ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Emerging Trends in Engineering and Technology (NCETET'16)

Lourdes Matha College of Science & Technology, Thiruvananthapuram

Vol. 3, Special Issue 3, August 2016

# Highly Secure E-T-C system via Adaptive Histogram Shifting

**Remya G R[1], Smitha J C[2]**

Student, Dept of CSE, Lourdes Matha college of Science and Technology, Trivandrum, India[1]

Assistant Professor, Dept of CSE, Lourdes Matha college of Science and Technology, Trivandrum, India[2]

**Abstract:** Here propose an efficient encryption then compression (ETC) system. The method composed of Encryption, Data hiding, Compression, Data extraction, Decompression and decryption. Encryption is done via prediction error clustering and random permutation. An adaptive histogram shifting (AHS) is used for data hiding. Wavelet compression is used to efficiently compress the encrypted image. An efficient histogram shifting method that modifies the pixel greyscale value within the range is proposed to embed data into the image and it provides good quality of marked images. Data hiding refers to hide data within a digital media. Media can be anything like audio, image and video. Hiding is done by modifying the contents of the digital media. Hiding process is done in such a way that modification of pixel values should be undetectable to the viewers. However, in various applications like military and medical applications, degradation of the over media is not allowed. So it is essential to introduce the data hiding in such a way that it is reversible and quality degradation after embedding is lowered.

**Keywords:** ETC, AHS, Data hiding, Data extraction.

## I. INTRODUCTION

In an application scenario, Sender wants to efficiently and securely transmit an image to receiver via an untrusted channel. In traditional Compression then Encryption (CTE) system shown in Fig. 1, first compress the original image and then encrypt it.

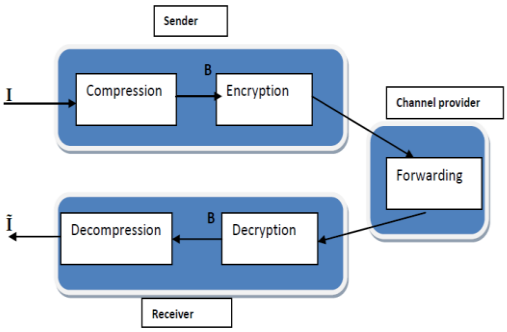


Fig.1. Compression-then-Encryption (CTE)

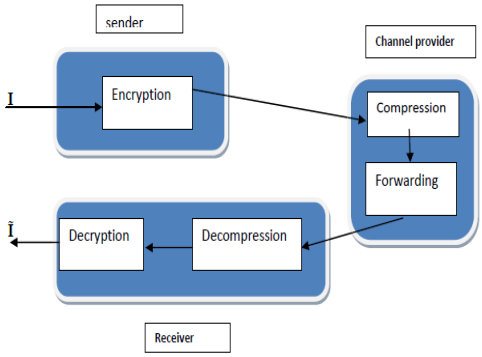


Fig. 2. Encryption-then-Compression (ETC)

But the sender has no incentive to compress the data, and hence, will not use its limited computational resources to run a compression algorithm before encrypting the data. This is especially true when sender uses a resource-deprived mobile device. In contrast, the channel provider has an overriding interest in compressing all the network traffic so as to maximize the network utilization [1]. So introduce a new method - ETC (Encryption then Compression) shown in Fig.2.

## II. LITERATURE REVIEW

Johnson et. al showed that the stream cipher encrypted data is compressible through the use of coding with side information principles, without compromising either the compression efficiency or the information-theoretic security. In addition to the theoretical findings, also proposed practical algorithms to losslessly compress the encrypted binary images [3]. Here describe the distributed source-coding problem and provide the principles behind code constructions for both lossless compression and compression with a fidelity criterion.

These code constructions will be used subsequently to construct systems which implement the compression of encrypted data. Distributed source coding considers the problem of compressing sources and that are correlated, but cannot communicate with each other. An important special case of this problem, upon which we will focus, is when needs to be sent to a decoder which has access to the correlated side-information. Schonberg et. Al later investigated the problem of compressing encrypted images

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Emerging Trends in Engineering and Technology (NCETET'16)
Lourdes Matha College of Science & Technology, Thiruvananthapuram
Vol. 3, Special Issue 3, August 2016

when the underlying source statistics is unknown and the sources have memory. By applying LDPC codes in various bit-planes and exploiting the inter/intra correlation [4]. This technique describes how to decode images using a model designed to capture the underlying 2-D structure of images. The result is more efficient compression of encrypted images and implements a practical scheme, based on LDPC (Low Density Parity Check) codes (for compressing encrypted images). Also describe how to apply this scheme to binary images. Here present a practical encoder and decoder for compressing encrypted images. Begin by assuming that full knowledge of the source statistics (p, h0, h1, v0, v1) is available to both encoder and decoder. Compress the encrypted source using a sparse linear transformation implemented with a matrix multiplication. The design of the transform matrix is based on LDPC codes. The decoder operates by running belief propagation over the factor graph. Thus proceed by describing the appropriate factor graph. The graphical model consists of three components connected together; the models for the source, the encryption, and the code.

Klinc and C. Hazay describe compression of data encrypted with block ciphers, such as the Advanced Encryption Standard [5]. As opposed to stream ciphers, such as the one-time pad, block ciphers are highly nonlinear and the correlation between the key and the cipher text is, by design, hard to characterize. If a block cipher operates on each block of data individually, two identical inputs will produce two identical outputs. While this weakness does not necessarily enable an unauthorized user to decipher an individual block. It can reveal valuable information; for example, about frequently occurring data patterns. To solve this problem, various chaining modes, also called modes of operation, are used with block ciphers. The idea is to randomize each plaintext block by using a randomization vector derived from previous encrypted inputs or outputs. This randomization prevents identical plaintext blocks from being encrypted into identical cipher text blocks. Here focus on the cipher block chaining (CBC) mode. The CBC mode is interesting because it is the most common mode of operation used with block ciphers. The CBC mode is interesting because it is the most common mode of operation used with block ciphers.

X. Zhang proposes a novel scheme for lossy compression of an encrypted image with flexible compression ratio [6]. A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original image, the better the quality of the reconstructed image. Jiantao Zhou describes that in many practical scenarios, image encryption has to be conducted prior to image compression. This has led to the problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be efficiently performed. In this paper, we design a highly efficient image encryption-then-compression (ETC) system, where both lossless and lossy compressions are considered [1]. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. Also demonstrate that an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images. More notably, the proposed compression approach applied to encrypted images is only slightly worse, in terms of compression efficiency, than the state-of-the-art lossless/lossy image coders, which take original, unencrypted images as inputs. In contrast, most of the existing ETC solutions induce significant penalty on the compression efficiency. The advantages and disadvantages of existing methods are shown in TABLE I.

TABLE I COMPARISON OF EXISTING METHOD

| Method | Advantages | Disadvantages |
|---|---|---|
| Lossy Compression And Iterative Reconstruction | Better Compression Efficiency | Complex Method |
| Distributed source coding problem | Simple | Less Efficient |
| Compression Of Data Encrypted With Block Ciphers | Better Compression Efficiency | Fundamental Compression |
| Compression Of Encrypted Images | Simple | Less Compression Gain is available |

## III.PROPOSED SYSTEM

Here present the details of the key components in proposed ETC system, namely, image encryption conducted by Sender, data hiding done by sender, image compression conducted by channel provider, and the data extraction, sequential decryption and decompression conducted by Receiver.

### A. ENCRYPTION

Here image encryption done via prediction error domain. Read the input image and resize into 255 × 255 format. Then an image predictor (GAP)[1] applied to each pixel in the image. The result of the GAP is a gradient image. Then find the prediction error (original image – GAP image).

For each pixel, the error energy estimator is defined by

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Emerging Trends in Engineering and Technology (NCETET'16)
Lourdes Matha College of Science & Technology, Thiruvananthapuram
Vol. 3, Special Issue 3, August 2016

$$\Delta_{i,j} = d_h + d_v + 2|e_{i-1,j}| \quad (1)$$

Where,

$$\begin{aligned} d_h &= |I_{i-1,j} - I_{i-2,j}| + |I_{i,j-1} - I_{i-1,j-1}| \\ &\quad + |I_{i,j-1} - I_{i+1,j-1}| \\ d_v &= |I_{i-1,j} - I_{i-1,j-1}| + |I_{i,j-1} - I_{i,j-2}| \\ &\quad + |I_{i+1,j-1} - I_{i+1,j-2}| \end{aligned} \quad (2)$$

Instead of treating the whole error image, divide the prediction errors into L clusters (K- means clustering). Heuristically find that L = 16 is an appropriate choice.The algorithmic procedure of performing the image encryption is then given as follows:

**Step 1:** Compute all the prediction errors of the whole image I.
**Step 2**: Divide all the prediction errors into L clusters.
**Step 3**: Perform two key-driven cyclical shift operations to each resulting prediction error block. Which is shown in Fig. 3.
**Step 4:** Apply random permutation.
**Step 5**: The assembler concatenates all the permuted clusters and generates the encrypted image.
**Step 6:** A message is hide in the encrypted image via Adaptive Histogram Shifting.

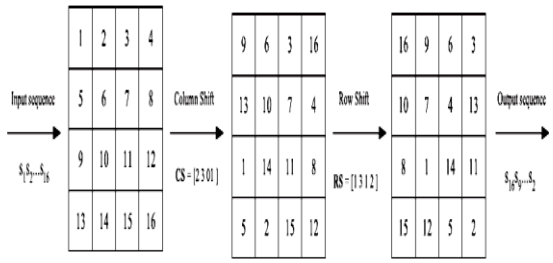


Fig. 3 Cyclical shift

B. HISTOGRAM SHIFTING

Histogram shifting is a data hiding method, its advantage is that the data embedded is large, visibility is good, the peak signal to noise ratio is high.

Histogram shifting algorithm[7] computes the histogram h(x). Then, a sequence of steps is performed as follows:[8]
**Step 1:** Generate the histogram h(x), x ϵ [0,255], of the host image I. Find the maximum and the minimum point pair (m1, z1) in the histogram as defined in (6).

$$\begin{cases} m_1 = \underset{x}{\operatorname{argmax}}\, h(x) \\ z_1 = \underset{x}{\operatorname{argmax}}\, h(x) \end{cases} \quad (3)$$

The maximum point $m_1$corresponds to the grey level that occurs most frequently in the host image I, and the minimum point $z_1$ might be the grey level which no or minimum number of pixels render within the image.
**Step 2:** Traverse the host image and for each pixel I(x, y) do the following modifying operation according to its gray level:

$$I'(x,y) = \begin{cases} I(x,y) + 1, & m_1 < I(x,y) < z_1 \\ I(x,y) + s_i, & I(x,y) = m_1 \\ I(x,y), & \text{otherwise} \end{cases} \quad (4)$$

C. COMPRESSION

Compression done for reducing size of image for flexible image transfer[2]. Wavelet compression is used here and is shown in Fig. 4. Wavelets are mathematical functions that cut up data into different frequency components.

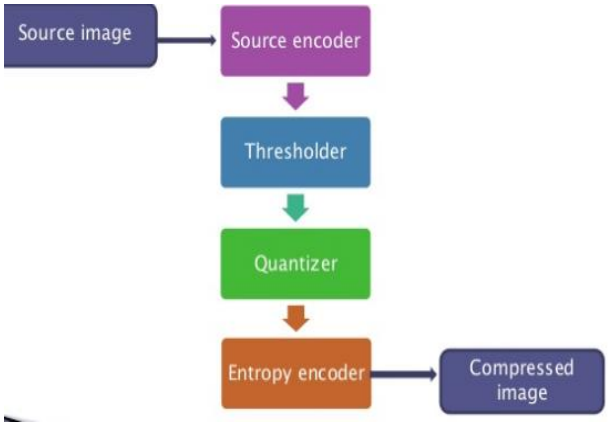


Fig. 4 Wavelet compression

D. DATA HIDING IN RECONSTRUCTION

The data extraction process needs the information of maximum and minimum points to make exact host image recovery and secret data extraction, the ($m_1$, $z_1$) pair is recorded or sent along with the marked image I' to the intended receiver. Upon receiving the marked image I', the extraction process performs the steps below to extract the secret message <$s_i$> is and the host image I.

**Step 1:** Traverse each pixels I'(x, y) in the received image and extract the secret data <$s_i$> using (5).

$$s_i = \begin{cases} 0 & I'(x,y) = m_1 \\ 1 & I'(x,y) = z_1 \end{cases} \quad (5)$$

**Step 2:** Examine all the marked pixels once again to transform them into their original gray levels in according with the following operation:

$$(x,y) = \begin{cases} I'^{(x,y)} - 1, & m_1 < I'(x,y) < z_1 \\ I'(x,y), & \text{otherwise} \end{cases} \quad (6)$$

The hiding capacity c of the algorithm can provide is equal to the frequency count of the maximum point in the input image, which can be expressed as

$$c = \max_{0 \le x \le 255} h(x) \quad (7)$$

Fig. 5 shows the architectural design of the system.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Emerging Trends in Engineering and Technology (NCETET'16)
Lourdes Matha College of Science & Technology, Thiruvananthapuram
Vol. 3, Special Issue 3, August 2016

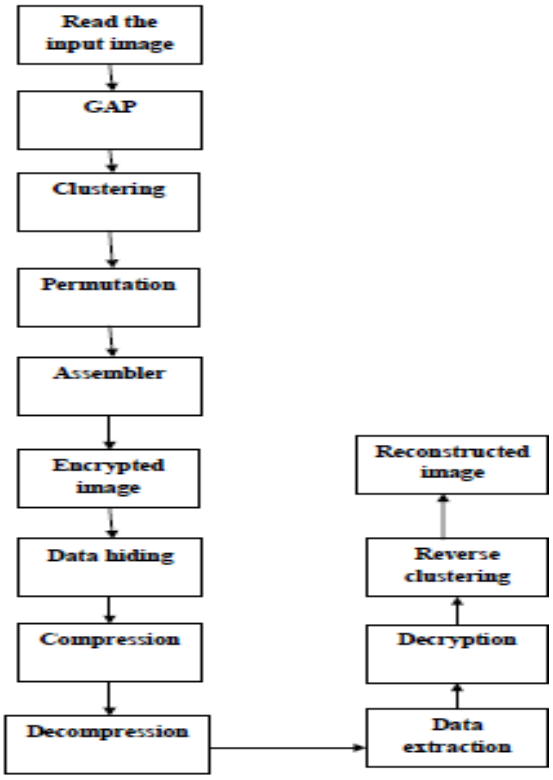


Fig. 6 Architectural design of the system

## IV. EXPERIMENTAL OBSERVATIONS

Experiments were carried out using a gray scale image to gauge the performance of the new system. In all cases, the new system outperformed the existing system in terms of quality as well as time taken to process the output image. Results of one such experiment is shown in the following figures:

Firstly, let's select an image as input to the proposed system. The input is shown in Fig 7.


Original image

In the first phase, GAP is applied to the input image and to get a GAP image which is shown in Fig. 8.

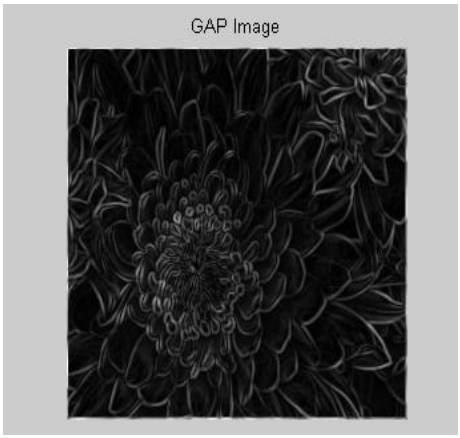


Fig .8 GAP image

In the next phase, find the error image and it is shown in figure Fig. 9.

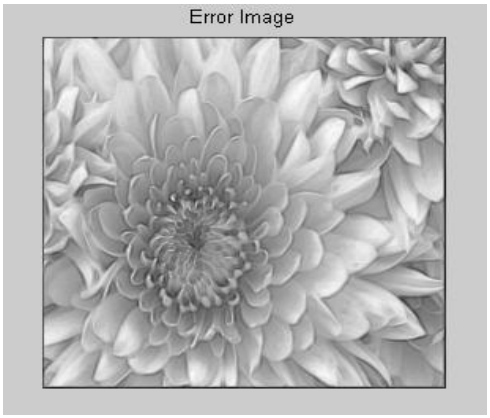


Fig 9 Error image

Clustering is applied to error image and it is shown in Fig. 10.

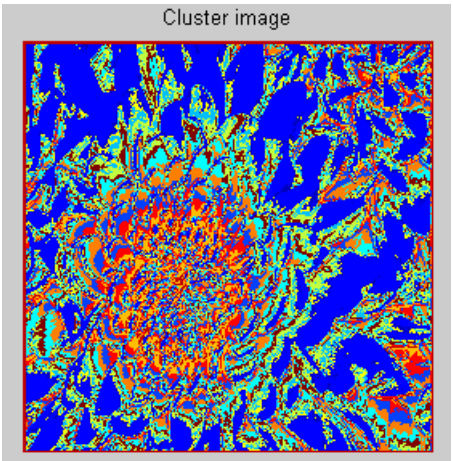


Fig. 10 Cluster image

In next phase cyclical shift is applied and we get encrypted image. Then a message is hiding in the encrypted image using histogram shifting. Resultant image is shown in Fig. 11.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Emerging Trends in Engineering and Technology (NCETET'16)

Lourdes Matha College of Science & Technology, Thiruvananthapuram

Vol. 3, Special Issue 3, August 2016

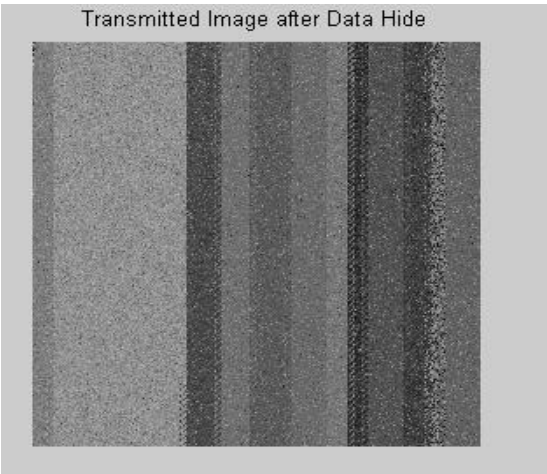


Fig. 11 Encrypted image with data hiding

At the receiver side hided data is extracted from the encrypted image. Then apply reverse clustering and it is shown in Fig. 12.

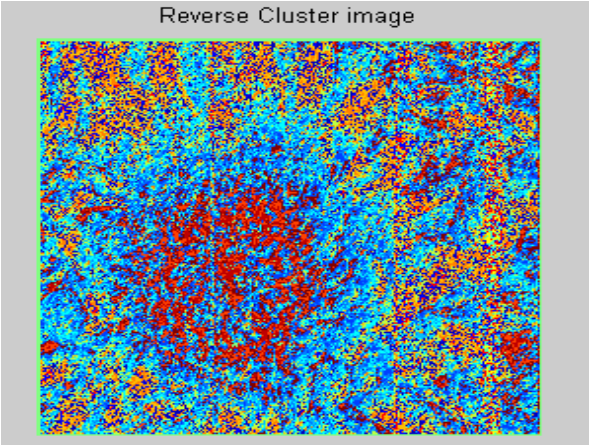


Fig. 12 Reverse cluster image

Finally we get the original reconstructed image and is shown in Fig. 13.


Fig. 13 Reconstructed image

Eight images shown in Fig. 14 are used as the test set. In Fig. 15, x-axis represents the image and y-axis represents PSNR values existing and our proposed system.

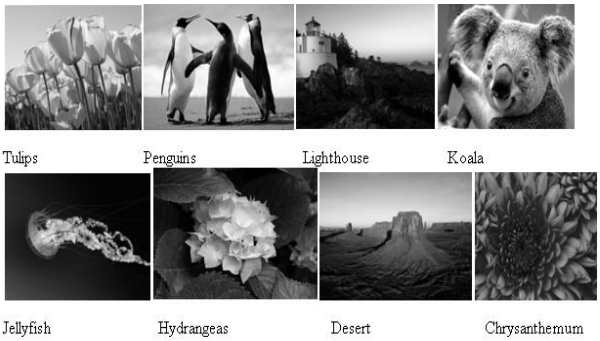


Fig.14. Picture Analysis

TABLE III PSNR COMPARISON OF EXISTING METHOD

| Name Of Image | PSNR | Bits Per Pixel(BPP) | SSIM |
|---|---|---|---|
| Chrysanthemum | 47.1683 | 6.5837 | 0.99 |
| Desert | 40.4910 | 7.3627 | 0.95 |
| Hydrangeas | 36.4508 | 6.8162 | 0.94 |
| Jellyfish | 38.8755 | 5.8184 | 0.92 |
| Koala | 38.1489 | 7.4449 | 0.96 |
| Lighthouse | 35.9753 | 7.0548 | 0.91 |
| Penguins | 38.8152 | 7.9053 | 0.94 |
| Tulips | 46.2214 | 10.2147 | 0.97 |

TABLE IIIII
PSNR COMPARISON OF PROPOSED METHOD

| Name Of Image | PSNR | Bits Per Pixel (BPP) |
|---|---|---|
| Chrysanthemum | 42.9257 | 9.0289 |
| Desert | 35.9149 | 10.0577 |
| Hydrangeas | 34.0539 | 9.2808 |
| Jellyfish | 35.3412 | 7.6354 |
| Koala | 36.6473 | 10.4690 |
| Lighthouse | 33.0940 | 9.8285 |
| Penguins | 34.0145 | 11.0143 |
| Tulips | 42.2214 | 10.2147 |

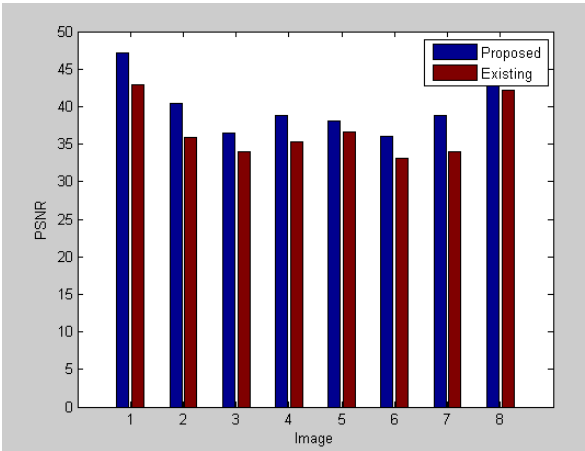


Fig. 15 Comparison of PSNR values

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Emerging Trends in Engineering and Technology (NCETET'16)

Lourdes Matha College of Science & Technology, Thiruvananthapuram

Vol. 3, Special Issue 3, August 2016

## V. CONCLUSION

In this paper, designed an efficient image Encryption and data hiding system. Within the proposed framework, the image encryption has been achieved via prediction error clustering and random permutation. Also, a lossless data hiding method based on histogram was proposed. The proposed histogram shifting method that modifies the pixel greyscale value within the range is proposed to embed data into the image and it provides good quality of marked images. Experimental results demonstrated that proposed scheme out performs other existing schemes.

## REFERENCES

[1] Jiantao Zhou," Designing an Efficient Image Encryption-Then-Compression system via Prediction Error Clustering and Random Permutation",in IEEE Transactions On Information Forensics And Security, Vol. 9, No. 1, January 2014.

[2] http://whatis.techtarget.com/definition/image-compression

[3] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[4] D. Schonberg, S. C. Draper, and K. Ramchandran, "On compression of encrypted images," in Proc. IEEE Int. Conf. Image Process., Oct. 2006, pp. 269–272.

[5] D. Klinc, C. Hazay, A. Jagmohan, H. Krawczyk, and T. Rabin, "On compression of data encrypted with block ciphers," IEEE Trans. Inf. Theory, vol. 58, no. 11, pp. 6989–7001, Nov. 2012.

[6] X. Zhang, "Lossy compression and iterative recobstruction for encrypted image," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 53–58, Mar. 2011.

[7] Lincy Rachel Mathews1 , Arathy C. Haran V. 2 ," Histogram Shifting Based Reversible Data Hiding", in International Journal of Engineering Trends and Technology (IJETT) – Volume 10 Number 10 - Apr 2014.

[8] Athira Ravi1 , Kavitha N Nair2," high capacity histogram shifting based reversible data hiding with data compression", in International Conference on Emerging Trends in Engineering and Management (ICETEM14) 30 – 31, December 2014, Ernakulam, India.