security keys of the presented PFE algorithm are $P_D = 2$ for the decomposition process and $P_E = 3$ for the encryption process. Security keys for the BPE-XOR algorithm are set to the initial register value of 20 and the shifting times are set to 10 for the Linear Feedback Shift Registers. For the SBE-AES and SBE-LBP algorithms, a 128-bit security key and the two most significant bit-planes are selected for encryption. All algorithms are implemented in Matlab codes.

Note that, for the sake of simplicity, this section uses these settings for all simulations, except for those cases with particular specifications.

The results in Figure 5.15 demonstrate that in the MATLAB implementation for image encryption the presented PFE algorithm outperforms the three existing methods. The results demonstrate that the PFE algorithm can encrypt images efficiently and also has the potential to perform in real-time applications such as wireless networks and communications.

www.manaraa.com

5.3.4 Security Analysis

Security is important not only for the encrypted objects but also for the encryption algorithms themselves. This section discusses some security issues of the presented PFE algorithm such as histogram and correlation analysis, key sensitivity testing, security key space, and several common attacks such as brute force attacks, noise attacks, and data loss attacks. The eight different-sized images shown in Figure 5.16 will be used as test images in this section.

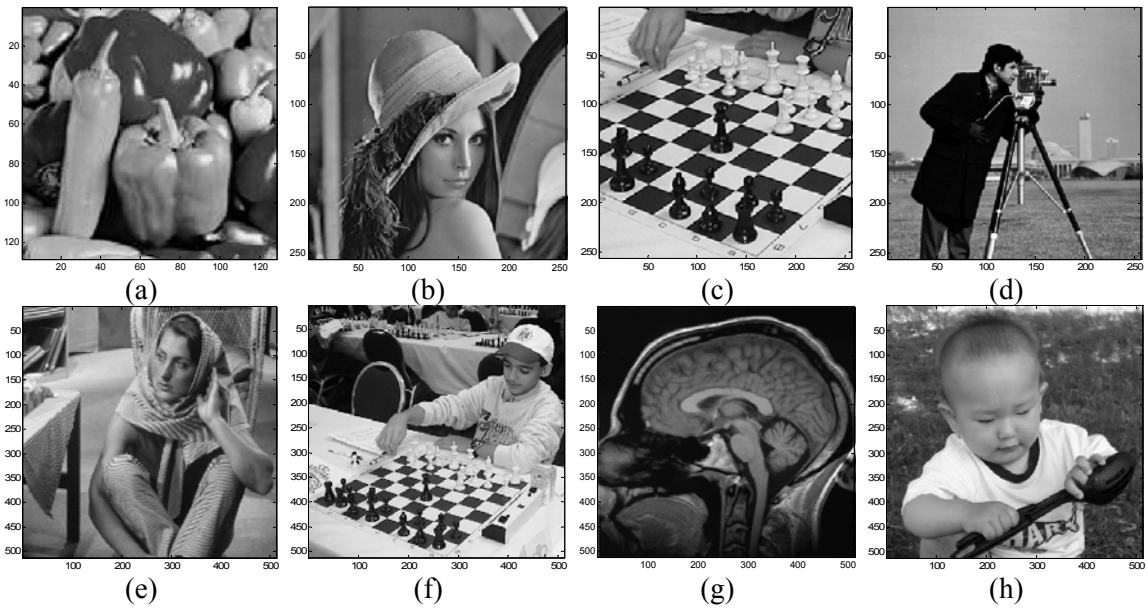


Figure 5.16: Test images with different sizes. (a) Pepper, 128×128; (b) Lena, 256×256; (c) Chess, 256×256; (d) Cameraman, 256×256; (e) Barbara, 512×512; (f) Chess player, 512×512; (g) Brain, 512×512; (h) Baby, 512×512.

5.3.4.1 Histogram Analysis

An image histogram is a graphic representation of the pixel intensity distribution of an image. To overcome the statistic attacks, the encrypted image should have a histogram with random behavior and uniform distribution [54, 56-58].

www.manaraa.com

Figure 5.17 gives an example of image encryption using the PFE algorithm. As can be seen, the encrypted image and its histogram are completely different from the original image. Visually, the encrypted image looks like a noise image. Its histogram has nearly uniform distribution that changes with different security keys. These demonstrate that the presented PFE algorithm has the ability to withstand the statistic attacks.

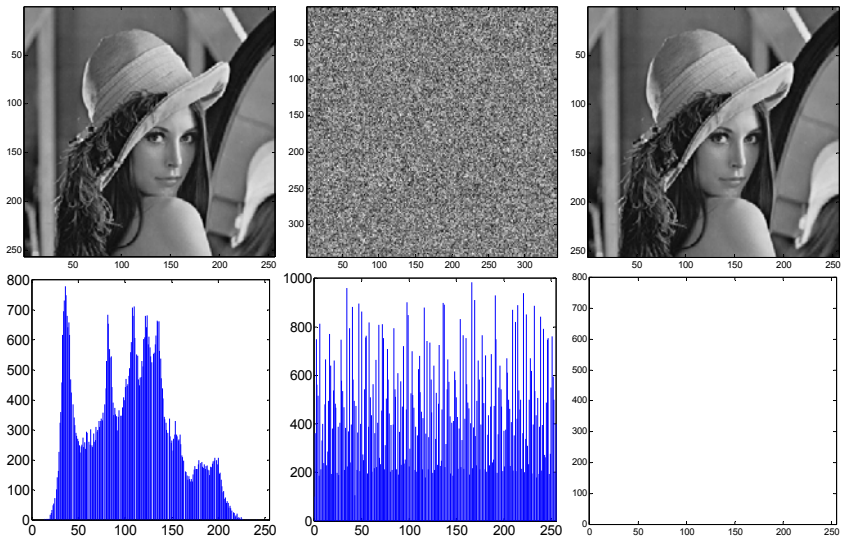
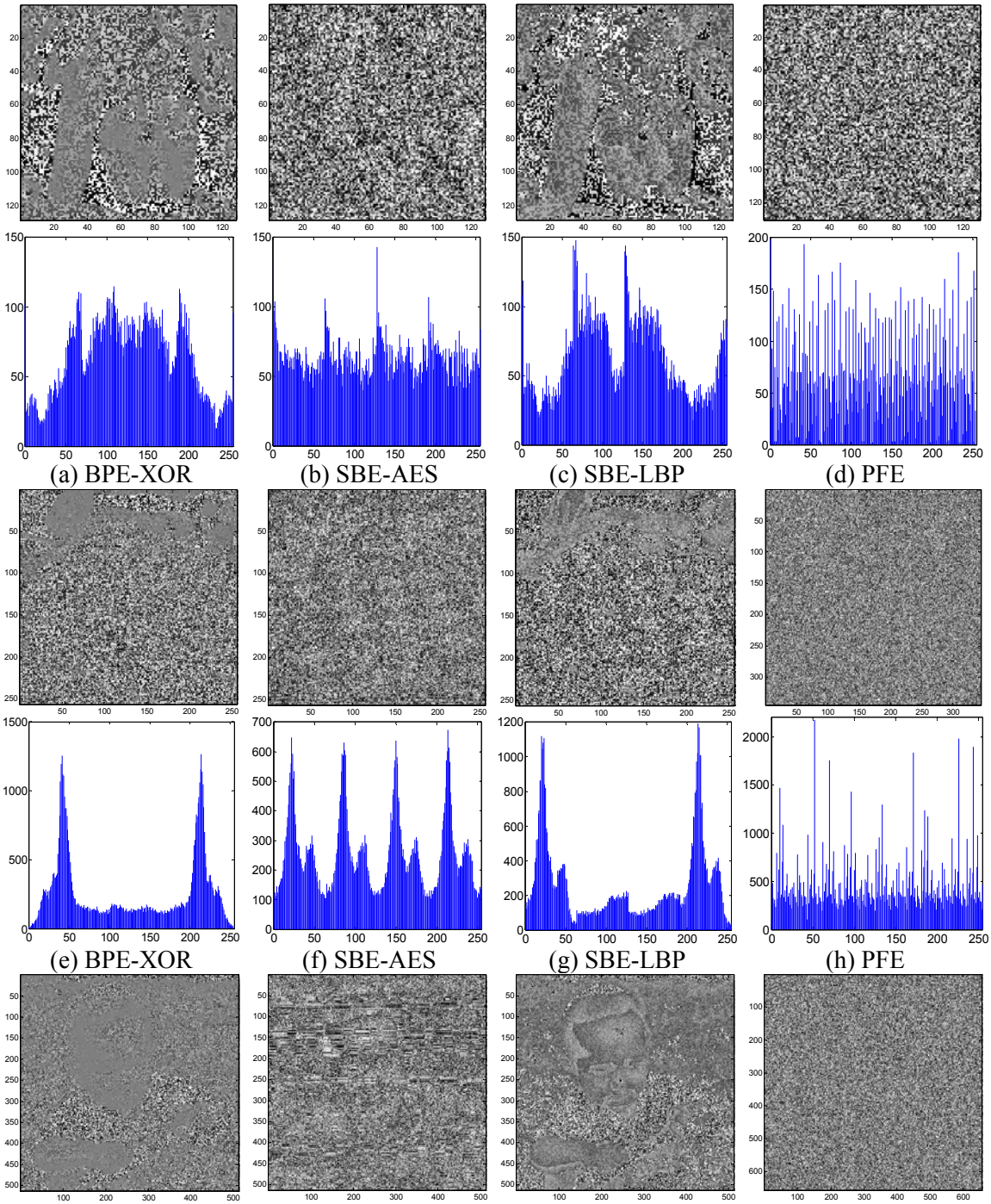


Figure 5.17: Image encryption using the PFE algorithm. (a) The original image and its histogram; (b) The encrypted image and its histogram; (c) The reconstructed image and the histogram of the difference between the reconstructed and original images.

Moreover, the reconstructed image in Figure 5.17(c) is visually the same as its original in Figure 5.17(a). Its SSIM value also demonstrates that they are identical. To further demonstrate quantitatively and graphically the difference between the reconstructed image and its original, the reconstructed image is subtracted from the original image pixel by pixel to generate a difference image. The histogram of the difference image given in Figure 5.17(c) demonstrates that all the pixels in the image are zeros, which proves that

www.manaraa.com

the reconstructed image is the same as the original. This is one of advantages of the presented PFE algorithm.



(a) BPE-XOR (b) SBE-AES (c) SBE-LBP (d) PFE

(e) BPE-XOR (f) SBE-AES (g) SBE-LBP (h) PFE

www.manaraa.com

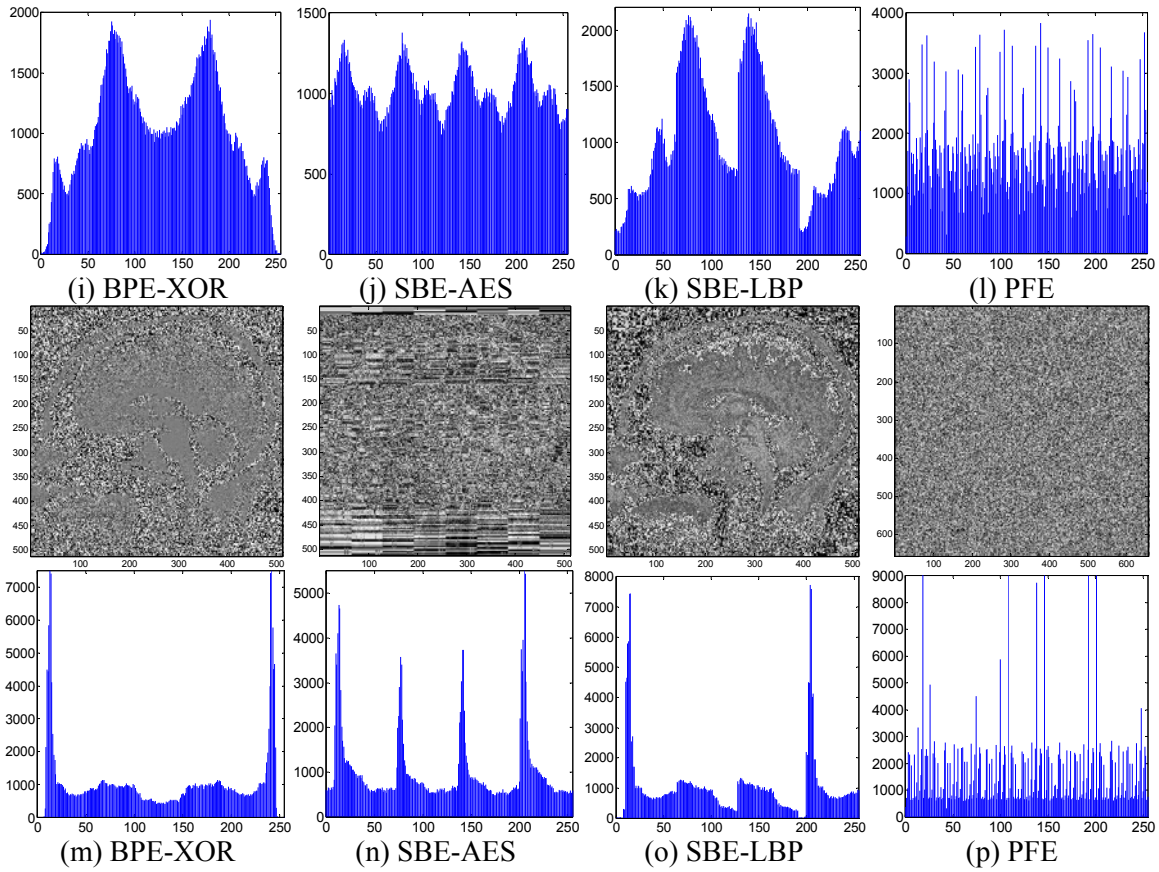


Figure 5.18: Comparison of the histograms of encrypted images as produced by different algorithms. The 1st column shows the images encrypted by the BPE-XOR and their histograms; the 2nd column shows the images encrypted by the SBE-AES and their histograms; the 3rd column shows the image encrypted by the SBE-LBP and their histograms; the 4th column shows the image encrypted by the presented PFE algorithm and their histograms. (a)-(d) shows the encrypted images of the "Pepper" image shown in Figure 5.16(a); (e)-(h) shows the encrypted images of the "Chess" image shown in Figure 5.16(c); (i)-(l) shows the encrypted images of the "Baby" image shown in Figure 5.16(h); (m)-(p) shows the encrypted images of the "Brain" image shown in Figure 5.16(g).

To compare the encryption performance of the presented PFE algorithm with those of the existing methods, four images are selected from Figure 5.16, and then encrypted using these algorithms, respectively. The encrypted images and their histograms are given in Figure 5.18. The resulting images encrypted by the BPE-XOR, the SBE-AES and the SBE-LBP algorithms contain some of the visual information of the original images. The

www.manaraa.com

intensity distribution of their corresponding histograms is inhomogeneous. However, the images encrypted by the presented PFE algorithm look visually like noise images. The histograms of these encrypted images are close to uniform distribution. This demonstrates that the performance of the presented PFE algorithm is superior to other methods in the face of statistic attacks.

5.3.4.2 Correlation Coefficient Analysis

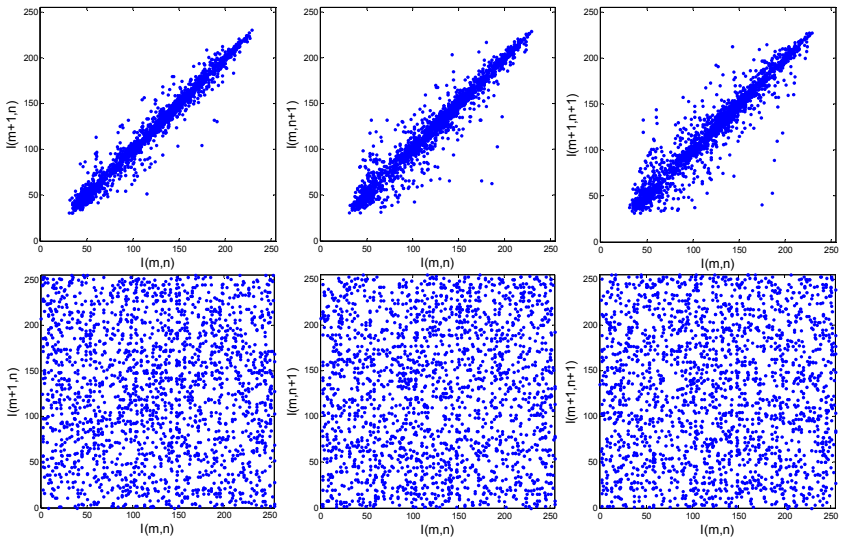
To further demonstrate how robust the presented PFE algorithm is when it comes to statistic attacks, this section analyzes the correlation between two horizontally, vertically and diagonally neighboring pixels in both the original and the encrypted images. The neighboring pixels are also called adjacent pixels in [54, 56-58].

First, this section analyzes the intensity distribution of two neighboring pixels in both the original image and the image encrypted by the presented PFE algorithm. 2048 sample pixels were randomly selected from the original image given in Figure 5.17(a) and the encrypted images from Figure 5.17(b), respectively.

Figure 5.19 plots the intensity distribution of these 2048 sample pixels and their horizontally, vertically and diagonally neighboring pixels. The top row in Figure 5.19 shows the intensity distributions of the pixels from the original image. The results demonstrate that the intensity values of neighboring pixels are equal or very close: their intensity distribution is located in or close to the diagonal line in the figures. The neighboring pixels in the original image are highly correlated. The bottom row in Figure 5.19 plots the distribution of pixels from the encrypted image. The results demonstrate

www.manaraa.com

that the neighboring pixels in the encrypted image have less correlation: their intensity values are spread out and are almost uniformly distributed across the entire data range of the image.



(a) Horizontal (b) Vertical (c) Diagonal

Figure 5.19: The pixel intensity distributions of two neighboring pixels at different directions in the original and encrypted Lena image from Figure 5.16. The top row shows the pixel intensity distributions of the original image; the bottom row shows the pixel intensity distributions of the encrypted image. (a) The pixel intensity distribution of two horizontally neighboring pixels, $I(m,n)$ and $I(m+1,n)$; (b) The pixel intensity distribution of two vertically neighboring pixels, $I(m,n)$ and $I(m,n+1)$; (c) The pixel intensity distribution of two diagonally neighboring pixels, $I(m,n)$ and $I(m+1,n+1)$. This demonstrates that the neighboring pixels at different directions in the encrypted image show less correlation and more random distribution in the entire data range.

To quantitatively assess the correlation of the neighboring pixels, the correlation coefficient of all horizontally, vertically and diagonally neighboring pixels in the original and encryption images are calculated. The correlation coefficient of two neighboring pixels is defined by [170, 171],

www.manaraa.com

$$r_{xy} = \frac{N\sum_{i=1}^{N} x_i y_i - \sum_{i=1}^{N} x_i \sum_{i=1}^{N} y_i}{\sqrt{\left(N\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2\right)\left(N\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2\right)}} \tag{92}$$

where x, y are the intensity values of two neighboring pixels and N is the total number of pixels selected from the image to be calculated, and $-1 \le r_{xy} \le 1$.

Two neighboring pixels x, y have a strong positive linear correlation if the correlation coefficient r_{xy} is close to +1. The positive values of the correlation coefficient r_{xy} indicate a relationship between two neighboring pixels x, y such that the values of x increase (or decrease) when the values of y increase (or decrease). However, a value of r_{xy} close to zero implies that there is a random, nonlinear relationship between the two neighboring pixels [171].

TABLE 5.4. CORRELATION COEFFICIENTS OF TWO NEIGHBORING PIXELS IN THE ORIGINAL AND ENCRYPTED IMAGES

Image Name	Original Image			Encrypted Image			Correlation Between two images
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	
Pepper	0.9147	0.9362	0.9351	-0.0036	-0.0016	0.0042	-0.0069
Lena	0.9401	0.9698	0.9699	-0.00087	0.0016	0.0028	-0.0019
Chess	0.9476	0.9071	0.9077	-0.00066	-0.0015	0.0028	0.000963
Cameraman	0.9343	0.9408	0.9412	0.0099	0.00081	0.005	0.000734
Barbara	0.8545	0.9539	0.9540	0.0043	0.0019	0.0045	0.000094
Chess player	0.9639	0.9475	0.9475	-0.00048	0.00053	0.0009	-0.0014
Brain	0.9866	0.9857	0.9857	-0.0013	-0.0011	0.001	-0.0033
Baby	0.9899	0.9846	0.9846	-0.00063	0.001	0.0022	0.000327

Table 5.4 gives the correlation coefficients of two horizontally, vertically and diagonally neighboring pixels for both the original images that appear in Figure 5.16 and the images encrypted by the presented PFE algorithm. The correlation coefficients of two

www.manaraa.com

neighboring pixels from the original images are close to one. This demonstrates that they have a strong positive relationship. However, the correlation coefficients of two neighboring pixels from the encrypted images are close to zeros, which means they have an extremely weak relationship.

To evaluate the relationship between the original images and the corresponding images encrypted by the presented PFE algorithm, the correlation coefficients of two pixels with the same locations in the original and encrypted images are calculated. They are given in the last column in Table 5.4. The results demonstrate that no linear correlation occurs between the original images and the encrypted image since the values of the correlation coefficients are close to zero.

TABLE 5.5. COMPARISON OF AVERAGE CORRELATION COEFFICIENTS OF TWO NEIGHBORING PIXELS FROM THE ORIGINAL AND ENCRYPTED IMAGES

Image Name	Original	BPE-XOR	SBE-AES	SBE-LBP	PFE
Pepper	0.9287	0.014825	0.03517	0.055918	-0.00153
Lena	0.9599	-0.00303	0.055022	0.050406	0.004461
Chess	0.9208	0.00216	0.026635	0.014548	0.001805
Cameraman	0.9388	0.001571	0.095544	0.093596	0.003426
Barbara	0.9208	-0.00307	0.024869	0.920733	0.00345
Chess player	0.9530	0.000844	0.040877	0.024003	0.000572
Brain	0.9860	-0.00063	0.205399	0.133599	0.000336
Baby	0.9864	0.001938	0.115748	0.053715	-0.0004
Average	**0.9493**	**0.001826**	**0.074908**	**0.168315**	**0.001515**

Table 5.5 compares the average values of the correlation coefficients of two neighboring pixels in three directions in both the original images and the images encrypted by four different algorithms. The results of all the original images are close to one. The fact that the correlation coefficients of the presented PFE algorithm's encrypted images are close to zero proves that the PFE algorithm outperforms other encryption algorithms. This is

www.manaraa.com

further confirmed by the average values of all the original images and of the images encrypted by each algorithm in the bottom row. This comparison further demonstrates that a strong relationship is presented between the neighboring pixels in the original image while a very weak correlation is present between the neighboring pixels in the images encrypted by the presented PFE algorithm.

5.3.4.3 Key Sensitivity Test

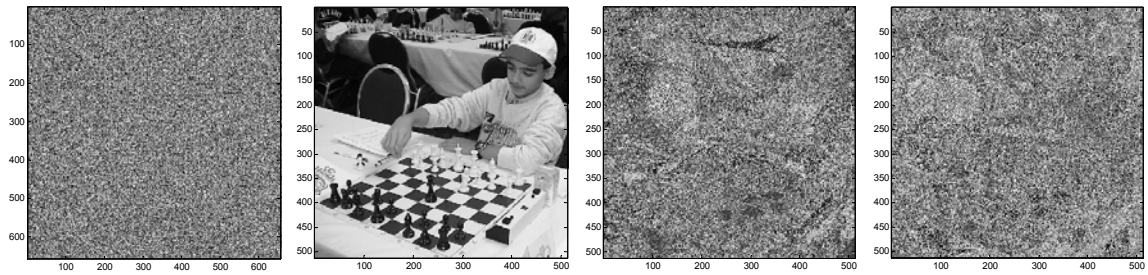
The security keys of the presented PFE algorithm are a combination of (1) P_D for image decomposition, (2) security key for bit-plane shuffling, (3) P_E for bit-plane encryption, and (4) the pixel value array for data mapping. These security keys are extremely important for the presented PFE algorithm. Users have the flexibility to choose the same or different security keys for both the decomposition and the encryption process. The number of the Fibonacci p-code bit-planes in the image decomposition process depends on the length of the Fibonacci p-code, which differs based on changes in the value of P_D.

An ideal encryption algorithm should be sensitive to changes in the security key [58]. A small change in the security key should result in a completely different encrypted image and vice versa. To test the key sensitivity of the presented PFE algorithm, different security keys are used to reconstruct the original image. Figure 5.20 gives an example. The image of the Chess player shown in Figure 5.16(f) is encrypted by the presented PFE algorithm, selecting $P_D = 3$ for the decomposition process and $P_E = 3$ for the encryption process, while reversing the order of the bit-planes for bit-plane shuffling. The original

www.manaraa.com

image is reconstructed using different P_D values for the decomposition process but keeping the security key P_E the same as it was in the encryption process.

The results given in Figure 5.20 verify that the original image can be reconstructed only when the correct security keys are used. Otherwise, the reconstructed images are completely different to their originals, even if P_D for the image reconstruction is only slightly different than it is for the image encryption, as the examples in Figures 5.20(c) and 5.20 (d). This demonstrates that the presented PFE algorithm is highly sensitive to changes in the security keys.



(a) (b) SSIM=1 (c) SSIM=0.03667 (d) SSIM=0.01756

Figure 5.20: Image reconstruction using the same P_E=*3* for the encryption process but different P_D for the decomposition process. (a) Encrypted image, $P_D = 3$; (b) Reconstructed image, $P_D = 3$; (c) Reconstructed image , $P_D = 5$; (d) Reconstructed image , $P_D = 0$. This demonstrates that the original image can be reconstructed completely only when the correct security keys are used.

5.3.4.4 Security Key Space

An $M \times N$ image is used here as an example to calculate the presented PFE algorithm's security key space. Assume that the security key P_D for the decomposition process has K_D possible choices. The number of the decomposed Fibonacci p-code bit-planes is n_B for a specific P_D. Since any new or existing method can be used for the bit-plane

www.manaraa.com

shuffling process, the maximum possible changes of bit-planes are $n_B!$ (the factorial of n_B). Assume that the possible choices of P_E for each bit-plane are K_E ($K_E \le M!N!$). The pixel value array for a specific image in the data mapping process is determined by the image decomposition and the bit-plane shuffling process. Therefore, the security key space for the presented PFE algorithm will be,

$$S = K_D n_B!\left(K_E\right)^{n_B} \le K_D n_B!\left(M!N!\right)^{n_B} \tag{93}$$

Table 5.6 gives examples of the key space based on the assumption of $K_E = 10$, the specific P_D values ($K_D = 1$) and a 64×64 grayscale image. This demonstrates that the security key space of the presented PFE algorithm is sufficiently large.

TABLE 5.6. SECURITY KEY SPACES WITH DIFFERENT P_D VALUES

P_D	0	1	2	3	…
n_B	8	12	15	19	…
$n_B!$	8!	12!	15!	19!	…
K_E	10	10	10	10	…
S	4.03×10^{12}	4.79×10^{20}	1.31×10^{27}	1.22×10^{36}	…

5.3.4.5 Brute Force Attacks

In cryptanalysis, the brute force attack [172] is an attack model in which the attacker performs an exhaustive search for all the possibilities of the encryption algorithm's security keys in order to guess what may be the correct security keys. Theoretically, this approach is feasible if the key space of the encryption algorithm is limited and the attacker knows the encryption algorithm.

www.manaraa.com

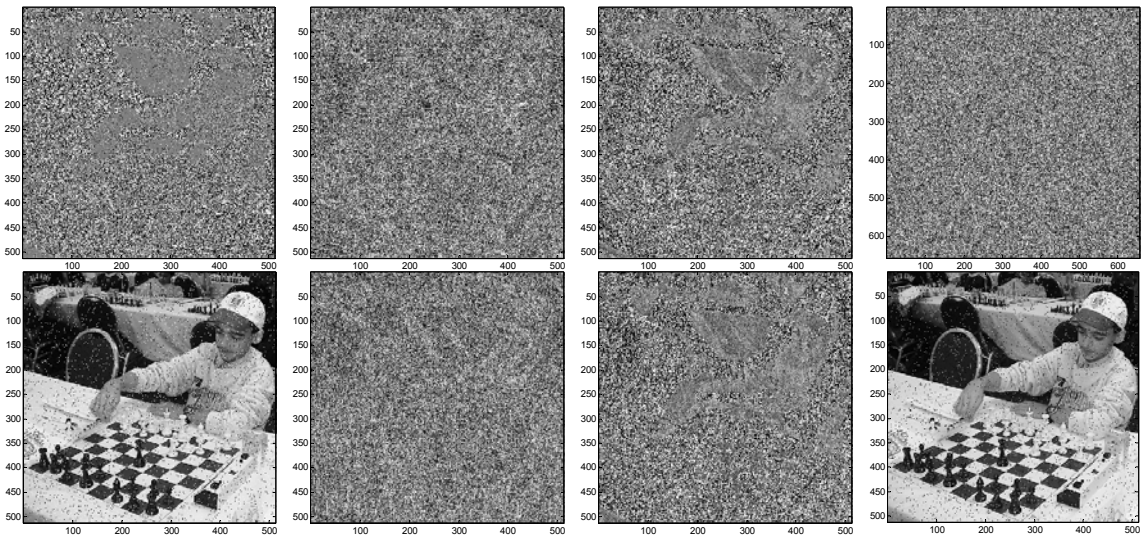
Based on the results of Table 5.6, the security key space of the presented PFE algorithm is large enough even if a specific value is selected for P_D and only 10 possible choices are chosen for P_E. As a result, it can be concluded that the presented PFE algorithm is able to withstand the brute force attack.

5.3.4.6 Noise Attacks

Communication and networking channels are generally subject to different types of noise. To test the robustness of the presented PFE algorithm against noise attacks, it can be compared to other existing bit-plane decomposition based encryption methods. The original image given in Figure 5.16(f) is encrypted using these encryption algorithms individually. The Salt & Pepper noise with a density of 0.05 is added to the encrypted images. The original image is then reconstructed from the noised encrypted images. The SSIM index is used to quantitatively evaluate the similarity between the reconstructed images and the original images. Figure 5.21 gives the results.

As shown in Figures 5.21(b) and (c), the original image cannot be reconstructed for the SBE-AES and SBE-LBP algorithms. The presented PFE algorithm and the BPE-XOR are able to reconstruct the original images although the images do show the presence of noise, as can be seen in Figures 5.21(a) and (d). The SSIM result of the presented PFE algorithm is higher than that of the BPE-XOR. This demonstrates that when it comes to resisting the noise attacks, the presented PFE algorithm performs better than other methods.

www.manaraa.com



(a) SSIM=0.4548 (b) SSIM=0.0204 (c) SSIM=0.0247 (d) SSIM=0.5068

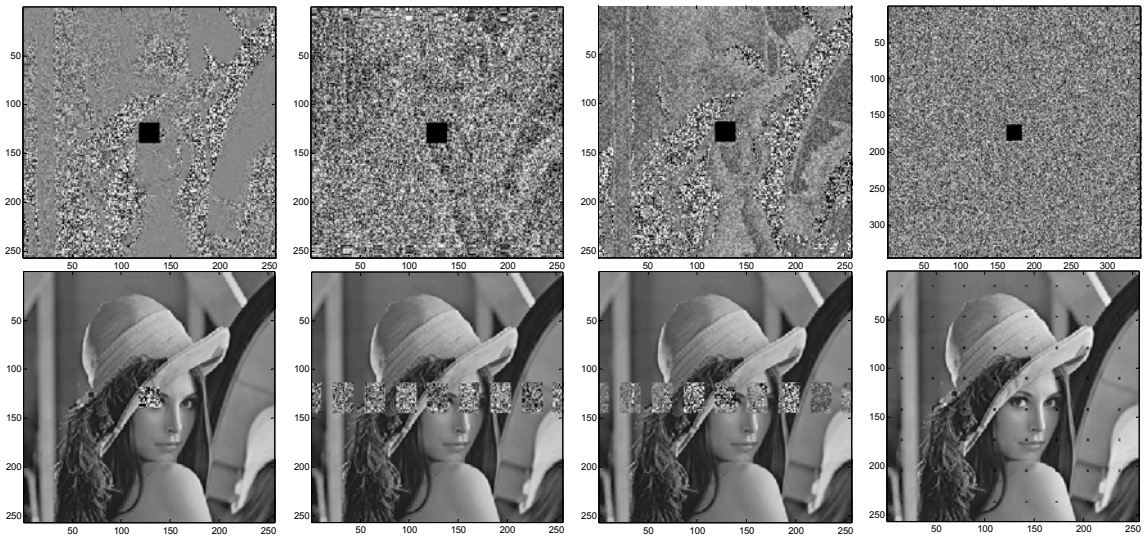
Figure 5.21: Performance comparison of different algorithms when subject to noise attacks. (a)-(d) shows the noised images encrypted by different algorithms and their corresponding reconstructed images. The top row shows the encrypted images with 0.05 Salt & Pepper noise added. The bottom row shows the reconstructed images from the corresponding noised encrypted images. (a) BPE-XOR; (b) SBE-AES; (c) SBE-LBP; (d) the presented PFE algorithm.

5.3.4.7 Data Loss Attacks

Data loss attacks can be used to test the encryption algorithm's ability to tolerate the risk of data loss in public media transmission channels.

The Lena image in Figure 5.16(b) was encrypted by the presented PFE algorithm and other existing methods. Pixel data within a 20×20 window at the center of the encrypted images was removed by replacing them with zeros. The original image is then reconstructed from the encrypted images, which featured data loss. The SSIM index measure was then used to evaluate the reconstructed images. The results are given in Figure 5.22.

www.manaraa.com



(a) SSIM=0.98942 (b) SSIM=0.88361 (c) SSIM=0.8921 (d) SSIM=0.96063

Figure 5.22: Comparison of performance of different algorithms subject to data loss attacks. (a)-(d) shows the images encrypted by different algorithms with data loss and the corresponding reconstructed images. The top row shows the encrypted images with data removal within a 20×20 center window. The bottom row shows the reconstructed images. (a) BPE-XOR; (b) SBE-AES; (c) SBE-LBP; (d) The presented PFE algorithm.

All the reconstructed images in the bottom row of Figure 5.22 contain the most information from the original image. These algorithms demonstrate a high performance level when it comes to resisting data loss attacks. Compared to other methods, however, the presented PFE algorithm preserves more visual information from the same data loss attack. The presented PFE algorithm's reconstructed image is more visually pleasing than those of the other algorithms, even though its SSIM value is slightly lower than that of the BPE-XOR. This demonstrates that the presented PFE algorithm outperforms other methods when subject to data loss attacks.

5.3.4.8 Plaintext Attacks

The plaintext is the original information to be encrypted. The ciphertext is the plaintext encrypted by an encryption algorithm. Two types of plaintext attacks exist: the known-

www.manaraa.com

plaintext attack and the chosen-plaintext attack [172, 173]. In chosen-plaintext attacks, the attacker has the flexibility to choose any type of useful information as plaintext in order to deduce the encryption algorithm's security keys or to reconstruct the original plaintexts from the unknown ciphertexts. If an encryption algorithm does not change the image data, it is highly possible that an attacker will be able to break the encrypted images, either partially or entirely, using plaintext attacks without knowing the encryption algorithm and its security keys.

In the presented encryption algorithm, the image data has been changed in the following four steps: (1) shuffling the order of all bit-planes; (2) scrambling pixel positions in the encryption process if the P_E is different for each bit-plane; (3) combining all encrypted bit-planes back to the gray levels using binary numeral system; (4) mapping the encrypted image data back into the grayscale image data range (between 0 and 255) using a data mapping function in equation (91). Therefore, the presented PFE algorithm changes both the image pixel locations and the intensity values. It does, therefore, have the ability to withstand plaintext attacks.

www.manaraa.com

5.4 Selective Object Encryption Using Truncated Fibonacci P-code Bit-plane Decomposition

This section investigates the application of Fibonacci P-code bit-plane decomposition for selective object encryption.

The Fibonacci p-code bit-plane decomposition has a large number of zero bit-planes as the p values increase. These zero bit-planes do not significantly enhance the security of the encryption algorithm but require higher computational costs. To avoid the redundancy of the Fibonacci p-code bit-plane decomposition, a new selective object encryption algorithm is introduced using the Truncated Fibonacci p-code bit-plane decomposition. Simulation results are given to show the performance of the new algorithm.

5.4.1 The New Selective Object Encryption Algorithm

2D images such as grayscale images, biometric images and medical images contain 2D data matrices. To improve the speed of the encryption process while protecting private information, one solution is to encrypt just an important part or region of an image. In order to encrypt selected objects, this section introduces a new encryption algorithm called "ObjectEcrypt". The selected object can be defined as an object in, a specific region of, or a selected part/region of an image or an entire image. Figure 5.23 shows the ObjectEcrypt algorithm. It can be used in real-time applications such as wireless networks and mobile phone services.

www.manaraa.com

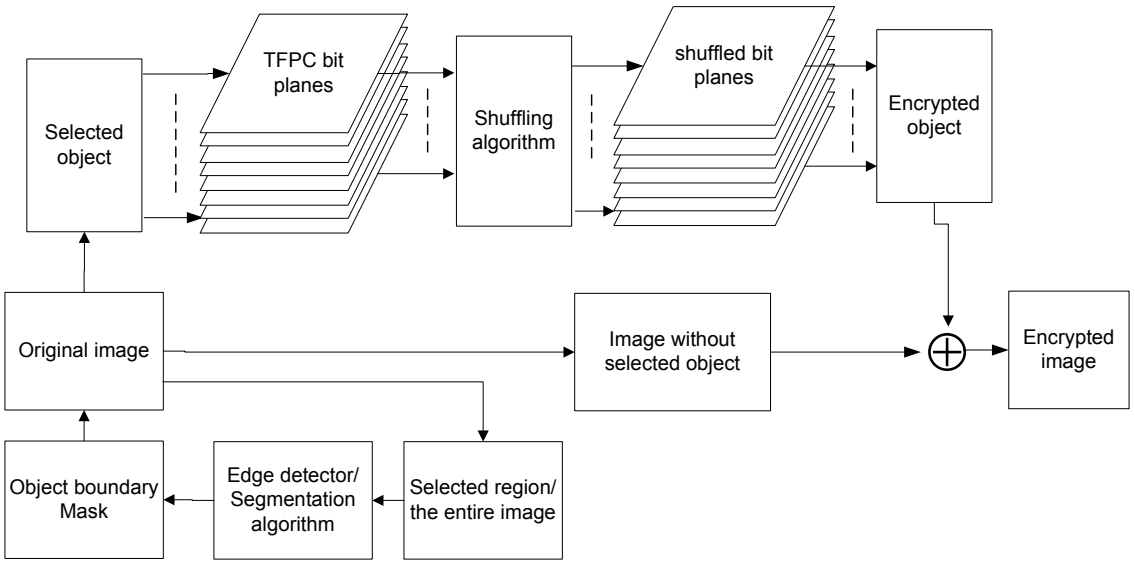


Figure 5.23: Block diagram of the ObjectEcrypt algorithm.

The ObjectEcrypt algorithm first creates a boundary mask of the selected object using an edge detector or segmentation algorithm. In this section, Canny edge detector is used to generate the object boundary mask. The algorithm then uses this mask to separate the original image into the selected object and the image without the object. The selected object is then decomposed into several TFPC bit-planes based on the specified parameter p. The parameter p, which has a large number of possible choices, can act as one of the ObjectEcrypt algorithm's security keys. An existing or new shuffling algorithm is used to shuffle the order of TFPC bit-planes. By combining all the shuffled bit-planes and scaling down all pixel values back to the range of gray levels, the encrypted object can then be obtained. Finally, in order to acquire the resulting encrypted image, the encrypted object is combined with the image from which the object was removed originally.

Users also have the flexibility to choose any new or existing method for the bit-plane shuffling process, such as inverting the order of the bit-planes. This section chooses the

www.manaraa.com

right-round shift to shuffle the order of TFPC bit-planes. To make the shifted TFPC of each image pixel satisfy the constraint in equation (90), p zero bit-planes are added in front of the most significant bit-plane before shifting all the TFPC bit-planes. Figure 5.24 shows the shift algorithm. The shifting process moves all bit-planes one bit position to their right side, while the p^{th} zero bit-plane is shifted to the position of the least significant bit-plane in the TFPC bit-planes. If the shifting times $r > 1$, the shifting process will move all bit-planes r bit positions.

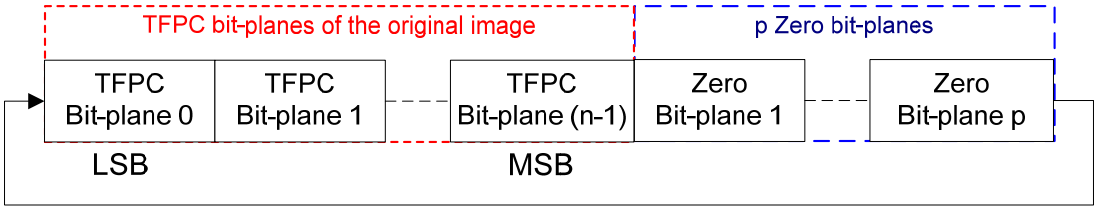


Figure 5.24: Block diagram of the shifting algorithm.

The ObjectEcrypt algorithm's security keys consist of the parameter p in the TFPC, the security keys in the shuffling algorithm and the information of the encrypted object, including the boundary mask and the data range before it was scaled down. In this section, the number of times to shift, parameter r, is the security key of the shifting algorithm. The shifting times r should be less than the sum of the parameter p and the number of TFPC bit-planes, i.e. $r < p + n$. These must be provided to authorize users who wish to implement the decryption process.

To reconstruct the original object/image in the decryption process, the encrypted object is extracted from the encrypted images using the object boundary mask. It is first scaled up to the original data range and decomposed to TFPC bit-planes. The order of these TFPC

www.manaraa.com

bit-planes is changed back to the original order using the left-round shift. By converting the TFPC bit-planes back to gray levels, the reconstructed image can be obtained.

3D images such as color images and 3D medical images contain several 2D data matrices called 2D components. By applying the ObjectEcrypt algorithm to its 2D components individually, the objects in 3D images can be encrypted.

5.4.2 Simulation Results

The selected object can take the form of an entire image or an object from a specific region within the image. This section provides examples of both these cases in order to demonstrate the performance of the ObjectEcrypt algorithm when it comes to encrypting selected objects in 2D and 3D images.

5.4.2.1 Object Encryption in 2D Images

Figure 5.25 gives an example of grayscale image encryption using the ObjectEcrypt algorithm with security keys of $p = 2, r = 5$. Figure 5.26 gives a medical image encryption example, $p = 2, r = 4$. The objects in these two examples are defined as entire images. In both examples, the ObjectEcrypt algorithm has encrypted the original images fully. The encrypted images in Figures 5.25(b) and 5.26(b) are unrecognizable.

The examples in Figures 5.25(c) and 5.26(c), which visually appear to be the same as their originals, verify that the original images can be completely reconstructed without distortion. Their corresponding histograms in Figures 5.25(f) and 5.26(f) also bear witness to this perfect reconstruction.

www.manaraa.com

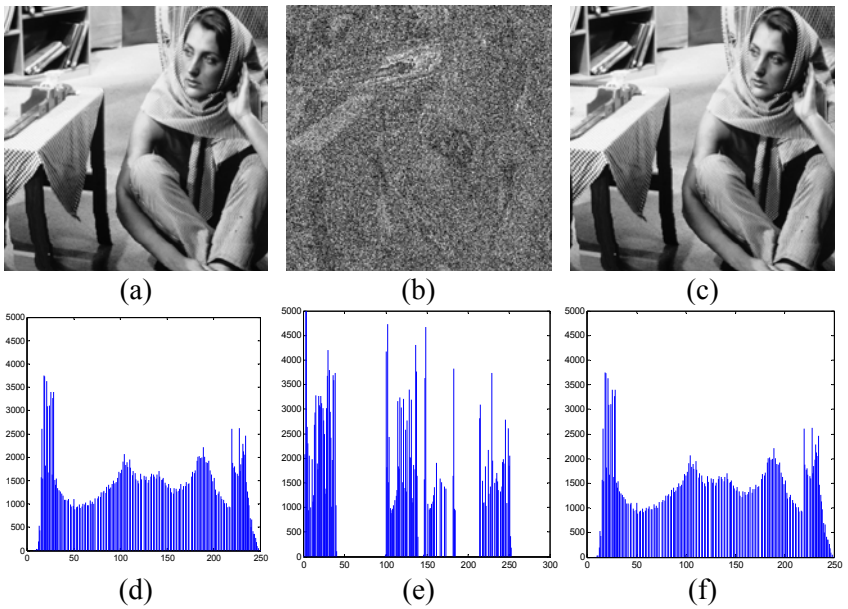


Figure 5.25: Grayscale image encryption, $p=2, r=5$. (a) Original grayscale image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the encrypted image.

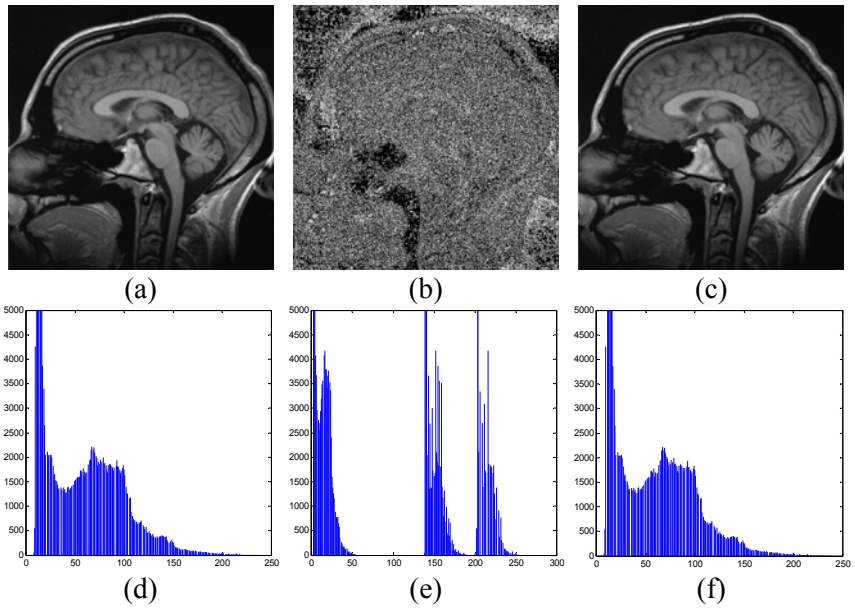


Figure 5.26: Medical image encryption, $p=2, r=4$. (a) Original medical image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the encrypted image.

www.manaraa.com

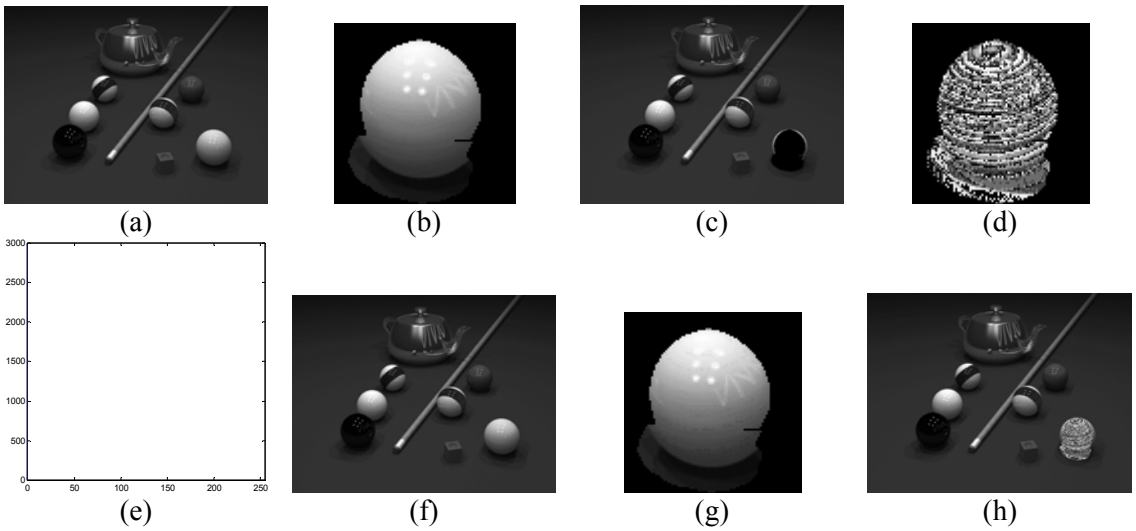


Figure 5.27: Selected object encryption in a grayscale image, $p=1, r=5$. (a) Original grayscale image; (b) Selected object; (c) Image without the selected object; (d) Encrypted image of the selected object; (e) Encrypted image; (f) Reconstructed object; (g) Reconstructed image; (h) Histogram of the difference between (a) and (g).

To achieve the goal of privacy protection in real-time applications, it is not necessary to encrypt the entire image/video. Instead, selectively encrypting important objects/regions in the image/video is an effective scheme. These important objects/regions usually contain private information such as human faces, fingerprints or patient's medical records, as well as text-based personal information. Figure 5.27 gives an example of the ObjectEcrypt algorithm for selected object encryption. Only the selected object has been fully protected. As a result, the computational cost of the encryption process is significantly less. This means that the ObjectEcrypt algorithm is well suitable for privacy protection in real-time applications.

The example in Figure 5.27 shows that both the selected object and the original image are fully recovered.

www.manaraa.com

5.4.2.2 Object Encryption in 3D Images

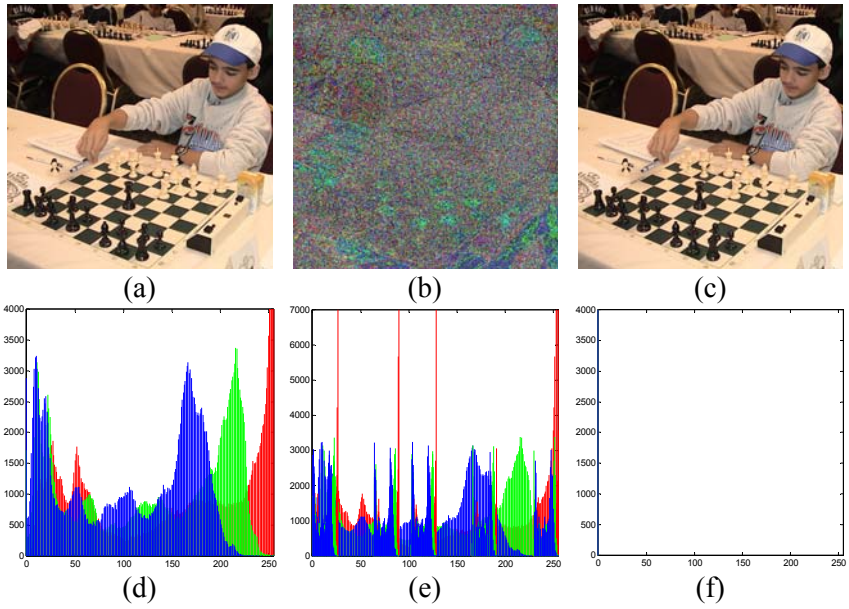


Figure 5.28: Color image encryption, $p=1, r=4$. (a) Original color image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the difference between (a) and (c).

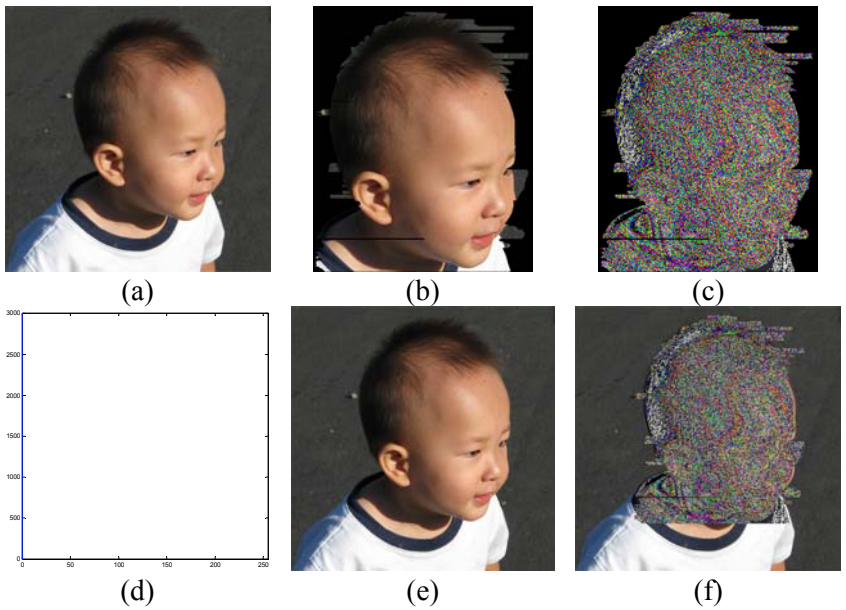


Figure 5.29: Selected object encryption in a color image, $p=3, r=5$. (a) Original grayscale image; (b) Selected object; (c) Encrypted image of the selected object; (d) Encrypted image; (e) Reconstructed image; (f) Histogram of the difference between (a) and (f).

www.manaraa.com

It is possible to encrypt the selected 3D objects by applying the ObjectEcrypt algorithm to their corresponding 2D components one by one. Figure 5.28 gives an example of the encryption of a color image defined as an object. Figure 5.29 shows the performance of the ObjectEcrypt algorithm for the selected 3D object encryption. The results prove that the ObjectEcrypt algorithm can protect private information while the original image/object remains completely recoverable.

5.4.3 Security Analysis

This section discusses security issues associated with the ObjectEcrypt algorithm such as security key space and plaintext attacks.

5.4.3.1 Security Key Space

The security key of the ObjectEcrypt algorithm is composed of the parameter p of the TFPC, the shifting times r of the shifting algorithm (given in this section) and the information of the encrypted object. The parameter p of the TFPC has a large number of selectable variations. The number of the TFPC bit-planes change as the value of p changes. Based on the discussion in Section 5.4.1, the shifting times r is less than the sum of the parameter p and the number of TFPC bit-planes ($r < p + n$). Thus, the parameter r also has a large number of possible choices. Furthermore, the selected object changes as its regions and the different ways of generating its boundary mask change. All these ensure that the possible number of combinations of the security keys for the ObjectEcrypt algorithm is sufficiently large. As a result, the algorithm has an extremely large security key space, which means that it is able to resist brute force attacks.

www.manaraa.com

5.4.3.2 Plaintext Attacks

Users have the flexibility to define the object to be encrypted as an entire image, a specific part or region of an image or as an object in an image or in a selected region of an image. They are also allowed to select any desired edge detection method or segmentation algorithm to obtain the object boundary mask. Therefore, the selected object is unpredictable and user-dependent. To encrypt the selected object, the ObjectEcrypt algorithm changes all the pixel data in the selected object by shuffling the order of its TFPC bit-planes. The data of the encrypted object is not useful for the purpose of plaintext attacks. As a result, the selected object is protected by a high level of security. The ObjectEcrypt algorithm can withstand plaintext attacks.

www.manaraa.com

5.5 The *(n, k, p)*-Gray Code and its Decomposition for Image Encryption

Both existing bit-plane decomposition based encryption methods and the encryption algorithms based on Fibonacci p-code bit-plane decomposition work only on binary bit-planes. This section introduces arbitrary based bit-planes for image encryption and investigates the applications of the *(n, k, p)*-Gray code in image encryption.

Using the *(n, k, p)*-Gray code bit-plane decomposition, this section introduces a new image encryption algorithm. Simulation results and a comparison are then given to demonstrate the performance of the new image encryption algorithm.

5.5.1 The New Image Encryption Algorithm

The basic idea of the new image encryption algorithm is to decompose images into the *(n, k, p)*-Gray code bit-planes, change the image pixel values of each bit-plane using the mod operation, shuffle the order of all *(n, k, p)*-Gray code bit-planes and pixel locations inside each bit-plane and combine all *(n, k, p)*-Gray code bit-planes to obtain the encrypted image. Figure 5.30 shows the new image encryption algorithm.

The new algorithm contains four processes: image decomposition, data encryption, bit-plane shuffling and pixel scrambling. First, it decomposes the original image with a size of $M \times N$ into several *(n, k, p)*-Gray code bit-planes using parameters, n_D and p_D. Then,

www.manaraa.com

it encrypts pixel data in each *(n, k, p)*-Gray code bit-plane using a mod operation defined by,

$$E(i,j) = (I(i,j) + Y(i,j)) \bmod n_D \tag{94}$$

where $I(i,j)$ and $E(i,j)$ are the pixel intensity values with location (i,j) in the original and encrypted *(n, k, p)*-Gray code bit-plane, respectively. n_D is the base of the *(n, k, p)*-Gray code in the image decomposition process. $Y(i,j)$ is the security key plane generated from the chaotic logistic map defined by,

$$\begin{cases} Y(i,j) = x\left[N(i-1)+j\right] \\ x(m) = rx(m-1)\left[1-x(m-1)\right] \end{cases} \tag{95}$$

where $1 \le i \le M$, $1 \le j \le N$, parameters in the chaotic logistic map $1 \le m \le MN$, $0 < x_0 < 1,\ 3.5699456 < r \le 4$ (as defined in [174]).

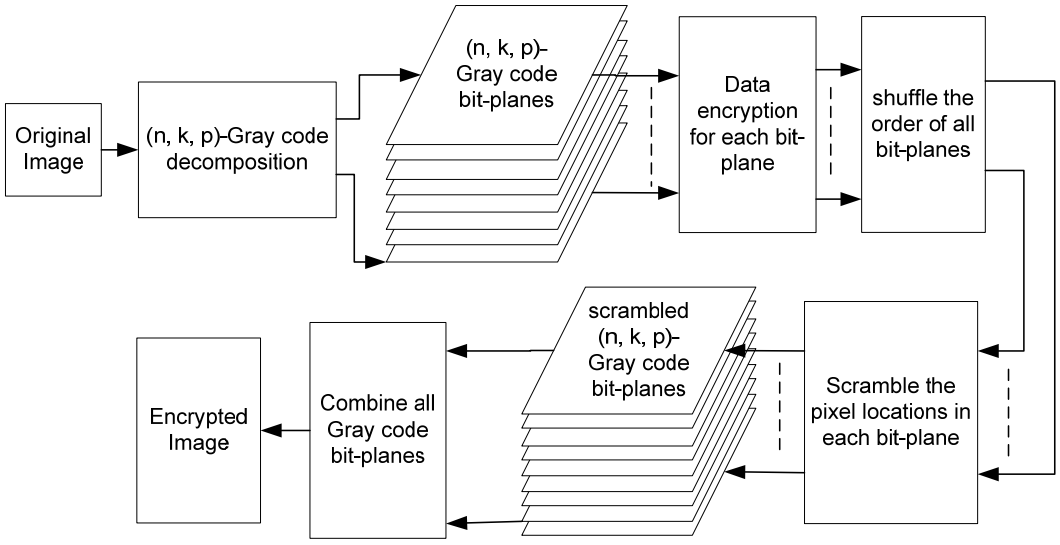


Figure 5.30: The image encryption algorithm using the *(n, k, p)*-Gray code bit-plane decomposition.

www.manaraa.com

Thirdly, the order of all bit-planes is shuffled by means of a shuffling method. Fourthly, the locations of all pixels in each bit-plane are scrambled using an image scrambling algorithm. The final encrypted image is obtained by combining all the scrambled *(n, k, p)*-Gray code bit-planes.

The security keys of the presented image encryption algorithm consist of the parameters in its four processes: (1) n_D and p_D for the image decomposition process; (2) x_0 and r in the logistic map for the data encryption process; (3) parameters for the bit-plane shuffling process; (4) parameters for the pixel scrambling process. Users have the flexibility to choose different security keys for each bit-plane in the pixel scrambling process, achieving a higher level of security.

To reconstruct the original image, authorized users should be provided with the correct combination of the security keys. The decryption process will first decompose the encrypted image into the *(n, k, p)*-Gray code bit-planes using n_D and p_D, then unscramble pixels in each bit-plane, then revert the order of the bit-planes back into its original, then apply a mod operation to each bit-plane using the security key plane obtained from the logistic map with parameters x_0 and r, and finally it will combine all the *(n, k, p)*-Gray code bit-planes to obtain the resulting reconstructed image.

In the decomposition process, the decomposition results and the number of the *(n, k, p)*-Gray code bit-planes are parameter-dependent and will change based on different parameters, n_D and p_D. The attackers will thus have difficulty predicting the decomposed results. Furthermore, the decomposed results will directly affect the

www.manaraa.com

performance of other processes in the running of the presented encryption algorithm. The original images will not be completely reconstructed if the user does not correctly decompose the encrypted image into their *(n, k, p)*-Gray code bit-planes, thereby achieving a higher level of security.

The data encryption process is designed to change image data using a mod operation similar to the XOR operation in the binary number system. The advantage of the mod operation is that it works on the arbitrary base and is able to change pixel values in each bit-plane without changing pixel data range. Furthermore, the security key plane is parameter dependent and changes as the parameters change in chaotic logistic map, x_0 and r.

By rearranging the order of the (n, k, p)-Gray code bit-planes, the bit-plane shuffling process is set to change the image pixel values. The pixel scrambling process is used to change the pixel locations in each (n, k, p)-Gray code bit-plane. Users have the flexibility to select any method (1) to shuffle the order of the bit-planes; (2) to change the pixel locations.

5.5.2 Simulation Results and Analysis

Since the presented image encryption algorithm offers users the flexibility to choose any existing or new method for shuffling the order of all the *(n, k, p)*-Gray code bit-planes and for scrambling pixel locations in each bit-plane, this section studies two different cases. Case #1 will demonstrate the use of the new *(n, k, p)*-Gray code Transforms for the bit-plane shuffling process and for performing pixel scrambling. Case #2 has been

www.manaraa.com

selected to demonstrate an existing approach to the shuffling and pixel scrambling processes. This should reveal how the presented encryption algorithm is adaptable to a variety of approaches. Note, $x_0 = 0.32$ and $r = 3.65$ are used for the chaotic logistic map in all simulations in this section.

***Case #1*:**

- For the bit-plane shuffling process, the order of all the *(n, k, p)*-Gray code bit-planes is reversed and then shuffled using the *(n, k, p)*-Gray code Transform provided in definition 4.5 in Chapter 4. The parameters of the *(n, k, p)*-Gray code Transform are called n_S and p_S.

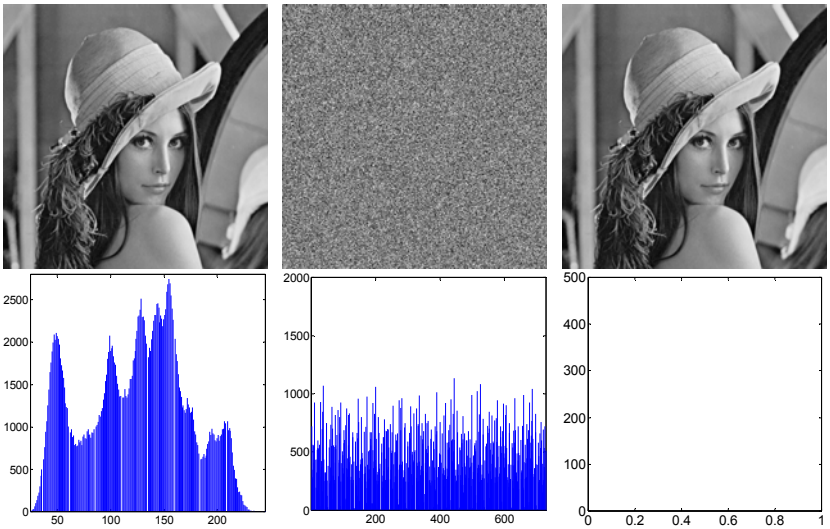
- The 2D P-recursive Transform from definition 4.9 in Chapter 4 with the recursive sequence selected to *(n, k, p)*-Gray code is used to scramble pixels in each bit-plane. Its parameters are called n_D and p_D.

For simplicity, the same base n and parameter p values are selected for image decomposition and for the bit-plane shuffling processes as well as for each bit-plane in the pixel scrambling process in the simulations, i.e. $n_D = n_S = n_E$, $p_D = p_S = p_E$.

Figure 5.31 gives an example of image encryption based on Case #1 with security keys: $n_D = n_S = n_E = 3$, $p_D = p_S = p_E = 6$ for image decomposition, for the bit-plane shuffling process and for all the *(n, k, p)*-Gray code bit-planes in the pixel scrambling process. The original image is fully encrypted (as shown in Figure 5.31(b)) and completely reconstructed (as shown in Figure 5.31(c)). The recovered image is visually the same as

www.manaraa.com

the original. The histogram of the difference between the reconstructed image and the original image in Figure 5.31(c) verifies this perfect reconstruction, since the difference between them is zero.



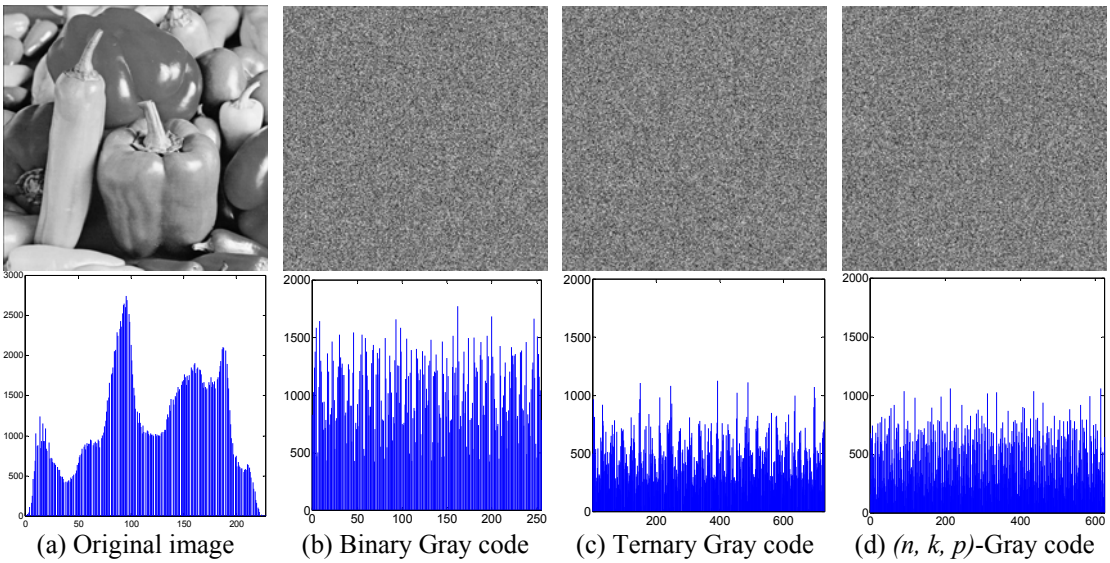
(a) (b) (c)

Figure 5.31: Case #1 Image encryption using the *(n, k, p)*-Gray code. (a) The original image and its histogram; (b) The encrypted image and its histogram, n=3, k=6, p=6; (c) The reconstructed image and the histogram of the difference between the reconstructed image and the original image.

Figure 5.32 shows several encrypted results using Case #1 with different base *n* and parameter *p* values. The original grayscale image (Figure 5.32(a)) is encrypted by the binary-reflected Gray code (Figure 5.32(b)) and the traditional ternary Gray code (Figure 5.32(c)), both of which are examples of the traditional *(n, k)*-Gray code. Figure 5.32(d) shows the encrypted result obtained by the new *(n, k, p)*-Gray code. As can be seen, the encrypted images are completely unrecognizable when compared to the original image. Visually, they look like noise images and their histograms are close to a uniform distribution. This ensures that unauthorized users have difficulty to decrypt the encrypted images. The encrypted images change with different base *n* and parameter *p* values, a fact

www.manaraa.com

that can be verified by their corresponding histograms. These encryption results and their histograms demonstrate that good encryption results can be obtained when the base *n* and p values change. The new *(n, k, p)*-Gray code demonstrates a superior performance when it comes to image encryption compared to other traditional Gray codes.



(a) Original image (b) Binary Gray code (c) Ternary Gray code (d) *(n, k, p)*-Gray code

Figure 5.32: Case #1 Image encryption using different types of Gray codes. (a) is the original image and its histogram; (b)-(f) are the encrypted images and their corresponding histograms; (b) Binary-reflected Gray code ,n=2, k=8, p=0; (c) Ternary Gray code n=3, k=6, p=0; (d) Presented (n, k, p)-Gray code n=2, k=4, p=7.

In the presented encryption algorithm for Case #1, the base *n* and parameter *p* of the *(n, k, p)*-Gray code act as security keys for image decomposition, bit-plane shuffling and pixel scrambling processes. The combinations of these security keys are extremely important for authorized users who wish to recover the original images. An example of image reconstruction is given in Figure 5.33. The original image can be completely reconstructed, as shown in Figure 5.33(b), only when the correct combination of the security keys is utilized. This prefect reconstruction can be verified by the histogram of

www.manaraa.com

the difference between the original image and the reconstructed image shown in Figure 5.33(b). If the incorrect security keys are used, the reconstructed images are unrecognizable, as seen in Figure 5.33(c)-(d).

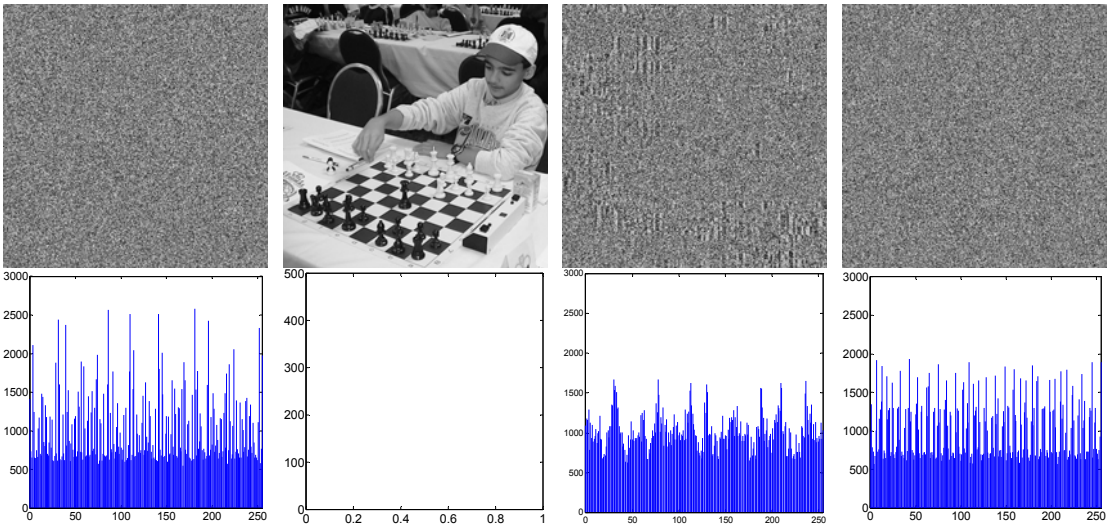


Figure 5.33: Case #1 Image reconstruction using different parameter p values. (a) encrypted image and its histogram, n=2, k=8, p=2; (b) reconstructed image and the histogram of deference between the reconstructed image and the original image, n=2, k=8, p=2; (c) reconstructed image and its histogram, n=2, k=8, p=1; (d) reconstructed image and its histogram, n=2, k=8, p=4.

The reconstructed results in Figure 5.33(c)-(d) may also lend themselves to an alternative direction for image encryption, namely, using one set of security keys to encrypt the original image and a different set of security keys to reconstruct the image so that the final encrypted image can be obtained. In this manner, the histogram of the encrypted image will be much closer to a uniform distribution. However, this method may incur unwanted computational costs since it will undoubtedly require more processes for image encryption and decryption than the algorithm being presented here.

www.manaraa.com

***Case #2*:**

- For bit-plane shuffling process, the order of all the *(n, k, p)*-Gray code bit-planes is reversed.

- The 2D cat map [56] is used to scramble the pixel locations in each *(n, k, p)*-Gray code bit-plane in the pixel scrambling process.

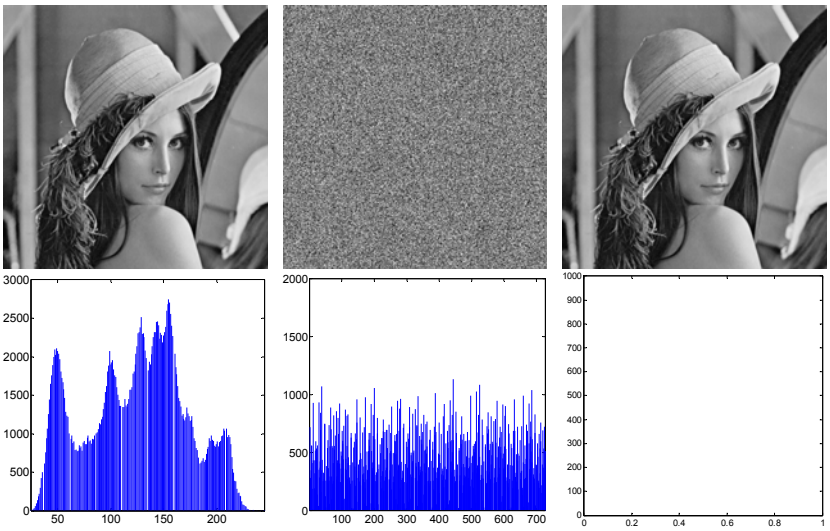


Figure 5.34: Case #2 Image encryption utilizing the *(n, k, p)*-Gray code. (a) The original image and its histogram; (b) The encrypted image and its histogram, n=3, k=6, p=6; (c) the reconstructed image and the histogram of the difference between the reconstructed image and the original image.

Figure 5.34 gives an encryption example of Case #2. The original image and the parameters for the image decomposition are the same as the example in Figure 5.31. The original image is fully encrypted and completely reconstructed. The encrypted image is visually similar to the noise image, while its histogram distribution is close to uniform – another advantage of the presented algorithm being presented here.

www.manaraa.com

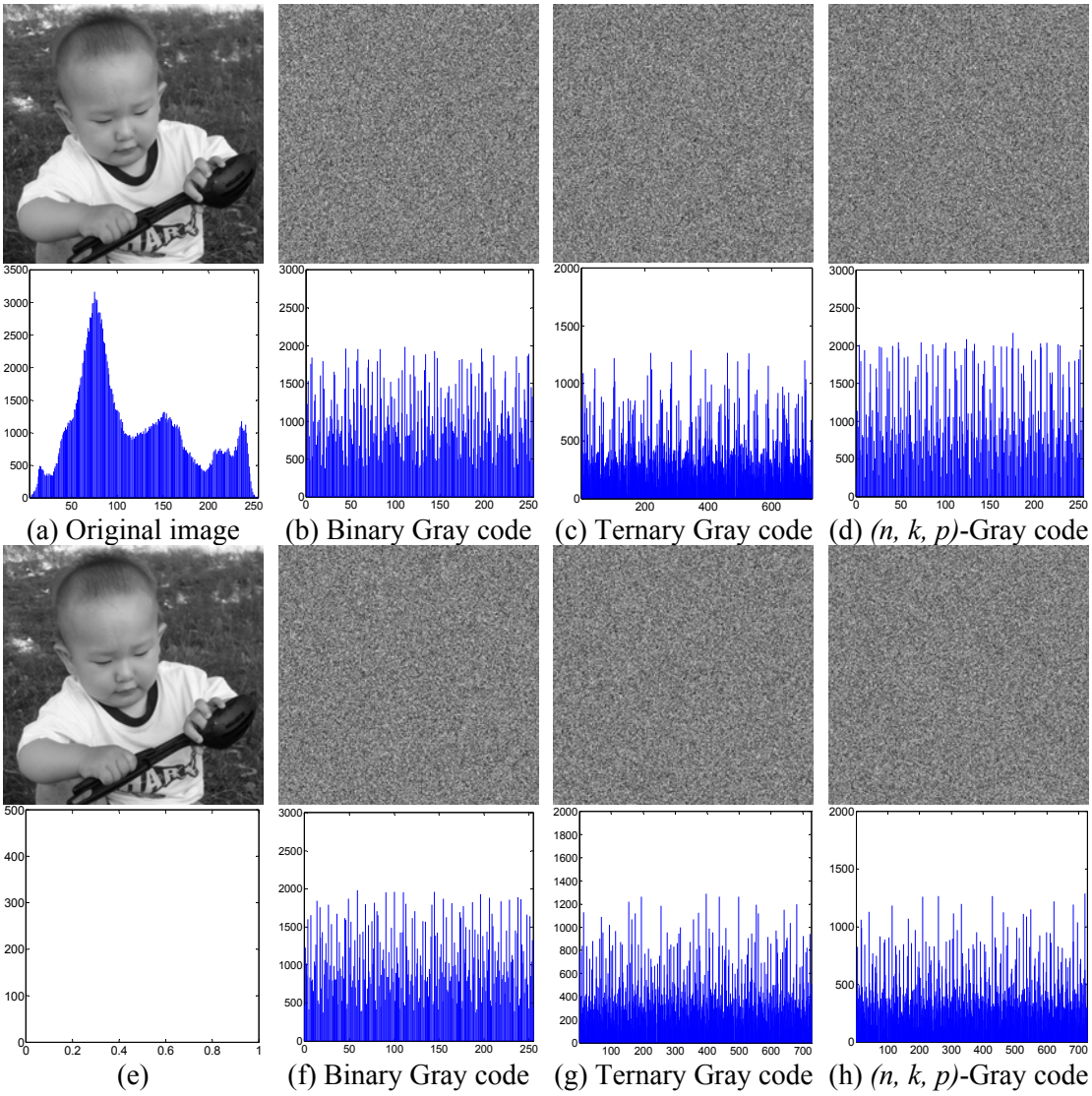


Figure 5.35: Comparison of image encryption using Case #1 and Case #2. (a) is the original image and its histogram; (e) is the reconstructed image and the histogram of the difference between the images in (a) and (e); (b)-(d) are the encrypted images using Case #1 and their corresponding histograms; (f)-(h) are the encrypted images using Case #2 and their corresponding histograms; (b) Binary Gray code, n=2, k=8, p=0; (c) Ternary Gray code, n=3, k=6, p=0; (d) the (n, k, p)-Gray code, n=2, k=8, p=1; (f)Binary Gray code, n=2, k=8, p=0; (f) Ternary Gray code, n=3, k=6, p=0; (g) the (n, k, p)-Gray code, n=3, k=6, p=1.

Figure 5.35 gives several images encrypted by Case #1 and Case #2 and their corresponding histograms. All the encrypted images are visually similar to noise images. Their corresponding histograms have an almost uniform distribution. There is no

www.manaraa.com

significant difference between Case #1 and Case #2 when it comes to image encryption. This comparison demonstrates that the presented encryption algorithm performs excellently for image encryption and that the new *(n, k, p)*-Gray code outperforms other traditional Gray codes, as can be seen in the histogram distribution.

5.5.3 Execution Performance Comparison

Efficiency is an important characteristic when it comes to evaluating the suitability of the encryption algorithm for real-time applications. The less time the encryption process takes, the more efficiently the algorithm can be said to encrypt images.

To demonstrate the performance quality of the presented algorithm, its execution time for image encryption can be compared with that of several existing bit-plane decomposition based encryption algorithms, such as the bit-plane encryption algorithm using exclusive-OR operations (BPE-XOR) [71], the selective bit-plane encryption algorithm using the AES algorithm (SBE-AES) [72] and the selective bit-plane encryption algorithm using the least significant bit-plane of images (SBE-LBP) [73]. This comparison is performed in Matlab on a computer running the Windows XP operating system with 4GB memory and an Intel Core2 Quad CPU Q6700.

Note that all execution times are based on the assumption of the worst case of all bit-planes being encrypted individually and separately. Of course, users have the flexibility to selectively encrypt any number of bit-planes to save execution time. However, the fewer the number of bit-planes to be encrypted, the lower the security level achieved.

www.manaraa.com

A 512×512 grayscale Lena image is cropped into different images of varying sizes from 64×64 to 512×512. These images are encrypted by the presented algorithm, the BPE-XOR, the SBE-AES and the SBE-LBP algorithms, respectively. Case #1 for the presented algorithm is used for this comparison. The encryption time is measured and plotted in Figure 5.36. In this example, the security keys of the presented algorithm are $n_D = n_S = n_E = 2$, $p_D = p_S = p_E = 2$. Security keys for the BPE-XOR algorithm are the initial register value of 20 and the shifting times are initialized to five for the Linear Feedback Shift Registers. For the SBE-AES and SBE-LBP algorithms, a 128-bit security key and the two most significant bit-planes are selected for encryption.

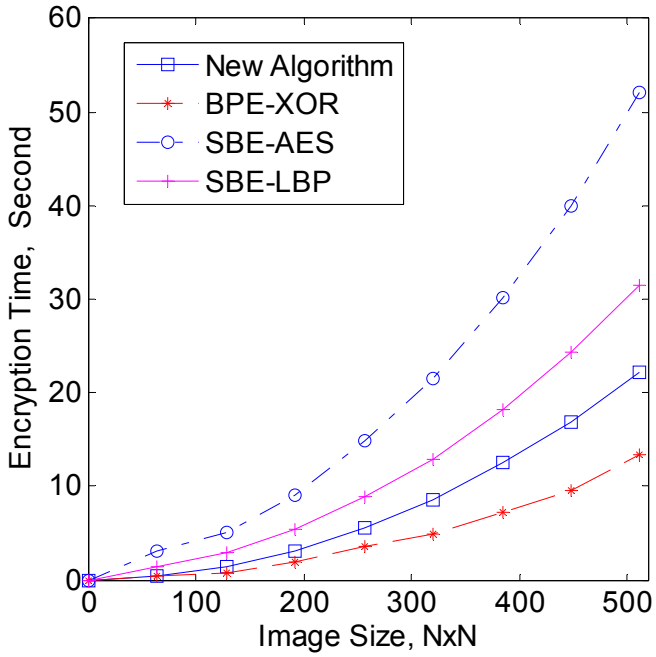


Figure 5.36: Comparison of image encryption using different algorithms.

The results in Figure 5.36 demonstrate that the presented algorithm possesses a superior encryption speed in the MATLAB implementation than the SBE-AES and SBE-LBP algorithms. Although the BPE-XOR algorithm does have the fastest encryption speed in

www.manaraa.com

the Matlab implementation, its security level is extremely low since the algorithm uses only the XOR operation for encryption, which is easy to detect and break.

To ensure the suitability of the presented encryption algorithm for real-time applications such as wireless communications and networking, the presented algorithm's speed of the image encryption/decryption requires further improvement. This can be accomplished by: (1) using parallel circuits or other hardware technologies to efficiently generate the *(n, k, p)*-Gray code; (2) selectively encrypting several of the most significant bit-planes in the encryption process.

5.5.4 Security Analysis and Comparison

Image encryption algorithms have been developed to ensure the security of images and videos. However, protected images are easily broken by unauthorized users if the security of an encryption algorithm is not carefully taken into account. Therefore, security is important for both the protected objects and for the encryption algorithm itself. This section discusses security issues associated with the presented encryption algorithm.

The presented encryption algorithm uses four techniques to improve the security level of the bit-plane decomposition based image encryption algorithms:

1) It introduces the *(n, k, p)*-Gray code bit-plane decomposition in place of traditional binary bit-plane decomposition. Its decomposition results and the number of decomposed bit-planes change in concert with changes in the values of the base *n* and parameter *p*. The attacker will thus have difficulty predicting the decomposed results. Furthermore, the correctly decomposed results are extremely important for authorized

www.manaraa.com

users to be able to reconstruct images, since they directly affect the success of data encryption, bit-plane shuffling and pixel scrambling processes.

2) In a similar manner to the binary XOR operation, the mod operation in the data encryption process works on the arbitrary base. It can keep the data range while changing pixel values.

3) The goal of the bit-plane shuffling is to change image pixel values by changing the order of the *(n, k, p)*-Gray code bit-planes. Bit-plane shuffling is a parameter-dependent process conducive to image encryption. It further increases the attacker's difficulty of decoding the images encrypted by the presented algorithm.

4) The pixel scrambling process is designed to scramble the pixel locations in each bit-plane. This process changes both the image pixel values and the image pixel locations. It enhances the presented algorithm's immunity to plaintext attacks.

TABLE 5.7. COMPARISON OF BIT-PLANE DECOMPOSITION BASED IMAGE ENCRYPTION ALGORITHMS

	BPE-XOR	SBE-AES	SBE-LBP	New Algorithm
Decomposition process	fixed	fixed	fixed	Parameter-dependent
Data encryption	XOR operation	XOR operation	XOR operation	Mod operation
Shuffling process	NO	NO	NO	Parameter-dependent
Pixel scrambling	NO	NO	NO	Parameter-dependent
Change image data	YES	YES	YES	YES
Change image pixel locations	NO	NO	NO	YES

www.manaraa.com

Table 5.7 compares the presented new encryption algorithm to several existing bit-plane decomposition based encryption methods, i.e. the BPE-XOR, SBE-AES and the SBE-LBP algorithms. In terms of security and from a cryptographic point of view, the new algorithm possesses more advantages than existing methods. As a result, the presented algorithm presents greater opportunities for improving the level of security protection compared to existing bit-plane decomposition based image encryption methods.

5.5.5 Security Key Space

For an encryption algorithm, the larger the key space is, the more possible combinations the security keys have. As a result, unauthorized users will have more difficulty obtaining the correct combination of security keys by means of an exhaustive search of all possible cases in the security key space and thus decoding the encrypted images.

The presented algorithm consists of four processes: image decomposition, data encryption, bit-plane shuffling and pixel scrambling. To demonstrate how the key space of the presented encryption algorithm is calculated, an $M \times N$ grayscale image with gray levels between 0 and 255 is used as an example.

- The input image is decomposed into B ($B = \lceil \log_{n_D} 255 \rceil$) bit-planes in the image decomposition process. The possible choices of the security keys, n_D and p_D, in this process are $K_1 = K_{n_D} \bullet K_{p_D} = (255-1)B = 254B$.

- In the data encryption process, the security key plane is generated from the logistic map specified by two parameters, the initial value x_0 and weight coefficient r.

www.manaraa.com

Those two parameters act as the security keys for the data encryption process. Theoretically, the number of their possible choices is unlimited because x_0 and r can be any real number within their limitation ranges: $0 < x_0 < 1$ and $3.5699456 \le r \le 4$. On the other hand, they may have a limited number of combinations since the output of the logistic map may have the same or similar results as some combinations of x_0 and r. Assume their possible choices are K_x and K_r, respectively. Thus, the possible choices of the security keys in the data encryption process are $K_2 = K_x K_r$.

- Any existing or new data shuffling algorithm can be used for the bit-plane shuffling process. Thus, the possible changes of the order of the bit-planes are $K_3 = B!$.

- Any existing or new image scrambling algorithm can be used for scrambling pixel positions in each bit-plane in the pixel scrambling process. Therefore, the possible changes in this process are $K_4 = (M!N!)^B$

Thus, if all the *(n, k, p)*-Gray code bit-planes are encrypted individually, the key space of the presented encryption algorithm is defined by

$$S = K_1 K_2 K_3 K_4 = 254 B K_x K_r B! \left(M!N!\right)^B \tag{96}$$

Table 5.8 gives some examples of the key space for a 12×12 grayscale image with different base *n* for four processes. Since n_D is specified in Table 5.8, $K_{n_D} = 1$. Assume that the possible choices of the parameters of the logistic map, x_0 and r, in the data

www.manaraa.com

encryption process are 10 respectively, i.e. $K_x = K_r = 10$. The examples of the key space in Table 5.8 show that the key space of the presented encryption algorithm is sufficiently large.

TABLE 5.8. EXAMPLES OF THE KEY SPACE OF THE PRESENTED ALGORITHM WITH DIFFERENT SECURITY KEYS

n_D	# of bit-planes	Image size	Key Space
2	8	12×12	2.4774×10^{146}
3	6	12×12	6.3027×10^{109}
4	4	12×12	2.6605×10^{73}
5	4	12×12	2.6605×10^{73}

Note: Assume $K_x = K_r = 10$ for the results in this table.

5.5.6 Plaintext Attacks

The plaintext is the original information to be encrypted. The ciphertext is the plaintext encrypted by an encryption algorithm [172, 173]. There are two types of plaintext attacks: the known-plaintext attack and the chosen-plaintext attack.

In the known-plaintext attack, the attacker tries to obtain the security keys of the encryption algorithm by studying a number of plaintexts and their corresponding ciphertexts. In the chosen-plaintext attack, on the other hand, the attacker can choose a number of plaintexts and obtain their corresponding ciphertexts. According to cryptanalysis, the chosen-plaintext attack is a more advanced form of attack because the attacker can select any useful information as plaintext to deduce the encryption algorithm's security keys; either that, or the attacker can reconstruct the original plaintexts from the unknown ciphertexts. Generally speaking, if an encryption algorithm can overcome the chosen-plaintext attack, it can also withstand other types of attacks such as ciphertext-only attacks and known-plaintext attacks.

www.manaraa.com

For the presented encryption algorithm, data encryption, bit-plane shuffling and pixel scrambling are all important processes. Using mod operation, the data encryption directly changes pixel values individually within each *(n, k, p)*-Gray code bit-plane. The bit-plane shuffling changes the bit positions of image pixels in the vertical direction. The pixel scrambling changes pixel positions in the horizontal direction. These processes are parameter-dependent and change the image pixel values based on the different security keys. As a result, unauthorized users will have difficulty breaking the encrypted images via plaintext attacks.

To test the performance of the presented algorithm for the plaintext attack, an $M \times N$ matrix defined in the following equation as a plaintext matrix, is designed to attack it.

$$T(i, j) = j + (i-1) * M \tag{97}$$

where i and j are integers, $1 \le i \le M, 1 \le j \le N$

The values of all elements in the plaintext matrix differ from each other. Using the plaintext and searching the pixel values (if the pixel values are not changed after encryption process), the changing positions of all image pixels can be located. This can be used to break the permutation-only based image encryption algorithms.

The data encryption, bit-plane shuffling and pixel scrambling processes in the presented encryption algorithm are able to change both the image pixel values and the image pixel locations. The encrypted results do not yield data that can be utilized in this plaintext attack. Figure 5.37 gives a visual example of this chosen-plaintext attack. The plaintext image (Figure 5.37(b)) is a 2D matrix defined in equation (97) and its corresponding

www.manaraa.com

ciphertext (given in Figure 5.37(e)) is obtained by the presented encryption algorithm. Figure 5.37(c) shows the reconstructed image using the chosen-plaintext attack. It is completely different from the original image (Figure 5.37(a)). The histogram (Figure 5.37(f)) of the difference between the original image and the reconstructed image also verifies that this chosen-plaintext attack cannot break the encrypted images.

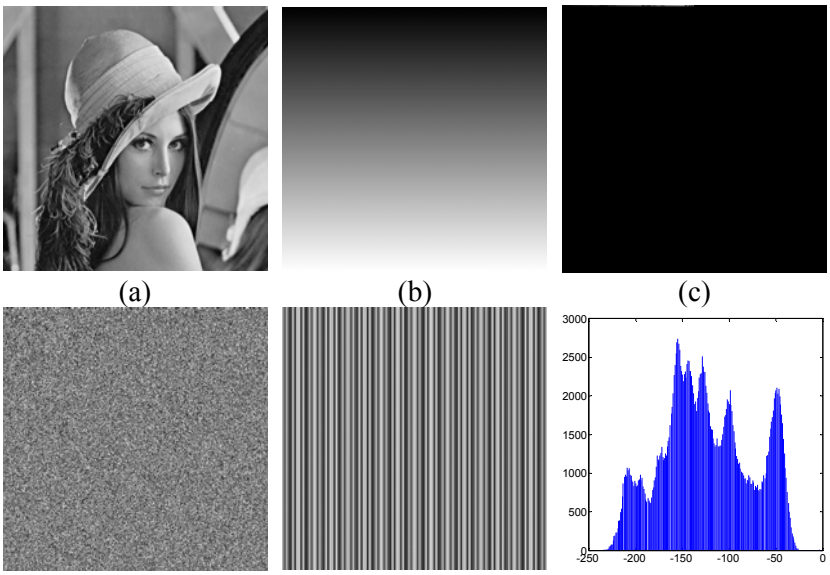


Figure 5.37: Chosen-plaintext attack for the presented encryption algorithm. (a) The original image; (b) The plaintext; (c) The reconstructed image using the chosen-plaintext attack; (d) The encrypted image with $n_D = n_S = n_E = 2,\ p_D = p_S = p_E = 1$; (e) The ciphertext; (f) Histogram of the difference between (c) and (a).

www.manaraa.com

5.6 Image Encryption Using the Discrete Parametric Cosine Transform

In the image encryption process, the original images can only be completely reconstructed when the correct security keys are utilized, such as security key K_1 shown in Figure 5.38. Otherwise, reconstructed images will appear unrecognizable. For example, if the security key K_2 in Figure 5.38 is used for the decryption process. Simulation examples can be found in Figures 5.20 and 5.33. This offers image encryption a possible new direction that uses one set of security keys (K_1 in Figure 5.38) to encrypt the original image and a different set of security keys (K_2 in Figure 5.38) to reconstruct the image in order to obtain the final encrypted image (the wrong image in Figure 5.38).

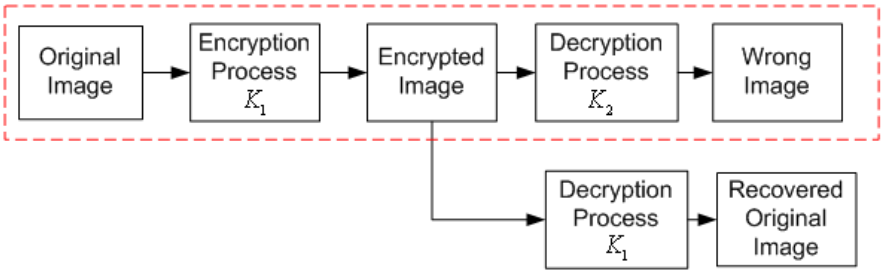


Figure 5.38: Block diagram of image encryption.

Based on the above concept, this section now introduces a new image encryption algorithm using the Discrete Parametric Cosine Transform (DPCT).

www.manaraa.com

5.6.1 Discrete Parametric Cosine Transform

This section first reviews the Discrete Parametric Cosine Transform (DPCT) and its properties. By extending the concept of the DPCT, the 2D Discrete Parametric Cosine Transform (2D DPCT) is then introduced.

5.6.1.1 DPCT

Let the sequence $(x_0, x_1, ..., x_{N-1})$ be mapped to $(X_0, X_1, ..., x_{N-1})$ by the following transformation [175].

$$X_k = \sum_{n=0}^{N-1} \mu_{n,k} x_n \cos\left[\frac{\pi}{M}\alpha_0 (n+\alpha_1)(k+\alpha_2)\right] \tag{98}$$

where $0 \le n,k \le N-1$ and coefficients $(N, M, \alpha_0, \alpha_1, \alpha_2, \mu_{n,k})$ are parameters. This transformation is called the Discrete Parametric Cosine Transform (DPCT).

Based on the definition in equation (98), the DPCT changes as the parameters $(N, M, \alpha_0, \alpha_1, \alpha_2, \mu_{n,k})$ change. For example,

1) If $M = N, \alpha_0 = 1, \alpha_1 = \alpha_2 = 0, \mu_{n,k} = \mu_n \mu_k$ and $\mu_p = \begin{cases} 1/\sqrt{2} & p = 0 \\ 1 & 0 < p \le N-1 \end{cases}$, then DPCT becomes the DCT-I,

$$X_k = \sqrt{\frac{2}{N}} \sum_{n=1}^{N-1} \mu_n \mu_k x_n \cos\left[\frac{\pi k}{N}\left(n+\frac{1}{2}\right)\right] \tag{99}$$

2) If $M = N, \alpha_0 = 1, \alpha_1 = \frac{1}{2}, \alpha_2 = 0$ and $\mu_{n,k} = \begin{cases} 1/\sqrt{N} & k = 0 \\ \sqrt{2/N} & 0 < k \le N-1 \end{cases}$, the DPCT is the DCT-II, i.e.

www.manaraa.com

$$X_k = \mu_{n,k} \sum_{n=1}^{N-1} x_n \cos\left[\frac{\pi k}{N}\left(n+\frac{1}{2}\right)\right] \tag{100}$$

3) If $M = N, \alpha_0 = 1, \alpha_1 = 0, \alpha_2 = \frac{1}{2}$ and $\mu_{n,k} = \sqrt{2/N}$, the DPCT is the DCT-III, namely,

$$X_k = \sqrt{\frac{2}{N}} \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi n}{N}\left(k+\frac{1}{2}\right)\right] \tag{101}$$

4) If $M = N, \alpha_0 = 1, \alpha_1 = \frac{1}{2}, \alpha_2 = \frac{1}{2}$ and $\mu_{n,k} = 2/\sqrt{N}$, the DPCT changes to the DCT-IV, i.e.

$$X_k = \sqrt{\frac{2}{N}} \sum_{n=1}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)\left(k+\frac{1}{2}\right)\right] \tag{102}$$

5.6.1.2 2D DPCT

Based on the 2D DCT, the DPCT can be extended to the 2D DPCT which is defined by,

$$X_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} \mu_{n_1,k_1} \mu_{n_2,k_2} x_{n_1,n_2} \cos\left[\frac{\pi}{M_1}\alpha_{10}\left(n_1+\alpha_{11}\right)\left(k_1+\alpha_{12}\right)\right] \times \cos\left[\frac{\pi}{M_2}\alpha_{20}\left(n_2+\alpha_{21}\right)\left(k_2+\alpha_{22}\right)\right] \tag{103}$$

From the definition in equation (103), there are 12 parameters in the 2D DPCT, i.e. $P = (N_1, M_1, \mu_{n_1,k_1}, \alpha_{10}, \alpha_{11}, \alpha_{12}, N_2, M_2, \mu_{n_2,k_2}, \alpha_{20}, \alpha_{21}, \alpha_{22})$. The 2D DPCT will be different when these parameters change. For example, the 2D DCT is a special case of the 2D DPCT. If $M_1 = N_1 = M_2 = N_2 = N, \alpha_{10} = \alpha_{20} = 1,$ and $\alpha_{11} = \alpha_{21} = \frac{1}{2}, \alpha_{12} = \alpha_{22} = 0$, $\mu_{n_1,k_1} = \mu_{k_1}$, $\mu_{n_2,k_2} = \mu_{k_2}$, the 2D DPCT becomes the 2D DCT,

$$X_{k_1,k_2} = \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} \mu_{k_1} \mu_{k_2} x_{n_1,n_2} \cos\left[\frac{\pi k_1}{N}\left(n_1+\frac{1}{2}\right)\right] \cos\left[\frac{\pi k_2}{N}\left(n_2+\frac{1}{2}\right)\right] \tag{104}$$

www.manaraa.com

where

$$\mu_k = \begin{cases} 1/\sqrt{N} & k = 0 \\ \sqrt{2/N} & 0 < k \le N-1 \end{cases}$$

The 2D DPCT is a complex cosine transform that requires 12 parameters, making it challenging to design for real world applications. However, these parameters make the 2D DPCT more powerful and provide robust characteristics. The 2D DPCT also offers users design flexibility when it comes to achieving the design requirements of real world applications.

In a similar manner to the inverse 2D DCT, the inverse 2D DPCT can be given by,

$$x_{n_1,n_2} = \sum_{k_1=0}^{N_1-1}\sum_{k_2=0}^{N_2-1} \mu_{n_1,k_1}\mu_{n_2,k_2} X_{k_1,k_2} \cos\left[\frac{\pi}{M_1}\alpha_{10}(n_1+\alpha_{11})(k_1+\alpha_{12})\right]\cos\left[\frac{\pi}{M_2}\alpha_{20}(n_2+\alpha_{21})(k_2+\alpha_{22})\right] \quad (105)$$

5.6.2 The New Image Encryption Algorithm

This section introduces a new image encryption algorithm using the presented 2D DPCT. The presented algorithm transforms the original images into the frequency domain using the presented 2D DPCT with $P = (N_1, M_1, \mu_{n_1,k_1}, \alpha_{10}, \alpha_{11}, \alpha_{12}, N_2, M_2, \mu_{n_2,k_2}, \alpha_{20}, \alpha_{21}, \alpha_{22})$. In order to convert the images back into the spatial domain and obtain the encrypted images, it uses an inverse 2D DPCT with different parameters $P' = (N_1', M_1', \mu_{n_1,k_1}', \alpha_{10}', \alpha_{11}', \alpha_{12}', N_2', M_2', \mu_{n_2,k_2}', \alpha_{20}', \alpha_{21}', \alpha_{22}')$. Figure 5.39 shows the encryption algorithm.

www.manaraa.com

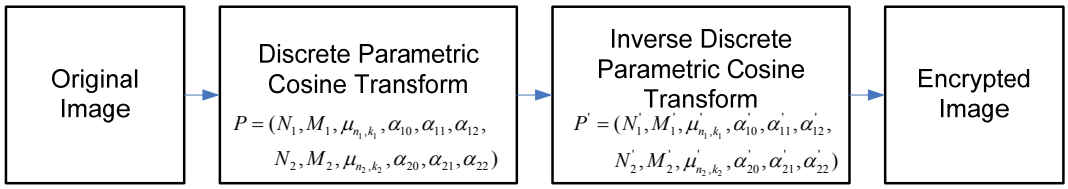


Figure 5.39: Block diagram of the image encryption algorithm

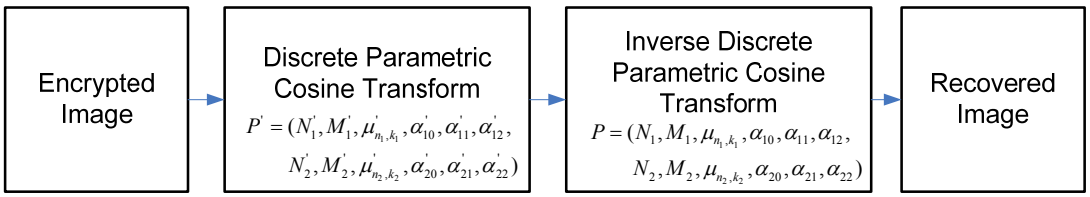


Figure 5.40: Block diagram of the image decryption algorithm

The presented encryption algorithm is a simple and straightforward process. The inverse process of recovering the original images (the image decryption algorithm) is depicted in Figure 5.40. The algorithm converts the encrypted image into the frequency domain using the 2D DPCT with parameters $P'=(N_1',M_1',\mu'_{n_1,k_1},\alpha'_{10},\alpha'_{11},\alpha'_{12},N_2',M_2',\mu'_{n_2,k_2},\alpha'_{20},\alpha'_{21},\alpha'_{22})$. The original image is reconstructed using the 2D inverse DPCT with $P=(N_1,M_1,\mu_{n_1,k_1},\alpha_{10},\alpha_{11},$ $\alpha_{12},N_2,M_2,\mu_{n_2,k_2},\alpha_{20},\alpha_{21},\alpha_{22})$ to transfer the image back into the spatial domain.

The presented algorithm can also be used to encrypt other types of images such as 2D and 3D medical images and color images. Color images or 3D medical images usually contain several 2D components. For example, color images have three color planes and 3D medical images consist of a number of slice images. The presented algorithm can encrypt all the 2D components individually and then combine the encrypted results to obtain the encrypted 3D medical images or color images.

www.manaraa.com

5.6.3 Experimental Results

In order to demonstrate the presented encryption algorithm's performance, this section provides several encryption results for grayscale, medical and color images. In all the examples in this section, the 2D DPCT and inverse 2D DPCT are specified as different types of the traditional 2D DCT, as described in Section 5.6.1.1. This takes advantage of the fact that these types of DCTs have inverse transforms that are easy to generate and implement.

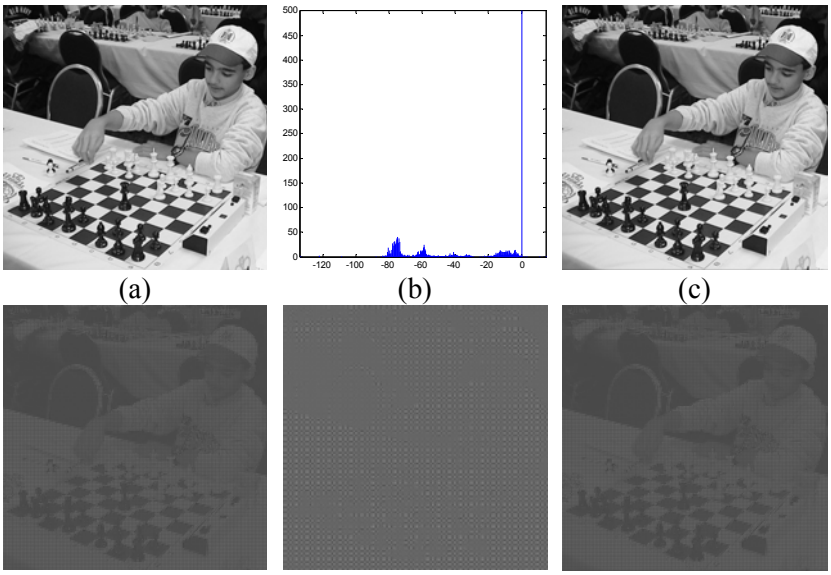


Figure 5.41: Grayscale image encryption using the same type of DPCT transforms with different window sizes. (a) Original image; (b) Histogram of the difference between the reconstructed image and the original image; (c) Reconstructed image; (d) the DPCT result of the original image; (e) Encrypted image; (f) The reconstructed DPCT result.

Figure 5.41 gives an example of the grayscale image encryption. The original image is converted into the frequency domain by specifying the 2D DPCT as the 2D DCT-II with a window size of 3×3. The DCT result of the original image is given in Figure 5.41(d). The encrypted image (Figure 5.41(e)) is obtained by transforming the DCT result in

www.manaraa.com

Figure 5.41(d) back into the spatial domain using the inverse 2D DCT-II with a window size of 7×7. It is completely unlike the original image.

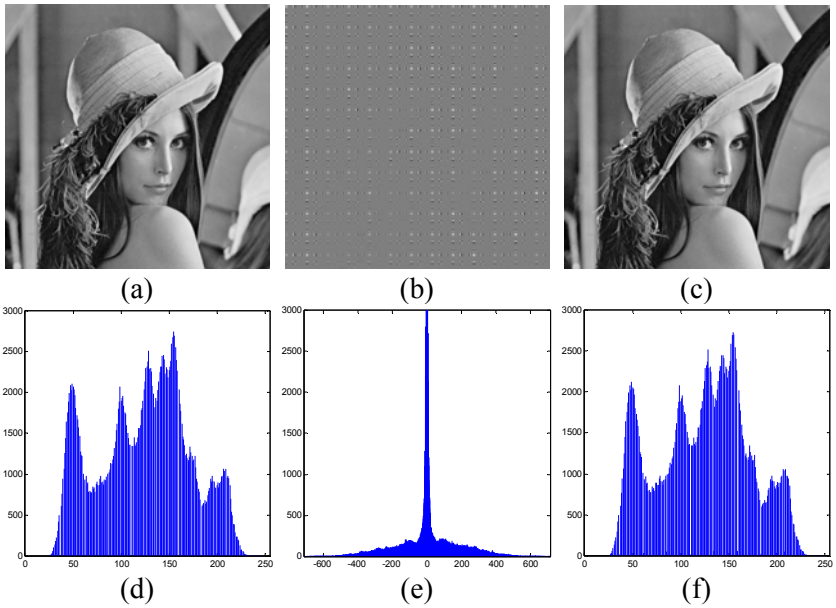


Figure 5.42: Grayscale image encryption using different types of DPCT transforms with different window sizes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the reconstructed image.

To reconstruct the original image, the encrypted image is applied to the 2D DCT-II with a window size of 7×7. The result is given in Figure 5.41(f). The reconstructed image (Figure 5.41(c)) is obtained using an inverse 2D DCT-II with a window size of 3×3. It is visually the same as the original image in Figure 5.41(a). However, the reconstructed image is slightly different compared to the original image based on the histogram (Figure 5.41(b)) of the difference between the reconstructed image and the original image. This is because the 2D DCT-II converts image data into the floating format while the original images are integer, for example, the pixel values of a grayscale image are integer gray levels from 0 to 255.

www.manaraa.com

Figure 5.42 shows another example of grayscale image encryption using different types of DPCTs and window sizes. The original image in Figure 5.42(a) is encrypted by a 2D DCT-III with a window size of 3×3 and an inverse 2D DCT-IV with a window size of 5×5. The reconstructed image and its histogram look identical to the original image.

Figure 5.43 gives an example of medical image encryption. In this case, the encryption process uses the same type of the DPCT but a different window size. 2D DCT-II with a window size of 3×3 and inverse 2D DCT-II with a window size of 10×10 were chosen for this example.

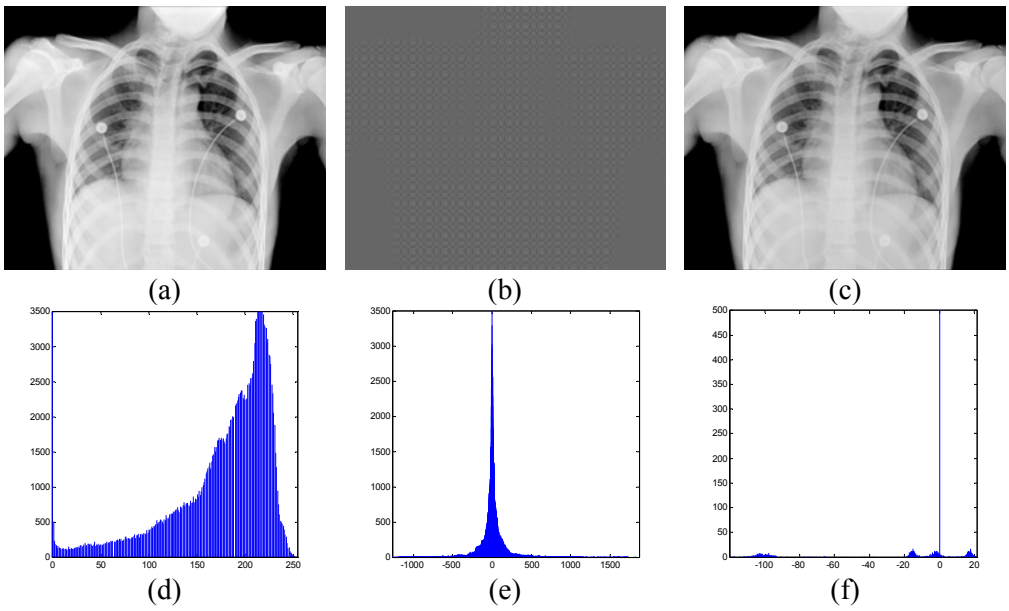


Figure 5.43: Medical image encryption using the same type of DPCT transforms with different window sizes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the difference between the reconstructed and original images.

Figure 5.44 gives another example of the medical image encrypted by different types of the DPCT and different window sizes. The encryption process uses the 2D DCT-II with a window size of 7×7 and the inverse 2D DCT-IV with a window size of 5×5.

www.manaraa.com

All these examples of 2D image encryption demonstrate that the image encryption process results in images that are completely different to the original images and that the original images are fully encrypted.

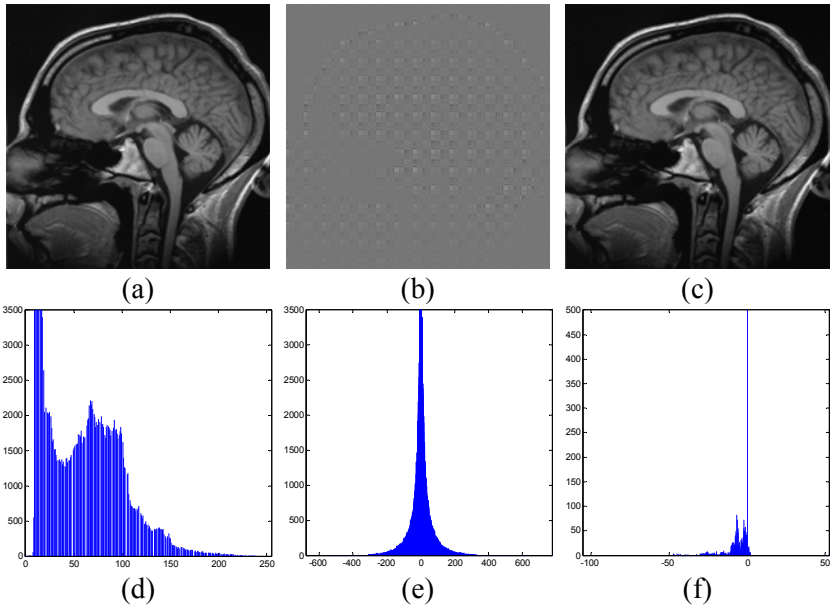


Figure 5.44: Medical image encryption using different types of DPCT transforms with different window sizes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the difference between the reconstructed image and the original image.

Figure 5.45 gives an example of color image encryption. All its 2D components are encrypted using the same parameters. The encryption process uses the 2D DCT-II with a window size of 4×4 and then the inverse 2D DCT-II with a window size of 11×11. This demonstrates that the original image can be partially encrypted by selecting the appropriate combination of security keys. Users can use different parameters for each 2D component to obtain the full encryption results. The reconstructed color image is slightly different to the original one which is verified by the difference histogram given in Figure 5.45(f).

www.manaraa.com

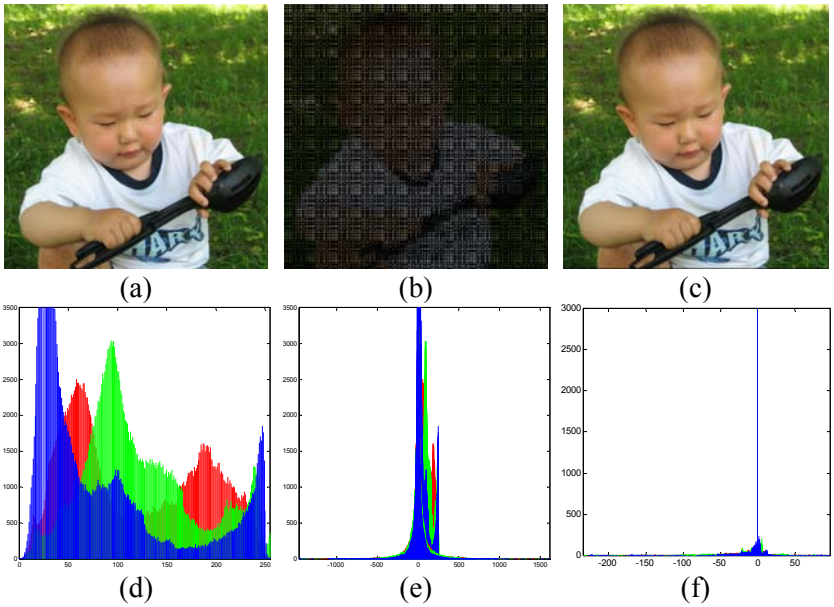


Figure 5.45: Color image encryption using the same parameters for each color planes. (a) Original image; (b) Encrypted image; (c) Reconstructed image; (d) Histogram of the original image; (e) Histogram of the encrypted image; (f) Histogram of the difference between the reconstructed image and the original images.

5.6.4 Security Analysis

This section discusses the security issues of the presented algorithm such as the security key space and the risk of attacks.

5.6.4.1 Security Key Space

The security keys of the presented algorithm consist of the parameters $P=(N_1, M_1, \mu_{n_1,k_1}, \alpha_{10}, \alpha_{11}, \alpha_{12}, N_2, M_2, \mu_{n_2,k_2}, \alpha_{20}, \alpha_{21}, \alpha_{22})$ for the 2D DPCT and $P'=(N_1', M_1', \mu_{n_1,k_1}', \alpha_{10}', \alpha_{11}', \alpha_{12}', N_2', M_2', \mu_{n_2,k_2}', \alpha_{20}', \alpha_{21}', \alpha_{22}')$ for the inverse 2D DPCT. This results in 24 security keys existing for the presented algorithm. Theoretically, each parameter has an unlimited number of possible values. However, each 2D DPCT should have an inverse matrix in order to reconstruct the original images in the decryption process. This means that the 2D

www.manaraa.com

DPCT has to be an invertible/nonsingular square matrix, namely, $N_1 = M_1 = N_2 = M_2$ and $N_1^{'} = M_1^{'} = N_2^{'} = M_2^{'}$. After applying these conditions, 16 security keys remain. These security keys are extremely important for the presented algorithm. The results in Figure 5.46 show that the original image can only be reconstructed if the correct security keys are used.

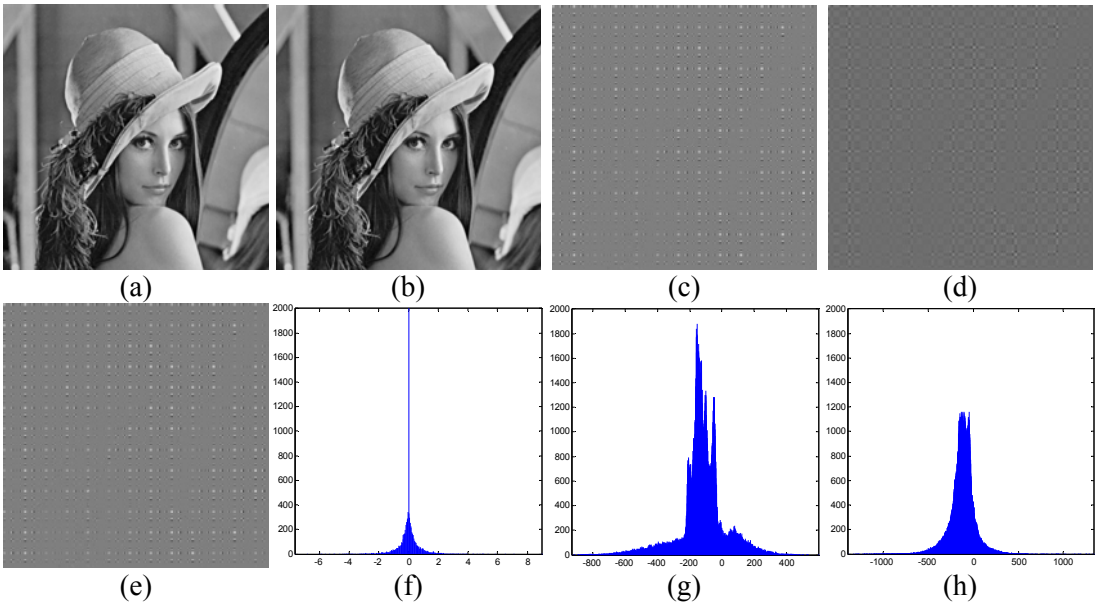


Figure 5.46: Image reconstruction using different security keys. (a) Original image; (b) Reconstructed image, 2D DCT-II with 5×5 and inverse 2D DCT-II with 8×8; (c) Reconstructed image, 2D DCT-II with 8×8 and inverse 2D DCT-II with 8×8; (d) Reconstructed image, 2D DCT-III with 8×8 and inverse 2D DCT-III with 5×5; (e) Encrypted image, 2D DCT-II with 8×8 and inverse 2D DCT-II with 5×5; (f) Histogram of the difference between (a) and (b); (g) Histogram of the difference between (a) and (c); (h) Histogram of the difference between (a) and (d).

A very large number of possible value choices exist for each parameter. Thus, the security key space of the presented algorithm is quite large. The algorithm can withstand the brute force attack in which attackers attempt to guess the algorithm's security keys by exclusively searching its key space.

www.manaraa.com

5.6.4.2 Plaintext Attacks

The presented algorithm changes the image data during the entire encryption process by applying the 2D DPCT and the inverse 2D DPCT to the images. All histograms of the encrypted images in Section 5.6.3 show that the pixel values of the encrypted image are completely different from the original images. Thus, the data of the encrypted images are not useful for the plaintext attacks. This ensures that the presented algorithm is able to withstand plaintext attacks.

www.manaraa.com

5.7 Summary and Discussion

This chapter has introduced two new image bit-plane decomposition methods. The truncated Fibonacci p-code bit-plane decomposition was introduced to reduce the redundancy of the Fibonacci p-code bit-plane decomposition. The *(n, k, p)*-Gray code bit-plane decomposition was introduced due to its ability to decompose images into arbitrary base bit-planes. The number of decomposed bit-planes and the content of each bit-plane are parameter-dependent. Both of these advantages are useful for image encryption.

To enhance the security level of the existing bit-plane decomposition based encryption methods, three new image encryption algorithms have been introduced combining the image bit-plane decomposition methods and the recursive sequence transforms presented in Chapter 4. The new encryption method based on the truncated Fibonacci p-code bit-plane decomposition was used successfully to encrypt the selected object, which was either a full image, part of an image, or a selected object in an image or a specific region in an image.

In addition, another new image encryption algorithm has been introduced using the discrete parametric cosine transform. This introduces a new direction for multimedia encryption, namely, the use of one combination of security keys for encrypting the original multimedia data and a different combination of security keys for reconstructing it to obtain the final encrypted multimedia data. The encryption process is an effective and straightforward way to transform data from the spatial domain to the frequency domain

www.manaraa.com

and back into the spatial domain. The idea behind the algorithm was to encrypt an image by changing the image data using the DPCT with different parameters. This new algorithm can be combined with an image compression process like JPEG, in such a way that the images can be encrypted and compressed simultaneously, making the algorithm suitable for real-time applications.

Simulation results and comparisons demonstrated the performance of all the algorithms for image encryption. Security analysis showed the algorithms' ability to withstand several common attacks such as the brute force, statistic, noise, data loss and plaintext attacks. The encryption algorithms clearly have the potential to be used for clinic applications such as privacy protection of medical images, and in biometrics security systems and video surveillance systems for homeland security purposes.

The next step is to investigate the algorithms' properties for error-resilient protection and the memory usage (spatial complexity) in comparison with existing encryption methods.

www.manaraa.com

Chapter 6

The Edge Map for Image Encryption

The edge map has been used for image enhancement, denoising, compression, segmentation and recognition but it has never been used for image encryption. This chapter presents the inventive work of using the edge map for image encryption. Two encryption algorithms are introduced combining the edge map with the 3D Cat Map for image encryption and with the chaotic logistic map for encrypting medical images for privacy protection. This concept is extended to produce a binary "key-image", which is either a bit-plane or an edge map obtained from any other image. Two additional encryption algorithms are introduced using the binary bit-plane and the edge map respectively. Simulation results and security analysis will be given to demonstrate the encryption algorithms' performance.

www.manaraa.com

6.1 Introduction

The edge map has been used for many different applications in image processing but it has never been used for image encryption. This chapter investigates and presents the inventive work on the application of the edge map for image encryption.

First, a new concept of image encryption is introduced using edge information [79]. This method separates the image into edges and the image without edges, and then encrypts them using encryption algorithms. Users have the flexibility to adopt any encryption method for encrypting edges or for encrypting the image without edges, or both, depending on different security requirements.

A novel image encryption algorithm is introduced based on this concept, using a new 3D Cat Map. This is an example to demonstrate the performance of this concept. The encryption algorithm can change the positions and values of the image pixels simultaneously using the 3D Cat Map transform. The edges and the image without edges of any given image change as the edge detection methods and their thresholds change. This ensures that unauthorized users will have difficulty decoding the encrypted images.

The edge map as a binary image can be used a security key. The edge map is then combined with the chaotic logistic map to encrypt medical images for privacy protection [80]. This method uses the edge map as a security key to encrypt image bit-planes by XOR operation. The chaotic logistic map, another random security generator, is used to protect the edge map and achieve a high level of security. The algorithm can be used to

www.manaraa.com

fully protect the selected objects/regions within images or the entire image. However, the edge map in this algorithm has to be sent to the authorized users for them to be able to reconstruct original images, since it is only obtained from the original image that is going to be encrypted. This will increase the data transmission complexity of the media transmission channels.

To overcome this problem, the edge map for image encryption is further extended into a binary "key-image", either a binary bit-plane or an edge map obtained from any other new/existing image [81]. Two new image encryption algorithms are introduced.

Since the edge information is frequently used in image/video compression, the encryption methods mentioned above can also be embedded into the image compression process in such a way that edge information is preserved in the compression process and the encryption process provides adequate security for images.

The rest of this chapter is organized as follows. Section 6.2 introduces the new concept of the image encryption using edge information and a new image encryption algorithm using the 3D Cat Map. Section 6.3 presents a medical image encryption algorithm using a combination of the edge map and chaotic logistic map. Based on the concept of the binary key-image, Section 6.4 introduces two image encryption algorithms using the binary bit-plane and the edge map respectively. Section 6.5 draws a conclusion.

www.manaraa.com

6.2 Image Encryption Using the Edge Map and 3D Cat Map

This section introduces a new concept for image encryption according to edge information. The basic idea is to separate the image into the edges and the image without edges, and encrypt them using any existing or new encryption algorithm. Users have the flexibility to encrypt the edges or the image without edges, or both. In this manner, different security requirements can be achieved. The encrypted images are difficult for unauthorized users to decode, providing a high level of security.

A new encryption algorithm is also introduced using the 3D Cat Map. The algorithm can be used for encrypting different types of multimedia data in a straightforward one-step process in real-time applications such as wireless communication and mobile phone services. It simultaneously changes image pixel locations and pixel data. Experimental results will be provided to demonstrate the algorithm's performance when it comes to image encryption.

6.2.1 The New Image-Edge Encryption Algorithm

2D multimedia data such as grayscale images, biometrics and 2D medical image are 2D data matrices. The new encryption algorithm first obtains the edge map of the image using an existing edge detection method with a specific threshold. It separates the image into edges and the image without edges, and then applies an existing or new encryption

www.manaraa.com

algorithm to encrypt the edges, or the image without edges, or both, combining the encrypted edges and the encrypted image without edges to generate the encrypted 2D image using any reversible fusion method. For example, set the encrypted edges into the imaginary part of the complex number, and put the image without edges into the real part of the complex number. The block diagram of the algorithm is shown in Figure 6.1.

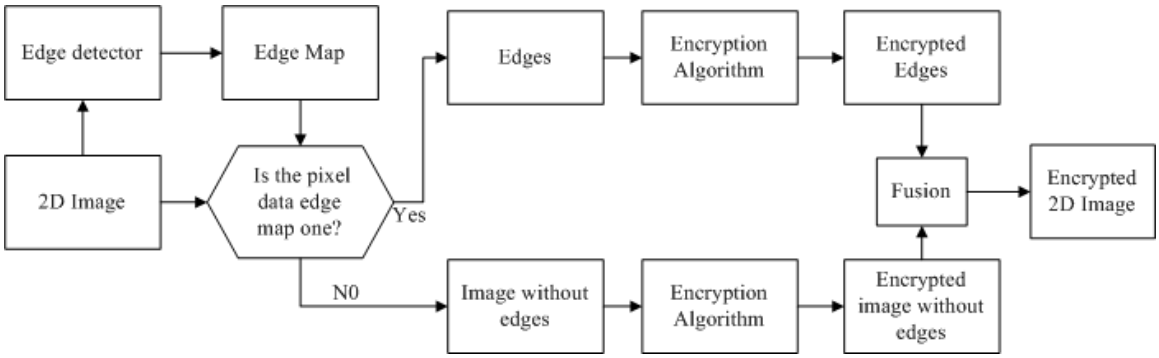


Figure 6.1: The new Image-Edge Encryption Algorithm.

Users have the flexibility to choose any existing or new edge detector and its threshold to get the edge maps of the images, and to encrypt the edges or the image without edges, or both, depending upon the different security requirements of real-time applications. They also have the flexibility to select any existing encryption algorithm or create a new algorithm for the encryption process. The security keys of the presented encryption algorithm are the security keys of the encryption algorithm being used to encrypt the edges and the image without edges.

To reconstruct the original image, the encrypted image is separated into the encrypted edges and the encrypted image without edges. They are decoded individually to reconstruct the edges and the image without edges. The reconstructed image can then be obtained by combing the recovered edges and the reconstructed image without edges.

www.manaraa.com

The 3D images contain several 2D data matrices. The 3D image encryption can be accomplished by encrypting three 2D data matrices one by one using the presented image-edge encryption algorithm.

6.2.2 The 3D Cat Map Based Image Encryption Algorithm

This section introduces a new 3D Cat Map and its corresponding transforms. As an example of the presented encryption concept, a new image encryption algorithm using this 3D Cat Map is also introduced.

6.2.2.1 The 3D Cat Map and its Transforms

Definition 6.1: The 2D Arnold cat map is a chaotic map defined as [56, 176].

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = (A \begin{bmatrix} x_n \\ y_n \end{bmatrix}) \bmod N = (\begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix}) \bmod N \tag{106}$$

where a, b are positive integers, $\det(A) = 1$.

Definition 6.2: The 3D Arnold cat map is defined as.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = (A \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix}) \bmod N = (\begin{bmatrix} 1 & a & b \\ c & ac+1 & bc \\ d & abcd & bd+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix}) \bmod N \tag{107}$$

where a, b, c, d are positive integers, $\det(A) = 1$.

Definition 6.3: Let (x, y) be the location of an image pixel with value I in an $N \times N$ image. The following transformation is called the cat map transform.

www.manaraa.com

$$\begin{bmatrix} x' \\ y' \\ I' \end{bmatrix} = \left(\begin{bmatrix} 1 & a & b \\ c & ac+1 & bc \\ d & abcd & bd+1 \end{bmatrix} \begin{bmatrix} x \\ y \\ I \end{bmatrix} \right) \bmod N \tag{108}$$

where a, b, c, d are positive integers, (x', y') is the new location of the pixel with a new value $I'(x, y)$, $x, y, x', y' = 1, 2, ...N$ and $0 \le I, I' \le 255$.

The above cat map transform can change the image pixel positions and pixel values simultaneously. It can efficiently encrypt the 2D images. Users have the flexibility to choose the number of iterations for applying the cat map transform to achieve different levels of security. The parameters a, b, c, d and iteration times n can act as security keys for image encryption.

To reconstruct the original image, the cat map transform cannot be directly utilized due to the mod operation in the transform. Therefore, two coefficient matrices are introduced: the row coefficient matrix and the column coefficient matrix.

The row coefficient matrix of the cat map transform $T_r(N, N)$ can be generated as

$$T_r(x, j) = \begin{cases} 1 & (x, x') \\ 0 & otherwise \end{cases} \tag{109}$$

where $x, j = 1, 2, ..., N$.

The column coefficient matrix of the cat map transform $T_c(N, N)$ can be generated as

$$T_c(i, y) = \begin{cases} 1 & (y', y) \\ 0 & otherwise \end{cases} \tag{110}$$

www.manaraa.com

where $i, y = 1, 2, ..., N$.

TABLE 6.1 COEFFICIENT MATRICES OF THE CAT MAP TRANSFORM FOR AN 8×8 IMAGE.

(a,b,c,d,n)	T_r	T_c
$(3,5,10,20,5)$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$

These two coefficient matrices will differ based on the combination of the parameters a, b, c, d and iteration times n. Some examples are given in the Table 6.1.

Definition 6.4: Let E be the encrypted image, T_r^{-1}, T_c^{-1} be the inverse matrices of the row and column coefficient matrices defined in equation (109) and (110) respectively. The following transformation is called the Inverse cat map transform:

$$R = T_r^{-1} E T_c^{-1} \tag{111}$$

where R is the reconstructed image.

To recover the pixel values of the original image, another one dimensional matrix is introduced. Let the input of cat map transform be $I = (0,1,2,...,255)$, the output of the cat map transform will be $I' = (I_1', I_2', I_3', ..., I_{256}')$ for a certain combination of the parameters a, b, c, d. The pixel value in the reconstructed image will be,

$$R(x, y) = \alpha - 1 \text{ for } I_\alpha' = E(x, y) \tag{112}$$

www.manaraa.com

where $R(x,y)$ is the pixel value of the reconstructed image with location (x,y), $E(x,y)$ is the pixel value of the encrypted image with location (x,y).

Each pixel value between 0 and 255 in original data matrix I has a unique corresponding value in the encrypted data matrix I'. In this manner, the pixel values of the original image can be recovered by searching the value in the encrypted data matrix I'.

6.2.2.2 The 3D Cat Map Based Image Encryption Algorithm

The 2D image is separated into the edges and the image without edges applying an existing edge detection method such as Sobel, Canny, Prewitt and many others. Both edges and the image without edges are encrypted applying the cat map transform. The encryption process is a straightforward process. The encrypted image can be obtained by combining the encrypted results with a format of the complex numbers.

The type of edge detection method and its threshold value, as well as the parameters and iteration times of the cat map transform, can act as the security keys for the presented 3D Cat Map based encryption algorithm. These security keys have a sufficiently large number of possible combinations. It is impossible for unauthorized users to deduce the correct combination of security keys by searching all possible cases. The encrypted images are extremely difficult for the unauthorized users to decode. As a result, the image can be protected by a high level of security.

www.manaraa.com

Algorithm	*The 3D Cat Map Based Image Encryption Algorithm*
Input	3D Image (or 2D image) to be encrypted
Step 1	Select an edge detection method and its threshold value.
Step 2	Separate the 3D image into their 2D components. (2D image: Skip this step.)
Step 3	Obtain the edge maps of all 2D components using the selected method of edge detection.
Step 4	Separate all 2D components into edges and the images without edges based the corresponding edge maps.
Step 5	Select the parameters (a,b,c,d,n) for the cat map transform.
Step 6	Encrypt all edges and the images without edges individually by applying the cat map transform defined in equation (108).
Step 7	Combine the encrypted edges and the encrypted image without edges for each 2D component into a format of the complex number. For example, put the encrypted edges into the imaginary part of the complex number, and put the image without edges into the real part of the complex number. (2D image: Combine the encrypted edges and the encrypted image without edges to get the encrypted 2D image.)
Step 8	Combine all encrypted components together to get the encrypted 3D image. (2D image: Skip this step.)
Output	The encrypted 3D image (or the encrypted 2D image)

To reconstruct the original image, authorized users will be provided with the correct security keys: the parameters and iteration times of the cat map transform. The decryption process is also straightforward. The encrypted image is separated into edges and the image without edges. They are decoded individually using the inverse cat map transform. By combining the recovered edges and the decrypted image without edges, the original image can be reconstructed. For 3D images, the original image can be reconstructed by recovering all 2D components one by one.

www.manaraa.com

Algorithm	*The 3D Cat Map Based Image Decryption Algorithm*
Input	The encrypted 3D Image (or 2D image) to be decrypted
Step 1	Separate the encrypted 3D image into their 2D components. (2D image: Skip this step.)
Step 2	Separate all 2D components into edges and the images without edges.
Step 3	Generate the row and column coefficient matrices T_r, T_c and image value matrix I' using the cat map transform and parameters (a,b,c,d,n)
Step 4	Apply the inverse cat map transform to all edges and images without edges separately to recover the pixel locations.
Step 5	Recover the pixel values of all edges and images without edges separately based on the equation (112).
Step 6	Combine the recovered edges and the reconstructed image without edges to get corresponding reconstructed 2D components. (2D image: Combine the recovered edges and the reconstructed image without edges to get reconstructed 2D image.)
Step 7	Combined all 2D components together to get the reconstructed 3D image. (2D image: Skip this step.)
Output	The reconstructed 3D image (or 2D image)

6.2.3 Simulation Results

The 3D Cat Map based image encryption algorithm has been successfully applied to several 2D and 3D images. In this section, some experimental results will be provided to show the performance of the presented encryption method. Canny edge detector is used

www.manaraa.com

to get the edge maps in the experiments. Both edges and the image without edges are encrypted in all examples in this section.

6.2.3.1 2D Image Encryption

The 2D image consists of only one 2D data matrix. Figure 6.2 gives an example of grayscale image encryption. The edges in Figure 6.2(b) contain all the pixels of the original image with the same locations of the edge map generated using Canny edge detector with threshold 0.1. The image without edges in Figure 6.2(c) is the result of the difference between the original image (Figure 6.2(a)) and its edges (Figure 6.2(b)).

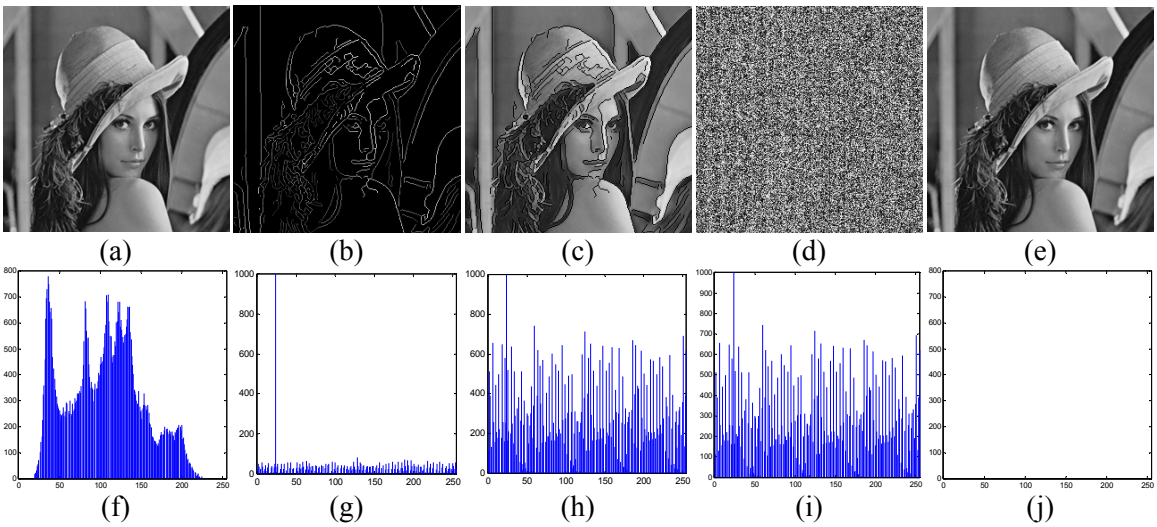


Figure 6.2: Grayscale image encryption using the Canny edge detector. (a) The original grayscale image; (b) Edges using Canny edge detector with threshold 0.1; (c) Image without edges; (d) Encrypted grayscale image (use the absolute intensity values to display the encrypted image), $a=15, b=17, c=18, d=100, n=20$; (e) Reconstructed image; (f) Histogram of (a); (g) Histogram of (b); (h) Histogram of (c); (i) Histogram of (d); (j) Histogram of the difference between (a) and (e).

Both of them are encrypted by the presented 3D Cat Map based image encryption algorithm with the security keys: $a=15, b=17, c=18, d=100, n=20$. The encrypted image shown in Figure 6.2(d) contains a data format of complex numbers in which the

www.manaraa.com

imaginary part is the encrypted edges and the real part is the encrypted image without edges. Its histogram in Figure 6.2(i) shows that the distribution of pixel values of the encrypted image is almost uniform. The encrypted image is significantly different from the original image. This makes the encrypted image completely unrecognizable.

The original image can be completely reconstructed without any distortion. The reconstructed image in Figure 6.2(e) is visually the same as the original image. This can be also demonstrated by the histogram of the difference between the original image and the reconstructed image shown in Figure 6.2(j).

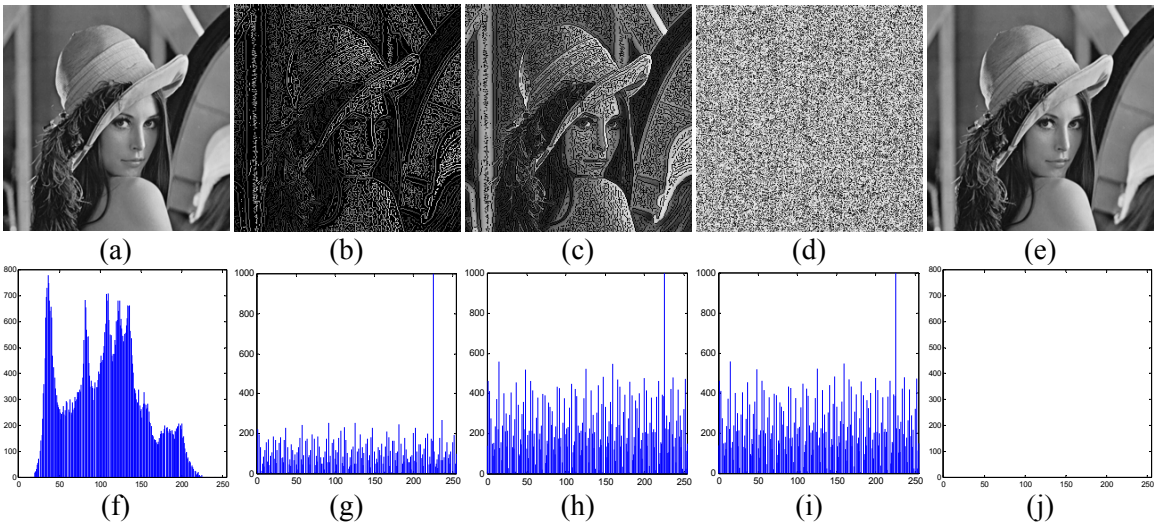


Figure 6.3: Grayscale image encryption using the Sobel edge detector. (a) The original grayscale image; (b) Edges using Sobel edge detector with threshold 0.1; (c) Image without edges; (d) Encrypted grayscale image with security keys, $a=3, b=5, c=10, d=20, n=5$; (e) Reconstructed image; (f) Histogram of (a); (g) Histogram of (b); (h) Histogram of (c); (i) Histogram of (d); (j) Histogram of the difference between (a) and (e).

Another example of grayscale image encryption is shown in Figure 6.3. In this example, the Sobel edge detector with threshold 0.1 are selected and different parameters of the 3D Cat Map, $a=3, b=5, c=10, d=20, n=5$, are set for the encryption process. The edges

www.manaraa.com

and the image without edges are different after applying different edge detection methods and thresholds. The original image can also be completely recovered without any distortion.

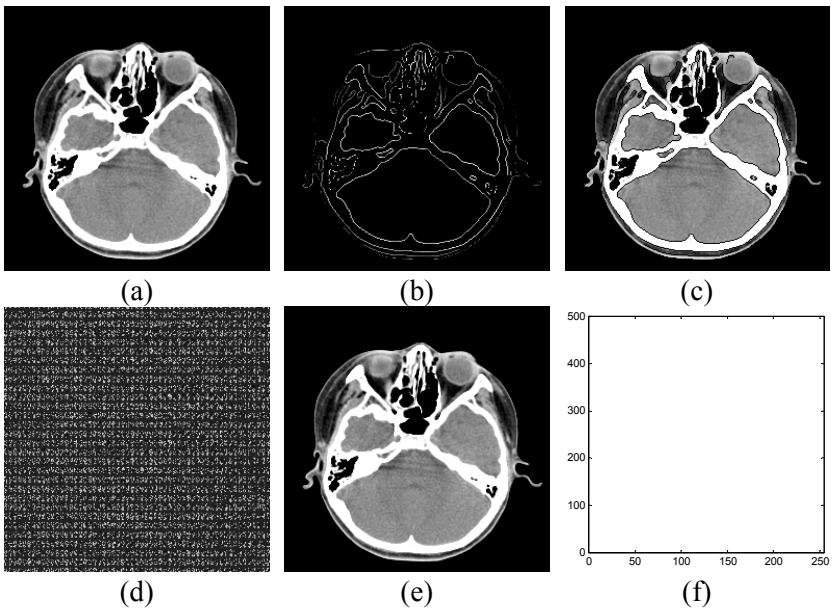


Figure 6.4: Medical image encryption using the Canny edge detector. (a) The original medical image; (b) Edges using Canny edge detector with threshold 0.3; (c) Image without edges; (d) Encrypted medical image with security keys, $a = 5, b = 7, c = 8, d = 10, n = 7$; (e) Reconstructed image; (f) Histogram of the difference between (a) and (e).

Figure 6.4 gives the results of medical image encryption, which is another example of 2D image encryption. The edge detection and encryption processes are the same as those in Figure 6.2 but the threshold for the edge detection process and the security keys in the encryption process are different. The original image can be fully encrypted (shown in Figure 6.4(d)) and reconstructed (shown in Figure 6.4(e)). It can be seen from the reconstructed image in Figure 6.4(e) and the histogram of the difference between the original image and the reconstructed image in Figure 6.4(f) which demonstrate the perfect reconstruction.

www.manaraa.com

6.2.3.2 3D Image Encryption

3D images such as color images contain several 2D components. 3D image encryption can be performed by encrypting their 2D components one by one.

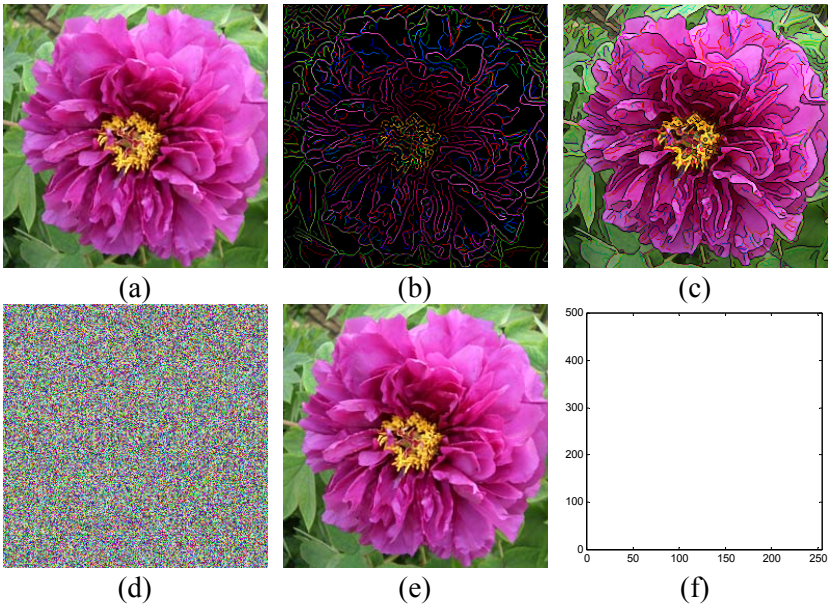


Figure 6.5: Color image encryption using the Canny edge detector. (a) The original color image; (b) Edges using Canny edge detector with threshold 0.1; (c) Image without edges; (d) Encrypted color image with security keys, $a=3, b=5, c=10, d=20, n=5$; (e) Reconstructed color image; (f) Histogram of the difference between (a) and (e).

Figure 6.5 gives an example of color image encryption. The Canny edge detection method and threshold 0.1 are used to obtain edges and the image without edges. The security keys for the encryption process are $a=3, b=5, c=10, d=20, n=5$. The original image can be completely recovered, as shown in Figure 6.5(e). The histogram in Figure 6.5(f) demonstrates this lossless reconstruction.

Figure 6.6 presents another example of color image encryption. The Sobel edge detector with threshold 0.3 is used to obtain the edges and the image without edges in this

www.manaraa.com

example. The results of the edges (shown in Figure 6.6(b)) and the image without edges (shown in Figure 6.6(c)) are different from those in Figure 6.5. The different combination of the parameters of 3D Cat Map, $a=5, b=7, c=8, d=10, n=7$, is also applied to the encryption process. The original image can also be completely reconstructed.

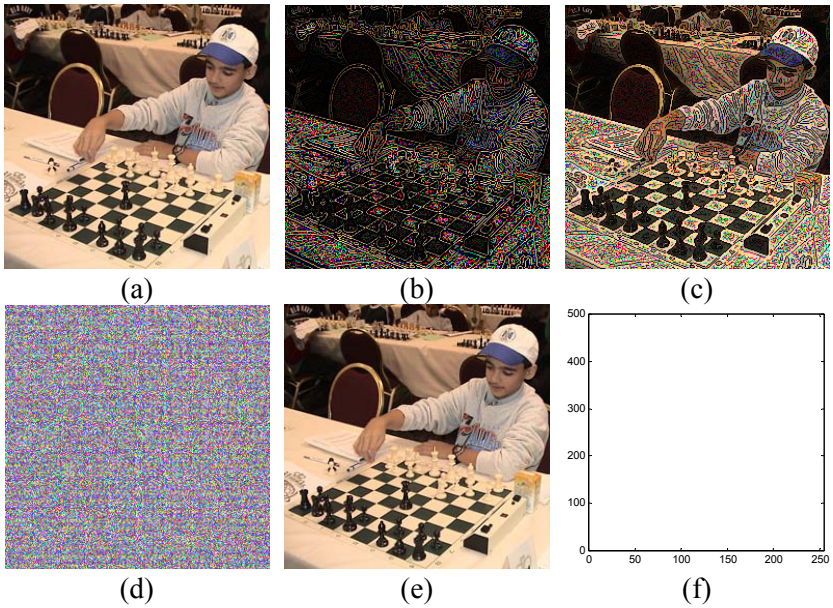


Figure 6.6: Color image encryption using the Sobel edge detector. (a) The original color image; (b) Edges using Sobel edge detector with threshold 0.3; (c) Image without edges; (d) Encrypted color image with security keys, $a=5, b=7, c=8, d=10, n=7$; (e) Reconstructed color image; (f) Histogram of the difference between (a) and (e).

The edge detector, threshold value and parameters of the 3D Cat Map are the same for all the 2D components of the color images that appear in Figures 6.5 and 6.6. Users have the flexibility to choose different edge detectors, thresholds, and parameters for each 2D component, thereby providing a higher level of security and the ability to meet the different security requirements of real-time applications, such as wireless communication and mobile phone services.

www.manaraa.com

6.2.4 Security Analysis

The security key space of the presented 3D Cat Map based image encryption algorithm consists of the type of edge detectors, threshold values, parameters and iteration times of the 3D Cat Map. Each of them has a sufficiently large number of possible variations. Therefore, the key space of the presented encryption algorithm is unlimited. It is impossible for unauthorized users to decode the encrypted image by means of an exhaustive searching for the possible choices in the security key space. As a result, the image is protected by a high level of security.

In cryptanalysis, the chosen-plaintext attack is an attack model in which the attacker can choose a number of plaintexts and then get their corresponding ciphertexts. In this manner, the attacker can choose any useful information as plaintext in order to deduce the security keys of encryption algorithms, or to reconstruct the original plaintexts from the unknown ciphertexts. If the image pixel values are not changed by the encryption process, the chosen-plaintext attack can break the encrypted image without knowing the encryption algorithm or its security keys.

The presented 3D Cat Map based image encryption algorithm changes image pixel values while changing the locations of all image pixels. This ensures that the encrypted image data is not useful in the case of a chosen-plaintext attack. As a result, the presented algorithm is able to withstand chosen-plaintext attacks.

www.manaraa.com

6.3 Medical Image Encryption Using the Edge Map and Chaotic Logistic Map

Edge Map is a binary image obtained from an image using different edge detectors or algorithms. It can be considered a random binary matrix since the edge map will change as the edge detectors and thresholds change. Therefore, the edge map can be used as a random binary security key to encrypt the binary bit-planes of an image by a simple XOR operation.

Based on this concept, a new image encryption algorithm is introduced combining the edge map and the chaotic logistic map. It is called the EdgeCrypt algorithm. Its applications for encrypting medical images are investigated. Of course, it can be used to encrypt other type of multimedia data such as grayscale images, biometrics, color images and videos.

6.3.1 The New Medical Image Encryption Algorithm

This section introduces a new algorithm, EdgeCrypt, to encrypt medical images using an edge map.

The underlying foundation of the EdgeCrypt algorithm is to encrypt medical images by changing the image data. It obtains the edge map of the medical image by applying a specific type of edge detector such as Canny, or Sobel, or Prewitt, or any other, with a certain threshold value. The algorithm then decomposes the medical image into several

www.manaraa.com

binary bit-planes, encrypts all bit-planes by performing an XOR operation between the edge map and each bit-plane, encrypts the edge map using a random bit sequence generated from the logic chaotic map, interleaves the encrypted edge map among the XORed bit-planes, reverses the order of all bit-planes, and combines them to obtain the final encrypted medical images. The block diagram of the EdgeCrypt algorithm is shown in Figure 6.7.

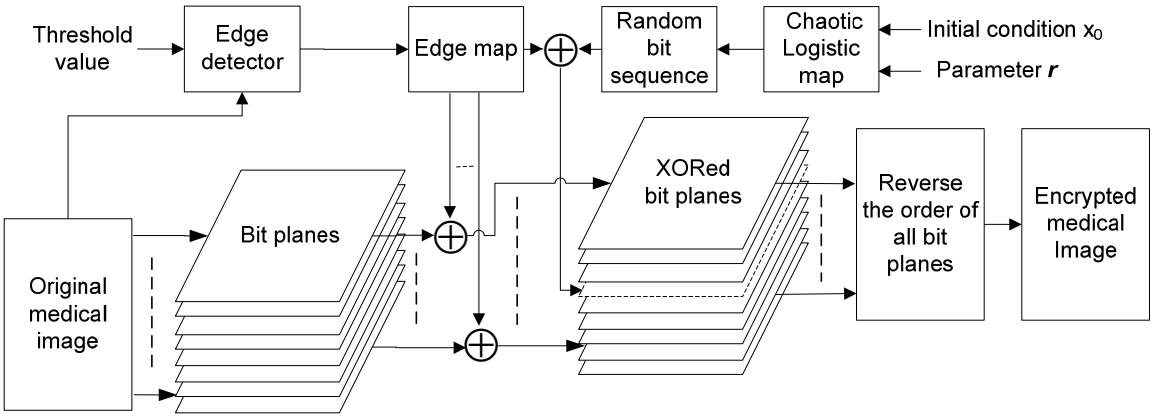


Figure 6.7: The block diagram of the EdgeCrypt algorithm.

To improve the security of the algorithm, a bit-plane shuffling process is added to change the values of image pixels in the vertical direction. Users have the flexibility to utilize any existing approach to shuffle the order of bit-planes. The order of the bit-planes is reversed in this section.

A random bit sequence generated from a logic chaotic map is used to encrypt the edge map. The encrypted edge map is obtained by performing an additional XOR operation between each bit of a random bit sequence and each pixel of the edge map. It is then interleaved among the XORed bit-planes. The chaotic logistic map is defined as follows.

www.manaraa.com

$$x_{n+1} = r x_n (1 - x_n) \tag{113}$$

where parameter r is a rational number, $3.5699456 < r \le 4$, $0 < x_n < 1$ and $n = 0,1,2,...$

If the size of the edge map is $M \times N$, the random bit sequence can be generated using the definition,

$$b_n = \begin{cases} 1 & x_n \ge 0.5 \\ 0 & x_n < 0.5 \end{cases} \tag{114}$$

where $n = 0,1,2,...,MN-1$.

The security keys for the EdgeCrypt algorithm include the initial condition x_0 and parameter r of the logic chaotic map, the interleaved location of the edge map, the type of the edge detector and its threshold value. Users have the flexibility to choose any existing approach for edge detection and select any threshold value for the edge detector. The edge map can also be interleaved into two bit-planes.

In the decryption process, authorized users do not have to know the type of the edge detector and its threshold value to reconstruct the original image, since the edge map has been sent to the users with the encrypted image. However, the edge map can only be completely recovered by using the correct security keys: the location to interleave the edge map as well as the initial condition x_0 and parameter r of the logic chaotic map.

The decryption process first decomposes the encrypted image into binary bit-planes. It then reverses the order of all bit-planes and extracts the edge map from the bit-planes. The edge map is reconstructed using security keys. The algorithm performs an XOR

www.manaraa.com

operation between the edge map and each bit-plane and combines the XORed bit-planes to obtain the reconstructed medical image.

6.3.2 Experimental Results and Analysis

The EdgeCrypt algorithm has been successfully implemented in more than 16 medical images. This section presents simulation examples to demonstrate the algorithm's performance for medical image encryption. The EdgeCrypt algorithm is compared with the AES algorithm to demonstrate its encryption efficiency. The algorithm is also proved to encrypt the selective objects /regions and other types of images.

The interleaved location of the edge map in all examples in this section is between the first bit-plane, which contains the most significant bits of all image pixels, and the second bit-plane, which contains the second most significant bits of image pixels.

6.3.2.1 Examples of Medical Image Encryption

Figure 6.8 gives an example of the MRI image encryption. The encrypted image in Figure 6.8(c) is completely different from the original MRI brain image in Figure 6.8(a). The histogram in Figure 6.8(g) shows the nearly equal distribution of the pixel values in the encrypted image. This makes it difficult for attackers to break the encrypted image.

The original image has been completely reconstructed. The reconstructed image in Figure 6.8(d) and its histogram in Figure 6.8(h) verify the reconstruction, since both are identical to the original image.

www.manaraa.com

The edge map in this example is generated by the Sobel edge detector with threshold 0.5. It is encrypted by logic chaotic map with the initial condition $x_0 = 0.6$ and the parameter $r = 3.65$.

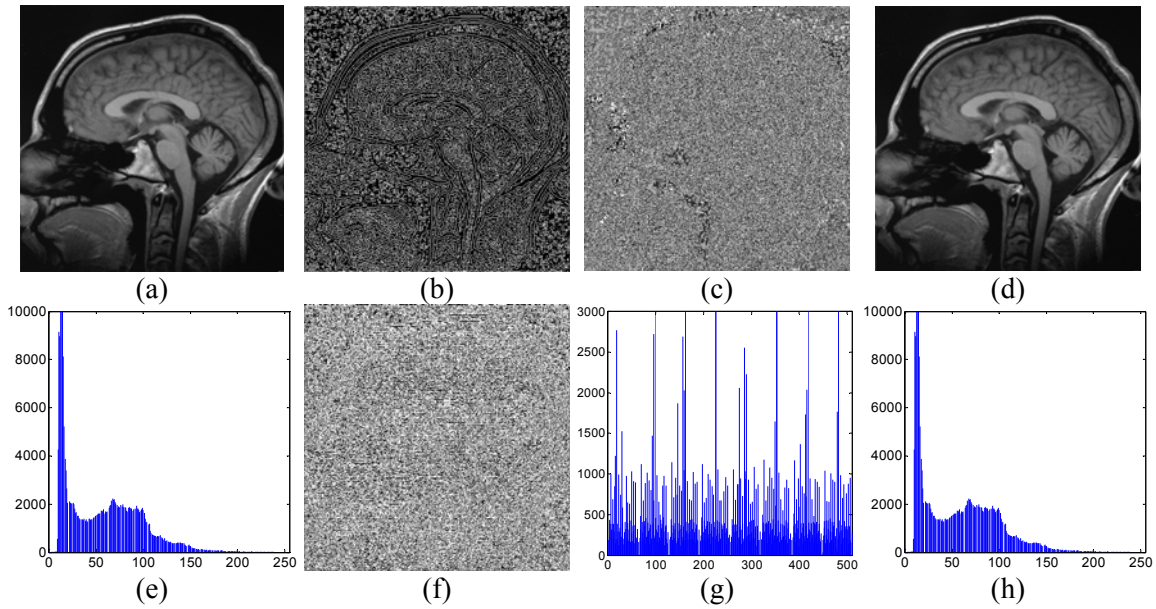


Figure 6.8: MRI image encryption. (a) The original MRI image; (b) The edge map obtained by Sobel edge detector with threshold 0.5; (c) The encrypted MRI image, (d) The reconstructed MRI image; (e) Histogram of the original MRI image; (f) The encrypted edge map, $x_0 = 0.6$, $r = 3.65$; (g) Histogram of the encrypted MRI image; (h) Histogram of the reconstructed MRI image.

An example of the CT image encryption is given in Figure 6.9. The original CT image has been fully encrypted (Figure 6.9(c)) and completely reconstructed (Figure 6.9(d)). The histogram of the difference between the original image and the reconstructed image verify this perfect reconstruction. The results show that the EdgeCrypt algorithm is able to fully encrypt the medical images.

www.manaraa.com

The edge map in this example is obtained from the Canny edge detector with threshold 0.1. It is also protected by the chaotic logistic map with security keys, $x_0 = 0.2$ and $r = 3.8$.

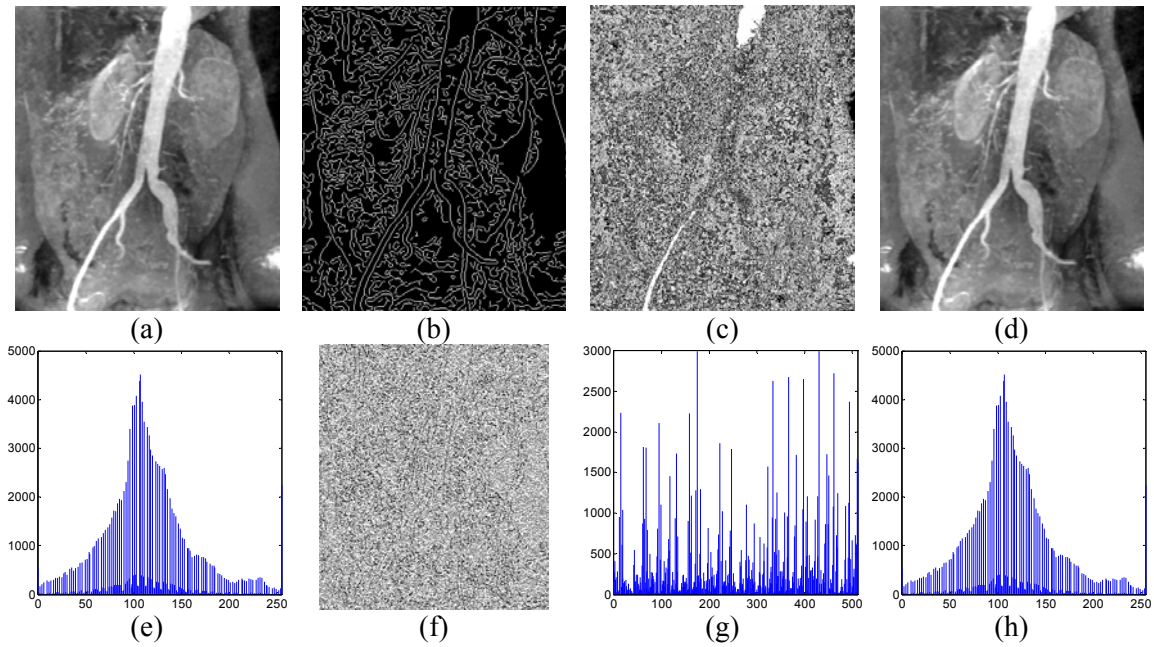


Figure 6.9: CT image encryption. (a) The original CT image; (b) The edge map obtained by Canny edge detector with threshold 0.1; (c) The encrypted CT image, (d) The reconstructed CT image; (e) Histogram of the original CT image; (f) the encrypted edge map, $x_0 = 0.2$, $r = 3.8$; (g) Histogram of the encrypted CT image; (h) Histogram of the reconstructed CT image.

Figure 6.10 gives an example of X-ray image encryption. The edge map in this example is obtained by the Prewitt edge detector with threshold 0.3. It is encrypted by the chaotic logistic map with security keys, $x_0 = 0.8$ and $r = 3.7$.

One interesting result is the encrypted image in Figure 6.10 (b), which shows that the EdgeCrypt algorithm can be used to protect the selected objects or regions within medical images that may contain important or private patient information. This is another advantage of the algorithm.

www.manaraa.com

The original X-ray image is also completely reconstructed in Figure 6.10(c) because the histogram of the difference between the reconstructed X-ray image and the original X-ray image is zero in Figure 6.10 (f). These results further verify the EdgeCrypt algorithm is a lossless encryption method.

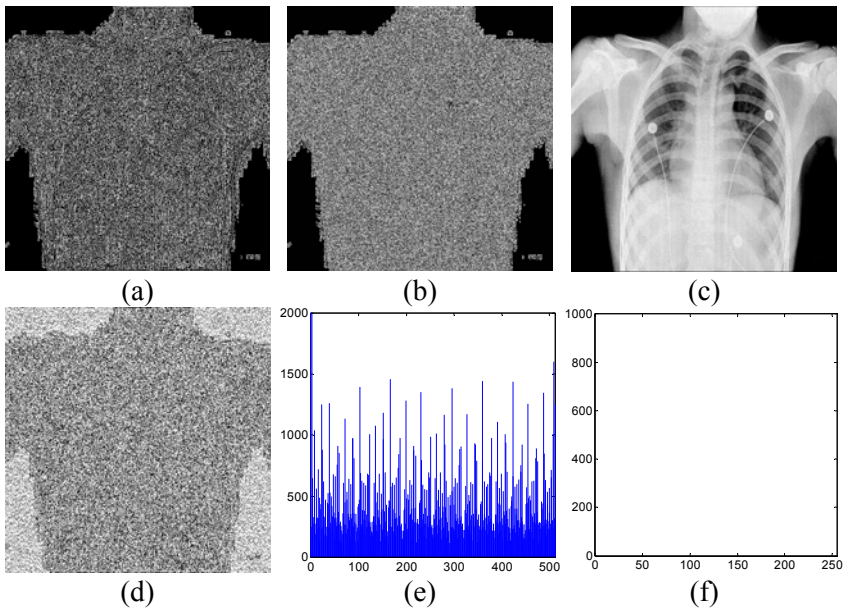


Figure 6.10: X-ray image encryption. (a) The edge map obtained by Prewitt edge detector with threshold 0.3; (b) The encrypted X-ray image; (c) The reconstructed X-ray image; (d) the encrypted edge map, $x_0 = 0.8$, $r = 3.7$; (e) Histogram of the encrypted X-ray image; (f) Histogram of the difference between the original X-ray image and the reconstructed image.

6.3.2.2 Performance Measure and Comparison

To show the efficiency of the EdgeCrypt algorithm for medical image encryption, it was compared with the AES algorithm implemented in [177] across several images.

The 512×512 MRI brain image shown in Fig. 6.8(a) is used as an example of the obtained results. The execution time of this MRI image encryption using the EdgeCrypt algorithm and the AES algorithm was measured by a computer running Windows XP

www.manaraa.com

operating system with 2GB memory and a CPU using Intel Core2 Quad Q6700. The AES algorithm took 521.67 seconds to encrypt the MRI image. However, the EdgeCrypt algorithm took only 17.78 seconds to encrypt the same MRI image. This demonstrates that the speed of the EdgeCrypt algorithm is far superior to that of the AES algorithm. This shows the suitability of the EdgeCrypt algorithm for real-time medical applications such as wireless medical networking and mobile medical services. Furthermore, since all its processes operate on the binary bit levels, the EdgeCrypt algorithm is easy to implement in hardware such as an FPGA.

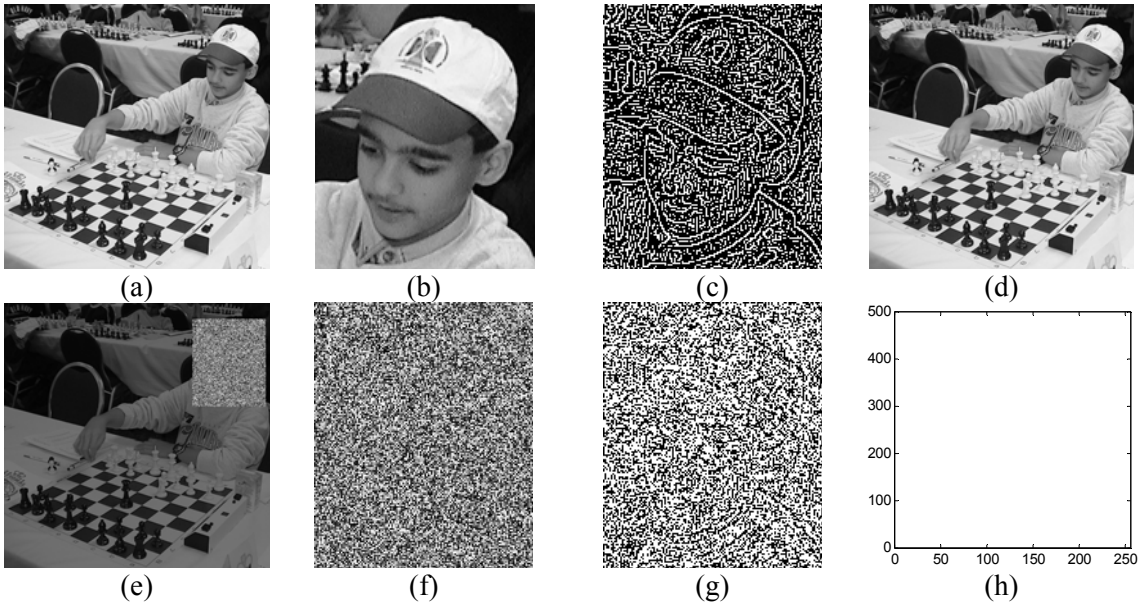


Figure 6.11: Grayscale image encryption. (a) Original image; (b) Selected object; (c) The edge map obtained by Roberts edge detector with threshold 0.4; (b) Encrypted image; (d) Reconstructed image; (e) Encrypted image; (f) Encrypted object; (g) The encrypted edge map, $x_0 = 0.8$, $r = 3.7$; (h) Histogram of the difference between the original image and the reconstructed image.

6.3.2.3 Other Applications

In addition, the EdgeCrypt algorithm is able to encrypt other types of images such as grayscale images or color images.

www.manaraa.com

Figure 6.11 gives an example of grayscale image encryption. This example shows that the EdgeCrypt algorithm can be used to ensure the security of grayscale images. It further demonstrates that the algorithm can encrypt the selected regions or objects in images for the purpose of privacy protection.

6.3.3 Cryptanalysis

Security is important not only for the encrypted objects but also for the encryption algorithm itself. The security issues of the EdgeCrypt algorithm are discussed in this section.

6.3.3.1 Security Key Space

The security keys of the EdgeCrypt algorithm consist of the location to interleave the edge map, the type of the edge detector and its threshold, as well as the initial condition and the parameter of the logic chaotic map. A large number of possible types of edge detectors can be used for the EdgeCrypt algorithm. The possible threshold values for a specific edge detector are unlimited. The initial condition x_0 and the parameter r of the logic chaotic map also have a sufficiently large number of possible variations. As a result, the possible number of combinations of these security keys is inexhaustible. Hence, the security key space of the EdgeCrypt algorithm is unlimited.

www.manaraa.com

6.3.3.2 Plaintext Attacks

An edge map is determined by the type of the edge detector, the threshold of the edge detector and the content of the original image. The pixel data of the encrypted bit-planes changes with different edge detectors and the original image data.

A pseudo-random bit sequence generated by the logic chaotic map is used to encrypt the edge map. This ensures that the edge map is well protected. It is then interleaved into the encrypted bit-planes. The order of all bit-planes is then reversed. The resulting encrypted image is the combination of all of them. These processes further change the image pixel data and result in a nearly equal distribution of the pixel values of the encrypted image. Thus, the data of the encrypted image is immune to plaintext attacks such as the known-plaintext attacks and the chosen-plaintext attacks. This allows encrypted medical images to be protected with a high level of security.

www.manaraa.com

6.4 Image Encryption Using Binary Key-images

Used as a random binary security key, the edge map is obtained from the same original images encrypted by the presented encryption algorithm in Section 6.3. Such an edge map is difficult for authorized users to reconstruct for the purpose of image decryption because the original images are not available. The encrypted edge map is interposed into the XORed bit-planes of the images in such a way that authorized users can receive the encrypted images and the edge map simultaneously. This allows authorized users to reconstruct the original images more easily. However, this method needs (1) an extra process to protect the security key matrix, for example, an edge map encryption process using chaotic logistic map; (2) more data to be transmitted to the users, such as the encrypted edge map.

To overcome this problem while improving the algorithm's efficiency and security levels, the concept of using the edge map as a random security key matrix is extended to produce a binary "key-image". This key-image takes the form of a binary bit-plane, an edge map or a binary image that is obtained from another new/existing image with the same size as the image to be encrypted. Based on this concept, two novel image encryption algorithms are introduced using the bit-plane and edge map respectively.

6.4.1 The New Image Encryption Algorithms

This section introduces a binary image as a "key-image" that is the same size as the image to be encrypted. Two image encryption algorithms are introduced using this key-

www.manaraa.com

image. One is called the BitplaneCrypt algorithm, while the other is called the EdgemapCrypt algorithm. Both are able to fully encrypt 2D and 3D images such as grayscale images, color images and medical images.

The underlying foundation of both algorithms is to change image pixel values by performing the XOR operation between the key-image and each bit-plane of the original image. This is followed by an image scrambling process that changes the locations of image pixels or blocks.

6.4.1.1 The BitplaneCrypt Algorithm

The BitplaneCrypt algorithm uses a binary bit-plane as the key-image. This bit-plane is extracted from another image which is different from the original image being encrypted.

Figure 6.12 describes the BitplaneCrypt algorithm. It generates the key-image by exacting the r^{th} bit-plane of the selected image, where r is the location of the bit-plane. The algorithm then decomposes the original image into its binary bit-planes and performs an XOR operation between each of these bit-planes and the key-image. The order of bit-planes is then inverted. The algorithm combines the bit-planes together. Finally, a selected scrambling algorithm is applied to the image to obtain the final encrypted image.

Since the 3D image contains several 2D data matrices called 2D components, the 3D image encryption can be accomplished by encrypting all its 2D components one by one.

Users have the flexibility to choose any new or existing image to generate the key-image. This image can be a public image or an image created by the users themselves. The key-

www.manaraa.com

image can be selected from one of the bit-planes of this image. Any image scrambling method can be used in the BitplaneCrypt algorithm. Therefore, the security keys of the algorithm consist of the image (or image location) that was used to generate the key-image, the location of the bit-plane chosen as the key-image and the security keys of the scrambling method, if applicable.

Algorithm-1	***The BitplaneCrypt Algorithm***
Input	The original 2D or 3D image to be encrypted.
Step 1	Choose a new or existing image with the same size of the original image, (convert the image into 2D if it is a 3D image).
Step 2	Obtain the key-image by extracting the r^{th} bit-plane of the image in Step 1.
Step 3	Decompose the original image or each component of the 3D image into its binary bit-planes.
Step 4	Perform the XOR operation between the key-image and each bit-plane in Step 3.
Step 5	Invert the order of all bit-planes.
Step 6	Combine all bit-planes together to obtain the 2D image or components
Step 7	Scramble the resulting image or components in Step 6 using a selected scrambling method to generate the resulting encrypted image. (For the 3D image, scramble its 2D components one by one).
Output	The encrypted 2D or 3D image.

Figure 6.12: The BitplaneCrypt algorithm

The correct security keys should be given to authorized users to generate the key-image. In the decryption process, the user unscrambles the encrypted image using a scrambling

www.manaraa.com

algorithm and its security keys. It then decomposes the image into bit-planes. Each bit-plane is applied to an XOR operation with the key-image. The order of bit-planes is reverted to the original order. The original image can be reconstructed by combining all bit-planes.

In a similar manner to the encryption process, the original 3D image can be reconstructed by decoding its 2D components one by one.

6.4.1.2 The EdgemapCrypt Algorithm

This section introduces a new image encryption algorithm using an edge map called the EdgemapCrypt algorithm. In this algorithm, the edge map is considered the key-image. Using a specific edge detector with a selected threshold value, the edge map is generated from another image with the same size as the original image.

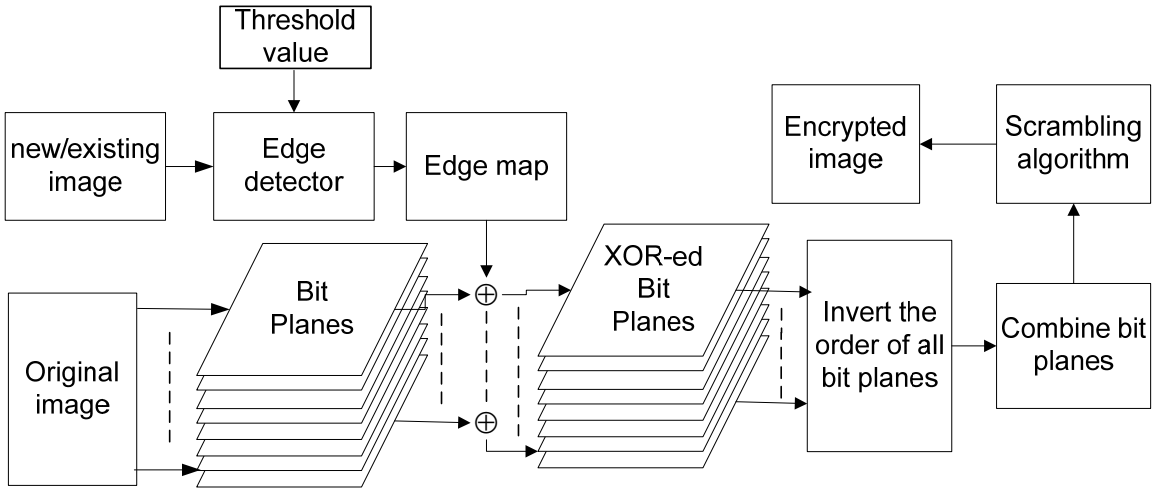


Figure 6.13: The EdgemapCrypt algorithm

The EdgemapCrypt algorithm first decomposes the original image into its binary bit-planes. By performing an XOR operation with the key-image (the edge map created from

www.manaraa.com

another image), each binary bit-plane is then encrypted. Next, the algorithm inverts the order of all XORed bit-planes and combines them together. The resulting image is scrambled using a selected scrambling algorithm to generate the final encrypted image. Figure 6.13 illustrates the EdgemapCrypt algorithm.

In a manner similar to the BitplaneCrypt algorithm, the EdgemapCrypt algorithm encrypts 3D images by working on their 2D components individually.

Any image with the same size as the original image can be used to generate the edge map, the key-image. It can be an image in the public online database or a new image generated by the user. The edge map can be obtained using any edge detector such as Canny, Sobel, or Prewitt. Users have the flexibility to choose any image, any edge detector and any threshold value to generate the edge map to be used as a key-image. They also have the flexibility to use any image scrambling method for the EdgemapCrypt algorithm. Therefore, this algorithm's security keys consist of the image or its location (used to generate the edge map), the type of edge detector, the edge detector's threshold and the security keys of the scrambling algorithm.

To reconstruct the original image, users should be provided with the security keys that will allow them to obtain the correct edge map. The decryption process first generates the edge map from the selected image using the security keys. It then unscrambles the encrypted image using the selected scrambling algorithm. Next, it decomposes the unscrambled image into its binary bit-planes and performs an XOR operation between the edge map and each bit-plane. The order of all bit-planes is restored to the original order. By combining all bit-planes, the reconstructed 2D image/component can be obtained.

www.manaraa.com

6.4.2 Experimental Results

The BitplaneCrypt and EdgemapCrypt algorithms have been successfully implemented in 18 different 2D and 3D images such as grayscale images, color images and medical images. To show the performance of the algorithms for 2D and 3D image encryption, several simulation results are given. For simplicity, both algorithms utilize the image scrambling algorithm based on the *(n, k, p)*-Gray code in [64] for computer simulation with the security keys: $n = 2, p = 0$. Figure 6.14 shows several 2D images used as test images or images to generate the key-image.

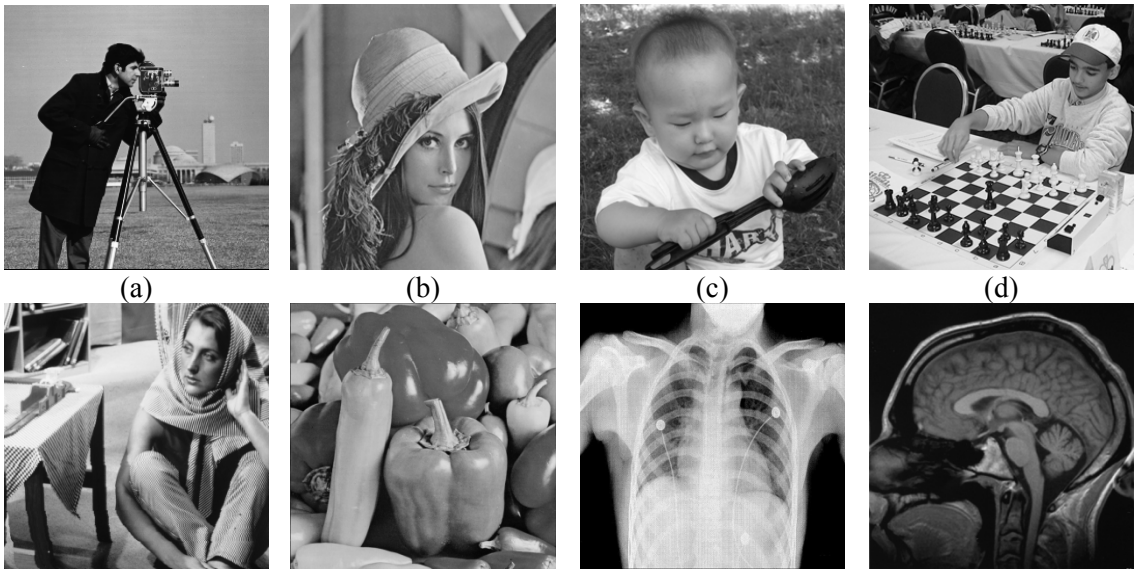


Figure 6.14: Test images. (a) Cameraman, 256×256; (b) Lena, 256×256; (c) Baby, 256×256; (d) Chessplayer, 256×256; (e) Barbara, 512×512; (f) Peppers, 512×512; (g) CT ribs image, 512×512; (h) MRI brain image, 512×512.

www.manaraa.com

6.4.2.1 2D Image Encryption

There are several types of 2D images such as grayscale images, medical images and biometrics. The 2D image can be decomposed into several binary bit-planes and encrypted one by one.

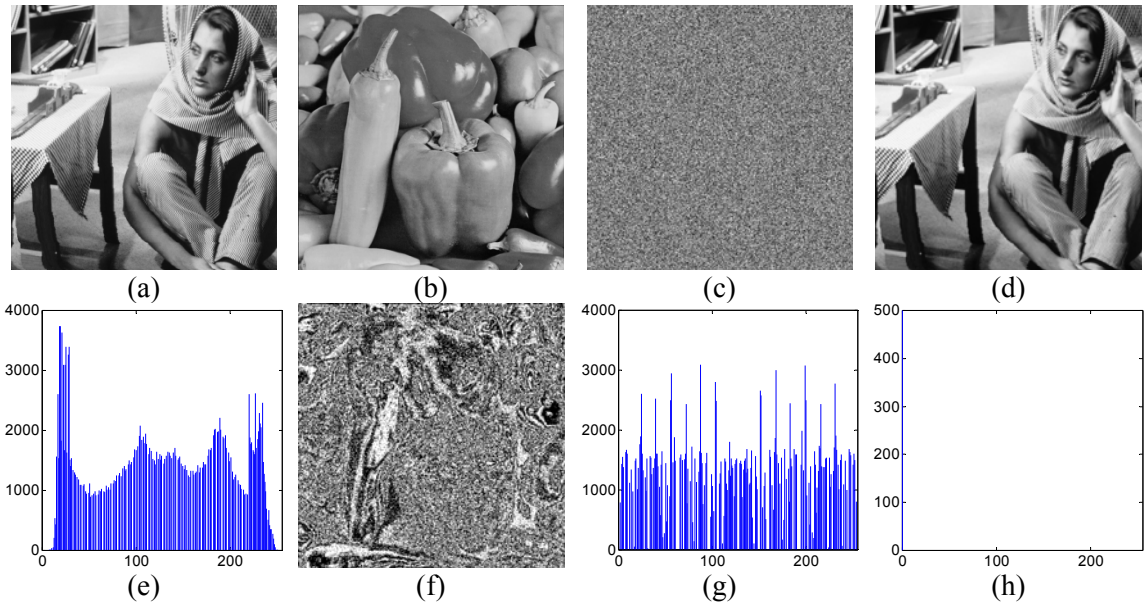


Figure 6.15: Grayscale image encryption using the BitplaneCrypt algorithm. (a) The original 512×512 grayscale image; (b) A 512×512 Peppers image; (c) The encrypted image; (d) The reconstructed image; (e) Histogram of the original image in (a); (f) The 5th bit-plane of the Peppers image in (b); (g) Histogram of the encrypted image in (c); (h) Histogram of the difference between (d) and (a).

Figure 6.15 gives an example of grayscale image encryption using the BitplaneCrypt algorithm. The key-image in this example is the 5th bit-plane of a 512×512 grayscale Peppers image. Figure 6.16 gives the result of a grayscale image encryption using the EdgemapCrypt algorithm. The key-image is obtained from a 256×256 grayscale Cameraman image using the Sobel edge detector with a threshold 0.3.

www.manaraa.com

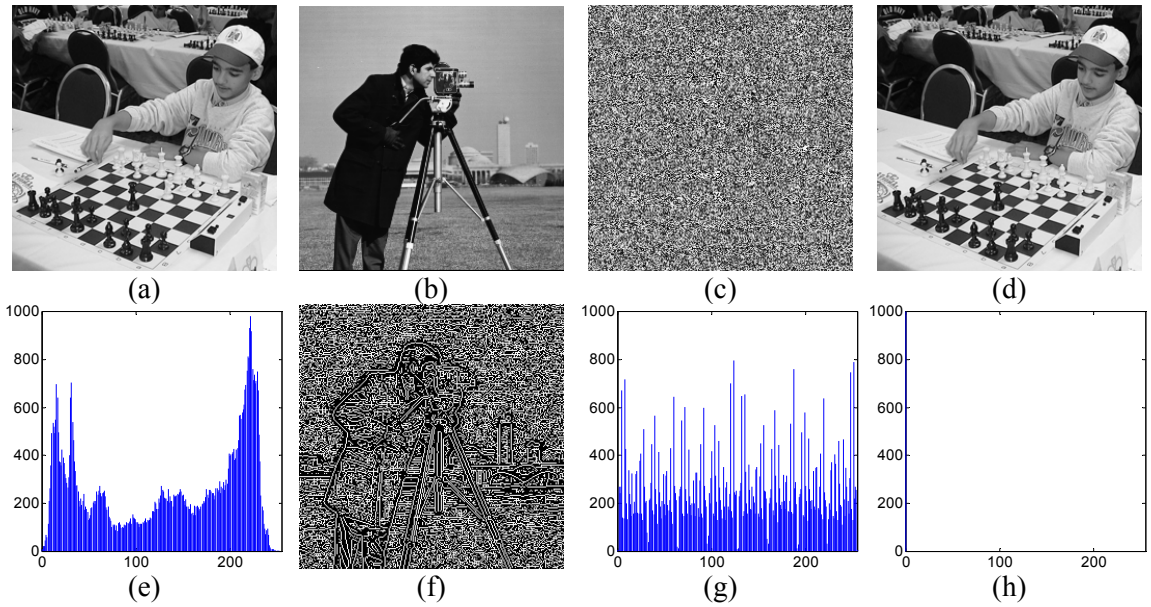


Figure 6.16: Grayscale image encryption using the EdgemapCrypt algorithm. (a) The original 256×256 grayscale image; (b) A 256×256 Cameraman image; (c) The encrypted image; (d) The reconstructed image; (e) Histogram of the original image in (a); (f) The edge map of the Cameraman image in (b), Sobel, 0.3; (g) Histogram of the encrypted image in (c); (h) Histogram of the difference between (d) and (a).

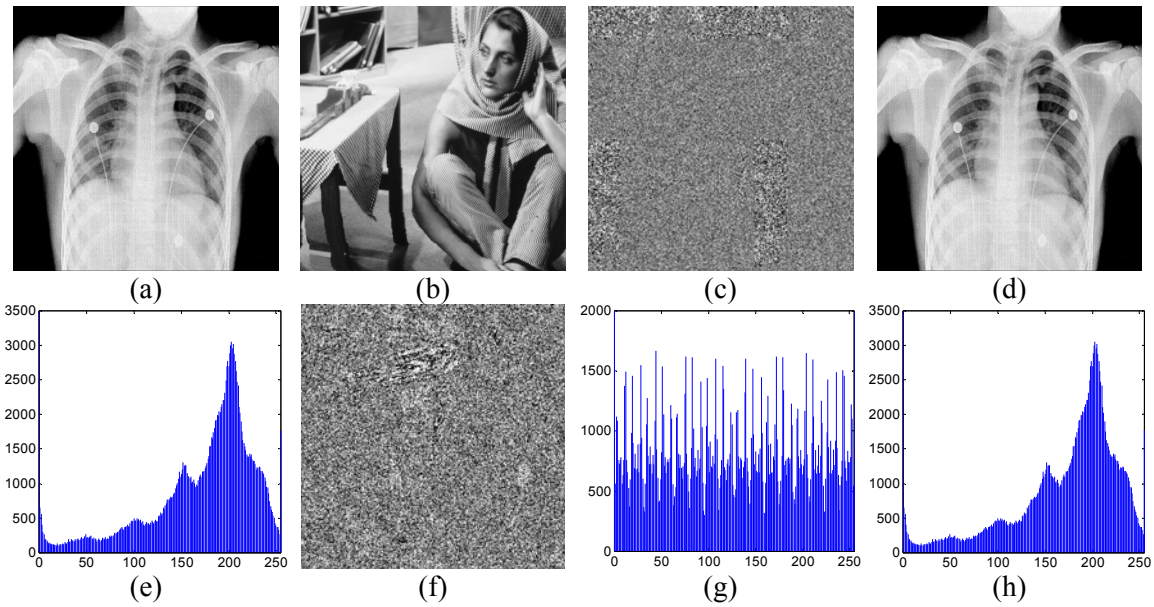


Figure 6.17: Medical image encryption using the BitplaneCrypt algorithm. (a) The original 512×512 CT ribs image; (b) A 512×512 Barbara image; (c) The encrypted image; (d) The reconstructed image; (e) Histogram of the original image in (a); (f) The 7th bit-plane of the Barbara image in (b); (g) Histogram of the encrypted image in (c); (h) Histogram of the reconstructed image in (d).

www.manaraa.com

From these results, the original images are fully encrypted as shown in Figures 6.15(c) and 6.16(c). The distributions of the pixel values of the encrypted images are almost equal in terms of grayscale value range, as shown in Figures 6.15 (g) and 6.16(g). This is one advantage of the presented algorithms. The original images are completely reconstructed. This can be verified by the reconstructed images in Figures 6.15(d) and 6.16(d) and the histograms of the differences between the original images and the reconstructed images in Figures 6.15(h) and 6.16(h).

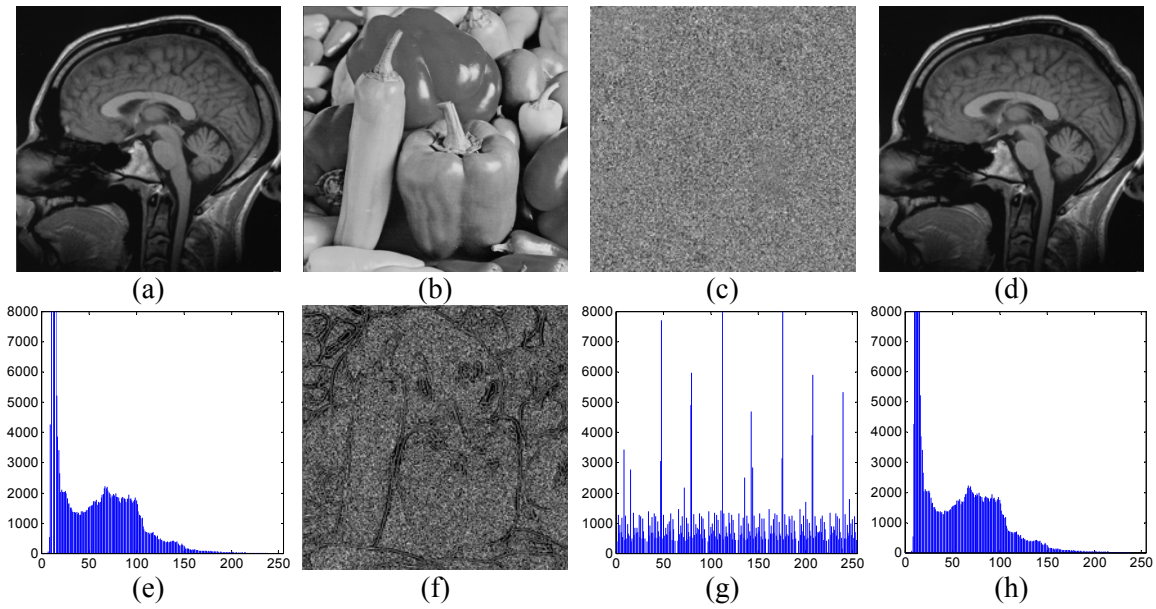


Figure 6.18: Medical image encryption using the EdgemapCrypt algorithm. (a) The original 512×512 MRI brain image; (b) A 512×512 Peppers image; (c) The encrypted image; (d) The reconstructed image; (e) Histogram of the original image in (a); (f) The edge map of the Peppers image in (b), Prewitt, 0.2; (g) Histogram of the encrypted image in (c); (h) Histogram of the reconstructed image in (d).

The medical image encryption examples, which use the BitplaneCrypt and EdgemapCrypt algorithms, are shown in Figures 6.17 and 6.18, respectively. The key-image of the BitplaneCrypt algorithm in Figure 6.17 is the 7th bit-plane of a 512×512

www.manaraa.com

grayscale Barbara image. The key-image of the EdgemapCrypt algorithm in Figure 6.18 is generated from a 512×512 grayscale Peppers image using a Prewitt edge detector with a threshold of 0.2. The original medical images are also fully encrypted and completely reconstructed. This full encryption can be demonstrated by the encrypted images in Figures 6.17(c) and 6.18(c) and their histograms in Figures 6.17(g) and 6.18(g). The reconstructed images in Figures 6.17(d) and 6.18(d) and their histograms in Figures 6.17(h) and 6.18(h) verify the perfect reconstruction.

6.4.2.2 3D Image Encryption

3D image encryption can be accomplished by using the presented algorithms to encrypt all the 2D components one by one.

Figures 6.19 and 6.20 show examples of color image encryption using the BitplaneCrypt and EdgemapCrypt algorithms, respectively. The key-image in Figure 6.19 uses the 4^{th} bit-plane of a 512×512 grayscale Chessplayer image. The key image in Figure 6.20 is an edge map generated from a 512×512 grayscale Barbara image using Canny edge detector with the threshold of 0.1.

The results show that the color images are fully encrypted and then completely reconstructed. The histograms in Figures 6.19(g) and 6.20(g) also verify that the distributions of the encryption images are equal in the data level range. The reconstructed images in Figures 6.19(d) and 6.20(d) and their histograms in Figures 6.19(h) and 6.20(h) demonstrate the complete reconstruction of the original images.

www.manaraa.com

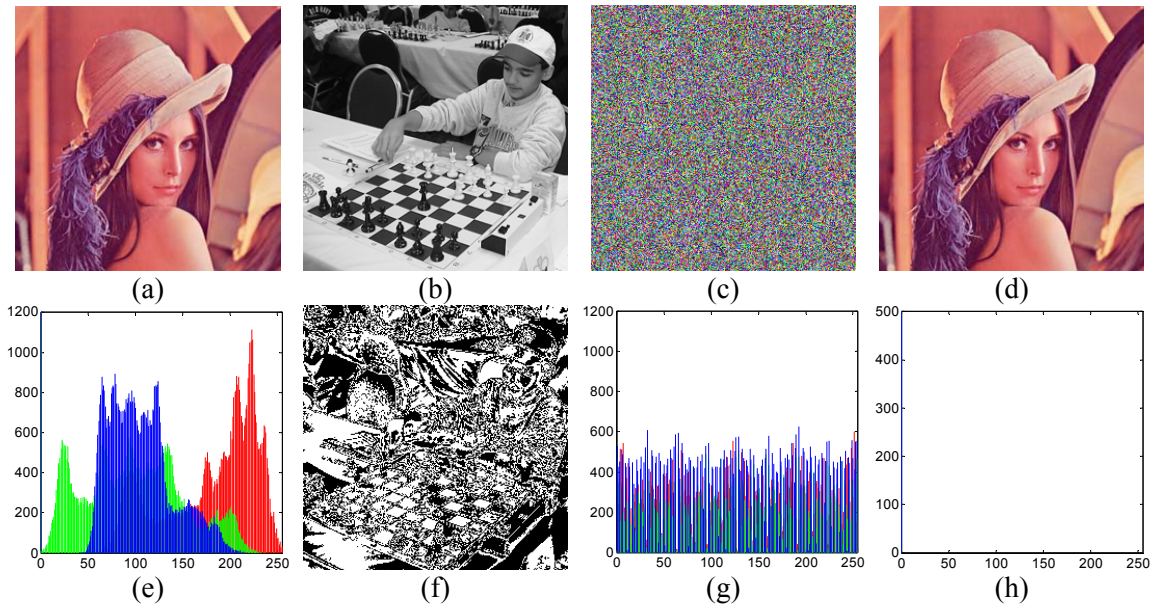


Figure 6.19: Color image encryption using the BitplaneCrypt algorithm. (a) The original 256×256 color image; (b) A 256×256 grayscale Chessplayer image; (c) The encrypted color image; (d) The reconstructed color image; (e) Histogram of the original image in (a); (f) The 4th bit-plane of the Chessplayer image in (b); (g) Histogram of the encrypted image in (c); (h) Histogram of the difference between (d) and (a).

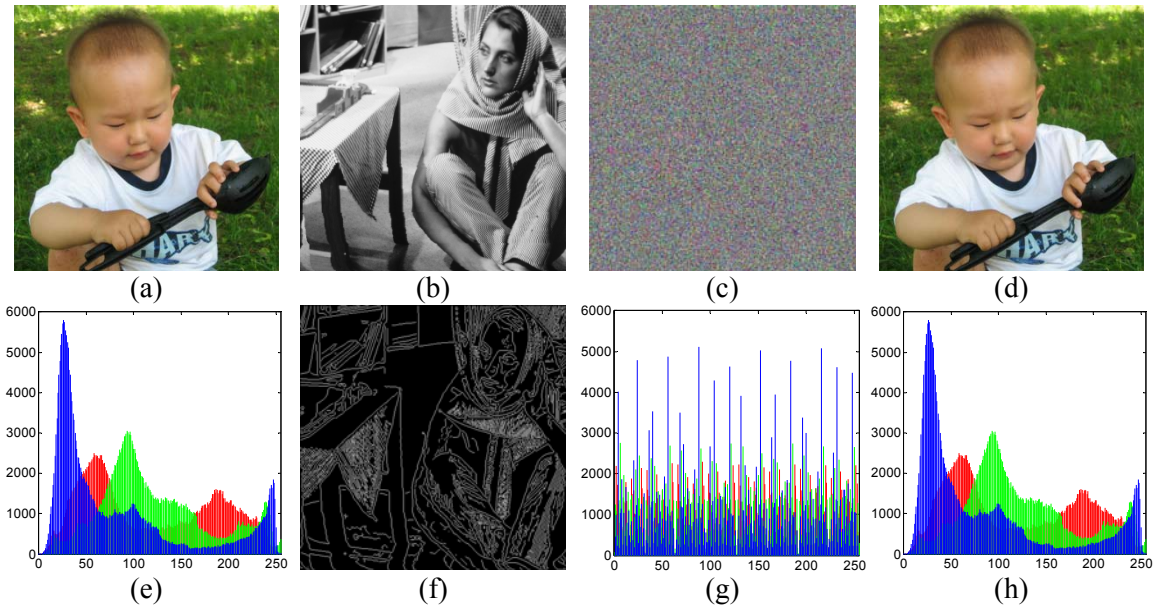


Figure 6.20: Color image encryption using the EdgemapCrypt algorithm. (a) The original 512×512 color image; (b) A 512×512 grayscale Barbara image; (c) The encrypted color image; (d) The reconstructed color image; (e) Histogram of the original image in (a); (f) The edge map of the Barbara image in (b), Canny, 0.1; (g) Histogram of the encrypted image in (c); (h) Histogram of the reconstructed image in (d).

www.manaraa.com

6.4.3 Security Analysis

Security is important for both the encrypted objects and the encryption algorithms. This section discusses some of the security issues associated with the BitplaneCrypt and EdgemapCrypt algorithms from the cryptography point of view.

6.4.3.1 Security Key Space

As established in Section 6.4.1, the security keys of the BitplaneCrypt algorithm are composed of a combination of the image (or the image's location), the location of the bit-plane being used as the key-image and the security keys of the scrambling algorithm. The security keys of the EdgemapCrypt algorithm, on the other hand, consist of the image (or that image's location), the type of edge detector, the edge detector's threshold and the security keys of the scrambling algorithm.

The combination of the security keys is extremely important for both of the presented algorithms. The original image can be completely reconstructed without distortion only when the correct security keys are used. This can be verified by the reconstructed images in Figures 6.21(b) and 6.22(b) and their histograms in Figures 6.21 (f) and 6.22(f). Otherwise, the reconstructed images cannot be recognized as shown in Figures 6.21 (c) and (d) and Figures 6.22 (c) and (d).

Any image with the same size as the original image can be used to generate the key-image for both algorithms. It therefore has a huge number of possible variations, assuming P_I. Each of its bit-planes can be used as a key-image for the BitplaneCrypt algorithm. If its gray levels are between 0 and 255, the number of possible variations of

www.manaraa.com

the key-image for this algorithm is $8P_I$. In addition, any image scrambling algorithm can be used to scramble the bit-planes in both algorithms. The security keys of the selected image scrambling algorithm are also part of the combination that makes up the security keys for the presented algorithms, assuming their possible variations are P_S and that it is not more than $M!N!$ if the original image is an $M \times N$ grayscale image. Thus, the security key space of the BitplaneCrypt algorithm for an $M \times N$ grayscale image is $8P_IP_S$.

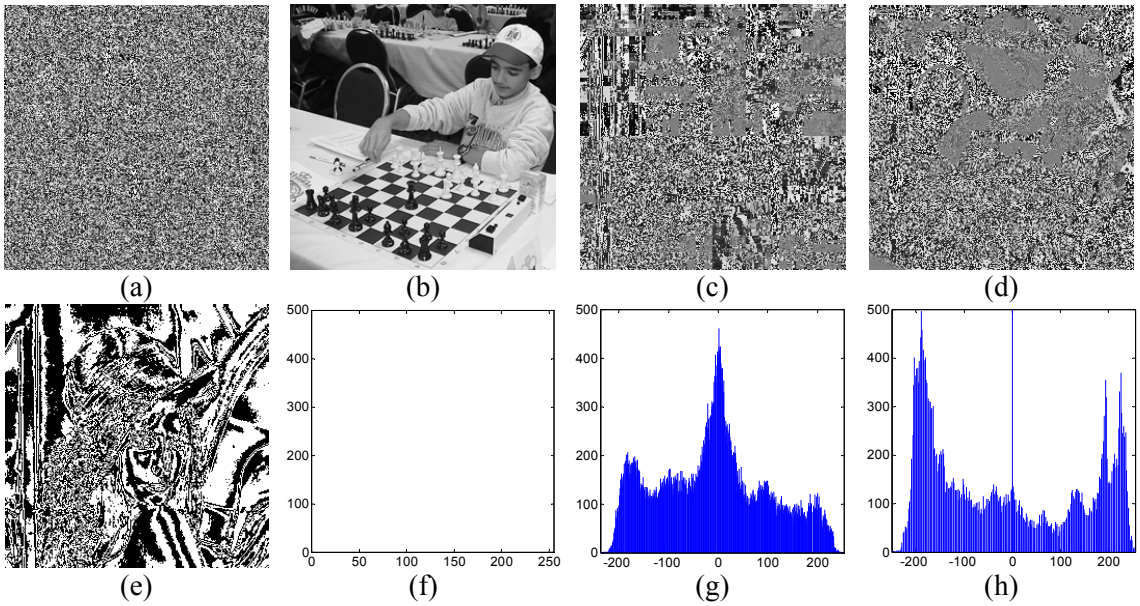


Figure 6.21: Grayscale image decryption using the BitplaneCrypt algorithm with different security keys. (a) The encrypted 256×256 grayscale Chessplayer image with security keys: the 4th bit-plane of the 256×256 grayscale Lena image and $n = 2, p = 0$ for the scrambling algorithm; (b) The reconstructed grayscale image using the correct security keys; (c) The reconstructed grayscale image using the same key-image and $n = 2, p = 2$ for the scrambling algorithm; (d) The reconstructed grayscale image using the 7th bit-plane of the 256×256 grayscale Lena image and the same security keys for the scrambling algorithm; (e) the key-image: the 4th bit-plane of the 256×256 grayscale Lena image; (f) Histogram of the difference between the original image and the reconstructed image in (b); (g) Histogram of the difference between the original image and the reconstructed image in (c); (h) Histogram of the difference between the original image and the reconstructed image in (d).

www.manaraa.com

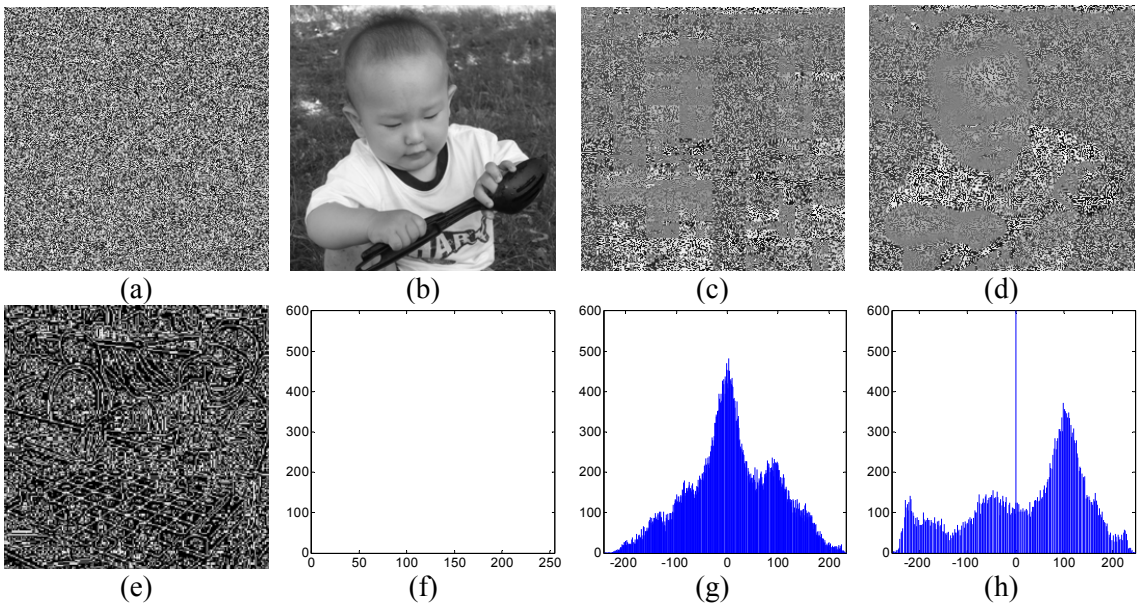


Figure 6.22: Grayscale image decryption using the EdgemapCrypt algorithm with different security keys. (a) The encrypted 256×256 grayscale Baby image with security keys: the 256×256 grayscale Chessplayer image, Prewitt, 0.5, and $n = 2, p = 0$ for the scrambling algorithm; (b) The reconstructed grayscale image using the correct security keys; (c) The reconstructed grayscale image using the same key-image and $n = 2, p = 1$ for the scrambling algorithm; (d) The reconstructed grayscale image using the security keys: the 256×256 grayscale Cameraman image, Sobel, 0.3, and the same security keys for the scrambling algorithm; (e) the key-image: the edge map of the 256×256 grayscale Chessplayer image, Prewitt, 0.5; (f) Histogram of the difference between the original image and the reconstructed image in (b); (g) Histogram of the difference between the original image and the reconstructed image in (c); (h) Histogram of the difference between the original image and the reconstructed image in (d).

Moreover, any edge detector can be used in the EdgemapCrypt algorithm, assuming its possible choice is P_E. The edge detector's threshold is a rational number from 0 to 1. However, not all the threshold values can achieve a desirable encryption result. The number of their possible choices may not be infinite, assuming P_{TH}. The security key space for the EdgemapCrypt algorithm is $P_I P_E P_{TH} P_S$.

www.manaraa.com

6.4.3.2 Brute Force Attacks

The Brute force attack is an attack model in which the attacker tries to guess the algorithms' security keys by conducting an exhaustive search for their possible combinations. Theoretically, this approach is feasible if the key space of the encryption algorithm is limited and the attacker knows the encryption algorithm.

Even if the security key spaces of both algorithms are not infinite, they are sufficiently large since a large number of possible images can be used to generate the key-image. As a result, the two algorithms are able to withstand the brute force attack.

6.4.3.3 Ciphertext-only Attacks

In cryptography, plaintext is the original information to be encrypted. Ciphertext is the encrypted plaintext. The ciphertext-only attack is an attack model in which an attacker tries to deduce the security keys by studying only the ciphertext [173]. This attack can be used to study the encrypted images and thus recover the original image data. If fewer portions of the images are encrypted, attackers can recover a greater amount of the original images without knowing the encryption algorithm and its security keys. If an encryption scheme cannot withstand such an attack, it can be said to have an extremely low security level.

As can be seen from the experimental results in Section 6.4.2, the encrypted images are visually unrecognizable and completely different from the original images. They contain almost none of the visual information of the original images. In their histograms, the

www.manaraa.com

distributions of the encrypted images are uniform, providing that the BitplaneCrypt and EdgemapCrypt algorithms can withstand cipher-only attacks.

6.4.3.4 Known-Plaintext Attacks

The known-plaintext attack is an attack model in which an attacker tries to obtain the security keys of an encryption algorithm by studying a number of plaintexts and the corresponding ciphertexts [173]. One condition of this attack is that the attacker should be in possession of some plaintexts and their corresponding ciphertext. If the encryption process does not change the image data, it is possible for the attacker to break the encrypted image, either partially or completely, without knowing the encryption algorithm and its security keys.

Two processes are able to render the encrypted image data unusable for attackers attempting this type of attack: 1) the XOR operation and the process of inverting the order of the bit-planes in the BitplaneCrypt and EdgemapCrypt algorithms are designed to change image data; and 2) the image scrambling algorithm is used to change image pixel positions. Thus, both processes allow the algorithms to withstand the known-plaintext attack.

6.4.3.5 Chosen-Ciphertext and Chosen-Plaintext Attacks

The chosen-ciphertext attack is an attack model in which the attacker can choose some ciphertexts and their corresponding plaintexts [173]. In this way, the attacker is able to deduce the security keys of encryption algorithms or recover the original plaintext from the unseen ciphertext.

www.manaraa.com

The chosen-plaintext attack is an attack model in which the attacker can choose a number of plaintexts and then deduce their corresponding ciphertexts [173]. As a result, the attacker can choose any useful information as plaintext to deduce the security keys of encryption algorithms, or reconstruct the original plaintexts from the unknown ciphertexts. If the image data does not change during the encryption process, those two attacks can break the encrypted image without knowing the encryption algorithm and its security keys.

From the analysis above, the presented algorithms are able to withstand the chosen-ciphertext and chosen-plaintext attacks due to the fact that both the image data and pixel locations are changed during the encryption process.

www.manaraa.com

6.5 Summary and Discussion

This chapter has introduced a new concept for image encryption using edge information. The general idea behind this concept is the separation of the image into edges and an image without edges using existing edge detectors, followed by the encryption of either the image without edges or the edges themselves (or both) using any encryption algorithm. The encrypted results are then combined to obtain the encrypted image. To meet the different security requirements of real-time applications, users have the flexibility to choose any method and its threshold for edge detection, to select any encryption method and its security keys for encryption process, and to encrypt either edges or image without edges, or both.

To show the performance of the concept, a new image encryption algorithm was introduced using a new 3D Cat Map as an example. The presented encryption algorithm was shown to encrypt different types of images efficiently and, due to the fact that it is able to change image pixel positions and pixel data at the same time, in a straightforward manner. The fact that the security keys of the presented 3D Cat Map based image encryption algorithm possess a sufficiently large number of possible combinations means that the encrypted images are extremely difficult for unauthorized users to decode. As a result, the images are protected with a high level of security. The presented encryption algorithm has been shown to resist the chosen-plaintext attacks because the encryption process changes the image pixel values.

www.manaraa.com

To extend this concept, the edge map has been used as a random binary security key matrix for image encryption. A new algorithm for medical image encryption has been introduced using the edge map. The algorithm encrypts medical images by combining four different processes to change image data. After the application of several encryption processes, a nearly uniform data distribution of the encrypted medical image has been obtained.

Users have the flexibility to choose any edge detector and its threshold values for the EdgeCrypt algorithm or interleave the edge map between any two bit-planes. The security keys of the EdgeCrypt algorithm possess an extremely large amount of possible combinations, which ensures that original images are protected with a high level of security. Examples were given to demonstrate that the EdgeCrypt algorithm can fully encrypt selected objects or regions within medical images or entire images. It has the ability to overcome plaintext attacks.

Since the edge map as a binary image can be obtained from any image, the edge map could be further extended into use with the concept of a binary "key-image", which takes the form of a binary bit-plane, edge map or binary image obtained from another image with the same size as the original. To demonstrate this, two image encryption algorithms have been introduced using this key-image. The key-image in the BitplaneCrypt algorithm is a bit-plane, while in the EdgemapCrypt algorithm it is an edge map.

Experiments demonstrated that both algorithms fully encrypt different types of images. Any image with the same size as the original can be used to generate the key-image. All edge detectors with any specified threshold value can be used to create the edge map as a

www.manaraa.com

key-image for the EdgemapCrypt algorithm. Any image scrambling method can be applied to both algorithms. All these factors ensure that the images can be protected with a higher security level.

Due to the fact that they operate at the binary levels, all algorithms are easy to implement in hardware and are suitable for multimedia protection in real-time applications such as wireless networks and mobile phone services.

www.manaraa.com

Part IV

Conclusion and Future Directions

www.manaraa.com

In order to overcome both the security limitations of traditional recognition systems and the efficiency and accuracy of object detection and identification, this dissertation has introduced a multimedia security system for the performance of object recognition and multimedia encryption for security and medical applications. This was achieved by embedding an enhancement process and a multimedia encryption process into the traditional recognition system. It was demonstrated that the multimedia security system can be used in various ways for security and medical applications.

To quantitatively evaluate the algorithm's enhancement performance, a new SDME measure was introduced according to the concept of the second derivative.

To improve the efficiency and accuracy of identifying suspected objects at security checkpoints in airports, a new 3D CT baggage image enhancement algorithm has been introduced, which combines the alpha weighted mean separation with histogram equalization. Computer simulations and comparisons demonstrated that the presented algorithm can significantly improve the visual quality of objects in original CT images while reducing background noise and outperforming other enhancement methods. Quantitative SDME measure results and 3D visualizations further proved that the presented algorithm's enhancement performance is excellent.

To improve the visual quality of medical images, thereby aiding the detection of early stage cancers and the reduction of mortality rates due to those cancers, a new nonlinear filter, AWQF, was introduced. It was shown that this filter can be designed as a nonlinear combination of different types of linear filters and can, therefore, offer users more design flexibility when it comes to meeting the specific and complicated requirements of real

www.manaraa.com

world applications. This filter was shown to enhance effectively the overall contrast of mammograms and improve local fine details.

For enhancing mammograms, a new HVS-based enhancement algorithm was introduced. Computer simulations, SDME measure results and comparisons all demonstrated that the presented HVS-based algorithm possesses a superior enhancement performance when it comes to improving the contrast of specific regions, objects and details in mammograms without generating artifacts or over-enhancing high-illuminated regions.

It was also demonstrated that the HVS-based image decomposition possesses the ability to separate abnormal regions, such as cancer cells, from original mammograms and represent them in single sub-images without using a thresholding or segmentation algorithm. When it comes to the automatic detection and diagnosis of breast cancer in the CAD systems, this is a particularly useful feature.

To overcome the problem that traditional unsharp masking is sensitive to noise, a new nonlinear unsharp masking scheme (NLUM) was introduced. The presented scheme has been shown to provide users with more design flexibility when it comes to meeting the specific and complex requirements of real world applications. Computer simulations have demonstrated that the presented NLUM scheme possesses a superior ability to enhance mammograms, especially the local contrast of specific regions and fine details.

To improve the quality of prostate MR images and help the detection of prostate cancer, a new enhancement algorithm has been introduced using alpha-trimmed mean separation

www.manaraa.com

and nonlinear filtering. Simulation results and comparisons have demonstrated that the algorithm has a superior performance when it comes to enhancing prostate MR images.

Combining the logarithmic enhancement technique with nonlinear filtering, another new algorithm for enhancing prostate MR images has been introduced. The presented algorithm incorporates the advantages of both methods and has the ability to enhance dark regions and fine details while suppressing noise. A training system was presented to optimize the algorithm's coefficients.

To encrypt multimedia data, five recursive sequences and their corresponding transforms has been introduced. These sequences include the P-Lucas sequence, P-recursive sequence, (n, k, p)-Gray code, Parametric M-sequence and the truncated P-Fibonacci sequence. The sequences have been shown to possess more comprehensive properties and can be specified to different new recursive sequences by changing the parameters. For example, the *(n, k, p)*-Gray code can derive the classical Gray code and ternary Gray code. Under different conditions, the P-recursive sequence can generate the P-Fibonacci sequence, P-Lucas sequence and the P-Gray code.

To encrypt 2D and 3D multimedia data efficiently, the dissertation has introduced a 2D P-recursive transform suitable for the above-mentioned recursive sequences. This allows the 2D multimedia encryption to be a straightforward one-step process and provides users with an open platform in which it is easy to input new recursive sequences into the transform and encryption algorithms.

www.manaraa.com

Two multimedia encryption algorithms have been introduced using the 2D P-recursive transform. It was demonstrated that all parameters in the recursive sequences are able to act as security keys in the presented multimedia encryption algorithms. The presented algorithms are able to encrypt multimedia data in the spatial domain and frequency domains respectively. Simulation results and comparisons have demonstrated the excellence of their encryption performance. Security analysis has shown that they are able to withstand common attacks such as data loss attacks and noise attacks.

To overcome the security weakness of the traditional bit-plane decomposition methods (i.e. the predictability of their decomposition results), two new parameter-dependent image bit-plane decomposition methods have been introduced, namely, the truncated Fibonacci p-code bit-plane decomposition (to reduce the redundancy of the Fibonacci p-code bit-plane decomposition) and the *(n, k, p)*-Gray code bit-plane decomposition (to decompose the image into arbitrary base bit-planes). Both their decomposed results and the number of decomposed bit-planes are parameter-dependent, making them useful for image encryption.

To overcome the security weakness of the permutation-only based encryption algorithms and to enhance the security level of the existing bit-plane decomposition based encryption methods, three new image encryption algorithms were introduced combining three parameter-dependent image bit-plane decomposition methods with the recursive sequence transforms. It was demonstrated that the presented encryption methods have the ability to encrypt a selected object, which can either be a full image, part of an image, a selected object in an image or a selected object in a specific region of the image.

www.manaraa.com

Based on the concept of using one combination of security keys to encrypt the original multimedia data and another combination of security keys to reconstruct them and obtain the final encrypted multimedia data, a new image encryption algorithm was introduced using the Discrete Parametric Cosine Transform (DPCT). Due to the fact that it uses the DPCT with varying parameter values, the algorithm was shown to be an effective and straightforward encryption process. It can also be combined with an image compression process such as JPEG so that images can be encrypted and compressed simultaneously for real-time applications.

Simulation results and comparisons have demonstrated the performance of these presented algorithms for image encryption. Security analysis demonstrated the ability of the presented algorithms to withstand several common attacks such as brute force, statistic, noise, data loss and plaintext attacks.

Despite the fact that it has been used for many image processing applications, the edge map has never been used for image encryption. To investigate the value of its applications in image encryption, a new concept of image encryption has been introduced using edge information. This concept uses any edge detector to separate the image into edges and the image without edges and then uses an encryption algorithm to encrypt either edges or the image without edges, or both of them, and finally combines the results to obtain the final encrypted image. To meet the different security requirements of real-time applications, users have the flexibility to choose any method (and its threshold) for edge detection, to select any encryption method and its security keys for the encryption process, and to encrypt either edges or image without edges, or both, as the user desires.

www.manaraa.com

To demonstrate the performance of this concept, a new image encryption algorithm was introduced using a newly introduced 3D Cat Map. The encryption algorithm was shown to be an efficient and straightforward process, able to change image pixel positions and pixel data at the same time.

To extend this concept, the edge map was used as a random binary security key matrix for image encryption. A new encryption algorithm has been introduced using the edge map for medical image encryption. It was shown that the encrypted medical images are visually close to noise images and have an almost uniform data distribution. Simulation results have demonstrated that the presented algorithm can fully encrypt selected objects, regions within images or entire images.

Since the edge map as a binary image can be obtained from any new or existing image, the edge map can be extended further into the concept of a binary "key-image", which can either be a binary bit-plane, an edge map, or a binary image obtained from another image that is the same size as the original. To demonstrate this, two image encryption algorithms have been introduced using this "key-image". Computer simulations have demonstrated that both algorithms are able to fully encrypt different types of images. Any new or existing image and edge detector can be used to generate the edge map, while any existing image scrambling method can be applied to the two presented algorithms.

Future research will involve (1) transferring the presented spatial domain based algorithms for image enhancement and encryption into the frequency domain, (2) implementing the presented algorithms in hardware, (3) developing the new algorithms in applications for enhancing night vision images. (4) investigating the applications of the

www.manaraa.com

presented enhancement measures and algorithms when subject to noise, (5) comparing the quality of the presented encryption algorithms' application to existing encryption methods for error-resilient protection and memory usage (spatial complexity).

www.manaraa.com

REFERENCE

[1] Joung-Youn Kim, Lee-Sup Kim, and Seung-Ho Hwang, "An advanced contrast enhancement using partially overlapped sub-block histogram equalization," *Circuits and Systems for Video Technology, IEEE Transactions on,* vol. 11, no. 4, pp. 475-484, 2001.

[2] Soong-Der Chen and A. R. Ramli, "Minimum mean brightness error bi-histogram equalization in contrast enhancement," *Consumer Electronics, IEEE Transactions on,* vol. 49, no. 4, pp. 1310-1319, 2003.

[3] Yeong-Taeg Kim, "Contrast enhancement using brightness preserving bi-histogram equalization," *Consumer Electronics, IEEE Transactions on,* vol. 43, no. 1, pp. 1-8, 1997.

[4] Soong-Der Chen and A. R. Ramli, "Contrast enhancement using recursive mean-separate histogram equalization for scalable brightness preservation," *Consumer Electronics, IEEE Transactions on,* vol. 49, no. 4, pp. 1301-1309, 2003.

[5] Yu Wang, Qian Chen, and Baeomin Zhang, "Image enhancement based on equal area dualistic sub-image histogram equalization method," *Consumer Electronics, IEEE Transactions on,* vol. 45, no. 1, pp. 68-75, 1999.

[6] M. Kim and Min Chung, "Recursively separated and weighted histogram equalization for brightness preservation and contrast enhancement," *IEEE Transactions on Consumer Electronics,* vol. 54, no. 3, pp. 1389-1397, 2008.

[7] Abdel-Ouahab Boudraa and El-Hadji Samba Diop, "Image contrast enhancement based on 2D Teager-Kaiser operator," in *2008 The 15th IEEE International Conference on Image Processing*, 2008, pp. 3180-3183.

[8] Haiguang Chen, A. Li, L. Kaufman, and J. Hale, "A fast filtering algorithm for image enhancement," *IEEE Transactions on Medical Imaging,* vol. 13, no. 3, pp. 557-564, 1994.

[9] Jong-Sen Lee, "Digital Image Enhancement and Noise Filtering by Use of Local Statistics," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. PAMI-2, no. 2, pp. 165-168, 1980.

[10] N. Petrick, Heang-Ping Chan, B. Sahiner, and Datong Wei, "An adaptive density-weighted contrast enhancement filter for mammographic breast mass detection," *IEEE Transactions on Medical Imaging,* vol. 15, no. 1, pp. 59-67, 1996.

[11] Wei Qian, L. P. Clarke, M. Kallergi, and R. A. Clark, "Tree-structured nonlinear filters in digital mammography," *IEEE Transactions on Medical Imaging,* vol. 13, no. 1, pp. 25-36, 1994.

[12] J. George and S. P. Indu, "Fast Adaptive Anisotropic Filtering for Medical Image Enhancement," in *2008 IEEE International Symposium on Signal Processing and Information Technology*, 2008, pp. 227-232.

[13] Atam P. Dhawan, Gianluca Buelloni, and Richard Gordon, "Enhancement of Mammographic Features by Optimal Adaptive Neighborhood Image Processing," *IEEE Transactions on Medical Imaging,* vol. 5, no. 1, pp. 8-15, 1986.

www.manaraa.com

[14] Richard Gordon and Rangaraj M. Rangayyan, "Feature enhancement of film mammograms using fixed and adaptive neighborhoods," *Applied Optics,* vol. 23, no. 4, pp. 560-564, 1984.

[15] Vincente H. Guis, et al., "Adaptive neighborhood contrast enhancement in mammographic phantom images," *Optical Engineering,* vol. 42, no. 2, pp. 357-366, 2003.

[16] W. M. Morrow, R. B. Paranjape, R. M. Rangayyan, and J. E. L. Desautels, "Region-based contrast enhancement of mammograms," *IEEE Transactions on Medical Imaging,* vol. 11, no. 3, pp. 392-406, 1992.

[17] R. M. Rangayyan, et al., "Improvement of sensitivity of breast cancer diagnosis with adaptive neighborhood contrast enhancement of mammograms," *IEEE Transactions on Information Technology in Biomedicine,* vol. 1, no. 3, pp. 161-170, 1997.

[18] Heang-Ping Chan, et al., "Digital Mammography: ROC Studies of the Effects of Pixel Size and Unsharp-Mask Filtering on the Detection of Subtle Microcalcifications," *Investigative Radiology,* vol. 22, no. 7, pp. 581-589, 1987.

[19] Fleming Y. M. Lure, Paul W. Jones, and Roger S. Gaborski, "Multiresolution unsharp masking technique for mammogram image enhancement," in *Medical Imaging*, Newport Beach, CA, USA, 1996, pp. 830-839.

[20] A. Polesel, G. Ramponi, and V. J. Mathews, "Image enhancement via adaptive unsharp masking," *IEEE Transactions on Image Processing,* vol. 9, no. 3, pp. 505-510, 2000.

[21] Giovanni Ramponi and Andrea Polesel, "Rational unsharp masking technique," *Journal of Electronic Imaging,* vol. 7, no. 2, pp. 333-338, 1998.

[22] Giovanni Ramponi, "A cubic unsharp masking technique for contrast enhancement," *Signal Processing,* vol. 67, no. 2, pp. 211-222, 1998.

[23] S. S. Agaian, B. Silver, and K. A. Panetta, "Transform Coefficient Histogram-Based Image Enhancement Algorithms Using Contrast Entropy," *IEEE Transactions on Image Processing,* vol. 16, no. 3, pp. 741-758, 2007.

[24] Jinshan Tang, Jeonghoon Kim, and E. Peli, "Image enhancement in the JPEG domain for people with vision impairment," *IEEE Transactions on Biomedical Engineering,* vol. 51, no. 11, pp. 2013-2023, 2004.

[25] Jinshan Tang, E. Peli, and S. Acton, "Image enhancement using a contrast measure in the compressed domain," *IEEE Signal Processing Letters,* vol. 10, no. 10, pp. 289-292, 2003.

[26] A. Laine, Fan Jian, and Yang Wuhai, "Wavelets for contrast enhancement of digital mammography," *IEEE Engineering in Medicine and Biology Magazine,* vol. 14, no. 5, pp. 536-550, 1995.

[27] A. F. Laine, S. Schuler, Fan Jian, and W. Huda, "Mammographic feature enhancement by multiscale analysis," *IEEE Transactions on Medical Imaging,* vol. 13, no. 4, pp. 725-740, 1994.

[28] A. Mencattini, et al., "Mammographic Images Enhancement and Denoising for Breast Cancer Detection Using Dyadic Wavelet Processing," *IEEE Transactions on Instrumentation and Measurement,* vol. 57, no. 7, pp. 1422-1430, 2008.

www.manaraa.com

[29] P. Heinlein, J. Drexl, and W. Schneider, "Integrated wavelets for enhancement of microcalcifications in digital mammography," *IEEE Transactions on Medical Imaging,* vol. 22, no. 3, pp. 402-413, 2003.

[30] P Sakellaropoulos, L Costaridou, and G Panayiotakis, "A wavelet-based spatially adaptive method for mammographic contrast enhancement," *Physics in Medicine and Biology,* vol. 48, no. 6, pp. 787-803, 2003.

[31] H. D. Cheng and Huijuan Xu, "A novel fuzzy logic approach to mammogram contrast enhancement," *Information Sciences,* vol. 148, no. 1-4, pp. 167-184, 2002.

[32] Farhang Sahba and Anastasios Venetsanopoulos, "Contrast enhancement of mammography images using a fuzzy approach," in *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE*, 2008, pp. 2201-2204.

[33] I. Stephanakis, G. Anastassopoulos, A. Karayiannakis, and C. Simopoulos, "Enhancement of medical images using a fuzzy model for segment dependent local equalization," in *2003 the 3rd International Symposium on Image and Signal Processing and Analysis*, 2003, pp. 970-975 Vol.2.

[34] Jianmin Jiang, Bin Yao, and A. M. Wason, "Integration of fuzzy logic and structure tensor towards mammogram contrast enhancement," *Computerized Medical Imaging and Graphics,* vol. 29, no. 1, pp. 83-90, 2005.

[35] Yicong Zhou, Karen Panetta, and Sos Agaian, "CT Baggage Image Enhancement Using a Combination of Alpha-Weighted Mean Separation and Histogram Equalization," in *Mobile Multimedia/Image Processing, Security, and Applications 2010*, Orlando, Florida, USA, 2010, pp. 77080G-12.

[36] Karen Panetta, Yicong Zhou, and Sos Agaian, "Nonlinear Unsharp Masking for Mammogram Enhancement," *IEEE Transactions on Image Processing,* 2009 *(Submitted)*.

[37] Yicong Zhou, K. Panetta, and S. Agaian, "Mammogram Enhancement Using Alpha Weighted Quadratic Filter," in *2009 The Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Minneapolis, Minnesota, 2009, pp. 3681-3684.

[38] Yicong Zhou, Karen Panetta, and Sos Agaian, "Human Visual System Based Mammogram Enhancement and Analysis," in *2010 The International Conference on Image Processing Theory, Tools and Applications*, Paris, France, 2010 (Accepted).

[39] Yicong Zhou, Karen Panetta, and Sos Agaian, "Nonlinear Filtering for Enhancing Prostate MR Images via Alpha-Trimmed Mean Separation," in *2010 IEEE International Conference on Systems, Man and Cybernetics, SMC 2010.*, Istanbul,Turkey, 2010 (Accepted).

[40] Karen Panetta, Yicong Zhou, and Sos Agaian, "Logarithmic Enhancement for Prostate MR Images Using Nonlinear Filtering," *IEEE Transactions on Medical Imaging,* 2010 *(In preparation)*.

[41] M. S. Kankanhalli and Guan Teo Tian, "Compressed-domain scrambler/descrambler for digital video," *IEEE Transactions on Consumer Electronics,* vol. 48, no. 2, pp. 356-365, 2002.

www.manaraa.com

[42] Ci Wang, Hong-Bin Yu, and Meng Zheng, "A DCT-based MPEG-2 transparent scrambling algorithm," *IEEE Transactions on Consumer Electronics,* vol. 49, no. 4, pp. 1208-1213, 2003.

[43] Tung-Shou Chen, Chin-Chen Chang, and Min-Shiang Hwang, "A virtual image cryptosystem based upon vector quantization," *IEEE Transactions on Image Processing,* vol. 7, no. 10, pp. 1485-1488, 1998.

[44] S. Sudharsanan, "Shared key encryption of JPEG color images," *IEEE Transactions on Consumer Electronics,* vol. 51, no. 4, pp. 1204-1211, 2005.

[45] J. M. Rodrigues, W. Puech, and A. G. Bors, "Selective Encryption of Human Skin in JPEG Images," in *2006 IEEE International Conference on Image Processing*, 2006, pp. 1981-1984.

[46] Chung-Ping Wu and C. C. J. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia,* vol. 7, no. 5, pp. 828-839, 2005.

[47] Guo-Sheng Gu and Guo-Qiang Han, "The Application of Chaos and DWT in Image Scrambling," in *2006 International Conference on Machine Learning and Cybernetics*, 2006, pp. 3729-3733.

[48] P. P. Dang and P. M. Chau, "Image encryption for secure Internet multimedia applications," *IEEE Transactions on Consumer Electronics,* vol. 46, no. 3, pp. 395-403, 2000.

[49] Howard Cheng and Xiaobo Li, "Partial encryption of compressed images and videos," *IEEE Transactions on Signal Processing,* vol. 48, no. 8, pp. 2439-2451, 2000.

[50] National Institute of Standards and Technology, "Data Encryption Standard (DES)," http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, Ed., 1999.

[51] Joan Daemen and Vincent Rijmen, "The Block Cipher Rijndael," in *Proceedings of the The International Conference on Smart Card Research and Applications*: Springer-Verlag, 2000.

[52] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, Ed., 2001.

[53] M. Grangetto, E. Magli, and G. Olmo, "Multimedia Selective Encryption by Means of Randomized Arithmetic Coding," *IEEE Transactions on Multimedia,* vol. 8, no. 5, pp. 905-917, 2006.

[54] Mohamed Amin and Ahmed A. Abd El-Latif, "Efficient modified RC5 based on chaos adapted to image encryption," *Journal of Electronic Imaging,* vol. 19, no. 1, pp. 013012-10, 2010.

[55] R. Bose and S. Pathak, "A novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system," *IEEE Transactions on Circuits and Systems I: Regular Papers,* vol. 53, no. 4, pp. 848-857, 2006.

[56] Guanrong Chen, Yaobin Mao, and Charles K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals,* vol. 21, no. 3, pp. 749-761, 2004.

www.manaraa.com

[57] Y Mao, G Chen, and SG Lian, "A novel fast image encryption scheme based on 3D chaotic Baker maps," *International Journal of Bifurcation and Chaos,* vol. 14, no. 10, pp. 3613-3624, 2004.

[58] N. K. Pareek, Vinod Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image and Vision Computing,* vol. 24, no. 9, pp. 926-934, 2006.

[59] Jiancheng Zou, Rabab K. Ward, and Dongxu Qi, "A new digital image scrambling method based on Fibonacci numbers," in *Proceedings of the 2004 International Symposium on Circuits and Systems*, 2004, pp. III-965-8 Vol.3.

[60] Wei Ding, Weiqi Yan, and Dongxu Qi, "Digital Image Scrambling," *Progress in Natural Science,* vol. 11, no. 6, p. 7, 2000.

[61] Jiancheng Zou and Rabab K. Ward, "Introducing two new image scrambling methods," in *2003 IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, 2003, pp. 708-711 vol.2.

[62] Rong-Jian Chen and Jui-Lin Lai, "Image security system using recursive cellular automata substitution," *Pattern Recognition,* vol. 40, no. 5, pp. 1621-1631, 2007.

[63] Yicong Zhou, Sos Agaian, Valencia M. Joyner, and Karen Panetta, "Two Fibonacci P-code Based Image Scrambling Algorithms," in *IS&T / SPIE Electronic Imaging 2008: Image Processing: Algorithms and Systems VI*, San Jose, CA, USA, 2008, pp. 681215-12.

[64] Yicong Zhou, Karen Panetta, and Sos Agaian, "Partial Multimedia Encryption with Different Security Levels," in *2008 IEEE Conference on Technologies for Homeland Security*, 2008, pp. 513-518.

[65] Yicong Zhou, Karen Panetta, and Sos Agaian, "P-recursive Sequence and Key-dependent Multimedia Scrambling," in *SPIE Defense, Security, and Sensing 2008: Mobile Multimedia/Image Processing, Security, and Applications 2008*, Orlando, FL, USA, 2008, pp. 69820H-12.

[66] Yicong Zhou, Karen Panetta, and Sos Agaian, "An Image Scrambling Algorithm Using Parameter Based M-sequences," in *2008 IEEE International Conference on Machine Learning and Cybernetics*, 2008, pp. 3695-3698.

[67] Yicong Zhou, Karen Panetta, and Sos Agaian, "Comparison of Recursive Sequence Based Image Scrambling Algorithms," in *2008 IEEE International Conference on Systems, Man and Cybernetics*, 2008, pp. 697-701.

[68] Yicong Zhou, Karen Panetta, and Sos Agaian, *Multimedia Encryption Using Recursive Sequences*. Saarbrücken, Germany: VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG, 2008 *(Invited publication)*.

[69] Shujun Li, et al., "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication,* vol. 23, no. 3, pp. 212-223, 2008.

[70] Shujun Li, Chengqing Li, Kwok-Tung Lo, and Guanrong Chen, "Cryptanalysis of an Image Scrambling Scheme Without Bandwidth Expansion," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 18, no. 3, pp. 338-349, 2008.

[71] Jong-Wook Han, Choon-Sik Park, Dae-Hyun Ryu, and Eun-Soo Kim, "Optical image encryption based on XOR operations," *Optical Engineering,* vol. 38, no. 1, pp. 47-54, 1999.

المنارة للاستشارات

www.manaraa.com

[72] M Podesser, H Schmidt, and A Uhl, "Selective bitplane encryption for secure transmission of image data in mobile environments," in *The 5th Nordic Signal Processing Symposium -NORSIG-2002*, on board Hurtigruten, Norway, 2002, p. 1037.

[73] Daesung Moon, et al., "An Efficient Selective Encryption of Fingerprint Images for Embedded Processors," *ETRI Journal,* vol. 28, no. 4, pp. 444-452, 2006.

[74] Yicong Zhou, Karen Panetta, Ravindranath Cherukuri, and Sos Agaian, "Selective Object Encryption for Privacy Protection," in *SPIE Defense, Security, and Sensing 2009: Mobile Multimedia/Image Processing, Security, and Applications 2009*, Orlando, FL, USA, 2009, pp. 73510F-10.

[75] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image Encryption Algorithms Based on Generalized P-Gray Code Bit Plane Decomposition," in *2009 The 43rd Asilomar IEEE Conference on Signals, Systems and Computers*, 2009, pp. 400 - 404.

[76] Karen Panetta, Yicong Zhou, and Sos Agaian, " *(n, k, p)*-Gray Code for Image Systems," *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans,* 2010 *(Submitted)*.

[77] Karen Panetta, Yicong Zhou, and Sos Agaian, "Image Encryption Using the P-Fibonacci Decomposition and Transform," *Signal Processing: Image Communication,* 2010 *(Submitted)*.

[78] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image Encryption Using Discrete Parametric Cosine Transform," in *2009 The 43rd Asilomar IEEE Conference on Signals, Systems and Computers*, Pacific Grove, CA, USA, 2009, pp. 395 - 399.

[79] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image Encryption Based on Edge Information," in *IS&T / SPIE Electronic Imaging 2009: Multimedia on Mobile Devices 2009*, San Jose, CA, USA, 2009, pp. 725603-11.

[80] Yicong Zhou, Karen Panetta, and Sos Agaian, "A Lossless Encryption Method for Medical Images Using Edge Maps," in *2009 The Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Minneapolis, Minnesota, 2009, pp. 3707-3710.

[81] Yicong Zhou, Karen Panetta, and Sos Agaian, "Image Encryption Using Binary Key-Images," in *2009 IEEE International Conference on Systems, Man and Cybernetics*, San Antonio, TX, 2009, pp. 4569-4574.

[82] D. Ampeliotis, A. Antonakoudi, K. Berberidis, and E. Z. Psarakis, "Computer Aided Detection of Prostate Cancer using Fused Information from Dynamic Contrast Enhanced and Morphological Magnetic Resonance Images," in *Signal Processing and Communications, 2007. ICSPC 2007. IEEE International Conference on*, 2007, pp. 888-891.

[83] A. Madabhushi, et al., "Automated detection of prostatic adenocarcinoma from high-resolution ex vivo MRI," *Medical Imaging, IEEE Transactions on,* vol. 24, no. 12, pp. 1611-1625, 2005.

[84] A. Fenster, et al., "Three-dimensional ultrasound imaging system for prostate cancer diagnosis and treatment," *Instrumentation and Measurement, IEEE Transactions on,* vol. 47, no. 6, pp. 1439-1447, 1998.

www.manaraa.com

[85] David A. Schafer, Christopher C. Ruth, and Carl R. Crawford, "Air calibration scan for computed tomography scanner with obstructing objects," USA: Analogic Corporation, Peabody, MA., 1999.

[86] David A. Schafer, Simon George Harootian, and Sorin Marcovici, "Area detector array for computer tomography scanning system," USA: Analogic Corporation, Peabody, MA., 2000.

[87] Jong Kook Kim, Jeong Mi Park, Koun Sik Song, and Hyun Wook Park, "Adaptive mammographic image enhancement using first derivative and local statistics," *IEEE Transactions on Medical Imaging,* vol. 16, no. 5, pp. 495-502, 1997.

[88] S. S. Agaian, K. Panetta, and A. M. Grigoryan, "Transform-based image enhancement algorithms with performance measure," *IEEE Transactions on Image Processing,* vol. 10, no. 3, pp. 367-382, 2001.

[89] Wikipedia. *Weber-Fechner law*. 2012; Available from: http://en.wikipedia.org/wiki/Weber%E2%80%93Fechner_law.

[90] Albert Abraham Michelson, *Studies in Optics*. Chicago: The University of Chicago Press, 1962.

[91] Wikipedia. *Contrast (vision)*. 2008; Available from: http://en.wikipedia.org/wiki/Contrast_(vision).

[92] M Jourlin and JC Pinoli, "A model for logarithmic image processing," *Journal of microscopy(Print),* vol. 149, no. 1, pp. 21-35, 1988.

[93] K. A. Panetta, E. J. Wharton, and S. S. Agaian, "Human Visual System-Based Image Enhancement and Logarithmic Contrast Measure," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics,* vol. 38, no. 1, pp. 174-188, 2008.

[94] Stephen DelMarco and Sos Agaian, "The design of wavelets for image enhancement and target detection," in *Mobile Multimedia/Image Processing, Security, and Applications 2009*, Orlando, FL, USA, 2009, pp. 735103-12.

[95] JE Cross and W McFarland, "Getting Started With The MATLAB Image Processing Toolbox," in *Proceedings of the 2002 ASEE Gulf-Southwest Annual Conference*, The University of Louisiana at Lafayette, 2002, p. Session III A 5.

[96] Yael Moses, Yael Adini, and Shimon Ullman, "Face recognition: The problem of compensating for changes in illumination direction," 1994, pp. 286-296.

[97] Yeong-Taeg Kim, "Contrast enhancement using brightness preserving bi-histogram equalization," *IEEE Transactions on Consumer Electronics,* vol. 43, no. 1, pp. 1-8, 1997.

[98] Lap-Ming Wun, Ray M. Merrill, and Eric J. Feuer, "Estimating Lifetime and Age-Conditional Probabilities of Developing Cancer," *Lifetime Data Analysis,* vol. 4, no. 2, pp. 169-186, 1998.

[99] *WHO Cancer Facts*. 2009.

[100] "What Are the Key Statistics About Prostate Cancer?," http://www.cancer.org/docroot/CRI/content/CRI_2_4_1X_What_are_the_key_statistics_for_prostate_cancer_36.asp.

[101] D.E. Stewart, et al., "Attributions of cause and recurrence in long-term breast cancer survivors," *Psycho-Oncology,* vol. 10, no. 2, pp. 179-183, 2001.

www.manaraa.com

[102] A. Fenster, et al., "Three-dimensional ultrasound imaging system for prostate cancer diagnosis and treatment," *IEEE Transactions on Instrumentation and Measurement,* vol. 47, no. 6, pp. 1439-1447, 1998.

[103] A. Madabhushi, et al., "Automated detection of prostatic adenocarcinoma from high-resolution ex vivo MRI," *IEEE Transactions on Medical Imaging,* vol. 24, no. 12, pp. 1611-1625, 2005.

[104] M. Jirari, "A Computer Aided Detection System for Digital Mammograms Based on Radial Basis Functions and Feature Extraction Techniques," in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, 2005, pp. 4457-4460.

[105] Rafayah Mousa, Qutaishat Munib, and Abdallah Moussa, "Breast cancer diagnosis system based on wavelet analysis and fuzzy-neural," *Expert Systems with Applications,* vol. 28, no. 4, pp. 713-723, 2005.

[106] Stelios Halkiotis, Taxiarchis Botsis, and Maria Rangoussi, "Automatic detection of clustered microcalcifications in digital mammograms using mathematical morphology and neural networks," *Signal Processing,* vol. 87, no. 7, pp. 1559-1568, 2007.

[107] H. Li, K. J. R. Liu, and S. C. B. Lo, "Fractal modeling and segmentation for the enhancement of microcalcifications in digital mammograms," *IEEE Transactions on Medical Imaging,* vol. 16, no. 6, pp. 785-798, 1997.

[108] Jinshan Tang, et al., "Computer-Aided Detection and Diagnosis of Breast Cancer With Mammography: Recent Advances," *IEEE Transactions on Information Technology in Biomedicine,* vol. 13, no. 2, pp. 236-251, 2009.

[109] Liyang Wei, Yongyi Yang, M. N. Wernick, and R. M. Nishikawa, "Learning of Perceptual Similarity From Expert Readers for Mammogram Retrieval," *IEEE Journal on Selected Topics in Signal Processing,* vol. 3, no. 1, pp. 53-61, 2009.

[110] Dinggang Shen, Yiqiang Zhan, and C. Davatzikos, "Segmentation of prostate boundaries from ultrasound images using statistical shape model," *IEEE Transactions on Medical Imaging,* vol. 22, no. 4, pp. 539-551, 2003.

[111] I. Larrabide, A. A. Novotny, R. A. Feij´oo, and E. Taroco, "A medical image enhancement algorithm based on topological derivative and anisotropic diffusion," in *Proceedings of the XXVI Iberian Latin-American Congress on Computational Methods in Engineering*, Guarapari, Esp´ırito Santo, Brazil, 2005.

[112] S. Maggio, et al., "Predictive Deconvolution and Hybrid Feature Selection for Computer-Aided Detection of Prostate Cancer," *IEEE Transactions on Medical Imaging,* vol. 29, no. 2, pp. 455-464, 2010.

[113] M. A. Tahir and A. Bouridane, "Novel Round-Robin Tabu Search Algorithm for Prostate Cancer Classification and Diagnosis Using Multispectral Imagery," *IEEE Transactions on Information Technology in Biomedicine,* vol. 10, no. 4, pp. 782-793, 2006.

[114] A. Papadopoulos, D. I. Fotiadis, and L. Costaridou, "Improvement of microcalcification cluster detection in mammography utilizing image enhancement techniques," *Computers in Biology and Medicine,* vol. 38, no. 10, pp. 1045-1055, 2008.

المنارة للاستشارات
www.manaraa.com

[115] Radhika Sivaramakrishna, et al., "Comparing the Performance of Mammographic Enhancement Algorithms: A Preference Study," *Am. J. Roentgenol.,* vol. 175, no. 1, pp. 45-51, 2000.

[116] Zhibo Lu, Tianzi Jiang, Guoen Hu, and Xin Wang, "Contourlet based mammographic image enhancement," in *The 5th International Conference on Photonics and Imaging in Biology and Medicine*, 2007, pp. 65340M-8.

[117] Chun-Ming Chang and A. Laine, "Coherence of multiscale features for enhancement of digital mammograms," *IEEE Transactions on Information Technology in Biomedicine,* vol. 3, no. 1, pp. 32-46, 1999.

[118] Gordana Derado, et al., "Wavelet Image Interpolation (WII): A Wavelet-Based Approach to Enhancement of Digital Mammography Images," in *Bioinformatics Research and Applications*, 2007, pp. 203-214.

[119] Jacob Scharcanski and Cláudio Rosito Jung, "Denoising and enhancing digital mammographic images for visual screening," *Computerized Medical Imaging and Graphics,* vol. 30, no. 4, pp. 243-254, 2006.

[120] Jinshan Tang, Xiaoming Liu, and Qingling Sun, "A Direct Image Contrast Enhancement Algorithm in the Wavelet Domain for Screening Mammograms," *IEEE Journal on Selected Topics in Signal Processing,* vol. 3, no. 1, pp. 74-80, 2009.

[121] K. Jafari-Khouzani and H. Soltanian-Zadeh, "Multiwavelet grading of pathological images of prostate," *IEEE Transactions on Biomedical Engineering,* vol. 50, no. 6, pp. 697-704, 2003.

[122] L. Lemaitre, et al., "Dynamic contrast-enhanced MRI of anterior prostate cancer: morphometric assessment and correlation with radical prostatectomy findings," *European Radiology,* vol. 19, no. 2, pp. 470-480, Feb 2009.

[123] Yi Wan and Dongbin Shi, "Joint Exact Histogram Specification and Image Enhancement Through the Wavelet Transform," *IEEE Transactions on Image Processing,* vol. 16, no. 9, pp. 2245-2250, 2007.

[124] X. H. Wang, R. S. H. Istepanian, and Yong Hua Song, "Microarray image enhancement by denoising using stationary wavelet transform," *IEEE Transactions on Nanobioscience,* vol. 2, no. 4, pp. 184-189, 2003.

[125] Jinzhu Yang, et al., "A Self-adaptive Brain Image Enhancement Algorithm Based on Wavelet Transform," in *2005 The 2nd International IEEE EMBS Conference on Neural Engineering*, 2005, pp. 41-44.

[126] N. D. Nanayakkara, J. Samarabandu, and A. Fenster, "Prostate segmentation by feature enhancement using domain knowledge and adaptive region based operations," *Physics in Medicine and Biology,* vol. 51, no. 7, pp. 1831-1848, Apr 2006.

[127] SS Agaian, K. Panetta, and AM Grigoryan, "A new measure of image enhancement," in *International Conference on Signal Processing & Communication*, Marbella, Spain, 2000, pp. 19-22.

[128] Ali M. Reza, "Realization of the Contrast Limited Adaptive Histogram Equalization (CLAHE) for Real-Time Image Enhancement," *The Journal of VLSI Signal Processing,* vol. 38, no. 1, pp. 35-44, 2004.

www.manaraa.com

[129] N. Strobel and S. K. Mitra, "Quadratic filters for image contrast enhancement," in *1994 The 28th Asilomar Conference on Signals, Systems and Computers*, 1994, pp. 208-212 vol.1.

[130] G. Ramponi, "Bi-impulse response design of isotropic quadratic filters," *Proceedings of the IEEE,* vol. 78, no. 4, pp. 665-677, 1990.

[131] Gershon Buchsbaum, "An Analytical Derivation of Visual Nonlinearity," *IEEE Transactions on Biomedical Engineering,* vol. BME-27, no. 5, pp. 237-242, 1980.

[132] M. K. Kundu and S. K. Pal, "Thresholding for edge detection using human psychovisual phenomena," *Pattern Recognition Letters,* vol. 4, no. 6, pp. 433-441, 1986.

[133] Eric Wharton, Sos Agaian, and Karen Panetta, "A logarithmic measure of image enhancement," in *Mobile Multimedia/Image Processing for Military and Security Applications*, Orlando, FL, USA, 2006, pp. 62500P-12.

[134] J Suckling, et al., "The mammographic image analysis society digital mammogram database," in *Proceedings of the 2nd international workshop on digital mammography*, 1994, pp. 375-378.

[135] Stephen M. Pizer, et al., "Adaptive histogram equalization and its variations," *Computer Vision, Graphics, and Image Processing,* vol. 39, no. 3, pp. 355-368, 1987.

[136] Rafael C. Gonzalez and Richard E. Woods, *Digital Image Processing*, 3 ed.: Pearson Prentice Hall, 2007.

[137] KA Panetta, EJ Wharton, and SS Agaian, "Logarithmic Edge Detection with Applications," *Journal of Computers,* vol. 3, no. 9, pp. 11-19, 2008.

[138] R. Oten and R. J. P. de Figueiredo, "Adaptive alpha-trimmed mean filters under deviations from assumed noise model," *IEEE Transactions on Image Processing,* vol. 13, no. 5, pp. 627-639, 2004.

[139] A. Restrepo and A. C. Bovik, "Adaptive trimmed mean filters for image restoration," *Acoustics, Speech and Signal Processing, IEEE Transactions on,* vol. 36, no. 8, pp. 1326-1337, 1988.

[140] A. Taguchi, "Data-dependent α-trimmed mean filters for image restoration," in *Circuits and Systems, 1994. ISCAS '94., 1994 IEEE International Symposium on*, 1994, pp. 289-292 vol.3.

[141] Eric Wharton, Sos Agaian, and Karen Panetta, "Comparative study of logarithmic enhancement algorithms with performance measure," in *Image Processing: Algorithms and Systems, Neural Networks, and Machine Learning*, San Jose, CA, USA, 2006, pp. 606412-12.

[142] F. Dufaux and T. Ebrahimi, "Scrambling for Privacy Protection in Video Surveillance Systems," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 18, no. 8, pp. 1168-1174, 2008.

[143] Shujun Li, et al., "On the Design of Perceptual MPEG-Video Encryption Algorithms," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 17, no. 2, pp. 214-223, 2007.

[144] Shiguo Lian, Zhongxuan Liu, Zhen Ren, and Haila Wang, "Commutative Encryption and Watermarking in Video Compression," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 17, no. 6, pp. 774-778, 2007.

www.manaraa.com

[145] K. Martin and K. N. Plataniotis, "Privacy Protected Surveillance Using Secure Visual Object Coding," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 18, no. 8, pp. 1152-1162, 2008.

[146] Jiangtao Wen, et al., "A format-compliant configurable encryption framework for access control of video," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 12, no. 6, pp. 545-557, 2002.

[147] Xiliang Liu and Ahmet M. Eskicioglu, "Selective encryption of multimedia content in distribution networks: Challenges and new directions," in *Second IASTED International Conference on Communications, Internet and Information Technology*, Scottsdale, AZ, USA, 2003, pp. 527-533.

[148] Bin B. Zhu, Mitchell D. Swanson, and Shipeng Li, "Encryption and authentication for scalable multimedia: current state of the art and challenges," in *Internet Multimedia Management Systems V*, Philadelphia, PA, USA, 2004, pp. 157-170.

[149] Shiguo Lian, Zhongxuan Liu, Zhen Ren, and Haila Wang, "Secure advanced video coding based on selective encryption algorithms," *IEEE Transactions on Consumer Electronics,* vol. 52, no. 2, pp. 621-629, 2006.

[150] Yinian Mao and Min Wu, "A joint signal processing and cryptographic approach to multimedia encryption," *IEEE Transactions on Image Processing,* vol. 15, no. 7, pp. 2061-2075, 2006.

[151] L Qiao and K Nahrstedt, "A new algorithm for MPEG video encryption," in *Proceedings of The 1st International Conference on Imaging Science, Systems, and Technology*, Las Vegas, NV, 1997, pp. 21–29.

[152] N. Bourbakis and A. Dollas, "SCAN-based compression-encryption-hiding for video on demand," *IEEE Multimedia,* vol. 10, no. 3, pp. 79-87, 2003.

[153] M. Yang, N. Bourbakis, and Li Shujun, "Data-image-video encryption," *IEEE Potentials,* vol. 23, no. 3, pp. 28-34, 2004.

[154] Jiancheng Zou, Rabab K. Ward, and Dongxu Qi, "The generalized Fibonacci transformations and application to image scrambling," in *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2004, pp. iii-385-8 vol.3.

[155] Xuelong Zhao, Qianmu Li, Manwu Xu, and Fengyu Liu, "A symmetric cryptography based on extended cellular automata," in *2005 IEEE International Conference on Systems, Man and Cybernetics*, 2005, pp. 499-503.

[156] T. Koshy, ed. *Fibonacci and Lucas Numbers with Applications*. 2001, Wiley-Interscience.

[157] S. Agaian, J. Astola, K. Egiazarian, and P. Kuosmanen, "Decompositional methods for stack filtering using Fibonacci p-codes," *Signal Processing,* vol. 41, pp. 101-110, 1995.

[158] David Z. Gevorkian, et al., "Parallel algorithms and VLSI architectures for stack filtering using Fibonacci p-codes," *IEEE Transactions on Signal Processing,* vol. 43, no. 1, pp. 286-295, 1995.

[159] RW Doran, "The Gray Code," *Journal of Universal Computer Science,* vol. 13, no. 11, pp. 1573-1597, 2007.

www.manaraa.com

[160] EN Gilbert, "Gray codes and paths on the n-cube," *Bell System Technical Journal,* vol. 37, no. 1, pp. 815-826, 1958.
[161] K. J. Sankar, V. M. Pandharipande, and P. S. Moharir, "Generalized Gray codes," in *Intelligent Signal Processing and Communication Systems, 2004. ISPACS 2004. Proceedings of 2004 International Symposium on*, 2004, pp. 654-659.
[162] Dennis R. Morgan, "Autocorrelation Function of Sequential M-Bit Words Taken from an N-Bit Shift Register (PN) Sequence," *IEEE Transactions on Computers,* vol. C-29, no. 5, pp. 408-410, 1980.
[163] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of Spread-Spectrum Communications--A Tutorial," *IEEE Transactions on Communications,* vol. 30, no. 5, pp. 855-884, 1982.
[164] Wei Ding, Weiqi Yan, and Dongxu Qi, "Digital Image Scrambling Technology Based on Gray Code," in *Proceedings of International Conference on CAD/CG*, 1999, pp. 116-119.
[165] D. Engel, E. Pschernig, and A. Uhl, "An Analysis of Lightweight Encryption Schemes for Fingerprint Images," *IEEE Transactions on Information Forensics and Security,* vol. 3, no. 2, pp. 173-182, 2008.
[166] S Dey, A Abraham, and S Sanyal, "An LSB Data Hiding Technique Using Prime Numbers," in *2007 The 3rd International Symposium on Information Assurance and Security*, 2007, pp. 101-108.
[167] Clemens Heuberger, "Minimal expansions in redundant number systems: Fibonacci bases and Greedy algorithms," *Periodica Mathematica Hungarica,* vol. 49, no. 2, pp. 65-89, 2004.
[168] Zhou Wang, Alan Conrad Bovik, Hamid Rahim Sheikh, and Eero P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing,* vol. 13, no. 4, pp. 600-612, 2004.
[169] Zhou Wang. *The SSIM Index for Image Quality Assessment*. 2003; Available from: http://www.ece.uwaterloo.ca/~z70wang/research/ssim/ssim_index.m.
[170] Wikipedia. *Correlation and dependence*.
[171] mathbits.com. *Correlation Coefficient*.
[172] Bruce Schneier, ed. *Applied Cryptography*. 2 ed. 1995, Wiley.
[173] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. New York: CRC Press, Inc., 1997.
[174] Dawei Zhao, Guanrong Chen, and Wenbo Liu, "A chaos-based robust wavelet-domain watermarking algorithm," *Chaos, Solitons & Fractals,* vol. 22, no. 1, pp. 47-54, 2004.
[175] Karen O. Egiazarian, Sos S. Agaian, and Jaakko T. Astola, "Parametric family of discrete trigonometric transforms," in *Image and Video Processing IV*, San Jose, CA, USA, 1996, pp. 42-53.
[176] Shiguo Lian, Yaobin Mao, and Zhiquan Wang, "3D Extensions of Some 2D Chaotic Maps and Their Usage in Data Encryption," in *2003 The 4th International Conference on Control and Automation*, 2003, pp. 819-823.
[177] J.J. Buchholz, "Matlab Implementation of the Advanced Encryption Standard," http://buchholz.hs-bremen.de/aes/aes.htm, 2001.

www.manaraa.com