

A Colored Image Encryption Method Based on Random Permutation

By

Shefa Walid Tawalbeh

Supervisor

Dr. Mahmood Al-Khassaweneh

Program: Master of Science in Computer Engineering/ Embedded Systems

Engineering

February 29, 2012

A Colored Image Encryption Method Based on Random Permutation

By

Shefa Walid Tawalbeh

B.Sc. Computer Engineering, Al-Yarmouk University, 2009

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science
in the Department of Computer Engineering, Yarmouk University, Irbid, Jordan.

Signature of Author:



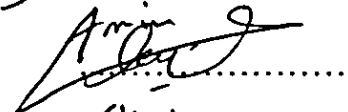
Committee Member

Signature and Date

Dr. Mahmood Al-Khassaweneh (Chairman)



Dr. Amin Al-Qudah (Member)



Dr. Shadi Alboun (External Examiner)



February 29, 2012

DEDICATION

This work is dedicated to my family and my friends,

Thank you for your continuous support, encouragement and love.

ACKNOWLEDGMENTS

First, all thanks and praises to Allah for giving me the ability to write this thesis.

After that, I would like to thank my supervisor Dr. Mahmood Al-Khassaweneh for his support, advice and ongoing guidance.

My heartfelt thanks to my family members for standing next to me and supporting me along my study period.

I would like to thank my friends, Lialy Talafhah, Haifa Omari and Reham Dagamseh for being beside me and giving me their continuous encouragement and love.

Finally, to everyone supported and encouraged me to finish this degree, thank you.

Sh. Tawalbeh

Table of Contents	Page
DEDICATION	
ACKNOWLEDGMENTS	
TABLE OF CONTENTS	
LIST OF TABLES	
LIST OF FIGURES	
ABSTRACT	
I. INTRODUCTION	
1.1 Introduction	12
1.2 Research Motivations	13
1.3 Aims of the Research	14
1.4 Contributions of the Thesis	15
1.5 Thesis Structure	16
II. Literature Survey	17
2.1 Literature Review.....	17
2.2 Basics of Encryption	22
2.2.1 Aims of Encryption.....	22
2.2.2 Image Encryption Security Requirements.....	23
2.2.3 Components of Encryption	24
2.3 Classification of Encryption Algorithms.....	25

2.4 Types of Encryption Attacks	28
2.5 Permutation Based Encryption	29
2.5.1 Random Pixel Permutation	30
2.5.2 Random Line Permutation	30
2.5.3 Chaotic Map-Based Permutation	31
2.6 Digital Image.....	33
III. Proposed Image Encryption Method	35
3.1 Introduction.....	35
3.2 Transformation Stage.....	37
3.3 Shuffling Stage.....	41
3.3.1 Permutation Technique	42
3.3.2 An Encryption Example	44
3.4 Decryption Technique	45
IV. Encryption Evaluation Metrics And Results.....	50
4.1 Overview.....	50
4.2 The Encryption Evaluation Metrics.....	51
4.2.1 Key Space.....	51
4.2.2 Correlation of Adjacent Pixels.....	51
4.2.3 Number of Pixels Change Rate.....	52
4.2.4 Histogram Uniformity.....	53
4.2.5 Mean Square Error.....	54

© Arabic Digital Library - Yarmouk University

4.3 Results and Discussions.....	55
4.3.1 Materials and Methods	55
4.3.2 Proposed Encryption Method Results and Discussions.....	57
V. CONCLUSIONS	66
VI. REFERENCES	67
VII. ARABIC ABSTRACT	76

List of Tables	Page
Table 1. Color space	34
Table 2. Test images characteristics	57
Table 3. NPCR results	59
Table 4. Comparison of NPCR of Lena	60
Table 5. Correlation r results of test images	60
Table 6. Comparison of correlation r of Lena	61

List of Figures	Page
Fig.1. Encryption technique	12
Fig.2. An encryption system.....	24
Fig.3. Symmetric encryption	25
Fig.4. Asymmetric encryption	26
Fig.5. Block cipher	27
Fig.6. Stream cipher	27
Fig.7. Cryptographic attacks.....	28
Fig.8. Random pixel permutation example	30
Fig.9. Random line permutation example	31
Fig.10. General architecture of a chaotic map	32
Fig.11. RGB encryption technique	35
Fig.12. The proposed encryption method stages	36
Fig.13. Transformation stage	37
Fig.14. Pixel transformation example	39
Fig.15. Image transformation example.....	40
Fig.16. Shuffling stage	41

Fig.17. N*N image	42
Fig.18. Shuffling rows of 6*6 image	43
Fig.19. Shuffling columns of 6*6 image	43
Fig.20. An encryption example	44
Fig.21. Decryption system	45
Fig.22. The proposed decryption technique	46
Fig.23. Decryption example	47
Fig.24. The proposed decryption technique of the transformed pixel	48
Fig.25. Test images	56
Fig.26.a. Proposed encryption method results: original image.....	58
Fig.26.b. Proposed encryption method results: encrypted image	58
Fig.26.c. Proposed encryption method results: decrypted image	58
Fig.27. MSE of Lena image	62
Fig.28.a. Histogram of red component: original red component	63
Fig.28.b. Histogram of red component: encrypted red component	63
Fig.29.a. Histogram of green component: original green component	64
Fig.29.b. Histogram of green component: encrypted green component	64
Fig. 30.a. Histogram of green component: original blue component 3	65
Fig. 30.b. Histogram of blue component: encrypted blue component	65

ABSTRACT

Tawalbeh, shefa Walid. A Colored Image Encryption Method Based on Random Permutation. Master of Science Thesis, Department of Computer Engineering, Yarmouk University, 2012 (Supervisor: Dr. Mahmood Al-Khassaweneh).

In communication and image storage, security becomes an important issue to protect data from unauthorized access. There are several ways to ensure security, and encryption is one of them. Image encryption is widely used in many applications to provide high levels of security such as internet communication, multimedia systems and medical imaging. The encryption process needs an encryption algorithm and a key. A colored image encryption method is proposed based on random permutation and will be applied on RGB image. This method will apply special transformation on pixels values through performing logical AND operation between their values and specific value in order to get new transformed image with new pixels values. The columns and rows of this transformed image are shuffled respectively using random permutation to produce the encryption key and the encrypted image. The generated key will be used in decryption method to get the original image.

Keywords: Permutation, Encryption, Decryption, Transformation and Shuffling

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Due to the rapid development of multimedia and network technology [1], security becomes very important issue and does a significant rule for content protection of digital images that are transmitted using internet from unauthorized user [2]. To ensure the security of images contents, encryption is a major tool. Encryption algorithm has a sequence of mathematical operations that generate alternate form of digital image data. To differentiate between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as ciphertext [3]. Figure 1 shows the encryption technique.

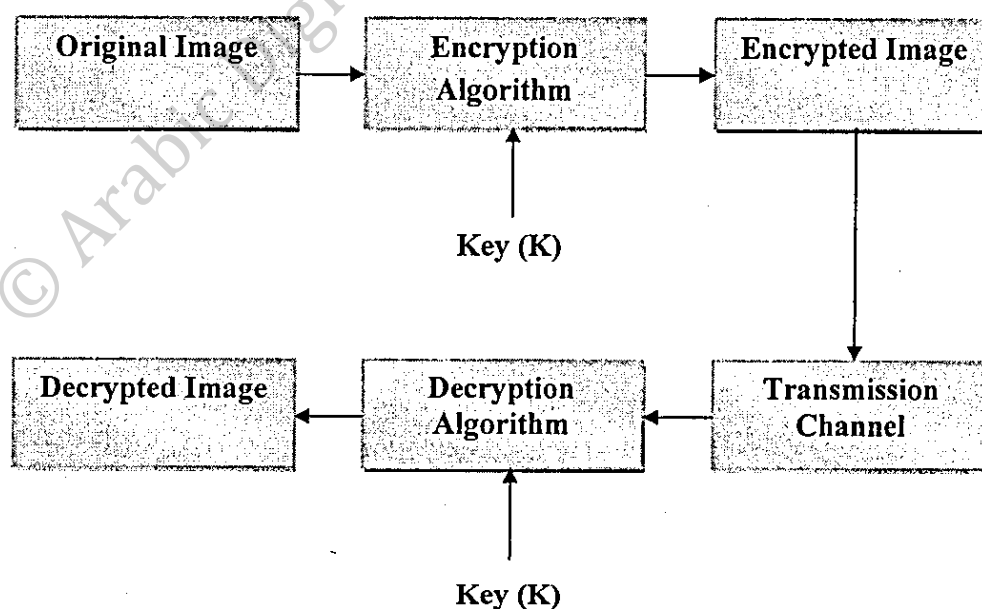


Fig.1: Encryption Technique

The ability of an algorithm to generate ciphertext that is not easily reverted to the original plaintext is a measure of the security of encryption. In order to allow both the sender and the recipient of the message to understand how the message has been encrypted, a key is used in image encryption algorithm [3]. It also used to ensure that nobody else knows how the message has been encrypted. To achieve a good encryption method, the algorithm should satisfy the following aspects: firstly, the used key must be sensitive to cipher key, second, the space of the key should be large enough to provide the infeasibility of brute force attacks [4]. Other metrics are used to evaluate the efficiency of an encryption method such as high Number of Pixels Change Rate NPCR, low correlation of adjacent pixels and high Mean Square Error MSE.

In this thesis, an encryption algorithm based on pixels transformation and permutation is proposed to fulfill the requirements of security of image encryption.

1.2 Research Motivations

Communication networks such as mobile networks and internet are widely developed and used. Transmission of messages through them is not suitable and not secure since they are public networks [5]. In order to provide the needed security, encryption techniques are applied.

In the last decades, several image encryption algorithms were proposed to encrypt the image. All algorithms in image encryption aim to obtain high level of security in encrypted image and to reduce computational complexity of the encryption and decryption algorithms. The basic characteristics in the field of security are confidentiality, data integrity, authentication, non-repudiation and robustness against noise and other external disturbances.

The security mechanism should be flexible. A good encryption scheme should resist all kinds of known attacks, such as the Known-plain text attack, the cipher text-only attack, the statistical attack, the differential attack and the various brute-force attacks.

To realize secure image encryption, many chaotic cryptosystems have been proposed. Image encryption algorithms based on chaotic systems are proposed to solve the problems of image encryption in the past decades [6, 7]. Chaotic map is defined as dynamic system that can be denoted by mathematical equations [8]. It is based on using one or more dimensional maps as pseudo random generators to provide a binary stream, which will be then XOR-ed with the plaintext to produce the ciphertext [9]. Some of these chaotic map algorithms are insecure [10] because of the lack of connection among plaintext and the existence of invalid and weak keys. RSA and DES are some algorithms for image encryption [11], but they are inefficient when the image is large.

1.3 Aims of the Research

Permutation encryption techniques are efficient because they need minimum memory requirements and encryption time [12]. In random line permutation Image encryption methods, permutation does not change pixel's amplitude, it only changes the position of a plain text line. These algorithms have high efficiency, and they can be used to encrypt analog media beside digital content. The encrypted image is too chaotic to be understood, which leads to high perceptual security.

In this master thesis, we propose a new image encryption algorithm based on pixel value transformation and random permutation. It consists of two stages. At the first stage, the pixels values are transformed by logical AND operation between them and specific values. At the second stage, shuffling operation is performed. This stage consists of two steps. At the first step, shuffling function shuffles the columns of the transformed image randomly and creates an encryption key. At the second step, another shuffle function receives the shuffled image that was resulted from the first step and the encryption key to shuffle its rows. The same key will be used at both stages, and it will be used to get the original image.

1.4 Contributions of the Thesis

This master thesis aims to implement a new algorithm for colored image encryption, based on pixels values transformation and random permutation. This method will apply special transformation on pixels values by performing logical AND operation between their values and specific values in order to get new transformed image with new pixels values. The columns and rows of this transformed image are shuffled respectively using random line permutation to produce the encryption key and final encrypted image. The generated key will be used in decryption method to get the original image.

1.5 Thesis Structure

Chapter two, provides a literature review of image encryption methods. It discusses image encryption basic goals, principles of encryption and classification of encryption algorithms. It also discusses the types of cryptographic attacks, permutation encryption and digital image concept.

Chapter three discusses the proposed method and its two stages. Transformation stage and permutation stage are presented. Examples are provided with numeric values. The decryption method is also illustrated.

Chapter four, discusses the evaluation metrics, which are used to evaluate the efficiency of the proposed image encryption method. It also provides the simulation results of the proposed method.

Chapter five, which is the last chapter in this thesis, discusses conclusions.

CHAPTER TWO

LITERATURE SURVEY

2.1 Literature Review

Due to the rapid development in communication networks, multimedia is widely used in applications such as broadcasting [13]. Education, commerce and politics are some aspects of daily life that related closely to multimedia data. To keep the security of this data, it must be protected before transmission through communication networks. Encryption is a typical protection method that can be used to ensure security of transmitted data. It transforms data from its original form to unclear form.

Data encryption standard (DES) is one of the most common traditional encryption methods [12]. IBM introduced it in 1975 to provide security for some businesses such as banks and other huge organizations. Image data cannot be encrypted directly by DES since it is large and DES deals the image data as traditional text data.

Ron Rivest, Adi Shamir and Leonard Adleman (RSA) is an encryption method that used to encrypt text or binary data. It cannot be used directly to encrypt multimedia data because of its large volume, its high redundancy and real time constraints [14]. Advanced Encryption Standard (AES) is one of the most modern encryption methods that use a key length of 128, 192 or 256 bits. The level of security of AES is strong because no discovered known attacks for it [15]. Table called an s-box is used in AES to implement byte substitution [16]. AES can be used on smart cards as an embedded method to perform data encryption in very short time [17].

Multimedia technology continues on its development, leading to develop some encryption standard such as JPEG and MPEG1/2 in the first half of the 1990s [13]. With the rapid development in internet technology and multimedia, new requirements for encryption are needed. Encryption methods based on chaos system were firstly proposed in 1989 [18]. Since 1990s, the attention to use chaotic functions to implement the process of encryption has been increased [2]. Chaos and cryptography have a close relationship, which makes chaos based encryption methods, good methods for secure communication and encryption. Methods based on chaos can provide high level of security, complexity and speed.

Several chaos based encryption methods were proposed [1, 18- 22]. In order to provide a fast and easy way to build cryptosystem, chaotic dynamics are used. Chaotic can provide many properties such as pseudorandom property, system parameters, its extreme sensitivity to initial conditions, system parameters and non-periodicity [1, 18, 23]. To provide a high level of security, pixels positions are shuffled and pixels gray values are changed simultaneously.

In [16] Gao proposed an algorithm based on hyper chaos. It consists of two steps. At the first step, total shuffling is applied to change the position of the plain image. A hyper chaotic system is used to generate a key stream, which is mixed with the shuffled image at the second step. This method provides high level of security and its key space is large enough to make brute-force attack infeasible.

An improvement to Gao algorithm was proposed in [1]. It combines diffusion with shuffling procedure, since there is no relativity between permutation and pixel values. Feedback

is also used in pixel encryption procedure to generate a key stream, which is relative to both the secret key and plaintext. According to security requirements, this method is secure and valid.

Chaotic map is defined as dynamic system that can be denoted by mathematical equations [8]. It is based on using one or more dimensional maps as pseudo random generators to provide a binary stream, which will be then XOR-ed with the plaintext to produce the ciphertext [24].

In [20], image encryption algorithm is based on two steps. The first step shuffles the positions of the pixels of the original image using Arnold cat map, and the second step uses Henon's chaotic system to encrypt the shuffled image. Arnold cat map is a two dimensional chaotic map .Henon's map is a two dimensional map with non-linearity. In this method, the first step uses Henon's map to convert map to one-dimensional chaotic map, which will be used to change the pixel values of the shuffled image. The last step applies XOR operation between shuffled image values and transformed matrix of pixel values.

In [6, 7, 9] Arnold cat map is used to shuffle the positions of pixels of the original image. Henon's chaotic system was used in the second step to encrypt the pixel values of the shuffled image [9] and Logistic chaotic map was used to encrypt the shuffled image pixels values [6].

In [21], pixels locations are shuffled and their values are changed. The gray image is divided into several bit planes. The pixels are shuffled by generated integer sequence and one time iteration of Arnold cat map to change the position of each bit-plane pixels by using multiple

chaotic systems, and then random integer vectors are generated to shuffle the positions of rows and columns of each bit-plane image.

In [21], an encryption method proposed using discrete cosine transform (DCT) domain. Logistic chaos system, which is a one-dimensional chaotic map, generates shuffling maps, which used to shuffle DCT coefficients. DCT coefficients are divided into 64 groups according to their frequency. Shuffling is applied on equal frequency coefficients. The encrypted images using this method are sensitive to initial keys and this scheme has variable key space.

Multi chaotic systems for image encryption were used to introduce a hybrid encryption technique (PCS and IME) [25]. This method uses four different chaotic systems to shuffle pixels by generated sequence from these systems. The encrypted image is highly securing image since the resulted key space is large enough to protect it from attacks even they invest large amount of resources.

Permutation encryption techniques are efficient because they need minimum memory requirements and encryption time [26]. In image encryption methods based on random line permutation, permutation does not change pixel's amplitude, it changes only a position of a plain text line. This algorithm has high efficiency, and it can be used to encrypt analog media beside digital content. The encrypted image is too chaotic to be understood, which leads to high perceptual security.

To fulfill the requirements of image encryption, a thesis was proposed based on combining three approaches to adjust the traditional encryption systems [27]. RC6 and Advanced Encryption Standard (AES) were used to perform diffusion. It uses Chaotic Baker map to perform permutation. The resulted encryption system is homomorphic using different modes of operations.

In order to protect JPEG images through encryption, a thesis was proposed [15]. It performs transformation by integer-to-integer transforms and frequency domain scrambling in DCT channels.

Dynamic shuffling and XOR processes are used in [28] to perform encryption. This method uses multiple pseudo random number generators to perform encryption multiple times to generate completely different cipher images. It uses three permutation shuffles, XOR process based on look-up table and a dynamic XOR process.

In this master thesis, a new image encryption method is implemented based on pixel value transformation and pixel position permutation. It is proposed to get high level of security in the encrypted image.

2.2 Basics of Encryption

Encryption algorithm has a sequence of mathematical operations that generate alternate form of digital image data by the generated encryption key. To differentiate between the two forms of data, the unencrypted data is referred to as the plaintext and the encrypted data as ciphertext. It is extremely difficult to obtain the original plaintext without the encryption key.

2.2.1 Aims of Encryption

Encryption techniques aim to fulfill the following goals [27]:

- Confidentiality.
- Data integrity.
- Non-repudiation
- Authentication.

Confidentiality means Protection of data from unauthorized access. Encryption method is considered confident when it provides high level of protection.

Data integrity means the ability of an algorithm to detect any alternation in data by all communication parities. In other words, information cannot be manipulated in unauthorized way.

Non-repudiation means the receiver receives the message and can prove to everyone that the sender sent the message indeed. The sender cant said he or she did not send the encrypted message.

Authentication is to confirm the truth of the data. Data authentication ensures the following: data does not come from claimed source, data has not been changed in any way and the degree of its change if it has been change [29, 30].

Modern encryption methods aim to provide all the above goals of encryption.

2.2.2 Image Security Requirements

To have an efficient Image encryption system, the system must be flexible and have high security performance [31]. To ensure the security, encryption methods must satisfy the following requirements:

- The encryption system must need an extremely computation time to destroy. Encrypted image must be ambiguous to ensure that unauthorized users do not have the ability to read it.
- In order to provide high performance encryption system, encryption and decryption algorithms should be fast.
- The security mechanism must be acceptable to design encryption system as a commercial product. It should be as prevalent as possible.
- Encryption method must ensure that there is no ability to expand the encrypted image data.

- The security mechanism should have flexibility.

2.2.3 Components of Encryption

Encryption generates a new form of data that differs from the original form. The original image cannot be easily reverted from the encrypted image. The characteristics of Encryption system are [13, 27]:

- Original Image that known as Plaintext
- Encrypted image that known as ciphertext.
- Encryption key, K_e .

The message to be encrypted is plaintext and the encrypted message is ciphertext. The encryption technique is shown in figure 2 [13].

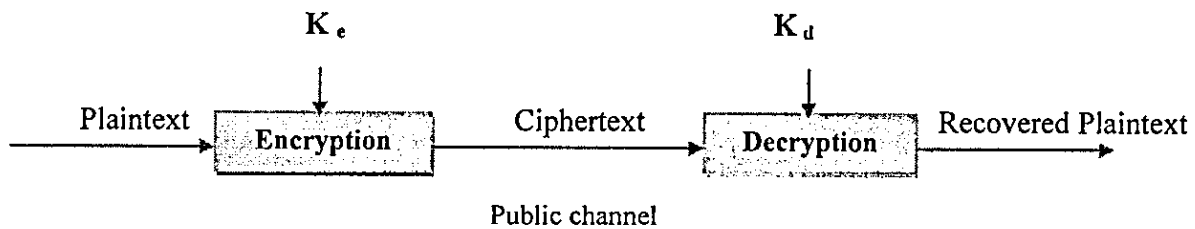


Fig. 2: An encryption system

2.3 Classification of Encryption Algorithms

Modern encryption methods provide two types of encryption, Symmetric and Asymmetric.

Symmetric encryption, which also known as secret key, the decryption key is the same key that was used to encrypt it [12, 32, 33]. The typical key size for DES is 56 bits and 128 bits for AES [34].

Asymmetric encryption, which also called public key, uses two different keys for encryption and decryption. A cipher transforms the plaintext into ciphertext and recovers the plaintext from ciphertext under the control of the key. The following figures show both types of encryption [13, 27]. RSA is one of encryption methods that uses public key.

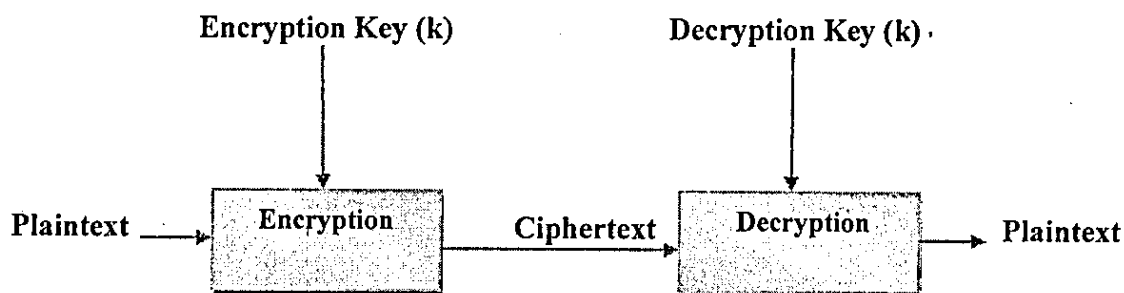


Fig. 3: Symmetric encryption

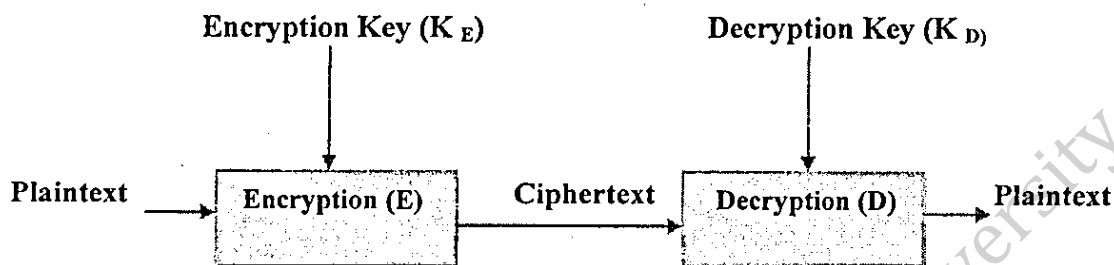


Fig. 4: Asymmetric encryption

In symmetric encryption, the key must be kept secret and must not be determined by any knowledge of the algorithm plus samples of the ciphertext. In asymmetric encryption, the decryption key must be secret and cannot be determined by the knowledge of the algorithm or the encryption key plus samples of the ciphertext.

Both types of encryption have their advantages and disadvantages. Secret keys are fast, but all parties must know the encryption key leading to dangerous situation when the number of involved parties increases [34]. Although public keys are more expensive, but one person has the secret part of the key and it can be distributed to everyone.

Symmetric encryption (Secret Key) can be divided into two classes: Block cipher and Stream cipher [35]. Figures 5 and 6 illustrate block and stream cipher respectively [13].

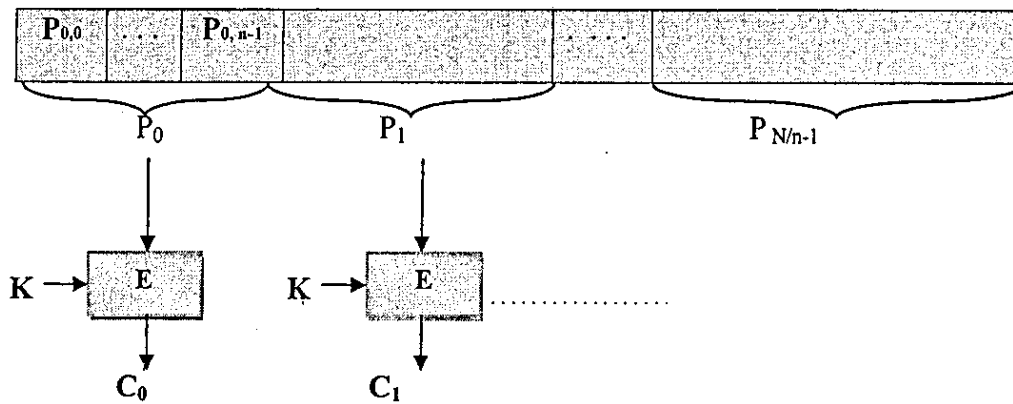


Fig. 5: Block cipher

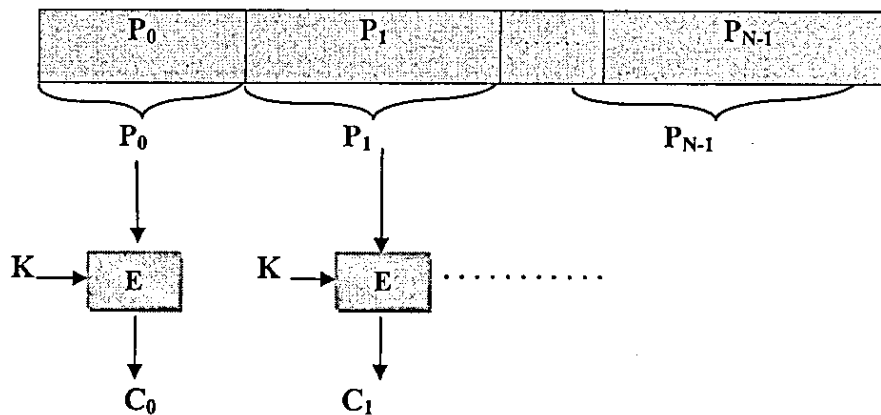


Fig. 6: Stream cipher

Stream cipher operates on a stream bit of data with unspecific size. Some methods operate data bit by bit and others operate data byte-wise [34]. Stream cipher uses random key sequence to modulate the plain image. It is important to decide how to generate the random key sequence. Several generators can be used such as Linear Feedback Shift Register (LFSR) generator [13]. The random sequence generation method is controlled by the initial vector and the key.

Encryption methods can also be divided according to the percentage of encrypted data into partial and full encryption. Partial encryption also called selective encryption.

2.4 Types of Encryption Attacks

In order to desolate the security of encryption algorithms, cryptographic attacks are designed. The goal of them is an attempt to decrypt the encrypted image and get the original data without any knowledge of the key.

There are two methods of attacks: plaintext-based attack and ciphertext-based attack. Both of them have three methods. The following figure shows them.

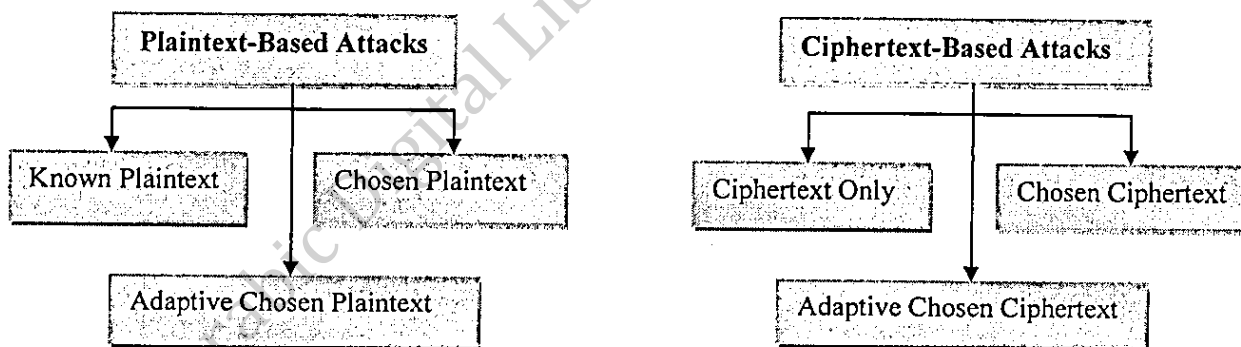


Fig. 7: Cryptographic attacks

Known plaintext attack The attacker knows the plaintext for some part of the ciphertext, and trying to get the rest part of the encrypted image using this known data [35]. This attack tries to find a relation between the plaintext and corresponding ciphertext.

Ciphertext only attack This attack does not know anything about the plaintext. It tries to get the original data from the ciphertext. This attack does not have access to plaintext. It does not use any encryption key. Brute force attack is one common used attack in ciphertext only and known plaintext attack. It tries every possible key.

Chosen plaintext attack The attack chooses a plaintext and encrypts it then studies the resulting ciphertext [35]. This attack is common against asymmetric encryption where the key is public. Differential attack is an example of this attack, which used against symmetric key block ciphers. It attempts to get the plaintext or some parts of it by applying some changes on the ciphertext and studying the resulted ciphertext [10, 36]. Tight encryption methods attempt to produce random ciphertext. Any change in the plaintext leads to random change in the resulting ciphertext.

Chosen ciphertext attack This attack chooses a ciphertext and tries to find a matching plaintext.

Adaptive Chosen Plaintext and Adaptive Chosen Ciphertext Attacks It is based on choosing more plaintexts or ciphertexts to make suitable attack based on most important results.

2.5 Permutation Based Encryption

Permutation is one of the common oldest encryption methods. It based on transforming the plaintext into unintelligible form by changing the adjacent relationship of the pixels. Random

pixel permutation, random line permutation and chaos-based permutation are examples of permutation. The following subsections discuss them in details.

2.5.1 Random Pixel Permutation

In random pixel permutation, the positions of plaintext pixels are changed under control of a random sequence [13]. The following figure shows an example of random line permutation [13].

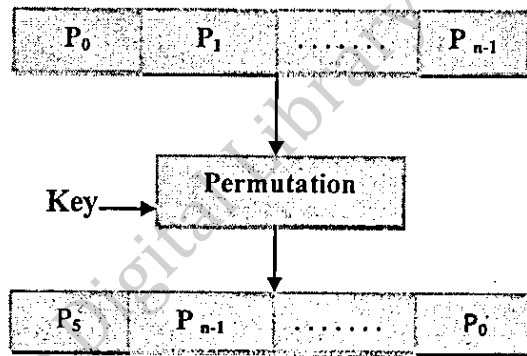


Fig. 8: Random pixel permutation example

The computational cost for this method is low. It can be used to encrypt arbitrary digital content.

2.5.2 Random Line Permutation

Random line permutation is similar to random pixel permutation, it changes the plaintext line position under the control of a random sequence. Figure 9 provides an example.

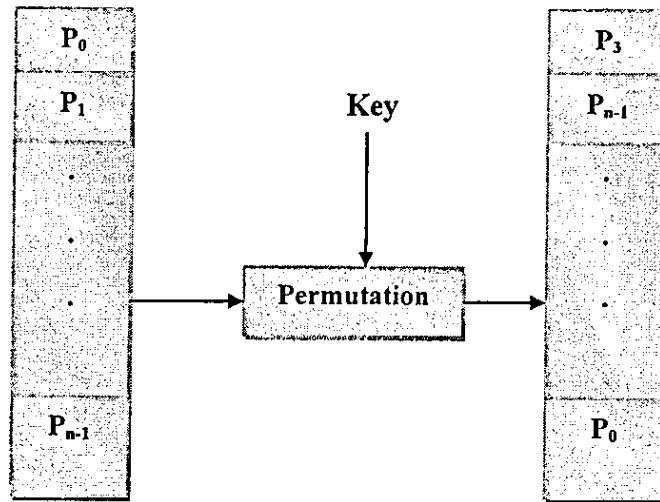


Fig. 9: Random line permutation example

In random line permutation, permutation does not change pixel's amplitude; it changes only a position of a plain text line. It can be used to encrypt analog media beside digital content. The encrypted image has high level of security since it is too chaotic to be understood.

2.5.3 Chaotic Map-Based Permutation

Chaotic map is defined as dynamic system that can be denoted by mathematical equations [8]. It has initial values act as an input, control parameters specify its action and the sequence produced by iterated maps as an output as shown in figure 10.

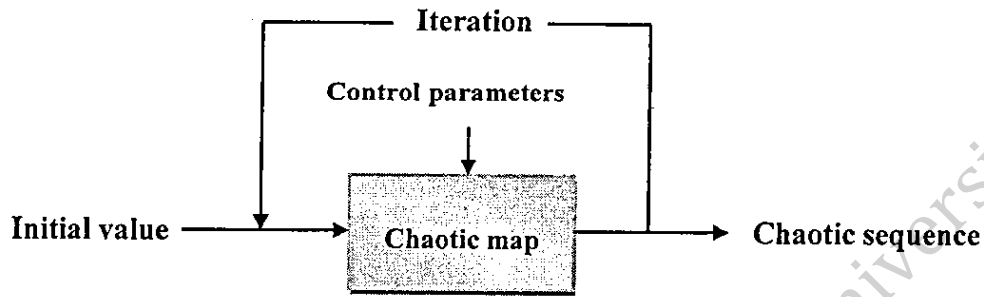


Fig. 10: General architecture of a chaotic map

Chaotic based map permutes the plaintext using chaotic map. The original position is the plaintext and the permuted position is the ciphertext. The chaotic map parameters present the key. Baker map and Arnold Cat map are examples of chaotic maps. Chaos system consists of two stages, confusion and diffusion stages [37]. Confusion stage does not change the pixels values; it permutes them with 2D chaotic map in secret order [38]. Pixel values are changed by diffusion stage to make change to whole image. Confusion stage aims to reduce the correlation between adjacent pixels followed by diffusion stage. Control parameters lead to permutation.

The selection of chaos maps should have the following properties: robust chaos, mixing properties and large parameter set [37].

Encryption methods based on chaos are suitable for large-scale data encryption such as images, videos and audio data [38].

2.6 Digital Image

Digital image is a representation of two-dimensional array. It consists of a set of digital values called pixels, which contain color information. Digital images have a specific number of rows and columns of pixels and can be considered as a matrix. The brightness of any color at any point is given by the pixel, which is the smallest element in an image. Two-dimensional array of integers presents these pixels values. The process of assigning an integer value to each pixel is quantization. Each pixel has a specific value that consists of one or more samples. The number of these samples differs between images. Images can be classified according to this number of samples to Bitmap, Grayscale and Colored images.

Bitmap images are black and white images with pixel color black or white and no other colors between them. Bitmap has zero for black bit and one for white to describe one pixel.

In grayscale images, one byte is used to describe a pixel. One channel of the image consists of eight bits planes. The number of combinations that resulted of eight bits is 256. A pixel can have zero value for black, 128 for gray and 255 for white.

RGB image combines three colors; red, green and blue. This combination can produce huge number of colors. It is stored as an array with size equal to m -by- n -by-3 data. Red, green and blue combination determines the color of each pixel value. RGB images are 24-bits images in which each component has eight bits. The following table illustrates image color space [39].

Table. 1: Image color space

Image properties	Bits resolution	Color space
Binary image(black and white)	1	2 colors
Grayscale	8	256 gray levels
Colored image	8	256 colors
Colored image	16	65536 colors
RGB (true color)	24	16,777,216 colors

The image quality increases when the number of bits increases leading to increasing in storage requirements. Digital images are used in several applications like medical and legal systems.

CHAPTER THREE

THE PROPOSED METHOD

3.1 Introduction

In this master thesis, a new image encryption technique is proposed based on transformation of pixels values and shuffling their locations. The following figure shows the general encryption technique of RGB image.

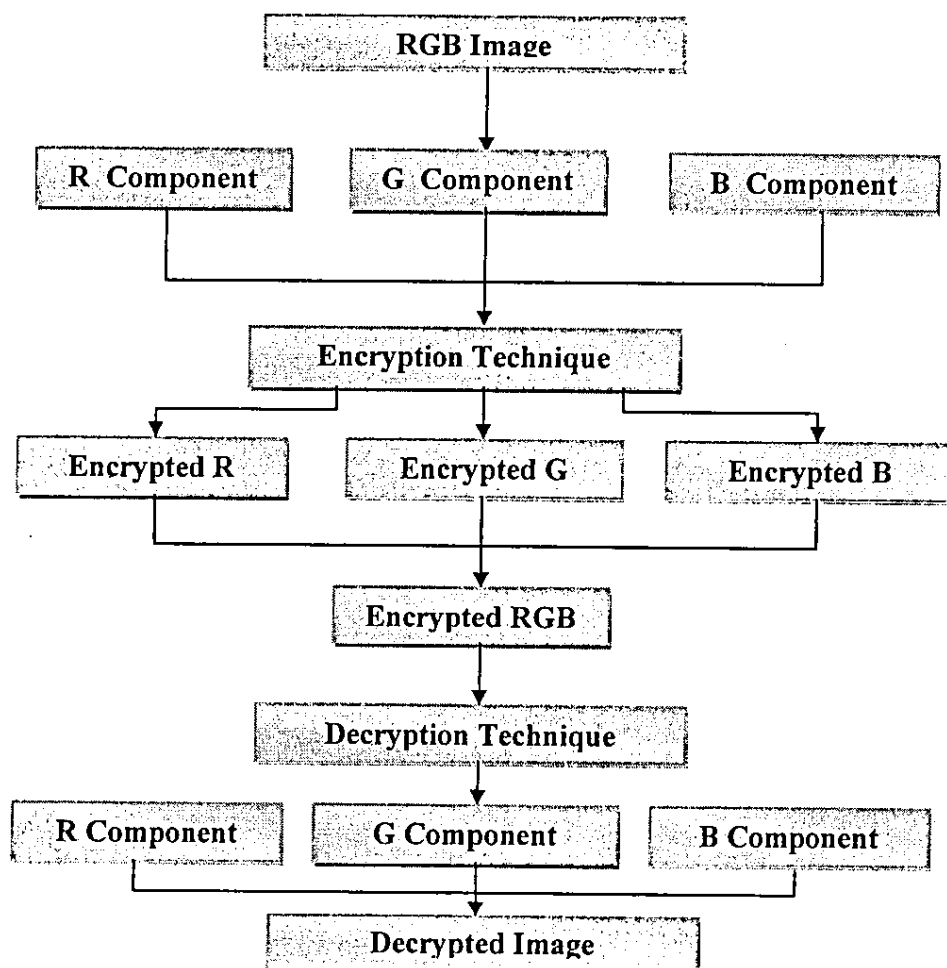


Fig. 11: RGB encryption technique

The algorithm is symmetric encryption in which one key will be used for encryption and decryption techniques. The proposed method will be used to encrypt the RGB images, which combine three components, red, green and blue. Each of them will be encrypted alone and the encrypted components are combined together to give completely encrypted image.

This encryption technique consists of two stages; transformation pixels values and shuffling pixels locations stages. The following figure illustrates the proposed method.

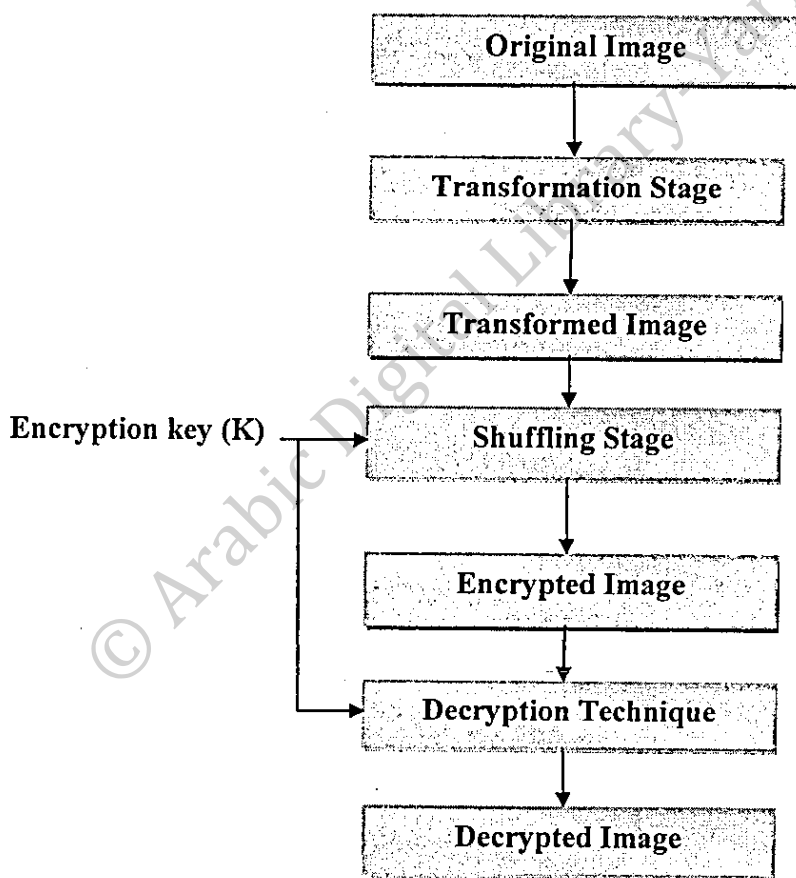


Fig. 12: The proposed encryption method stages

The encryption key is generated during shuffling stage. This generated key will be used to shuffle the columns of the image at the first step of shuffling stage and to shuffle the rows of the resulted image at the second stage. The encryption key is used in decryption technique to get the original image. The generated key of transformation stage will be embedded with the transformed image. In decryption technique, the bits of each pixel are rearranged to get the original value of each pixel.

3.2 Transformation Stage

In this stage, the values of pixels are changed to get new values for them. The transformation is based on masking specific bits in each pixel value. The masking key is embedded with the transformed pixel. Mask operation is performed by performing logical And operation between each pixel value and 85(decimal). Another logical And operation is performed between 170(decimal) and each pixel value to get the key. The resulted pixels values are combined together to produce the new transformed image. The following figure shows the transformation of values operation.

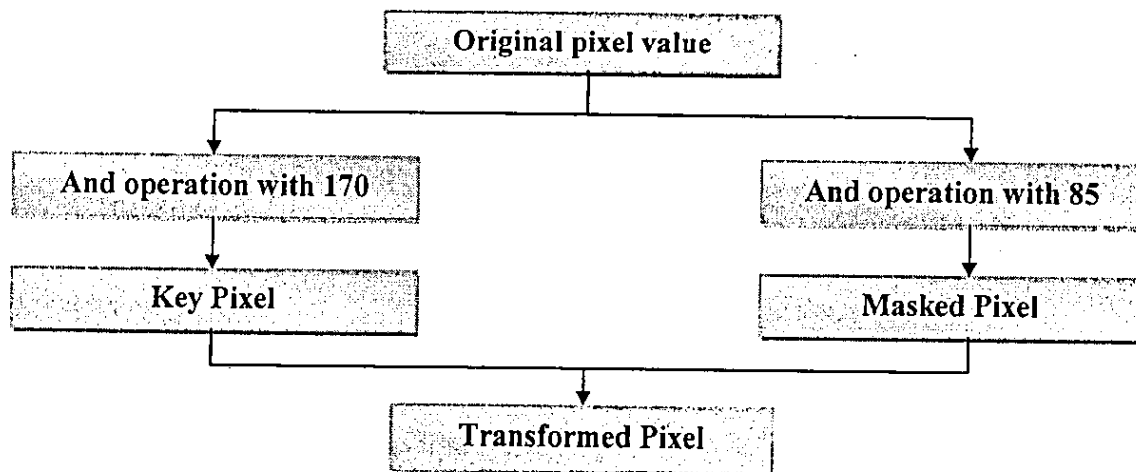


Fig. 13: Transformation stage

The binary value of 85 is **01010101**. When performing logical AND operation between each pixel and this value, it will produce the same bits values when AND them with ones and zeros or masked values when AND them with zero. The unchanged bits, which will be resulted from logical AND operation with ones will be combined together to produce four bits which are the least most significant bits of the transformed pixel.

The binary value of 170 is **10101010**. The unchanged bits that will be resulted from logical AND operation with ones bits are combined together to produce the most significant bits of the transformed pixel. The selected resulted four bits from logical AND operation with 85 are combined with the resulted selected bits from logical AND operation with 170 to generate the final transformed pixel value.

As mentioned above, the transformation will be applied on each pixels of red, green and blue components. Each component forms matrix of equal number of rows and columns. The final RGB matrix is a combination of resulted transformed matrix of each component.

The following numeric example illustrates the transformation operation. If the pixel value equals to 135 (decimal), logical AND operation with 85 will produce five (decimal) with binary value **00000101**. The logical AND operation with 170(decimal) produces 130(decimal) with binary **10000010**. The resulted four bits from the first AND operation are combined with the resulted four bits from the second AND operation to produce a new pixel value equals to 57(decimal) with binary value **00111001**. The following figure shows this example in details.

(170) 1 0 1 0 1 0 1 0

Logical AND Operation

(135) 1 0 0 0 0 1 1 1

(130) 1 0 0 0 0 0 1 0

1 0 0 1

(85) 0 1 0 1 0 1 0 1

Logical AND Operation

(135) 1 0 0 0 0 1 1 1

(5) 0 0 0 0 0 1 0 1



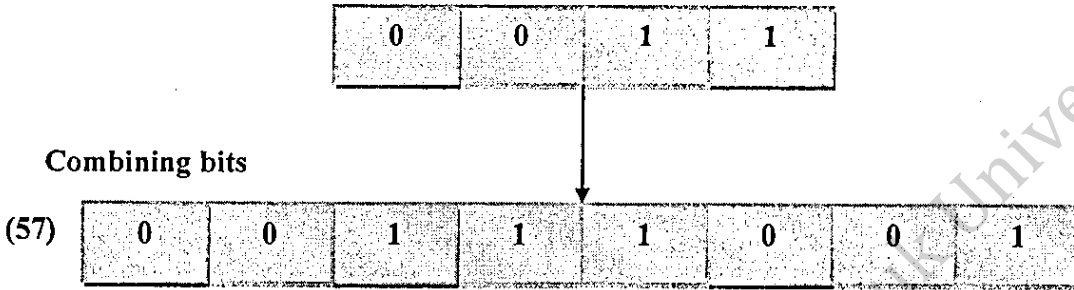


Fig. 14: Pixel transformation example

The following diagram shows transformation example applied on an image with size of 4*4 pixels.

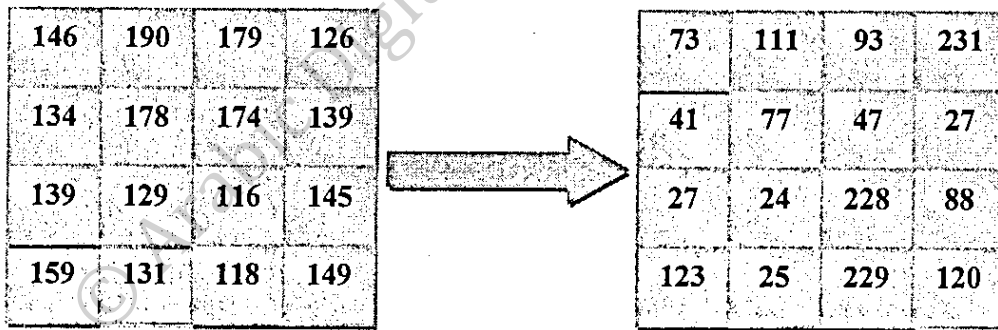


Fig. 15: Image transformation example

The resulted transformed image will be permuted at the second stage, which will shuffle the columns of it at the first step. The resulted shuffled image will be used as an input to the second step of shuffling to shuffle its rows to produce the final encrypted image.

3.3 Shuffling Stage

This stage aims to change the pixels locations to get new shuffled image. It performs shuffling operation using random permutation. This stage consists of two steps; the first step shuffles the columns of the transformed image and the second step shuffles the rows of resulted image. The encryption key is generated randomly and it will be used in both steps as encryption key. The following figure shows the shuffling stage.

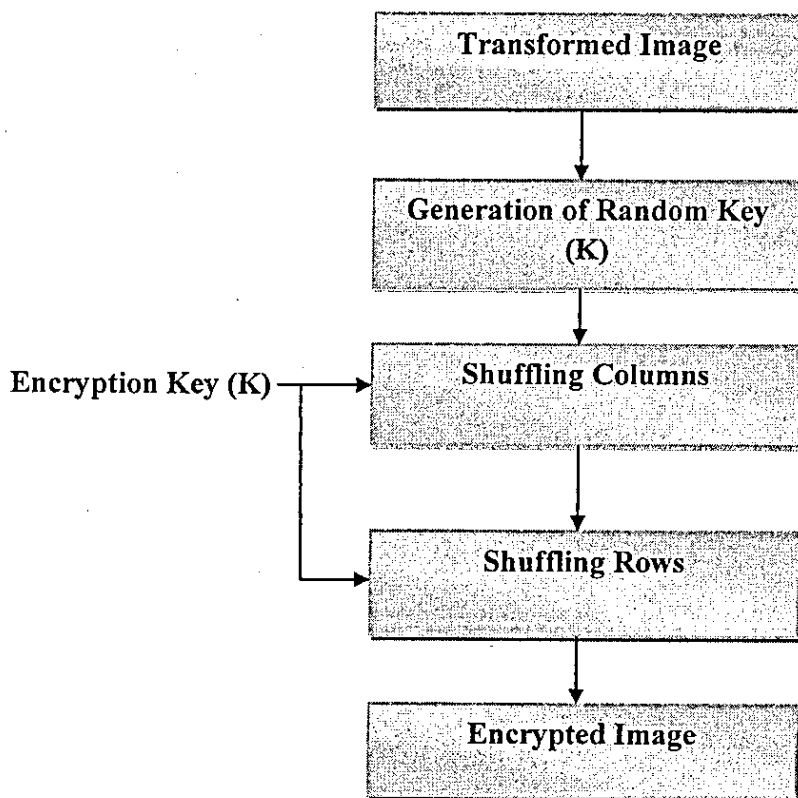


Fig. 16: Shuffling operation

3.3.1 Permutation Technique

In this proposed method, the permutation operation is performed based on random line permutation. An encryption key is generated randomly which will be used to shuffle the columns and the rows of the transformed image respectively. This operation does not change the values of pixels; it changes the positions of the columns and rows of image.

Suppose we have an image with size equals to $N \times N$, where N is the number of rows or columns of the image. The key will take values between one and N . These values are the original locations or the indexes of each row and column of the image before shuffling. If the first row of 4×4 image is permuted with the fourth row, and the location of the second row and third row does not change, the key will be $[4 \ 2 \ 3 \ 1]$. Figure 17 presents $N \times N$ image.

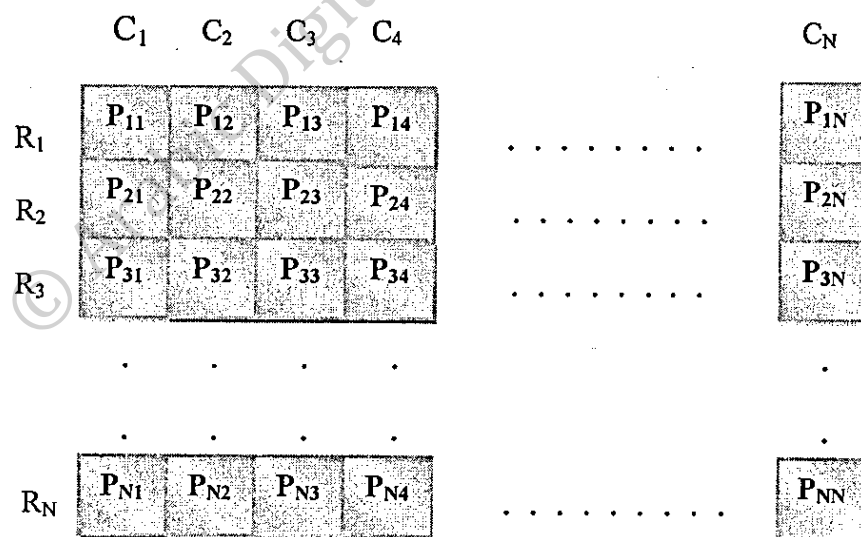


Fig. 17: $N \times N$ image

Where C_1 denotes the location of the first column in the image, R_1 is the first row of the image and P_{12} is a pixel, which locates at the first row and the second column of the image. If the image size is $6*6$, the resulted image of applying the shuffling operation on the image rows is:

P_{11}	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
P_{61}	P_{62}	P_{63}	P_{64}	P_{65}	P_{66}
P_{21}	P_{22}	P_{23}	P_{24}	P_{25}	P_{26}
P_{31}	P_{32}	P_{33}	P_{34}	P_{35}	P_{36}
P_{41}	P_{42}	P_{43}	P_{44}	P_{45}	P_{46}
P_{51}	P_{52}	P_{53}	P_{54}	P_{55}	P_{56}

Fig. 18: Shuffling rows of $6*6$ image

The generated key is [1 6 2 3 4 5]. If the same key is applied on the columns of $6*6$ image, the resulted image will be as the following figure:

P_{11}	P_{16}	P_{12}	P_{13}	P_{14}	P_{15}
P_{21}	P_{26}	P_{22}	P_{23}	P_{24}	P_{25}
P_{31}	P_{36}	P_{32}	P_{33}	P_{34}	P_{35}
P_{41}	P_{46}	P_{42}	P_{43}	P_{44}	P_{45}
P_{51}	P_{56}	P_{52}	P_{53}	P_{54}	P_{55}
P_{61}	P_{66}	P_{62}	P_{63}	P_{64}	P_{65}

Fig. 19: Shuffling columns of $6*6$ image

3.3.2 An Encryption Example

In this example, the transformed matrix that has been generated in transformation example is used as an input to the shuffling operation. The generated key is [4 2 3 1]. The following figure illustrates an encryption example.

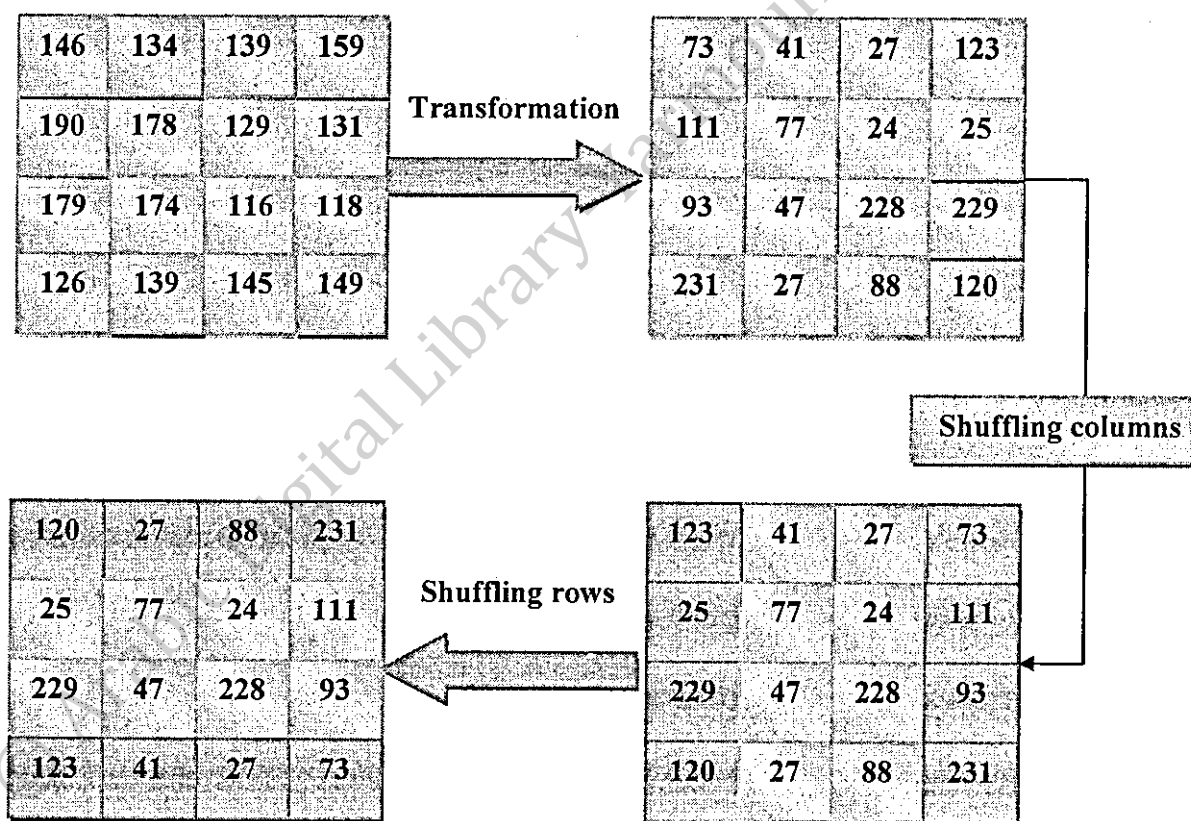


Fig. 20: An encryption example

3.4 Decryption Technique

To get the original plain image, decryption technique is needed. In this technique, red, green and blue components are decrypted separately. Figure 18 illustrates the proposed decryption system.

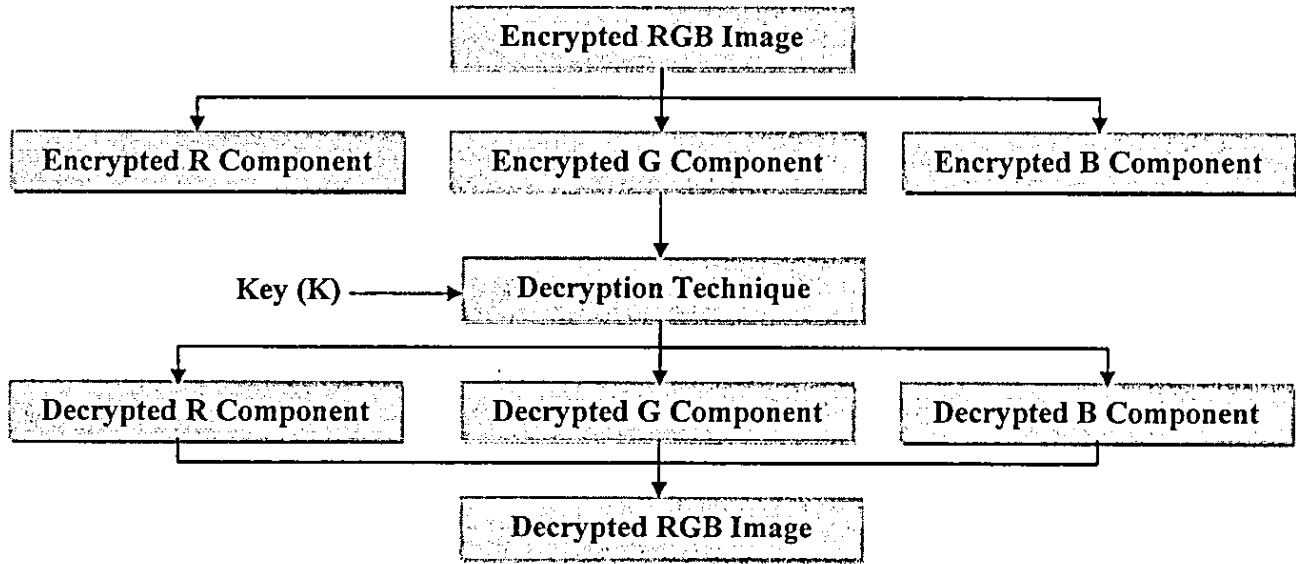


Fig. 21: Decryption system

This proposed encryption method uses two stages to decrypt the original image. The first stage gets the transformed image that was used as input to the shuffling function. The second stage uses the transformed image to get the original pixels values of the original image. To get the transformed image, the shuffled image is decrypted using two steps. The first step is to get the original pixels locations of the rows of the transformed image and the second step aims to get the original pixels locations of the columns of the transformed image. Figure 19 illustrates the decryption stages.

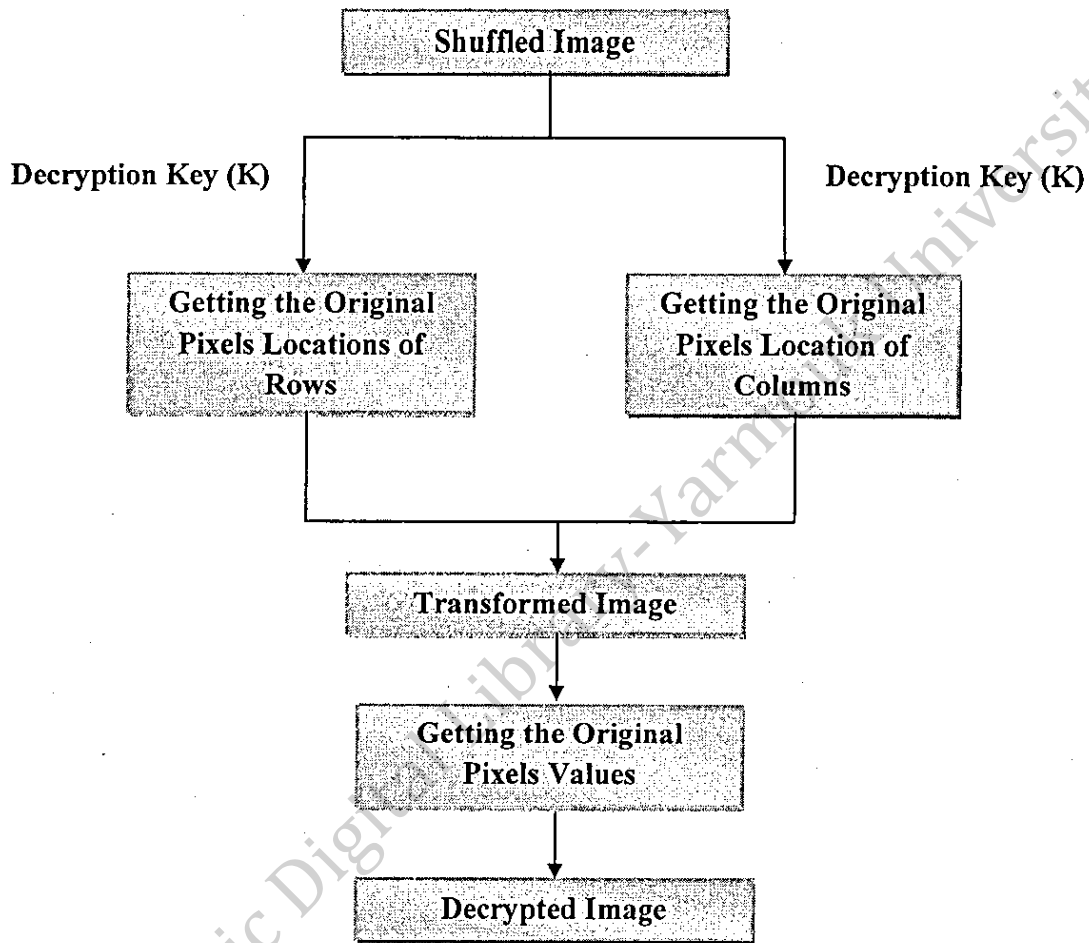


Fig. 22: The proposed decryption technique

The following figure shows an encrypted image of 4*4 pixels. The decryption stages are applied on it to get the decrypted image. This example uses the resulted encrypted image from the previous encryption example. The decryption key is the same encryption key which equals to [4 2 3 1].

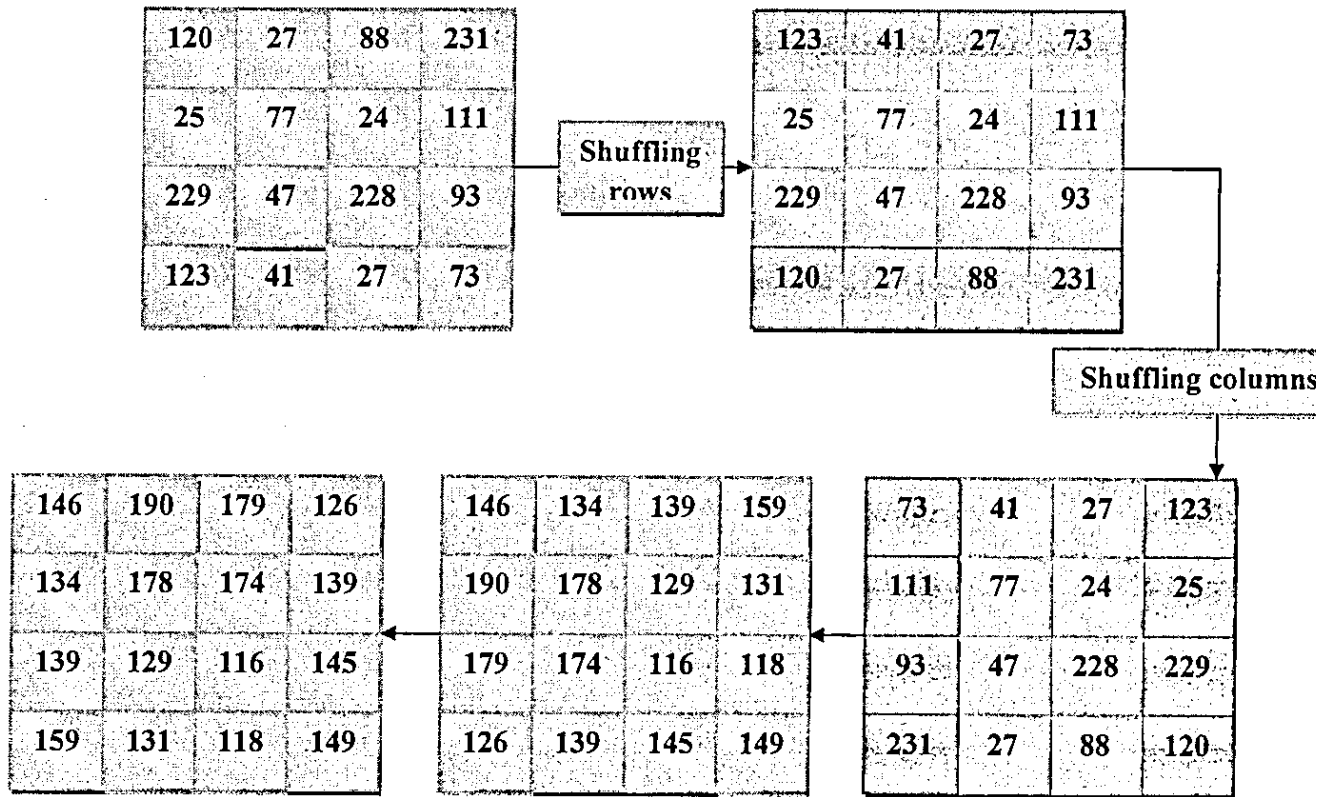
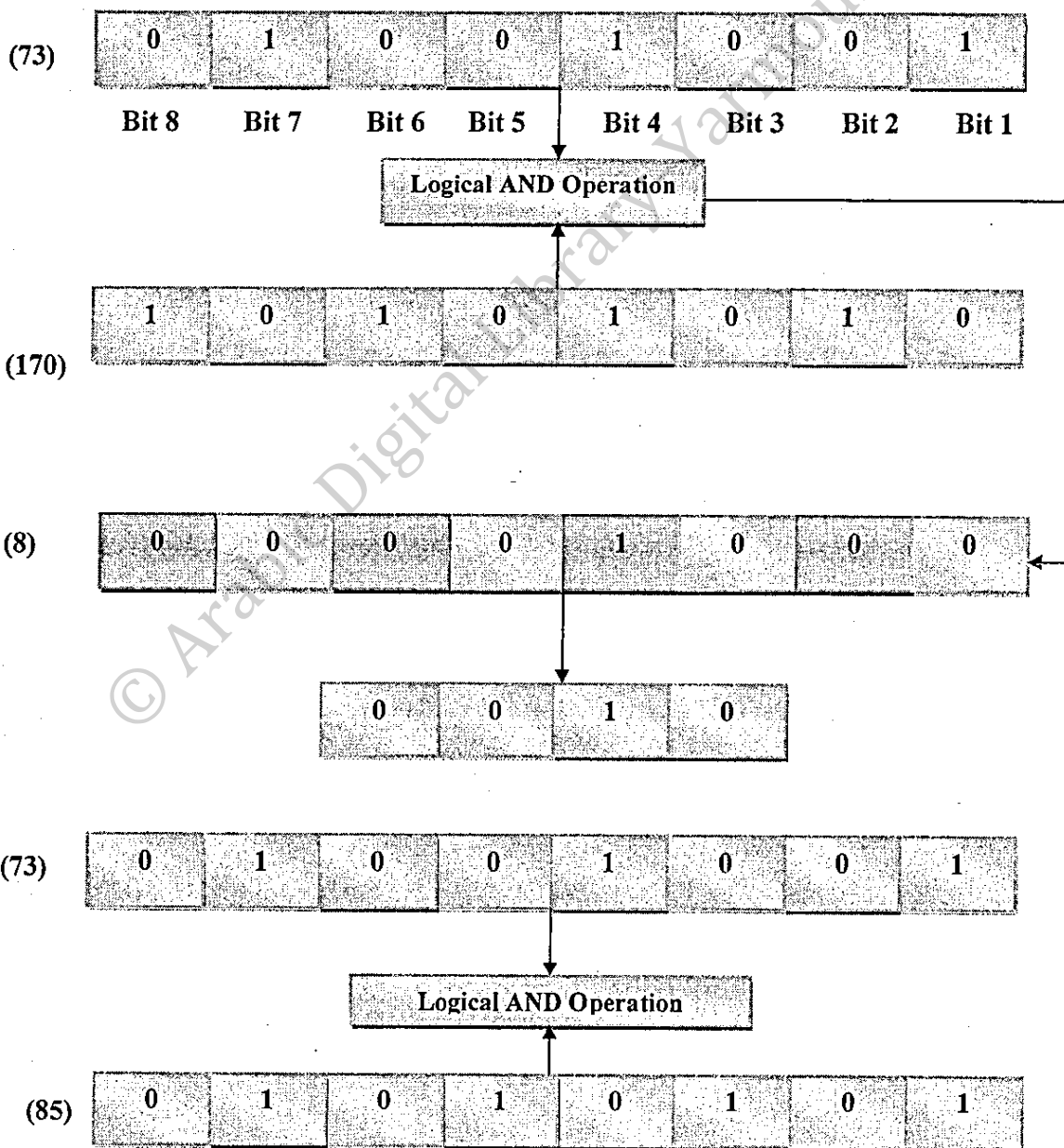
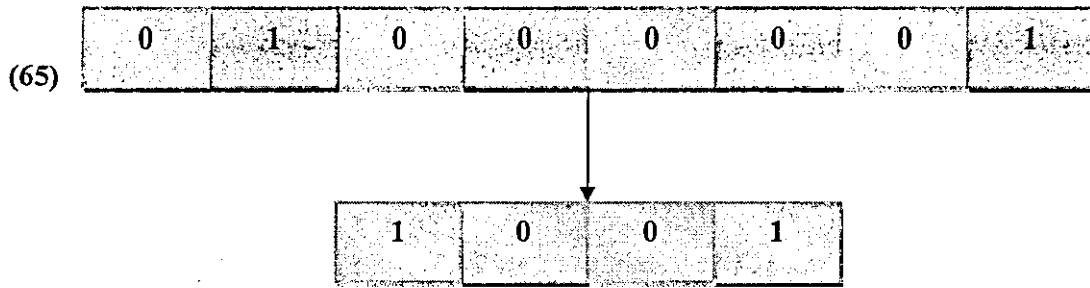


Fig.23: Decryption example

To illustrate how to get the original image from the transformed image, the following example takes one pixel value from the above transformed image and decrypts it to get its original value. The transformed pixel value is 73 with 01001001 binary values. Its original value is 146 with 10010010 binary values.





Combining bits



**Fig. 24: The proposed decryption technique
of the transformed pixel**

CHAPTER FOUR

ENCRYPTION EVALUATION METRICS AND RESULTS

4.1 Overview

An encryption algorithm changes the pixels values to make them different from their values of the original image. To have an efficient encryption algorithm, these changes must be performed in an irregular manner to get a maximum difference in pixels values between encrypted and original image. In addition, the encrypted image must be independent of the original image with a low correlation between them.

An encrypted image can be examined by the visual inspection. When the encrypted image has more hidden features of the original image, the encryption method is more efficient. The encrypted image cannot be judged by visual inspection only; it must be evaluated by other evaluation metrics to decide its degree of encryption.

Another important parameter that can be used to evaluate the encryption algorithm randomization is diffusion. To have a good diffusion characteristic, the encrypted image and the original image must have a complex relationship that cannot be easily predicted.

The evaluation metrics that will be used to evaluate the proposed encryption method are key space, correlation of adjacent pixels, Number of Pixels Change Rate, histogram uniformity and Mean Square Error.

4.2 Encryption Evaluation Metrics

4.2.1 Key Space

Different keys can be used in encryption system. The total number of the encryption keys is key space [40]. Encryption system can be evaluated as good system if its key is sensitive, sufficient and has a large space to prevent attackers from decrypting the original data [25]. The key of Encryption algorithm must be large enough to resist the brute-force attack [11, 30, 36, 41]. Completely different encrypted/decrypted image must result when any modification in single bit in secret key is performed [36]. High sensitive key is needed by secure image encryption systems to ensure that the encrypted image cannot be decrypted correctly although the difference between encryption and decryption key is small [31, 42].

4.2.2 Correlation of Adjacent Pixels

Correlation of adjacent pixels is an important metric that can be used to evaluate an encryption algorithm. It is measured between two vertically and horizontally adjacent pixels [43]. In the original image, the correlation between two adjacent pixels is high, while it is low between adjacent pixels in the encrypted image [35, 43, 44]. An efficient encryption algorithm aims to eliminate the correlation of pixels. In the proposed work, correlation coefficient is calculated between two adjacent rows and two adjacent columns of the original and the encrypted image.

Correlation of adjacent pixels can be given by [43]:

$$r = \frac{\sum_{i=1}^N (x_i - x_m)(y_i - y_m)}{\sqrt{\sum_{i=1}^N (x_i - x_m)^2} \sqrt{\sum_{i=1}^N (y_i - y_m)^2}} \quad (1)$$

Where:

$[x_i]$: The pixel intensity of the original image.

$[x_m]$: The mean value of original image intensity.

$[y_i]$: The pixel intensity of the encrypted image.

$[y_m]$: The mean value of the encrypted image intensity.

$[N]$: Number of rows of the image.

4.2.3 Number of Pixels Change Rate

To analyze the differential attack, Number of Pixels Change Rate (NPCR) is used. The attack attempts to find out a meaningful relationship between the original image and the encrypted image [45]. The attack changes only one pixel of the encrypted image and denotes the change of the resulted image. To test the effect of one pixel change, NPCR is a common measure. In the

proposed method, NPCR is used to calculate the difference between two adjacent pixels of the original image and the encrypted image.

Let $O(i, j)$ and $E(i, j)$ denote the values of the original and encrypted image at pixel (i, j) respectively. NPCR is defined in the following equation:

$$NPCR = \frac{1 - \sum_{i,j}^N D(i, j)}{N \times N} \times 100\% \quad (2)$$

Where:

$[N]$: The number of rows of the image.

$$D(i, j) = \begin{cases} 0, & \text{if } O(i, j) \neq E(i, j) \\ 1, & \text{if } O(i, j) = E(i, j) \end{cases} \quad (3)$$

4.2.4 Histogram Uniformity

The distribution of pixels in an image is illustrated by the image histogram by graphing the occurrence of each gray level of the image. The histogram of the encrypted image should be very different from the histogram of the original image. In addition, the distribution of the encrypted image should be a uniform distribution.

4.2.5 Mean Square Error

Mean Square Error (MSE) is an important metric to test the performance of the encryption technique. It is calculated between the original image and the decrypted image [45]. The errors in the decrypted fractional orders evaluate the MSE. If $O(i, j)$ and $D(i, j)$ denote the values of the original and decrypted image at pixel (i, j) respectively, $[N]$ is the number of rows of the original image, then the MSE can be calculated as [46]:

$$MSE = \frac{1}{N \times N} \sum_{i=1}^N \sum_{j=1}^N [|O(i, j) - D(i, j)|]^2 \quad (4)$$

In the proposed work, MSE is calculated for one thousand iterations. By using the proposed decryption technique, a decryption key is used to decrypt the image. MSE is calculated between the resulted decrypted image and the original image.

4.3 Results and Discussions

In this section, the experimental results obtained by applying the proposed encryption method will be presented.

4.3.1 Materials and Methods

In this thesis, the encryption algorithm consists of two phases:

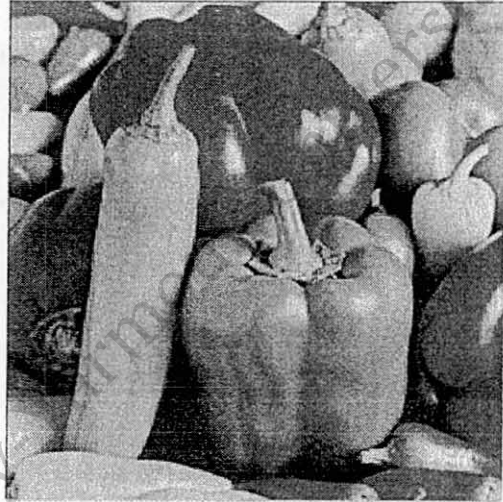
- 1- Transformation of pixels values phase, to get new values of pixels. This stage is applied to the three components of the original image, red, green and blue.

- 2- Shuffling phase, in which the image is shuffled randomly. It consists of two stages; the first stage shuffles the columns of the transformed image and the second stage shuffles the rows of the resulted image. An encryption key is generated to perform shuffling operation. This key is generated randomly and will be used in the decryption technique. This stage is also applied to red, green and blue components.

Encryption and decryption algorithms will be implemented using MATLAB software, the test images that will be used are RGB images and shown in figure 22. Table 2 shows the characteristics of these images.



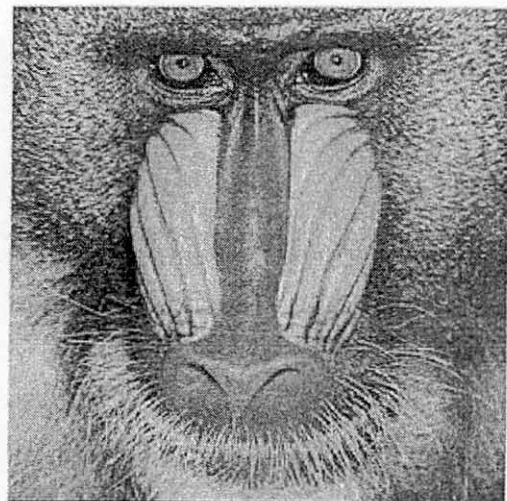
(a)



(b)



(c)



(d)

Fig. 25: Test images; a) Barbara, b) Peppers, c) Lena and d) Mandrill

Table .2: Test images characteristics

Image	Size	Format	Pixel Representation
Barbara	256*256	.JPG	Unit8
Peppers	256*256	.JPG	Unit8
Mandrill	256*256	.BMP	Unit8
Lena	256*256	.BMP	Unit8

4.3.2 Proposed Encryption Method Results and Discussions

The obtained results of the proposed encryption method are shown in figure 23. The first image presents the original image, the second image presents the encrypted image and the third image is the decrypted image.



(a)

(b)

(c)

Fig. 26: Proposed encryption method results; a) Original images, b) Encrypted images

and c) Decrypted images

From this figure, we observe the huge difference between the original images and the encrypted images; the encrypted images are intelligible. The encrypted image is evaluated by metrics to identify the quality of the encryption method.

The encryption evaluation metrics results are also calculated using MATLAB software. Key space, NPCR, MSE and histogram uniformity results are shown.

A. NPCR Results

NPCR is calculated for one hundred iterations of encryption. The average value is calculated and shown in table 3 for the four test images.

Table .3: NPCR results

Image	NPCR (%)
Barbara	99.6465
Peppers	99.4581
Mandrill	99.6307
Lena	99.6839

From the above table we observe that the values of NPCR are high. These high values show the big difference between the original image and the encrypted image. Table 4 compares the NPCR of the proposed method and obtained NPCR of methods of [25] and [47].

Table .4: Comparison of NPCR of Lena

Method	The proposed method	Method of [25]	Method of [47]
NPCR	99.6839%	99.6135%	99.52%

B .Correlation of Adjacent pixels Results

Correlation of adjacent pixels is calculated for two adjacent rows and two adjacent columns of the original and encrypted image. The encryption method is applied for one hundred iterations. The average value is calculated and shown in table 5 for the four test images.

Table .5: Correlation r results of test images

Image	Horizontal r of original image	Vertical r of original image	Horizontal r of encrypted image	Vertical r of encrypted image
Barbara	0.9594	0.9115	0.0312	0.0905
Peppers	0.9629	0.9565	0.0539	0.0971
Mandrill	0.8531	0.8675	0.0497	0.0684
Lena	0.9542	0.8913	0.0405	0.1625

The above table shows the difference between the correlation of the original images and encrypted images. The correlation of the original images is high while it is low in the encrypted images. Table 6 compares the resulted correlation r of Lena of the proposed method and the method of [47].

Table .6: Comparison of correlation r of Lena

Method	Horizontal r of original Lena	Vertical r of original Lena	Horizontal r of encrypted Lena	Vertical r of encrypted Lena
Proposed method	0.9542	0.8913	0.0405	0.1625
Method of[47]	0.9597	0.9792	0.1257	0.0581

C. Mean Square Error Results

An encryption key was generated randomly and used to decrypt the encrypted image. One thousand encryption keys were generated and the MSE is calculated between the resulted decrypted images and the original image. The obtained MSE of Lena image is shown in figure 27.

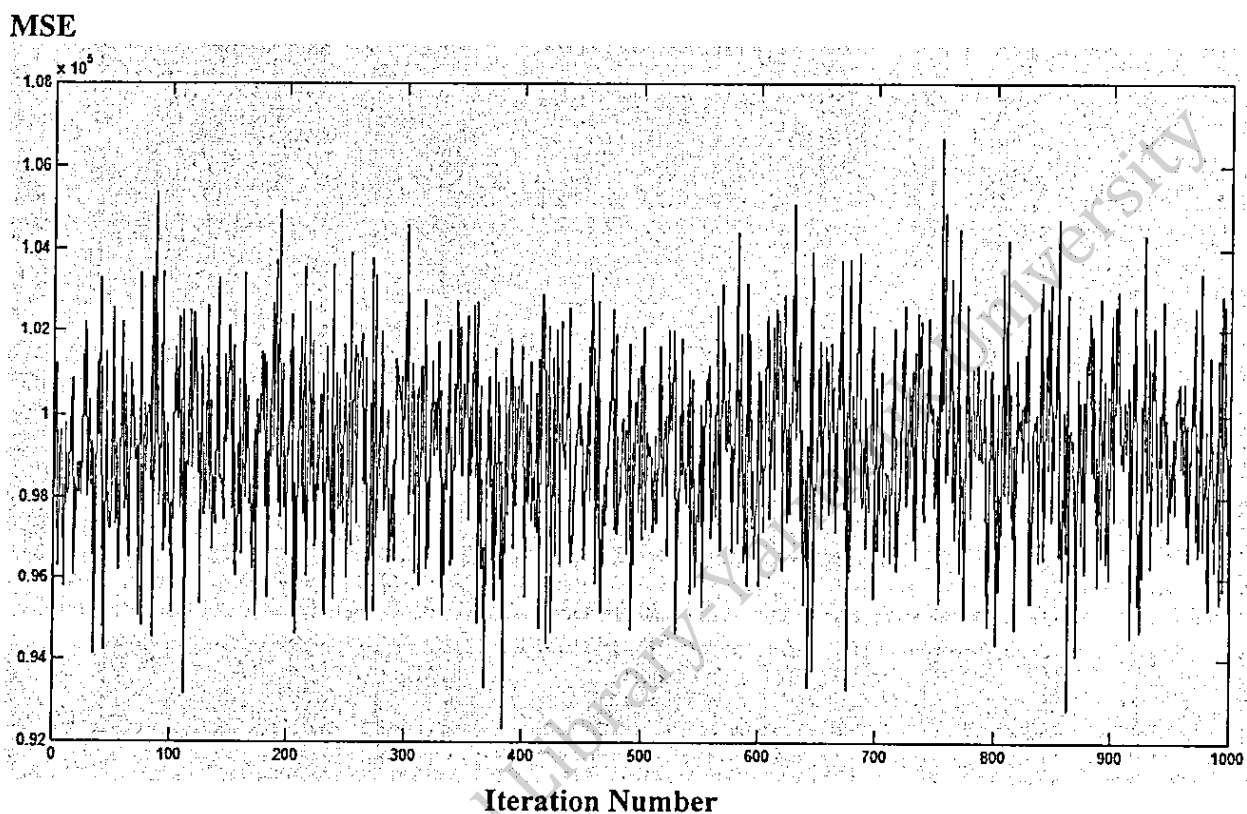
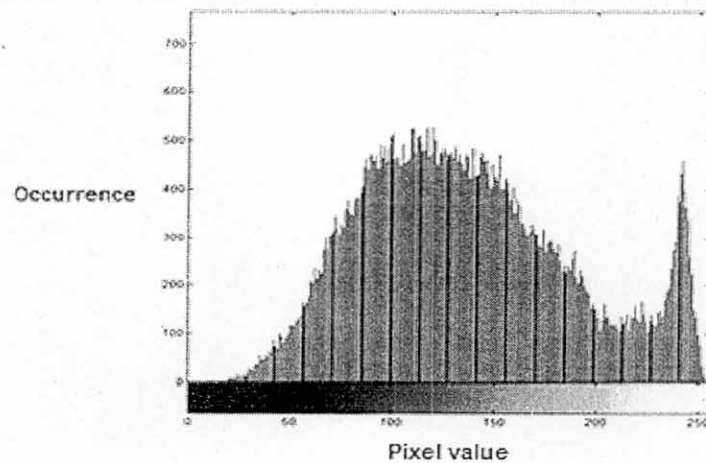


Fig. 27: MSE of Lena image

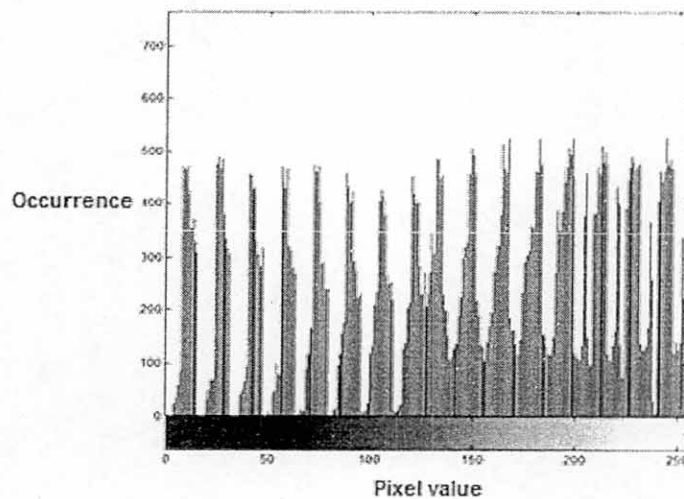
The previous figure shows that MSE is high which means the encrypted image is very secure. If the attacker tries to get the original image, he/she will try different keys. The difference between the original image and the decrypted image using these keys is high. Therefore, the original image is not easily reverted and it is very difficult to obtain the original image by trying different keys.

D. Histogram Uniformity

The histogram of the resulted encrypted image differs from the histogram of the original image. The resulted histogram is nearly uniform. Figures 28, 29 and 30 show the histograms of the three components of the original image and the encrypted image.



(a)

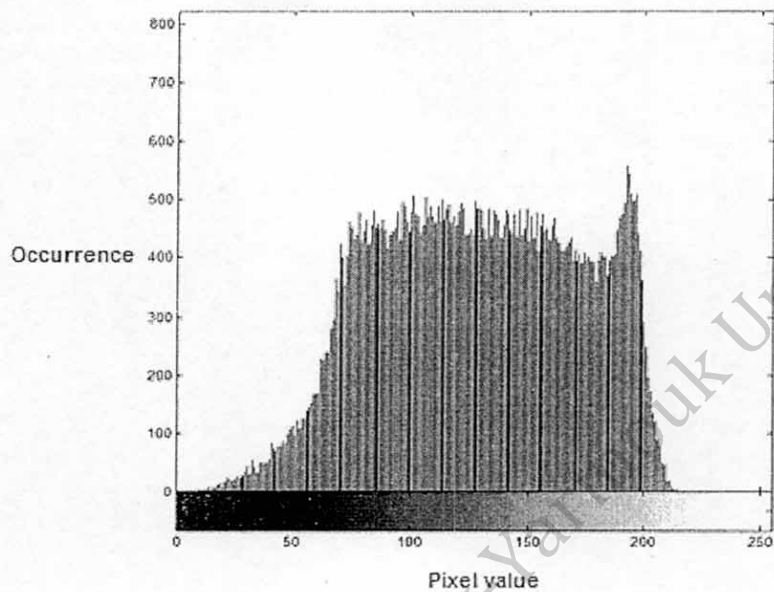


(b)

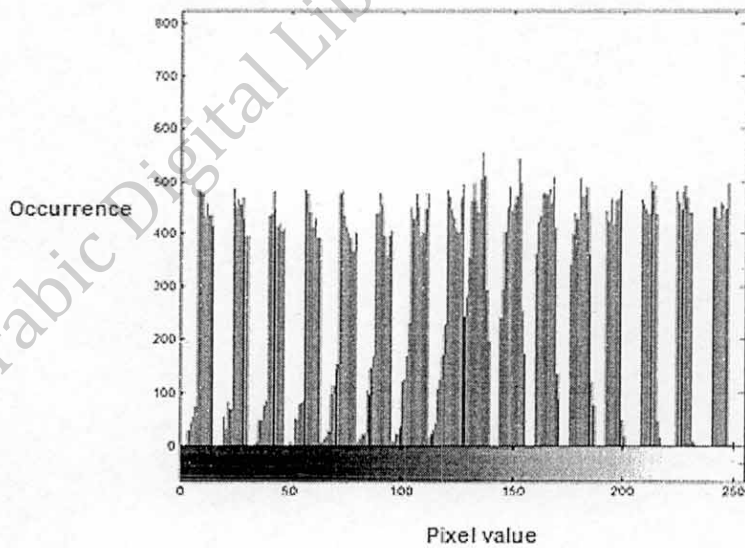
Fig. 28: Histogram of red component; a) Original red component

b) Encrypted red component

From above figure, we note the big difference in histogram between the red component of the original image and the encrypted image. The histogram of the encrypted image is nearly uniform. This difference refers to change of pixels values of the encrypted image.

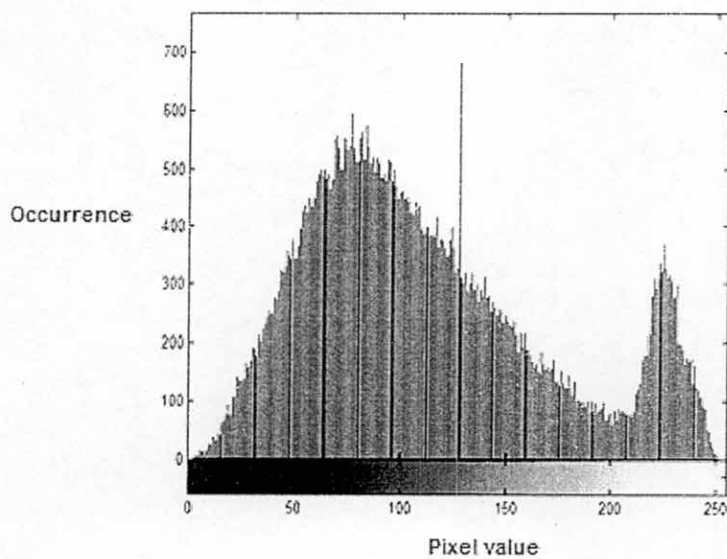


(a)

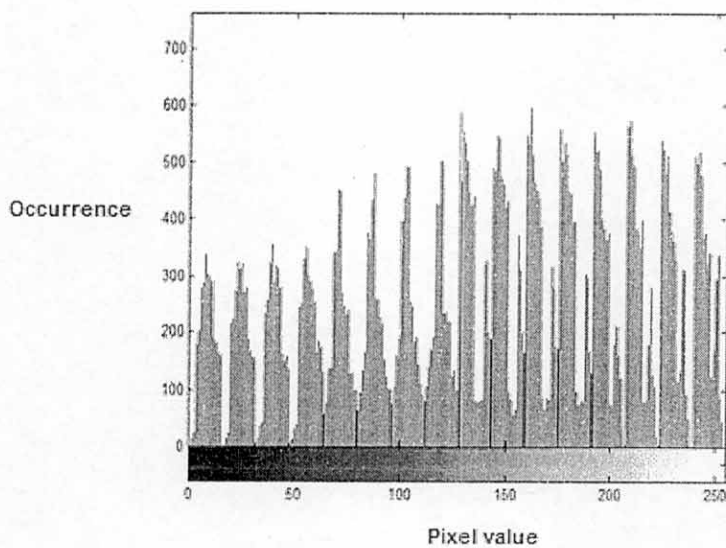


(b)

Fig. 29: Histogram of green component a) Original green component
b) Encrypted green component



(a)



(b)

Fig. 30: Histogram of blue component a) Original blue component
b) Encrypted blue component

CHAPTER FIVE

CONCLUSIONS

In this master thesis, a new colored image encryption algorithm was proposed. The proposed algorithm consists of two stages; transformation of pixels values stage and shuffling of columns and rows stage. The main goal of this algorithm was to get a high secure encryption system in which the original image cannot be easily reverted. The needed time for encryption is low which makes this algorithm an efficient encryption method.

The obtained experimental results shows the efficiency of the proposed algorithm according to the encryption evaluation metrics, which are NPCR, MSE, Correlation of adjacent pixels and histogram uniformity.

REFERENCES

[1] Xin Ge, Fen-lin Liu, Bin Lu and Jie Ren , "Improvement of an Encryption Algorithm Based on Hyper-Chaos," *Information Science and Engineering (ICISE), 2009 1st International Conference on*, pp.1303-1306, 26-28 Dec. 2009.

[2] R.Kadir, R.Shahril and M.A. Maarof, "A modified image encryption scheme based on 2D chaotic map," *Computer and Communication Engineering (ICCCE), 2010 International Conference on*, pp.1-5, 11-12 May 2010.

[3] (2000) The Symantec website. [Online]. Available: <http://www.symantec.com/>

[4] Chen Zaiping, Li Haifen, Dong Enzeng and Du Yang, "A Hyper-Chaos Based Image Encryption Algorithm," *Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2010 2nd International Conference on* , vol.2, pp.188-191, 26-28 Aug. 2010.

[5] Kwok-Wo Wong, Bernie Sin-Hung Kwok, and Wing-Shing Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", 2006.

[6] Yue Wu, J.P.Noonan, S Agaian , "A wheel-switch chaotic system for image encryption," *System Science and Engineering (ICSSE), 2011 International Conference on*, pp.23-27, 8-10, June 2011.

[7] A. Kumar and M. K. Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, pp. 372-382, 2011.

[8] H.H. Nien, W.T. Huang, C.M. Hung, S.C., Chen, S.Y. Wu, C.K. Huang and Y.H. Hsu, "Hybrid image encryption using multi-chaos-system," *Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on* , vol.1, pp.1-5, 8-10 Dec. 2009.

[9] Yan Cheng, Shu Yang and Shi-feng Li, "Image Encryption of Multiple Keys Method Based on Chaotic Maps," *Pervasive Computing Signal Processing and Applications (PCSPA), 2010 First International Conference on* , vol., no., pp.891-894, 17-19 Sept. 2010.

[10] Long Min and Huang Lu , "Design and Analysis of a Novel Chaotic Image Encryption," *Computer Modeling and Simulation, 2010. ICCMS '10. Second International Conference on* , vol.1,pp.517-520, 22-24 Jan. 2010.

[11] A.Jolfaei and A. Mirghadri, "A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1," *Artificial Intelligence and Computational Intelligence (AICI), 2010 International Conference on* , vol.2, pp.369-373, 23-24 Oct. 2010.

[12] Marwa Abd El-Wahed, Saleh Mesbah and Amin Shoukry," Efficiency and Security of Some Image Encryption Algorithms", *Proceedings of the World Congress on Engineering*, vol 1, July 2 - 4, 2008.

[13] S. Lian. (2006). *Multimedia Content Encryption*. (1st Ed.) [Online]. Available [http:// http://www.auerbach-publications.com](http://www.auerbach-publications.com).

[14] Yoon, J. W and Kim, H, "An image encryption scheme with a pseudorandom permutation based on chaotic maps", *Communications in Nonlinear Science and Numerical Simulation*, 15(12), pp. 3998-4006. Elsevier B.V, 2010.

[15] S. Bahaetdn "An image encryption algorithm robust to post-encryption bitrate conversion", Master. Dissertation, Dept Electrical and Electronics Eng., Univ. Middle East Technical, Sep. 2006.

[16] Venkatachalam, S.P, Vignesh, R, Sathishkumar, G.A, "An improved s-box based algorithm for efficient image encryption," *Electronics and Information Engineering (ICEIE), 2010 International Conference On* , vol.1, no., pp.V1-428-V1-431, 1-3 Aug. 2010.

[17] Chi-Feng Lu, Yan-Shun Kao, Hsia-Ling Chiang and Chung-Huang Yang, "Fast implementation of AES cryptographic algorithms in smart cards," *Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on*, pp. 573- 579, Oct. 2003.

[18] T. Gao, and Z .Chen, "A new image encryption algorithm based on hyper-chaos", *Physics Letters A*, pp. 394-400, 2007.

[19] Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos ", *Physics Letters*, pp. 5973–5978, 2008.

[20] Chen Wei-bin and Zhang Xin, "Image encryption algorithm based on Henon chaotic system," *Image Analysis and Signal Processing, 2009. IASP 2009. International Conference on*, vol.1, pp.94-97, 11-12 April. 2009.

[21] Huan Zhang, Ruhua Cai , "Image encryption algorithm based on bit-plane scrambling and multiple chaotic systems combination," *Intelligent Computing and Integrated Systems (ICISS), 2010 International Conference on*, pp.113-117, 22-24 Oct. 2010

[22] Weihai Li and Nenghai Yu , "A robust chaos-based image encryption scheme," *Multimedia and Expo, 2009. ICME 2009. IEEE International Conference on*, vol., pp.1034-1037, June 28 2009-July 3 2009.

[23] Mazleena Salleh , Subariah Ibrahim and Ismail Isnin, "Image encryption algorithm based on chaotic mapping", 2003.

[24] Mao-Yu Huang, Yueh-Min Huang and Ming-Shi Wang, "Image encryption algorithm based on chaotic maps," *Computer Symposium (ICS), 2010 International*, pp.154-158, 16-18 Dec. 2010.

[25] C.K. Huang, Y.H. Hsu, W.Y .Chen, Changchien, S.K.Hung, Liu .C.M., C.H. Tian and Y.R , "High security image encryption by two-stage process," *Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on*, pp.1-5, 8-10 Dec. 2009.

[26] H. Lian-xi, L. Chuan-mu, L. Ming-xi, "Combined image encryption algorithm based on diffusion mapped disorder and hyper chaotic systems" ,*Computer Applications*, pp. 1892-1895, Aug. 2007.

[27] Ibrahim El-Ashry, "Digital image encryption", Master. Dissertation, Dept. Electronics and Electrical Communications Eng., Univ. Menofia, 2010.

[28] Vreugdenhil, J.; Iverson, K.; Katti, R.S, "Image encryption using dynamic shuffling and XORing processes," *Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on*, pp.734-737, 24-27 May 2009.

[29] Che-Yen Wen and Kun-Ta Yang,1 , "Image authentication for digital image evidence", *Forensic Science Journal* , pp. 1-11, 2006.

[30] D. Chattopadhyay, M. K. Mandal and D. Nandi, " Symmetric key chaotic image encryption using circle map ", *Indian Journal of Science and Technology*, vol. 4, no. 5, May. 2011.

[31] Ibrahim F. Elashry, Osama S. Farag Allah, Alaa M. Abbas, S. El-Rabaie Fathi, and E. Abd El-Samie , "Homomorphic image encryption", *Journal of Electronic Imaging*, (Jul-Sep 2009).

[32] Alireza Jolfaei and Abdolrasoul Mirghadri, " Survey: Image Encryption Using A5/1 and W7", *Journnl of Computing*, vol. 2, no. 8, 2010.

[33] Alireza Jolfaei and Abdolrasoul Mirghadri , "Survey: Image Encryption Using Salsa20", *IJCSI International Journal of Computer Science Issues*, vol. 7, no. 5, September.2010.

[34] Andreas.UHI; Andreas pommer. (2005). Image and video encryption. (1st Ed) [Online]. Available <http://www.springeronline.com>

[35] S. R. Maniyath and M. Supriya, "An Uncompressed Image Encryption Algorithm Based on DNA Sequences", *Image (Rochester, N.Y.)*, pp. 258-270, 2011.

[36] Bo He, Fang Zhang, Longyan Luo, Maokang Du and Yong Wang, "An Image Encryption Algorithm Based on Spatiotemporal Chaos", *Image and Signal Processing, 2009. CISP '09. 2nd International Congress on*, pp.1-5, 17-19 Oct. 2009.

[37] Abhishek Misra, Ashutosh Gupta, and Damodar Rai, "Analyzing the Parameters of Chaos Based Image Encryption Schemes", *World Applied Programming*, vol. 1, no.5, pp. 294-299. Dec 2011.

[38] Lian, S, Sun. J and Wang, Z. (n.d.). "Security Analysis of A Chaos-based Image Encryption Algorithm", 2005.

[39] Mohammad Ali Baniyounes, "An Approach to Enhancement Image Encryption Using Blocked-Based Transformation Algorithm", Doctor of philosophy, Univ. Sains, 2009.

[40] Musheer Ahmad and M. Shamsher AlamA, "New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", *International Journal on Computer Science and Engineering*, vol.2 (1), pp. 46-50, 2009.

[41] R.Raja Kumar, A.Sampath and P.Indumathi, "Enhancement and Analysis of Chaotic Image Encryption Algorithms", *CCSEA, CS & IT 02*, pp. 143–153, 2011.

[42] K.Sakthidasan ,Sankaran and B.V.Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", *International Journal of Information and Education Technology*, vol. 1, no. 2, June. 2011.

[43] O.A. Panicker, A.Jabeenaa, A.Hassan Mujeebb, "Advanced image encryption and decryption using sandwich phase diffuser and false image along with cryptographical enhancement," *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, pp.833-837, 18-20 Oct. 2010.

[44] H.E.H. Ahmed, H.M. Kalash and O.S.F Allah, "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images," *Electrical Engineering, 2007. ICEE '07. International Conference on*, pp.1-7, 11-12, April. 2007.

[45] M.Prasad and K.L.Sudha, " Chaos Image Encryption using Pixel shuffling", Computer Science and Information Technology, 2011.

[46] M.R. Kumar, C.L .Linslal, V.P.M. Pillai and S.S. Krishna, "Color image encryption and decryption based on jigsaw transform employed at the input plane of a double random phase encoding system," *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on* , pp.860-862, 18-20 Oct. 2010.

[47] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption", *Optics Communications*, 282(11), pp. 2123-2127, Elsevier B.V, 2009.

تشفير الصور الملونة باستخدام التبدل العشوائي

اعداد:

شفاء وليد طوالبه

المُلخص

في مجال الاتصالات وتخزين الصور، تصبح السرية مسألة هامة لحماية البيانات من الوصول غير المصرح به. هناك عدة طرق لضمان السرية، والتشفير هو واحد منها. يستخدم التشفير على نطاق واسع لتشفير الصورة في العديد من التطبيقات لتوفير مستويات عالية من الأمان مثل الاتصال عبر الإنترنت، وأنظمة الوسائط المتعددة والتصوير الطبي. تحتاج عملية التشفير إلى خوارزمية التشفير ومفتاح التشفير. في هذه الأطروحة سوف يتم تشفير الصور الملونة على أساس تغيير قيم الصورة عن طريق تنفيذ عملية منطقية بين قيم الصورة وقيم محدد من أجل الحصول على صورة جديدة. في الخطوة التالية سيتم إجراء مجموعة من التبدلات العشوائية في أعمدة الصورة ومن ثم تعديل صفوف الصورة الناتجة من تبديل الأعمدة العشوائية. مفتاح التشفير سيتم انتاجه بطريقة عشوائية حتى يستخدم في عملية التشفير وفي عملية فك التشفير للحصول على الصورة الأصلية. توفر هذه الطريقة المقترحة مستوى عال من السرية بحيث يصعب الوصول إلى الصورة الأصلية من قبل الذين يحاولون الوصول إليها.