Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMAGE ENCRYPTION USING ENHANCED FOUR STAGE ENCRYPTION

[1]SANGAPU VENKATA APPAJI, [2] DR. GOMATAM V S ACHARYULU

[1]Assistant Professor, Department of IT, Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabd, Telangana, India, appaji_sv@yahoo.co.in
[2]Retired Professor, Department of CSE, Geethanjali college of Engineering and Technology, Hyderabad, Telangana, India,
darsangvs@yahoo.co.in

ABSTRACT

Secure communication for the information is very important role in digital era. There are several encryption techniques introduced to communicate the data from one location to the other. In digital communication, the images are encrypted using several techniques. In this paper, an encrypt scheme to encrypt bit map images is proposed using enhanced four stage encryption. Different analytic studies are performed on the images for finding the traces of the original image in the encrypted image. Comparative studies are performed on different encrypted images of the same image to trace back the original image. The results show that no patterns of the original image found in the encrypted image.
Keywords: *plain text, cipher text, bit map images, cipher images, four stage encryption.*

1. INTRODUCTION

Over the computer network images, videos and other multimedia data are shared among connected users almost every day. As the days are passing, the usage of internet and sharing the images over social networks is increasing exponentially. Provision of security to multimedia content is a major concern. Image security and encryption has become important area of research in the field of information security. Image encryption can be broadly classified into two types – encryption with compression and encryption without compression [1-14].

Over the years many image cryptographic algorithms have been proposed by the researchers [1-14]. Major interest of this paper is regarding a cryptographic technique associated with bit map images. Given a bit map image, the encrypted image is an unreadable (or cipher) a square image. Given a bit map image bmp image, the encrypted image is an unreadable (or cipher) image with a square image format. Decryption of an encrypted image with proper key should result in retrieval of original image.

2. RELATED WORK: FOUR STAGE ENCRYPTION

In the Four Stage Encryption System (FSE) [15], the input alphabet may be any set, a set of strings of some alphabet or any other symbols or simply the binary set {0, 1}. Unlike in other cryptosystems, the output alphabet in this system is different from input alphabet and generated at run time as strings of input alphabet A of size n. Let α be the plaintext string to be decrypted. Let $K = K_0\ K_1\ K_2$ be the three stage key, K_i is an element of A^+. The output alphabet Z is generated with the help of key K0. The output alphabet set Z is constructed as $Z = \cup a \in A\ aA^{index(K_o(index(a)))}$ and $m = |Z| = |A|(\sum a \in A$ index(K0(index(a)))), where $K_0(i)$ stands for the $(i \bmod |K0|)^{th}$ letter of K_0. The output alphabet is permuted using a permutation matrix M generated by another key K_1. Then with the key K_2 a sequence of 'n' numbers $m_1, m_2 \ldots m_n$, such that $m_1 + m_2 +, \ldots, + m_n = |Z| = m$. First m_1 elements of the permuted alphabet are taken as the set Z_1 , the next m_2 elements are taken as the set Z_2, and so on and finally the last m_n elements are taken as set Z_n giving rise to a partition $\{Z_1, Z_2, \ldots Z_n\}$ of Z. Each alphabet of the plain text α is encrypted into a word, the size of which also may vary with each occurrence.

Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

While decrypting the procedure of encryption is repeated up to partitioning the output alphabet. The plain text is taken as to be null string. Search for an output alphabet, which is a pre-string of the cipher text. The input alphabet corresponding to the block in which the above output alphabet is concatenated to the plain text. The output alphabet is deleted from the cipher text. The process is repeated until the cipher text is empty.

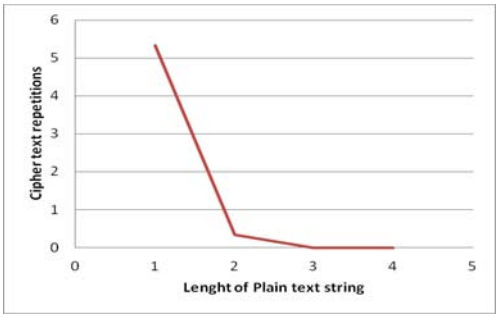

Fig. 2.1 Graph for maximum number of cipher text repetitions.

The FSE experimental results [16, 17, 18] are shown in the graph. The graph represents the Maximum number of cipher text repetitions among ten thousand executions with key "she went to uk" with different lengths one, two, three, and four. Clearly the plain text length of 3 or more the graph line fall down to zero, i.e. the number of cipher text repetitions is zero. The enhanced four stage encryption algorithm described in the paper[19].

3. IMAGE ENCRYPTION PROCESS

An image is also string of bits. Leaving the header part, the data part can be encrypted using Enhanced Four Stage Encryption [19]. To be more specific, let us consider a 24-bit bitmap image. The first 54 bytes consists of the header. Then onwards the data starts. We can consider bit-strings of some fixed length as the input alphabet. Keeping the memory constraints into consideration, we have taken the set of all nibbles (4 bit-strings) as the input alphabet, so that the size of the input alphabet is $2^4 = 16$. These alphabets, for the sake of study and analysis, are denoted by a, b, … , p. Now the key can be any string with these alphabets. Given an image, its data part is encrypted. The length of the cipher is much more than the length of the plain text. Depending on this size, the length and breadth are decided by rounding off the length appropriately. This size should include a provision to store the length and breadth of the original image. Further, if needed, the data may be padded with dummy bits. Accordingly the encrypted image is formed by appropriately organizing the header. A overview of process is given in Fig. 3.1 and Fig. 3.2. A detailed Algorithm is given in next section.

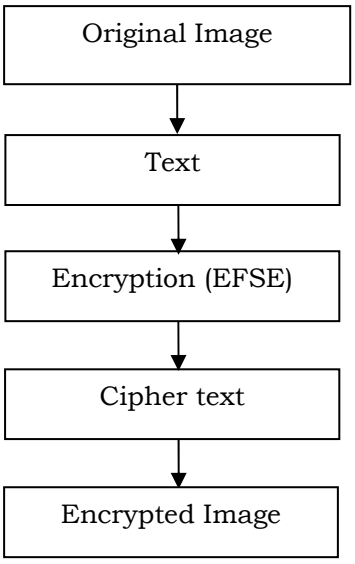

Fig. 3.1 Image Encryption Process

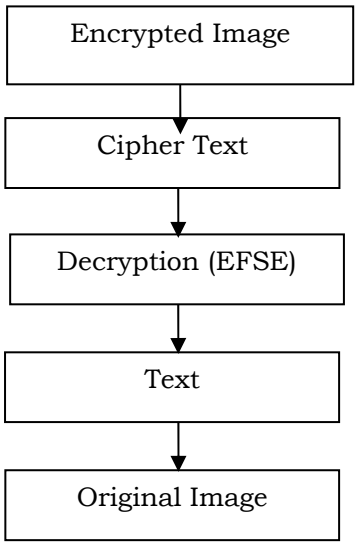

Fig. 3.2 Image Decryption Process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1 Image Encryption Algorithm

Let the image to be encrypted be plain.bmp, a 24-bit bitmap file, and let K = K_0 K_1 K_2 be the key framed with letters a to p.

Input: A bit map image as input.

Output: An encrypted image as output

Step 1: Open plain.bmp in read mode.

Step 2: Reach 18th byte. Read four bytes, which contain the width in the little-endian format. Let the width be ow. The next four bytes contain height. Let the height be oh.

Step 3: ow and oh contain 8 nibbles each, which are converted into characters a to p, are encrypted with the key K using Enhanced Four Stage Encryption and written to a new file crypt.txt.

Step 4: Reach 54th byte of plain.bmp, where the data starts. Read nibble by nibble and convert into characters - a to p. Encrypt each character with the key K using Enhanced Four Stage encryption and append it to ciphet.txt.

Step 5: Now let the size of the file (number of characters in the file) be n. Let k be the smallest positive integer such that k*k >= n.

Step 6: Create header of a bitmap file with width and height as k. Let this file be cipher.bmp.

Step 7: The data bytes are filled with the characters of cipher text each covered back to nibbles and appended to cipher.bmp.

Step 8: The file cipher.bmp is returned.

3. 2. Image Decryption Algorithm

Input: An encrypted image as input

Output: An original image or decrypted image as output.

Step 1: Open cipher.bmp in read mode.

Step 2: Reach 18th byte. Read four bytes, which contain the width in the little-endian format. Let the width be ow. The next four bytes contain height. Let the height be oh.

Step 3: ow and oh contain 8 nibbles each, which are converted into characters a to p, are decrypted with the key K using Enhanced Four Stage Encryption and written to a new file drcipher.txt.

Step 4: Reach 54th byte of cipher.bmp, where the data starts. Read nibble by nibble and convert into characters - a to p. Decrypt each character with the key K using Enhanced Four Stage Encryption and append it to drcipher.txt.

Step 5: Now let the size of the file (number of characters in the file) be n. Let k be the smallest positive integer such that k*k >= n.

Step 6: Create header of a bitmap file with width and height as k. Let this file be Plain.bmp.

Step 7: The data bytes are filled with the characters of drcipher text each covered back to nibbles and appended to Plain.bmp.

Step 8: The file palin.bmp is returned.

4. ANALYSIS

The image encryption algorithm is implemented and applied on images (Target, Alpha, Deer, Car, Lenna, and Tux) which are different sizes as shown in the figures 4.1(a) to 4.6(a). The encrypted images are as shown in the figures 4.1(b) to 4.6(b).

All the encrypted images are square shaped, in material whether the original image is a square or rectangle in shape. Hence the dimensions of the original image are beyond expectations. More ever the encrypted image is to large in size if the original image is rectangle no pattern can be traced out in the encrypted image because of the square nature of the encrypted image.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 4.1 (a)Original Image-Target (For visual purpose original image of size 9X9 is enlarged to 36X36)

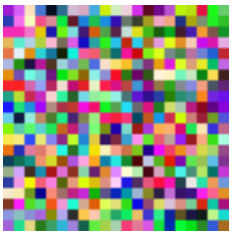

Fig 4.1 (b) Encrypted image-Target (For visual purpose encrypted image of size 21x21 isenlarge to 84x84)

Fig 4.2 (a) Original Image – Alph (For visual purpose original image of size 11X11 is enlarged to 44X44)

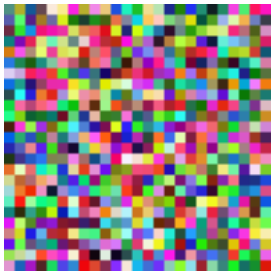

Fig 4.2 (b) Encrypted image-Alph (For visual purpose encrypted image of size 25x25 is enlarge to 100X100)

Fig 4.3 (a) Original Image – Deer (For visual purpose original image of size (18x24) is enlarged to (72x96)

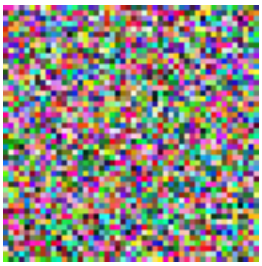

Fig 4.3 (b) Encrypted image-Deer (For visual purpose encrypted image of size 48X48 is enlarge to 96X96)

Fig 4.4 (a) Original Image – Car (For visual purpose original image of size (36x18) is enlarged to (72x36)

Fig 4.4 (b) Encrypted image-Car (For visual purpose encrypted image of size 58X58 is enlarge to 116X116

Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

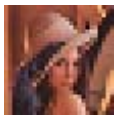

Fig. 4.5 (a) Original Image – Lenna (For visual purpose original image of size (27x27)is enlarged to (54x54)

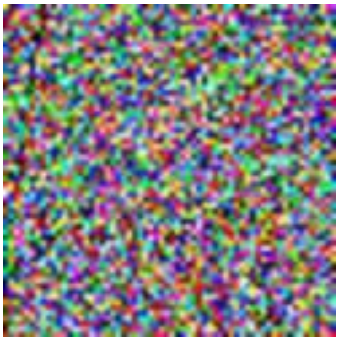

Fig 4.5 (b) Encrypted image-Lenna (For visual purpose encrypted image of size (62x62) is enlarge to (124x124)

Fig. 4.6(a) Original Image-Tux size (48x55)

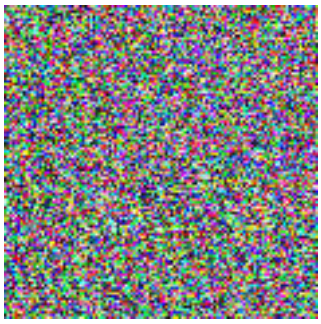

Fig. 4.6 (b) Encrypted Tux image size is (117x117)

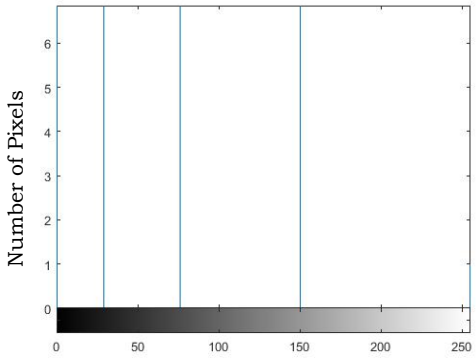

Fig. 4.7 (a) Histogram of Original Image: Target

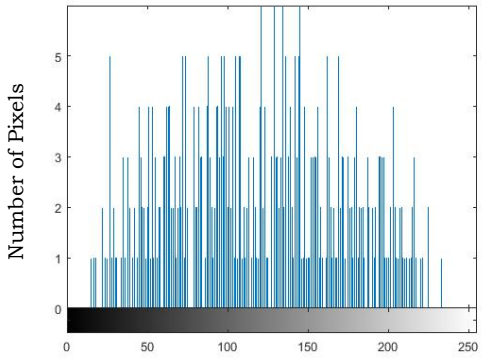

Fig. 4.7 (b) Histogram of Encrypted Image: Target

Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

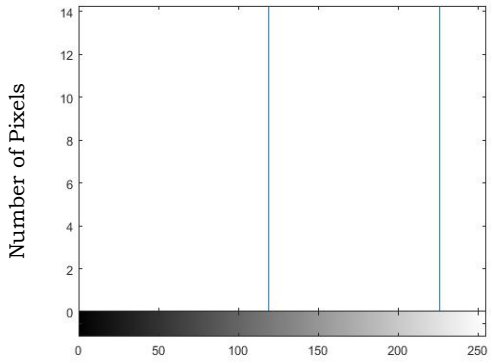

Fig. 4.8 (a) Histogram of Original Image: Alph

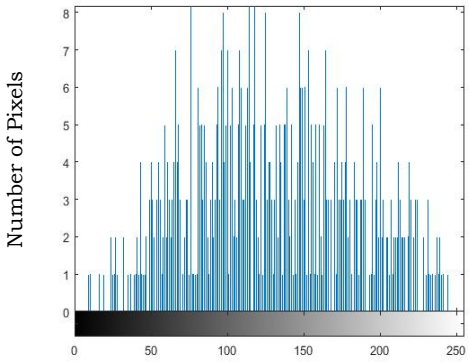

Fig. 4.8 (b) Histogram of Encrypted Image: Alph

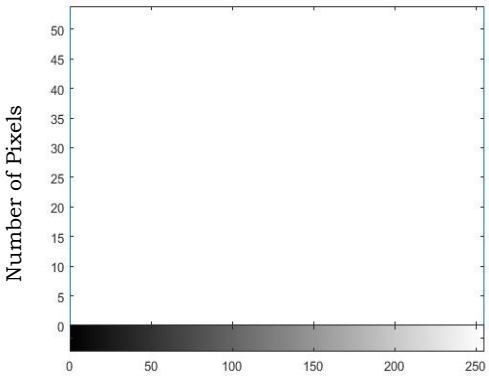

Fig. 4.9 (a) Histogram of Original Image: Deer

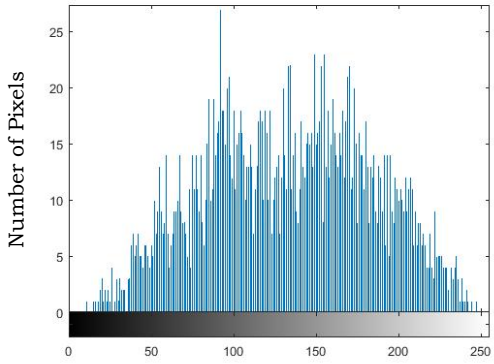

Fig. 4.9 (b) Histogram of Encrypted Image: Deer

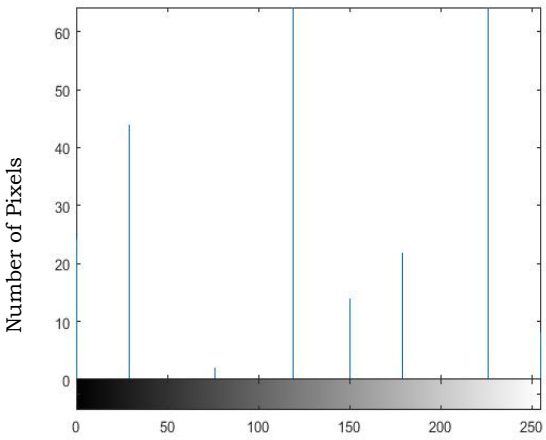

Fig. 4.10 (a) Histogram of Original Image: Car

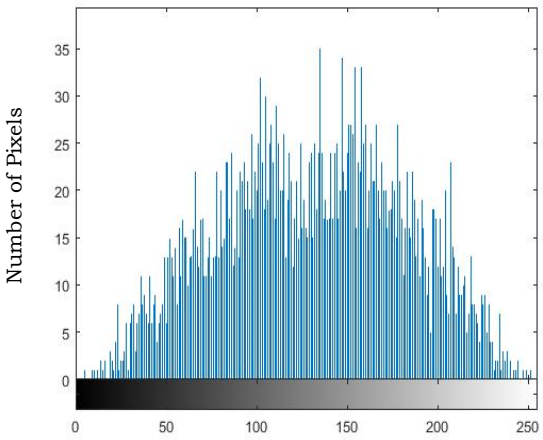

Fig. 4.10 (b) Histogram of Encrypted Image: Car

Journal of Theoretical and Applied Information Technology
15th December 2017. Vol.95. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

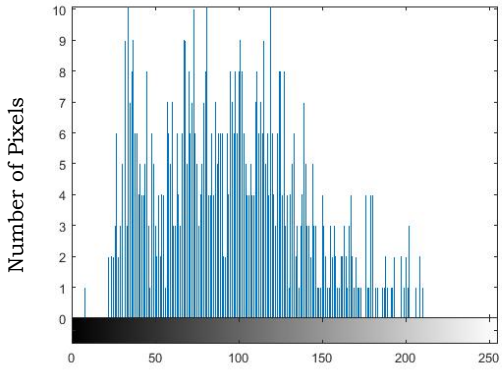

Fig. 4.11 (a) Histogram of Original Image: Lenna

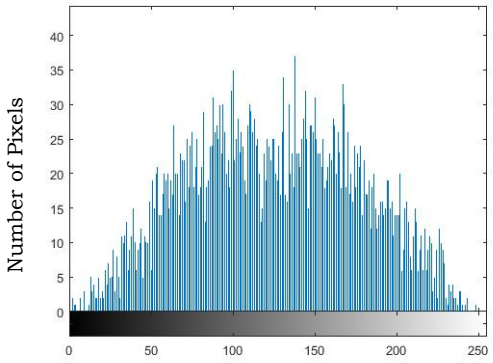

Fig. 4.12 (b) Histogram of Encrypted Image: Lenna

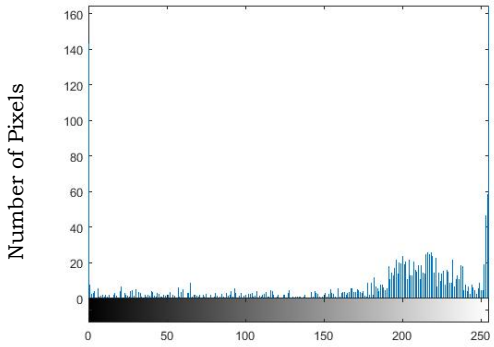

Fig. 4.12 (a) Histogram of Original Image: Tux

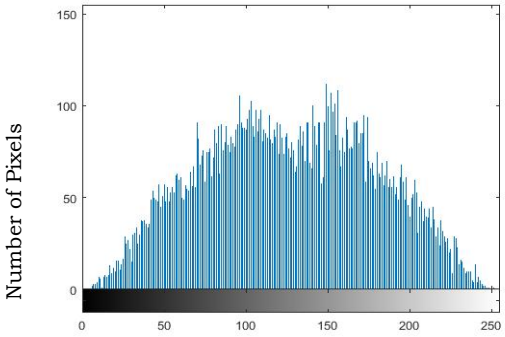

Fig.4.12 (b) Histogram of Encrypted Image: Tux

4.1 Histogram Analysis

The histogram is a distribution of RGB values in image. The intensity values are shown on the horizontal axis and pixel values are on the vertical axis. These original and encrypted images are converted in to gray scale. Histogram diagrams of original and encrypted images are shown in figures 4.7(a) to 4.12(a) and 4.7(b) to 4.12(b).

The distribution of pixels clearly shows that there is a variation of pixels in the original and encrypted images. Since the image "Deer" is a black and white image there are only two intensity values namely 0 and 255. Hence the histogram of deer we see only two bars on two extremes. But the encrypted image has several intensity values separated over entire range of 0 to 255. This can be shown by figures 4.9(a) and 4.9(b). The image Alpha also contains only two colors yellow and gray. Hence the histogram contains two bars. Whereas the encrypted image has several bars in the range of 0 to 255 as shown in figures.4.8 (a) and 4.8(b). Similar observations can be considered other figures too. Hence, the original and encrypted images are vast difference leaving no scope to guess the even a part of the original image from the encrypted one.

The encrypted image obtained by Enhanced four stage encryption process was subjected to several filters together with salt and pepper varying the values of parameters. We found that in none of the filters the traces of original image could be obtained. The image is encrypted with two different keys and various kinds of weighted image addition and differences are taken. None of these reveal the original image. These observations indicate the strength of the Enhanced Four Stage Encryption relative to several recent image encryptions. After applying the Speckle and Noise with a value of 0.05 and Salt and pepper with a value 0.10 on encrypted images of 4.1(b) to 4.6 (b) then the resultant filtered images are shown in the figures 4.13 to 4.24. Clearly no traces of original images are observed on the encrypted images.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig. 4.13 Spckle and Noise with a values 0.05 to the encrypted Alpha image

Fig. 4.14 Spckle and Noise with a values 0.05 to the encrypted Alpha image

Fig. 4.15 Spckle and Noise with a value 0.05 to the encrytped Deer image

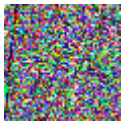

Fig. 4.16 Spckle and Noise of Car

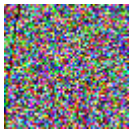

Fig. 4.17 Spckle and Noise of Lenna

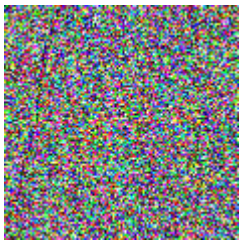

Fig. 4.18 Spckle and Noise of Tux

Fig. 4.19 Salt and pepper with a values 0.10 to the encrypted Alpha image

Fig. 4.20 Salt and pepper with a values 0.10 to the encrypted Alpha image

Fig. 4.21 Salt and pepper with a value 0.10 to the encrytped Deer image

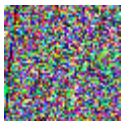

Fig. 4.22 Salt and pepper with a values 0.10 of Car

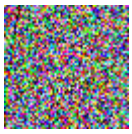

Fig. 4.23 Salt and pepper with a values 0.10 of Lenna

Fig. 4.24 Salt and pepper with a values 0.10 of Tux

4.2 Difference of two encrypted images with two keys

By applying the enhanced four stage encryption on images with one key and another key with a variation of single letter. The difference of two encrypted images and variation fo encrypted images reveal that two encrypted images have a lot of difference. This fact shown in figures 4.25(a-d) to 4.30(a-d) and the table 4.1.

Fig. 4.25 (a) Original image: Target

Fig .4.25 (b)) Encrypted Image -Target with the key K_0=appaji,K_1=hadapencil,K_2=inbookandbag

Fig 4.25.14 (c) Encrypted Image -Target with the key K_0=appaji,K_1=hadapencil,K_2=inbookandba

Fig 4.25 (d) Difference of encrypted images

Fig 4.26 (a) Original image: Alph

Fig 4.26 (b) Encrypted Image -Alph with the key K_0=appaji,K_1=hadapencil,K_2=inbookandbag

Fig 4.26 (c) Encrypted Image -Alph with the key K_0=appaji,K_1=hadapencil,K_2=inbookandba

Fig 4.26 (d) Difference of encrypted images

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig 4.27(a) Original image: Deer

Fig 4.27 (b) Encrypted Image -Deer with the key K_0=appaji,K_1=hadapencil,K_2=inbookandbag

Fig 4.27 (c) Encrypted Image -Deer with the key K_0=appaji,K_1=hadapencil,K_2=inbookandba

Fig 4.27 (d) Difference of encrypted images

Fig 4.28 (a) Original image: Car

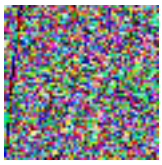

Fig 4.28 (b) Encrypted Image -Car with the key K_0=appaji,K_1=hadapencil,K_2=inbookandbag

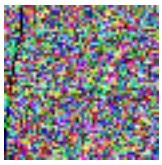

Fig 4.28 (c) Encrypted Image -Car with the key K_0=appaji,K_1=hadapencil,K_2=inbookandba

Fig 4.28 (d) Difference of encrypted images

Fig 4.29 (a) Original image: Lenna

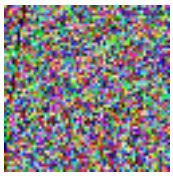

Fig 4.29 (b) Encrypted Image -Lenna with the key K_0=appaji,K_1=hadapencil,K_2=inbookandbag

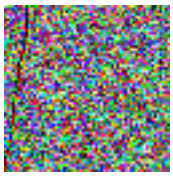

Fig 4.29 (c) Encrypted Image -Lenna with the key K_0=appaji,K_1=hadapencil,K_2=inbookandba

Fig 4.29 (d) Difference of encrypted image

Fig 4.30 (a) Original image: Tux

Fig 4.30 (b) Encrypted Image -Tux with the key K_0=appaji,K_1=hadapencil,K_2=inbookandbag

Fig 4.30 (c) Encrypted Image -Tux with the key K_0=appaji,K_1=hadapencil,K_2=inbookandba

Fig 4.30 (d) Difference of encrypted images

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4.1. Comparison of two encrypted images at Threshold value 20

Image Name	Total Number of Pixels(A)	Number of Pixels at Threshold Value 20(B)	Ratio= **B/A**	Standard devotion of difference of two encrypted images
Target	441	5	0.0113	30.1090
Alph	625	4	0.0064	31.8400
Deer	2304	4	0.0017	11.9424
Car	3364	6	0.0018	58.1678
Lenna	3844	1	2.6015e-04	15.4130
Tux	13689	7	5.1136e-04	11.4388

4.3 Difference of original image and decrypted images with a slight variation of Key

An original image is encrypted with a key encrypted image so obtained is decrypted with another key having a single letter variation. The decrypted images so obtained and the original images are considered. The difference is taken in order to know whether any phases of original image left out in the above decrypted image. This study is performed on all six images considered. The results are shown in figures 4.31(a-d) to 4.36(a-d)) and table 4.1 It is concluded that no traces of the original image is left in the encrypted and decrypted image.

Fig 4.31 (a) original image-Target

Fig 4.31 (b) Encrypted image-Target with the key K0=appaji,K1=hadapencil,K2=inbookandbag

Fig 4.31 (c) Decrypted image-Target with the key K0=appaji,K1=hadapencil,K2=inbookandba

Fig 4.31 (d) Difference of Orginala and decrypted image

Fig. 4.32 (a) original image-Alph

Fig 4.32 (b) Encrypted image-Alph with the key K0=appaji,K1=hadapencil,K2=inbookandbag

Fig. 4.32 (c) Decrypted image-Alph with the key K0=appaji,K1=hadapencil,K2=inbookandba

Fig. 4.32 (d) Difference of Orginala and decrypted image

Fig. 4.33 (a) original image-Targe

Fig 4.33 (b) Encrypted image-Deer with the key K0=appaji,K1=hadapencil,K2=inbookandbag

Fig. 4.33 (c) Decrypted image-Deer with the key K0=appaji,K1=hadapencil,K2=inbookandba

Fig. 4.33 (d) Difference of Orginala and decrypted image

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fig. 4.34 (a) original image-Car

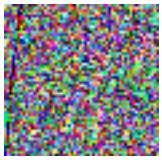

Fig. 4.34 (b) Encrypted image-Car with the key K0=appaji,K1=hadapencil,K2=inbookandbag

Fig. 4.34 (c) Decrypted image-Car with the key K0=appaji,K1=hadapencil,K2=inbookandba

Fig. 4.34 (d) Difference of Orginala and decrypted image

Fig. 4.35 (a) original image-Lenna

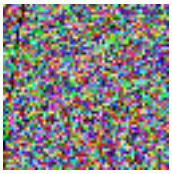

Fig. 4.35 (b) Encrypted image-Lenna with the key K0=appaji,K1=hadapencil,K2=inbookandbag

Fig. 4.35 c) Decrypted image-Lenna with the key K0=appaji,K1=hadapencil,K2=inbookandba

Fig. 4.35 (d) Difference of Orginala and decrypted image

Fig. 4.36 (a) original image-Tux

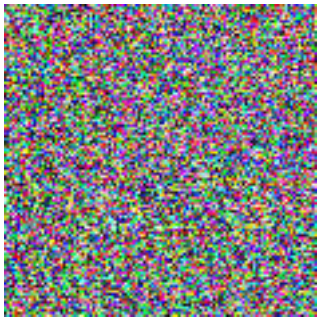

Fig. 4.36 (b) Encrypted image-Tux with the key K0=appaji,K1=hadapencil,K2=inbookandbag

Fig. 4.36 (c) Decrypted image-Tux with the key K0=appaji,K1=hadapencil,K2=inbookandba

Fig. 4.36 (d) Difference of Orginala and decrypted image

Table 4.2. Comparison of original and encrypted images at Threshold value 20

Image Name	Total Number of Pixels(A)	Number of Pixels at Threshold Value 20(B)	Ratio= **B/A**	Standard devotion of difference of two encrypted images
Target	81	0	0	11.0768
Alph	121	0	0	15.4506
Deer	432	48	0.1111	108.7028
Car	648	25	0.0386	73.0142
Lenna	729	81	0.1111	57.5006
Tux	2640	3	0.00113	11.1484

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

5. CONCLUSIONS

By above studies, one can realize that enhanced four stage encryption is strong enough and no patterns of original image are observed in the encrypted image. In this paper an image encryption algorithm is proposed using an enhanced four stage encryption. The image encryption algorithm encrypts the bitmap images with different keys. The images are encrypted and decrypted with a slight difference of one letter and the encrypted images differences are taken. The standard deviation has been noted between two encrypted images. It is observed that the two encrypted images are different. No similar patterns are observed in the encrypted images. The results show that no patterns of the original image found in the decrypted image.

REFERENCES

[1] G. M. Priya and P. V. Kumari. Compression of Quasi-Group Encrypted Grayscale Images. International Journal of Scientific and Research Publications, vol. 2, No. 7, pp. 1-4, July 2012.

[2] S. S. Kumar and H. Mangalam. Wavelet-based Image Compression of Quasi Encrypted Grayscale Images.International Journal of Computer Applications (0975 – 8887), vol. 45, No.12, pp. 35-39, May 2012.

[3] R. Ye. A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism.In Proc. Of Optics Communications, vol. 284, No. 22, pp. 5290-5298, Oct. 2011.

[4] S. Tedmori and N. Al-Najdawi. Lossless image cryptography algorithm based on discrete cosinee transform.The International Arab Journal of Information Technology, vol. 9, No. 5, pp. 471-478, September 2012.

[5] S. Al-Maadeed, A. Al-Ali and T. Abdalla. A New Chaos-Based Image-Encryption and Compression Algorithm. Journal of Electrical and Computer Engineering, vol. 2012, pp. 1-11, 2012.

[6] F. Ahmed,M. Y. Siyal and V. U. Abbas. A Perceptually Scalable and JPEG Compression Tolerant Image Encryption Scheme. In Proc. Of IEEE conference on Fourth Pacific-Rim Symposium on Image and Video Technology (PSIVT), pp. 232-238, Nov. 14-17, 2010.

[7] D. Luciano and Gordon Prichett. Cryptology: From Caesar Ciphers to Public-Key Cryptosystems. The College Mathematics Journal, vol. 18, No. 1, pp. 2-17, January 1987.

[8] G.P. Biswas. Diffie–Hellman technique: extended to multiple two-party keys and one multi-party key.Published in IET Information Security, vol. 2, No. 1, pp. 12– 18, 2008.

[9] R. Sharma. A Novel Approach to combine Public-key encryption with Symmetric-key encryption. The International Journal of Computer Science & Applications, Vol. 1, No. 4, pp. 8-15, June 2012.

[10] Prabha, D. Lakshmi. "An efficient chaos-based chaotic maps using block encryption ciphers method.", International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue6- June 2013.

[11] Ganeshkumar, K., D. Arivazhagan, and S. Sundaram. "Advance Cryptography Algorithm for Symmetric Image Encryption and Decryption Scheme for Improving Data Security." Journal of Academia and Industrial Research (JAIR)2.10 (2014): 563.

[12] Khaled Loukhaoukha, Jean-Yves Chouinard, and Abdellah Berdai, "A Secure Image Encryption Algorithm Based on Rubik's Cube Principle", Journal of Electrical and Computer Engineering Volume 2012.

[13] https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

[14] Sivaranjani, K. , Mended algorithm for image encryption based on random shuffling technique,2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp.1-4,2013.

[15] Gomatam V S Acharyulu, Sangapu V Appaji, " Four Stage Encryption," International Journal of Research in Computer and Communication Technology, Vol. 1, Issue 4, pp. 129-132, Sep. 2012.

[16] Gomatam V S Acharyulu, Sangapu V Appaji, "Analysis of Four Stage Encryption," International Journal of Research in Computer and Communication Technology, Vol. 1, Issue 6, Nov. 2012, pp. 338-339.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[17] Sangapu Venkata Appaji, Dr.Gomatam V S Acharyulu, " A Study Of four Stage Encryption: Experimental Results." **2014** IEEE International Conference on Computational Intelligence and Computing Research (**ICCIC**), Park Engineering College, Coimbatore, Dec, 18-20, 2014.

[18] Sangapu Venkata Appaji, Dr.Gomatam V S Achrayulu, "Four Stage Encryption Generalizations: Partitioned output Crypto System," International Journal of Computer Applications (0975 – 8887),Volume 108 – No 17, December 2014, pp:26-23.

[19] Sangapu Venkata Appaji, Dr. Gomatam V S Acharyulu "Enhanced Four Stage Encrytption", International Journal of Control Theory and Applications", Vol.10, Number 11, 2017.