Encryption Protected Reversible Data Hiding for Secret Communication

Sowmyashree
ME Student
Thakur College of Engineering and Technology
Kandivili (E), Mumbai

Sanjay Sharma
Assistant Professor
Thakur College of Engineering and Technology
Kandivili (E), Mumbai

ABSTRACT

Security has become an important issue with the proliferation of digital communication. Multimedia sources such as images plays an important role in security of data communication. Data hiding technique can be used to implant secret data in host images where existence of data is undisclosed which reduces chances of unauthorized access. Some applications containing legal considerations require recovery of the cover image after extraction of secret data where reversible data hiding comes into view. Limitations of existing data hiding schemes in terms of robustness against digital attacks are major obstacles in the security of hidden data. Content protection scheme that integrates both encryption and data hiding for its protection and authentication will provide major protection against security attacks. This paper presents an efficient spatial domain reversible data hiding technique and also proposes implementation of image encryption upon reversible data hiding technique to protect the stego-image against attacks during communication. Histogram shifting based reversible data hiding technique results significant embedding capacity and achieve good reversibility property of images. Proposed approach guarantees PSNR 48db or more for most of the images like crowded, semi crowded and textured images.

General Terms

Security, Reversible Data Hiding, Encryption, Steganography, Steganalysis

Keywords

Digital rights Management, Histogram shifting, Prediction difference, Mode Value, Entropy, Correlation

1. INTRODUCTION

Increased use of digital communication makes security as an important issue. Multimedia sources such as images plays can used as carrier medium for secure data communication. The security and protection which is needed for creation, storage, transfer, and evaluation of multimedia contents require an integrated Digital Rights Management framework [1]. Data hiding and encryption are the primary tools to develop DRM applications. Limitations of currently existing data hiding schemes in terms of embedding capacity, embedding distortion, and robustness against digital attacks are major obstacles to realizing efficient DRM systems. Content protection system that integrates both encryption and data hiding for its protection and authentication will provide sufficient protection against active as well passive adversary attacks to enforce DRM policies [2]. Figure 1 shows traditional communication system without secrecy. Figure 2 shows secret communication system with data hiding.

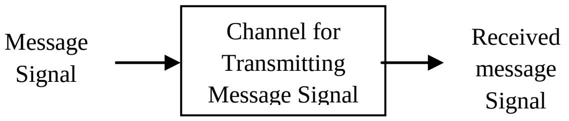


Figure 1: Traditional Communication Scheme

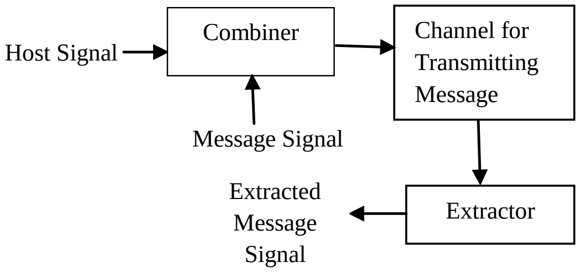


Figure 2: Secret communication system using data hiding

1.1 Need for Reversible Data Hiding

Data hiding is nothing but concealing secret message in cover media. Two sets of data are linked in data hiding process, a set of the embedded data and a set of the cover media data [3]. The association between these two sets of data characterizes different applications. In concealed communications, the hidden data may often be irrelevant to the cover media. In authentication, embedded data are closely related to the cover media. Invisibility of hidden data is an important requirement in these applications. Many of data hiding methods causes significant distortion due to data hiding and original media cannot be inverted back. In few applications, like medical diagnosis and law enforcement, it is essential to reverse the marked media back to the original cover media after the hidden data are retrieved for some legal considerations [3]. The data hiding systems fulfilling these requirements are referred to as reversible or lossless data hiding. The key characteristics of reversible data hiding techniques are embedding capacity, perceptibility, robustness and security [4]. Embedding capacity refers to the amount of information that can be hidden in the cover medium. Security refers the inability of the hacker to extract hidden information. Perceptibility means the inability to detect the hidden information. Robustness is the amount of modification the stego-medium can withstand before an adversary can destroy the hidden information. Many of the existing data hiding techniques are not reversible [5] [6] [7].

1.2 Need for Image encryption

The stego image during communication may subject to different types of security attacks. Steganalysis is the way to detect hidden messages. The goal of steganalysis is to identify whether a payload is encoded into images, and attempt to recover that payload. Hence, the security of Hidden Communication is major challenge of effective Data hiding. In order to avoid eavesdropping, the hidden contents must be invisible both perceptually and statistically. Visual attack and statistical attacks are two categories of steganalytic attacks [9]. In Visual Attacks the presence of hidden information is detected by visual inspection eye or by a computer. The attack is based on guessing the embedding layer of an image and then visually inspecting that layer to look for any unusual modifications in that layer. In case of statistical attack higher order statistics of the image are used to reveal tiny alterations in the statistical behavior caused by data embedding and hence can successfully detect even small amounts of data hiding with very high accuracy. Thus encryption of stego image will make an attacker's job difficult by converting image into unreadable form, ensuring protected against unauthorized access and modification during transfer. Image encryption will also help to keep the cover image secret.

2. RELATED WORK

Many state of art reversible data hiding techniques are proposed in literature. Based on embedding domain there are two categories of reversible data hiding techniques [2]. Spatial and transform domain. Spatial domain techniques include direct manipulation of pixels of the image including Difference Expansion [9], Histogram Shifting and Vector Quantization [10]. Histogram shifting methods achieves high embedding capacity along with guarantee of preserving high visual quality of the cover image after lossless data extraction. In this section various histogram based reversible data hiding techniques have been discussed**.**

Zhicheng Ni. et. al [3] designed a reversible data hiding using histogram of original image. The peak point and zero point in the histogram are used to embed the data. Peak point is the grayscale value which maximum number of pixels in the image contains and a zero point corresponds to the grayscale value which no pixel in the given image. Advantages of this method are having good embedding capacity and PSNR above 48db. Drawbacks of this algorithm are height of peak pixels are limited, thus capacity has finite limit.

Many authors have used histogram of prediction difference image for embedding. The main idea behind this is increasing peak points in the histogram for embedding data by exploring similarity characteristics of neighbor pixels.

Wen Tseng et al [11] proposed a reversible data hiding scheme by using predicators to generate on prediction error. By exploiting the expansion of the difference between a pixel and its predictive value the secret data is encoded in the cover image. This method is capable of providing a great embedding capacity without making noticeable distortion.

Luo et al. [12] utilized the pixel prediction strategy to generate predicted pixels to increase the height of peak in prediction error histograms. Because the prediction error is significantly narrowed down in a limited range, the height of peak point has been increased and the embedding payload has been improved. Yung et al [13] used a difference segmentation strategy and pseudo pixel generation to increase the height of peak in the prediction error histogram. The embedding payload in his method is higher than that of Luo *et al*.'s method.

Ching et. al [14] proposed a prediction based reversible data hiding which uses pixel frequency of each 3×3 blocks as mode value to compute prediction differences. Advantages of this method are peak values are increased. But this method uses sequential scanning of image for embedding which is improved in proposed method by using inverse S order of image scanning.

Varsaki et.al. [15] Proved that these reversible data hiding techniques are weak against security attacks. Embedded data can be easily damaged by the alteration of stego-image. In order to overcome this, our proposed hybrid approach integrates image encryption with data hiding. Stego image before transmission can be encrypted by using hash encryption. In order to extract the secret data the image to be decrypted at the receiver side.

3. PROPOSED SCHEME

The proposed hybrid scheme of data hiding and image encryption consists of 4 phases.

- Data Hiding in cover image
- Encryption of Stego-image
- Decryption of Stego-image
- Data Extraction and Image Recovery

The content owner embeds the secret data in the image and encrypts the whole image using encryption key. Upon receiving receiver decrypts image using the key and extracts the data and recovers original image. Figure 3 shows block diagram of proposed hybrid approach. .Data hiding scheme along with data extraction and image recovery is described in section 3.1 and Encryption and decryption scheme is described in section 3.2

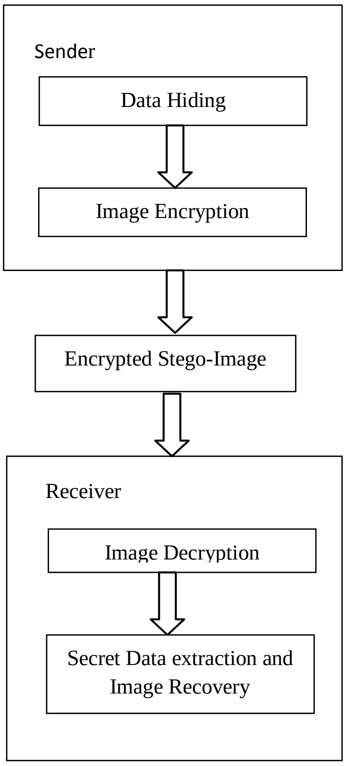


Figure 3: Proposed Hybrid approach for secret communication

3.1 Data Hiding and Extraction Scheme

Section 3.1.1 describes steps in Data Hiding algorithm and Section 3.1.2 describes steps in Data Extraction and Image Recovery.

3.1.1 Steps in Data Hiding

Step 1: Generation of mode value

Grayscale cover image is divided into 4×4 sized blocks. Each block having 16 pixels. Frequency of occurrence of each pixel value is counted. The pixel with highest frequency is used as mode value. Many existing approaches [13] [16] divides image into 3×3 sized blocks. But for a 512×512 image it results formation of incomplete blocks and we may need to resize the image. This can be overcome by using 4×4 block size in proposed approach. It also saves the time taken to scan the blocks.

Total No. of blocks $T = MXN / 4X4$. (T=16384). Figure 2 shows an example for single block. Each block Bk has 16 pixels $\{Bk \mid k=1,2\ldots.T\}$

0	3	1	2
1	2	3	4
3	0	5	1
1	3	5	3

Figure 4: Example of Single block of image with 16 pixels.

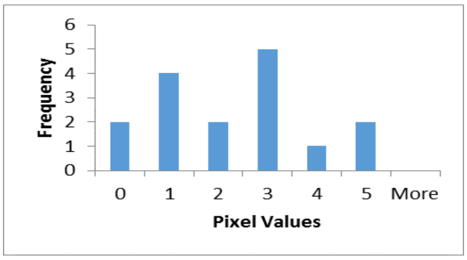


Figure 5: Histogram of single block of Image

The Figures 4 and 5 shows example of single image block and histogram respectively. In the given example,

Frequency of occurrence of pixel 0 = 2
Frequency of occurrence of pixel 1 = 4
Frequency of occurrence of pixel 2= 2
Frequency of occurrence of pixel 3 = 5
Frequency of occurrence of pixel 4 = 1
Frequency of occurrence of pixel 5 = 2

Thus Mode value is 3 with maximum frequency 5. Thus Mode value= 3. In Ching et. al's[13] approach it is not specified how to choose mode value for the block containing more than one maximum frequency values. Our proposed approach solves this problem by using following method. Mode Value= average (Sum of 2 or more pixels with equal maximum frequency). For Example, suppose Frequency of occurrence of pixel 1, 3 and 2 =5, Mode value= average of (1+3+2) =3. Mode values are store in mode value table which is used for hiding and restoration procedure.

Step 2: Computation of prediction difference image by using mode value

For each block, prediction difference of each pixel d_i = (Mode value-pixel value) where i= 1,2…..16

Predictive differences are stored in an array for construction of predictive difference image. Predictive difference image for single block shown in fig 2 is as shown in figure 6.

3	0	2	1
2	1	0	-1
0	3	-2	2
2	0	-2	0

Figure 6: Predictive difference image for single block

Step 3: Find zero and peak points from the predictive difference histogram

Histogram of predictive difference image consists of positive group ($0 \leq d_i \leq 255$) and negative group ($-255\leq d_i \leq -1$). In figure 7 each group has one peak point and one zero point. Peak point in positive group is pixel value 0 with maximum frequency 5 and zero point is pixel value 4 with minimum frequency 0. Similarly peak point in negative group is pixel value -2 with maximum frequency 2 and zero point is -3 with minimum frequency 0. After finding two pairs of peak and zero points they should be stored to be used in extraction procedure.

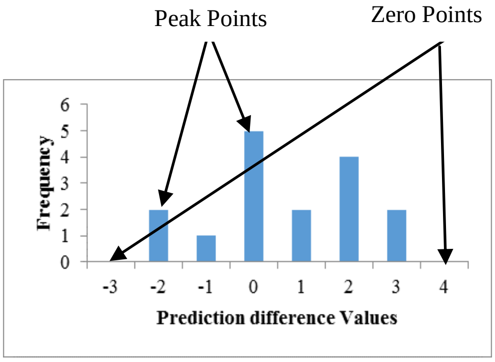


Figure 7: Predictive difference histogram showing peak and zero points.

Step 4: Shift the Pixels of predictive difference histogram

In order to create space for embedding secret message in peak points, the pixels of predictive difference image should be shifted. In the positive group, all the pixels which fall between peak point and zero point are shifted one bit right. Where as in negative group they are shifted left thus creating empty space next to peak points as shown in figure 8 and 9. The predictive difference is increased one bit, $d_i = d_i+1$, if prediction difference d_i Є [1, 3]. The predictive difference is decreased one bit, $d_i = d_i-1$, if prediction difference d_i Є [-2, -3].

4	0	3	2
3	2	0	-1
0	4	-2	3
3	0	-2	0

Figure 8: Shifted prediction differences

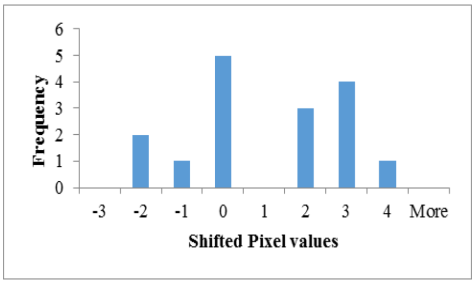
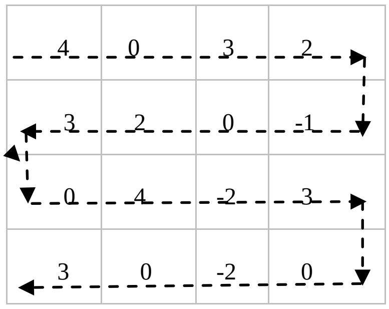


Fig 9: Shifted prediction difference Histogram

Step 5: Embed the secret message

Secret message is converted to binary. Shifted predictive difference image is scanned in inverse S order [17]. If the secret message bit is 1, the peak point of positive group is increased by 1. Otherwise it is unchanged. Similarly peak point is decreased by 1 in the negative group. If the secret message bit is 0, peak points in both the groups are unchanged. This process is repeated until all the bits are embedded.



4	0	3	2
3	2	0	-1
0	4	-2	3
3	0	-2	0

Figure 10: Inverse S order scanning

Figure 10 shows inverse S order scanning. If message is 1111111, the grayscale values change as shown in figure 11 and 12.

4	1	3	2
3	2	1	-1
1	4	-3	3
3	1	-3	1

Figure 11: Grayscale values after embedding message

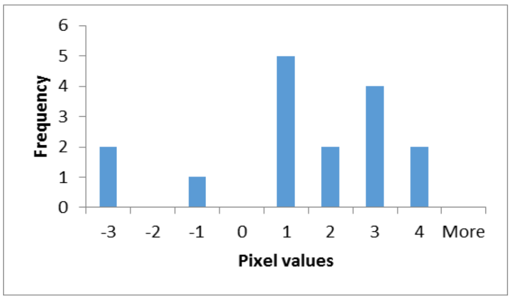


Figure 12: Histogram after embedding message

Step 6: Construct the stego-image by predictive difference.

To construct the stego image, prediction difference image with embedded data is divided into 4×4 non-overlapping blocks. The system finds the predictive value m_k *of* block B_k and subtracts the pixel values of block B_k by using the mode value in the previously recorded index table. After the blocks are computed completely, we can obtain the stego-image, which has been hidden the secret messages. In our example mode value is 3. Pixel values of hidden message image are subtracted by 3 as shown in figure 13.

4	1	3	2
3	2	1	-1
1	4	-3	3
3	1	-3	1

-1	2	0	1
0	1	2	4
2	-1	6	0
0	2	6	2

Figure 13: Construction of Stego-image

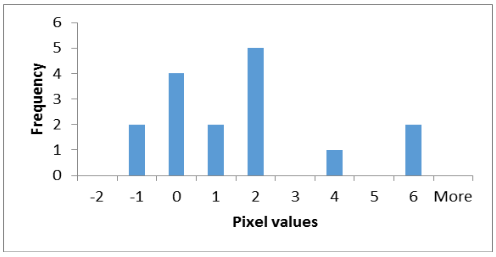


Figure 14: Histogram of Stego-image

3.1.2 Steps in Secret Data Extraction and Restoration Procedure

The data extraction and image recovery are reverse procedure of data hiding method discussed above.

Step 1: Partition the stego-image and compute prediction difference image.

The stego-image is divided into 4X4 non-overlapping blocks The predictive difference will be evaluated for each block using subtracting each pixel value by mode of respective blocks which is previously stored in index table. In our example mode value is 3 for block shown in figure 15.

-1	2	0	1
0	1	2	4
2	-1	6	0
0	2	6	2

4	1	3	2
3	2	1	-1
1	4	-3	3
3	1	-3	1

Figure 15: computing Prediction Difference image from the Stego-image

Step 2: Extract the secret data and restoration shifting predictive difference

Peak points and zero points in positive group and negative group recorded during embedding procedure has to be used in extraction process. This is the exact reverse process of embedding. Scan the image in inverse S order. While scanning, wherever peak points are found extract secret message bit 0. If peak point= peak point +1 (Positive group) then secret message bit 1 is extracted and pixel value is reset to peak value by subtracting 1. Similarly wherever peak point-1 (negative group) is encountered extract message bit 1 and reset the pixel value to peak value by adding 1.

For Example, in our example peak point in positive group is 0. While scanning the image wherever 0 is encountered extract message bit 0. Wherever 1 is encountered, extract secret message bit 1 and set pixel to 0. Similarly peak point in negative group is -2. Wherever -2 encountered extract message bit 0 and wherever -3 encountered extract message bit 1 and reset pixel value to -2. Finally message bits 1111111 is obtained. Figure 16 shows image after extraction. Repeat the above steps for all the blocks until the secret data are extracted completely.

4	1	3	2
3	2	1	-1
1	4	-3	3
3	1	-3	1

4	0	3	2
3	2	0	-1
0	4	-2	3
3	0	-2	0

Fig 16: Extraction of hidden message bits

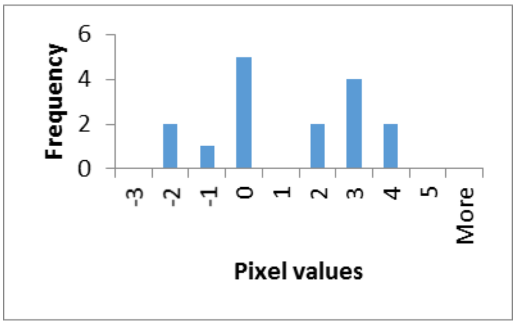


Fig 17: Histogram of message extracted image

Step 3: Shift pixels of histogram and Restore the predictive differences.
All the pixels which are shifted in prediction difference image before embedding are shifted back. i .e. shifted left one bit in positive group and right in negative group as shown in figure 18 and 19.

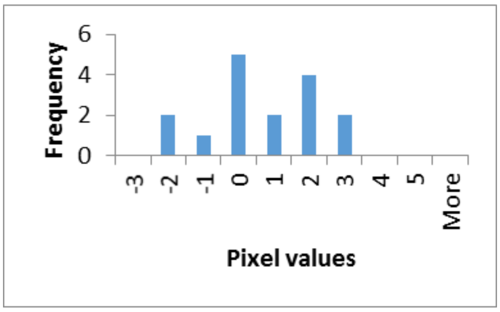


Fig 18: Histogram of shifted predictive differences

3	0	2	1
2	1	0	-1
0	3	-2	2
2	0	-2	0

Fig 19: Grayscale values after shifting

Step 4: Restore to original image.
Shifted predictive difference image should be divided into blocks to compute original image from predictive difference image. Using mode values of respective blocks stored in index table pixel values are subtracted. Repeat the above steps sequentially until the blocks are computed completely. Finally, we can obtain the original image by the restoration procedure. Figure 20 shows pixel values which are subtracted by mode value 3.

3	0	2	1
2	1	0	-1
0	3	-2	2
2	0	-2	0

0	3	1	2
1	2	3	4
3	0	5	1
1	3	5	3

Fig 20: Restoration of original image

3.2 Image Encryption and Decryption scheme

In the hybrid approach, after performing steps in Data hiding steps (section 3.1.1) the stego image is encrypted. For encryption the proposed method uses hash image encryption algorithm [18].

3.2.1 Key Generation

The key generation algorithm is based on pseudorandom number generation concept [19]. Number of bytes n is given as input to key generation algorithm. The program generates n number of random number which is treated as secret key. These secret keys are converted into bits for performing encryption and decryption. These secret keys are shared by only sender and receiver.

Key Generation Algorithm is as follows:
Step 1: Read parameter n where n is the number of bytes in the key.
Step 2: Convert that into bits by computing n*8
Step 3: Store binary representation of key as bin_x.
Step 4: Calculate the next bit as bin_x_n_minus_1.
Step 5: For each bits in the key (the first bit is always a 0)
Step 6: Calculate x_n = 1 - 2* bin_x_N_Minus_1 * bin_x_N_Minus_1.
If x_n is positive, the corresponding bit in the key is 1, otherwise it is zero.
Step 7: Convert the bits of the key into bytes, and store them in output array, key.
Step 8: The kth entry in key is the 8 bit number represented by taking every (n/8) th entry in bin_x storing from k.

3.2.2 Encryption and Decryption

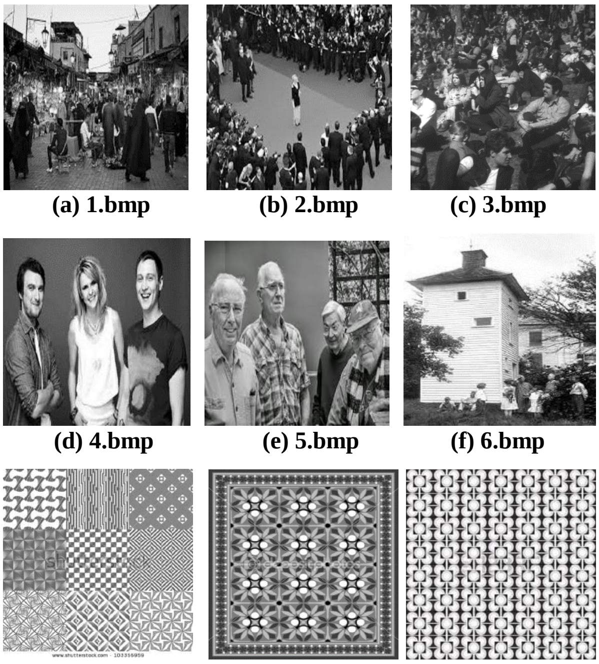
In the image encryption part, stego image and secret key are passed as input to the algorithm. The algorithm calculates the length and breadth of image. XOR operation is performed between pixels values of cover image and binary values of generated key values. After performing XOR operation between pixels values of cover image and binary values of secret keys, the input image is converted into encrypted image i.e.; without the knowledge of secret keys no one can identify original image.

In the decryption part, encrypted image and secret key are passed as input to the algorithm. Again algorithm performs XOR operation between pixels values of encrypted image and secret keys which results as original input image as aim of cryptography approach.

4. RESULTS AND DISCUSSION

Experiments are carried out using MATLAB version 7.11 environment. Experiments are carried on grayscale bitmap images of size 512×512 images. In the first phase, the secret data in binary form is hidden in cover image. Cover image is encrypted and sent to the receiver. Receiver decrypts the image in order to extract the hidden message. Security is measured in terms of Entropy [20] [21] and Correlation [22]. Image quality analysis is done by using parameter PSNR [23]. For a payload of 8000 bits our approach gives higher PSNR

(Peak Signal to Noise Ratio) thus proving high reversibility characteristics after data extraction. For the result analysis images are categorized as crowded images, semi crowded images and textured images. Figure 16(a)-(i) shows different images used in experiments.



(a) 1.bmp **(b) 2.bmp** **(c) 3.bmp**

(d) 4.bmp **(e) 5.bmp** **(f) 6.bmp**

(g)7.bmp **(h) 8.bmp** **(i) 9.bmp**

Figure 16(a)-(i): Different images used in experiments.

Table 1 shows PSNR, entropy and correlation values measured for above images.

Table 1: PSNR, entropy and Correlation values for different categories of images.

Image Type	Image	PSNR (dB)	Entropy of Encrypted Image	Correlation between original and encrypted image
Crowded Images	1.bmp	50.8311	7.9579	0.0012
	2.bmp	51.3439	7.9583	0.0018
	3.bmp	51.2352	7.9580	0.0047
Semi Crowded Images	4.bmp	50.0458	7.9595	0.0012
	5.bmp	49.6070	7.9653	0.0028
	6.bmp	48.7256	7.9587	0.0031
Textured Images	7.bmp	48.3130	7.9568	0.0019
	8.bmp	49.3966	7.9585	0.0036
	9.bmp	48.2005	7.9699	0.0017

4.1 Security Analysis

The entropy values obtained shows the high level of security. That is the encrypted image is random compared to original Image. Entropy values shown in table are almost equal to 8 which theoretical value of maximum randomness of the encrypted image.

The correlation coefficient values range between +1 and -1. Low correlation indicates high level of dissimilarity between two images [22]. Values shown in table one are very low indicating strong dissimilarity between original and encrypted image. Thus Entropy and correlation values indicated our approach is a strong image encryption. Also Encryption algorithm uses 256 bit key providing large key space (2^{256}) and makes brute force attack difficult.

4.2 Image Quality Analysis

Quality of reconstruction of image is measured by using Peak Signal to Noise Ratio (PSNR). Typical PSNR for images are between 30 to 50db for bit depth of 8-bit. From the results shown in Table 1 it is clear that crowded and semi crowded images are giving better PSNR values as compared to textured images depending upon illumination condition and smoothed and non-smoothed blocks. As crowded image gives better PSNR values because of its statistical landscape features and high frequency components resulting better correlation values between image blocks.

5. CONCLUSION

Focusing on security of secret data transfer, we proposed an encryption protected reversible data hiding scheme. By using block pixel frequency to compute prediction difference image number of peak points in the histogram is increased, thus resulting in significant embedding capacity and also preserving reversibility properties of cover image without loss of hidden data. Our scheme of reversible data hiding resulted high quality of image reconstruction by achieving PSNR more than 48db. Data hiding followed by encryption provides high level security to hidden data making it difficult to decrypt the image. Also encrypted cover image can be kept secret and is robust against few possible security attacks.

6. ACKNOWLEDGEMENT

I would like to express my sincere thanks to my project guide **Dr. R. R. Sedamkar,** Professor, Computer Engineering Department, Thakur College of Engineering and Technology for his great support and guidance throughout my research work

7. REFERENCES

[1] William Ku and Chi-Hung Chi, 2004, Survey on the technological aspects of Digital Rights Management, School of Computing. National University of Singapore Science Drive 2.

[2] Hafeez M.A. Malik, “Data hiding techniques for Digital rights Management of Multimedia Archives”, Master Thesis, University of Illinois, Chicago, 2006

[3] Z. Ni, Yun Q. Shi, N. Ansari, and W. Su, “Reversible Data Hiding,” *IEEE Tran. Circuits and Systems for Video Technology, vol. 16, no. 3, PP. 354-362, 2006.*

[4] D.R.Denslin Brabin1, Dr.J.Jebamalar Tamilselvi2,” Reversible Data Hiding: A Survey, ISSN (Print) : 2320 – 9798 ISSN (Online): 2320 – 9801 International Journal of

Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, 2013

[5] C.W. Honsinger, P.W. Jones, M. Rabbani, and J.C. Stoffel, “Lossless recovery of an original image containing embedded data,” US Pat.#6,278,791, 2001.

[6] J. Fridrich, M. Goljan, and R. Du, “Lossless data embeddingnew paradigm in digital watermarking,” EURASIP Journ. Appl. Sig. Proc., vol.2002, no. 02, pp. 185–196, 2002.

[7] J. Tian, "Wavelet-based reversible watermarking for authentication," Proc. of SPIE Sec. and Watermarking of Multimedia Cont. IV, vol. 4675, no. 74, 2002.

[8] Ms.G.S.Sravanthi , Mrs.B.Sunitha Devi , S.M.Riyazoddin & M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", *Global Journal of Computer Science and Technology Graphics & Vision,* Volume 12 Issue 15 Version 1.0 , Online ISSN: 0975-4172 & Print ISSN: 0975-4350, 2012

[9] J. Tian , "Reversible Data Embedding Using a Difference Expansion, *IEEE Tran. Circuits and Systems for Video Technology*, vol. 13, issue 8, pp. 890-896. 2003

[10] Chin-Chen Chang, Wei-Liang Tai and Chia-Chen Lin (2006). A Reversible Data Hiding Scheme Based On Side Match Vector Quantization, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 10.

[11] Hsien-Wen Tseng*, Chi-Pin Hsieh, "Prediction-based reversible data hiding", Information Sciences, *Elsevier*, ISSN: 2460–2469, 2009

[12] L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong,"Reversible image watermarking using interpolation technique," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 1, pp. 187–193, 2010.

[13] Yung-Chen Chou and Huang-Ching Li, "High Payload Reversible Data Hiding Scheme Using Difference Segmentation and Histogram Shifting", *Journal of Electronic Science and Technology*, VOL. 11, NO. 1, 2013

[14] Ching-Te Wang, Ching-Lin Wang, Lin-Chun Li, Sheng-You Guo," The Image High Capacity and Reversible Data Hiding Technique Based on Pixel Frequency of Block", *IEEE*, 978-1-4577-2119-9/12, 2011

[15] E. Varsaki, V. Fotopoulos, A. N. Skodras, "A reversible data hiding technique embedding in the image histogram "*Hellenic Open University Journal of Informatics*, Technical Report HOU-CS-TR-2006-08-GR,2007.

[16]H. L. Yeh, "Prediction-Based Reversible Data Hiding," Master Thesis, Department of Computer Science and Information Management, Providence University, Taiwan, Republic of China, 2007.

[17] Rajkumar Ramaswamy,Vasuki Amurugam, "Lossless data hiding based on histogram modification", *The International Arab Journal of Information Technology*, Vol. 9, No. 5, 2012

[18] Manish kumar, Manu Bhai Jha, "GUI Based Encryption and Decryption of Image with Secure Image Steganography", *International Journal of Scientific Research and Education*, Volume 2, Issue 7, ISSN (e): 2321-7545, 2014

[19] L. Blum, M. Blum And M. Shub, "A Simple Unpredictable Pseudo-Random Number Generator", Society For Industrial And Applied Mathematics, Siam J. Comput., Vol. 15, No. 2,1986

[20] Yue Wu, Joseph P. Noonan, Sos Agaian, Shannon Entropy based Randomness Measurement and Test for Image Encryption, *Elsevier*, arXiv:1103, 5520 v1[cs.CR], 2011

[21] Yue Wu, Yicong Zhou, George Saveriades, SosAgaian, Joseph P. Noonan, Premkumar Natarajan, Local Shannon entropy measure with statistical tests for image randomness, *Elsevier*, Information Sciences, 323–342, 2013

[22] A.A.Goshtasby, Similarity and Dissimilarity Measures, *Advances in Computer Vision and Pattern Recognition (Springer)*, DOI 10.1007/978-1-4471-2458-0_2, 2013

[23]Ravi Kumar, Munish Rattan, "Analysis of Various Quality Metrics for Medical Image Processing", *IJARCSSE*, Volume 2, Issue 11, November 2012 ISSN: 2277 128X