International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.2, 2015

RESEARCH ARTICLE

ISSN: 2321-7758

DEVELOPING AN IMAGE ENCRYPTION-THEN-COMPRESSION SYSTEM

RUTUJA GARDI[1], RASIKA INAMDAR[2], POOJADEVI GHODAKE[3], SUWARNA GODAGE[4]

[1,2,3,4]Students of VPCOE

Article Received: 12/04/2015 | Article Revised on:17/04/2015 | Article Accepted on:20/04/2015

ABSTRACT

In this approach, image encryption is conducted before image compression. The problem may arise how to design a pair of image encryption and compression algorithm, by which compressing the encrypted images can be done efficiently.

Here, a highly efficient image encryption-then-compression (ETC) system is defined, in which both lossless and lossy compression are considered. The given image encryption scheme operated in the prediction error domain which is shown to be able to provide a reasonably high level of security. [1]

In this method, an arithmetic coding-based approach is exploited to efficiently compress the encrypted images. But the proposed compression approach applied to encrypted images is somewhat bad in terms of compression efficiency when compare with the state-of-the-art lossless/lossy image coders in which original, unencrypted images are taken as inputs.

KEY WORD-Compression of encrypted image, encrypted domain signal processing.

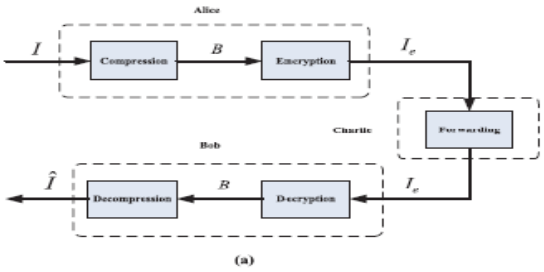
INTRODUCTION

This system explains the complete functionality designed and developed for image encryption then compression. With the proposed approach, a pair of image encryption and compression algorithms are designed such that compressing the encrypted image can still be efficiently performed. This system reveals the image encryption scheme can be operated in the prediction error domain which is able to provide a reasonably high level of security. This system is not only enhancing the high problem generated in case of compression of encrypted images. It is not intended to use this system to maximize the bandwidth while transmission, rather secured image level of security but also a greater compression performance which would be the major problem generated in case of compression of encrypted images. Transmissions retained.[1]

1. Traditional Approach

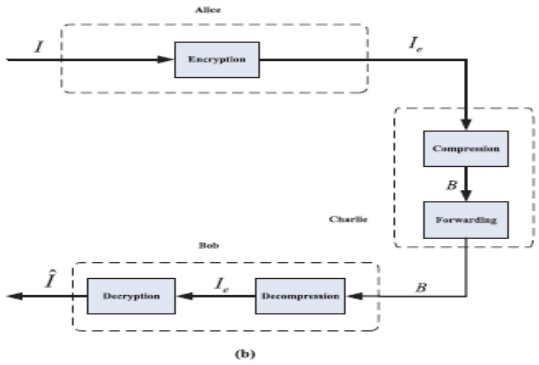
The traditional approach of transmitting redundant data over a

Bandwidth constrained insecure channel is to first compress it and then encrypt which leads the security issues.[1]



2. ETC Approach

This Method investigates reversing the order of compression and encryption, without compompromising either the compression efficiency or the information security.[1]



Guidelines For Manuscript Preparation

Abbreviations and Acronyms

ETC – encryption then compression,

CTE – compression then encryption

GAP – gradient adjusted predictor

MED - median edge detector

AC - arithmetic coding

De-AC – arithmetic decoding

De-P – de-permutation

Related work

- **Lossless Compression of Encrypted grey level and color images[5]**

The paper was proposed on the concept of the feasibility of lossless compression of encrypted images.

- **Arithmetic coding for Data Compression[6]**

Arithmetic coding removes redundancy in the encoding of data which is an effective mechanism. The advantage of arithmetic coding for data compression are its optimality and its inherent separation of coding .

- **Performance Study on Image Encryption Schemes[8]**

In this paper, we classify various image encryption schemes and analyze them with respect to various parameters like tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security.

- **Secure Compression: Theory & Practice**

Generally, encryption and compression being used together. For analyzing both systems there has not been a formal framework and usually the system contains compression followed by encryption process. Paper explains entropy-restricted semantic security. Paper present a new, efficient cipher, called the squeeze cipher, that combines compression and encryption into a single primitive and provably achieves our entropy-restricted security.

- **Image Encryption Using Block-Based Transformation Algorithm[7]**

In this paper, a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm is introduced. In this Blowfish algorithm is used, in which original image was divided into blocks, which rearranged into transformed image using an algorithm called transformation algorithm. After that, using the Blowfish algorithm transformed image was encrypted.

MATH

Equations[1]

1. Calculation of Prediction Errors :

$e_{ij}=I_{ij}\tilde{}\ I_{ij}$

where,

I_{ij}=Pixel

I_{ij}=Prediction

2. Calculation of Error Energy Estimator :

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

Where;

$d_h = |I_{i-1,j} - I_{i-2,j}| + |I_{i,j-1} - I_{i-1,j-1}| + |I_{i,j-1} - I_{i+1,j-1}|$

$d_v = |I_{i-1,j} - I_{i-1,j-1}| + |I_{i,j-1} - I_{i,j-2}| + |I_{i+1,j-1} - I_{i+1,j-2}|$

3. Conditional Entropy measurement :

$\Sigma_{0<l<L-1} H(\tilde{e}|q_i <= \Delta < q_{i+1}) P(q_i <= \Delta < q_{i+1})$

where,

$H(\tilde{e}|q_i <= \Delta < q_{i+1})$ is the entropy of prediction error sequence.

Set Theory

1. $I = \{I_1, I_2, I_3, \ldots I_n\}$

where,

I_i = Image

2. $I=f(x,y)$

Where,

x = Horizontal spatial co-ordinate

y = Vertical spatial Co-ordinate

3. $G = \{0,1,2...255\}$

Where,

G = Gray level Intensity

4. $e_{ij}=\{e_{00},e_{01}, \ldots e_{n,k}\}$

Where

$e_{i,j}$ = set of prediction error

5. $C = \{C_0,C_1,C_2,\ldots C_k\}$

Where,

C = SetofClustering Index

6. $\Delta_{i,j}=\{\Delta_{i+1,j}, \Delta_{i,j+1} \ldots \Delta_{i-n,j-n}, \Delta_{i+n,j+n}$

Where,

$\Delta_{i,j}$=Set of Error energy estimator

ETC SYSTEM

- **Encryption :**

1. This step includes actual encryption of the image.

2. Firstly, image is given as input to the GAP. From which predictions of the are obtained.[2]

3. Each predictions are sequentially mapped and mapped prediction error is obtained.[2]

4. These prediction errors are divided into clusters and permutation operation is applied to each cluster

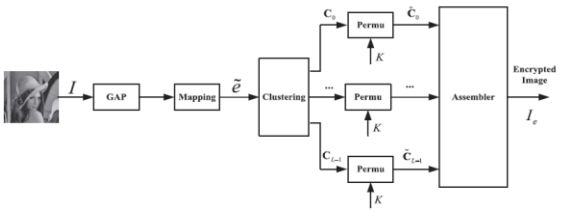


Fig. Encryption Process [1]

5.Two key-driven cyclical shift operation performed for prediction error , and data is arranged by Raster-scan order.

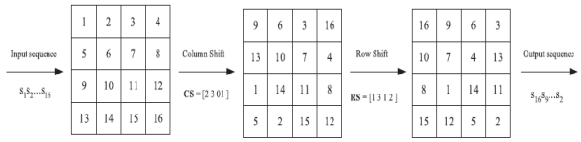


Fig. Cyclic shift[1]

6. Then cluster index is obtained. It is applied to the assembler, which concatenates the clusters and the encrypted image is obtained.

- **Compression :**

1. This step includes compression of the encrypted image.

2. Encrypted image is the input for the compression method.

3. That encrypted bit streams are employed to the [1]. De-assembler which divides the image into cluster index.

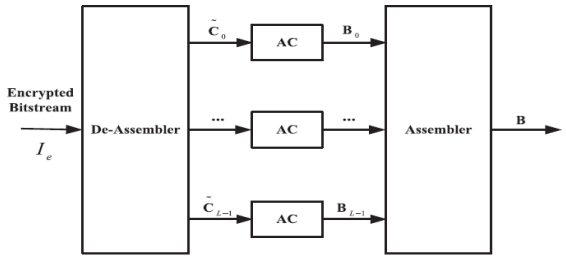


Fig. Compression Process [1]

4. Then arithmetic coding method is applied to cluster index which gives compressed and encrypted bit streams.

5. It is again applied to the assembler which concatenates and gives encrypted compressed image.

- **Decryption and Decompression :**

1. This step includes decryption and decompression of the encrypted and compressed image.[1]

2. Encrypted compressed image is employed to the De-assembler whichdivides the image into bit streams.

3. Arithmetic decoding method is applied to bit streams which gives decompressed cluster index.

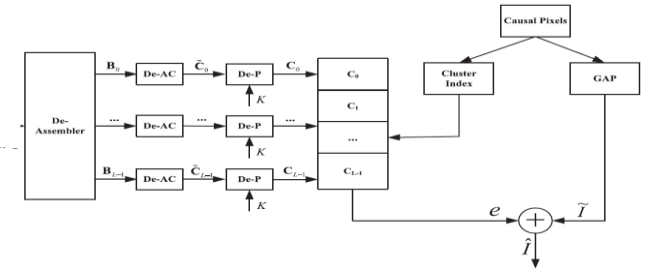


Fig. Decryption and Decompression Process [1]

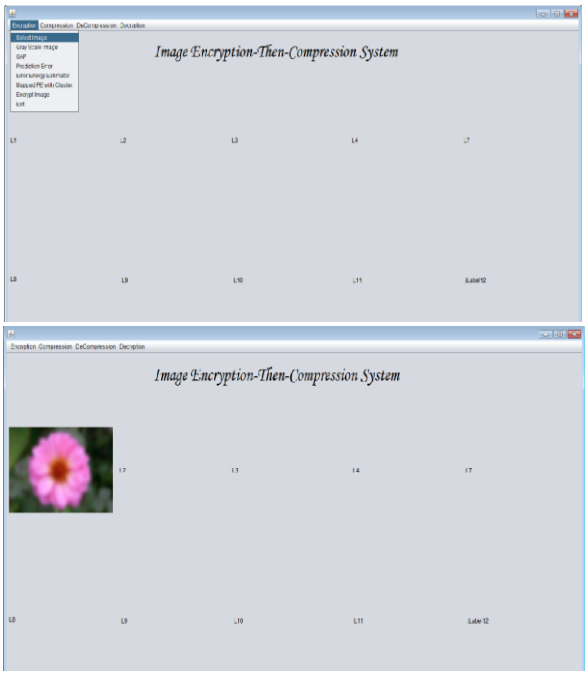
4.Then permutation operation is applied with the key and decrypted clusters are obtained.

5. They are employed to the assembler which gives decrypted and decompressed image, which is the required output.

RESULT WINDOWS

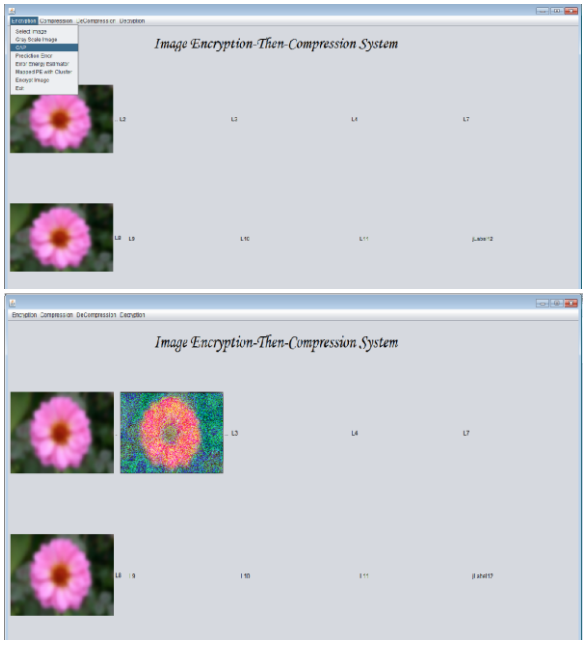
- Encryption Process

1. Selection of image :

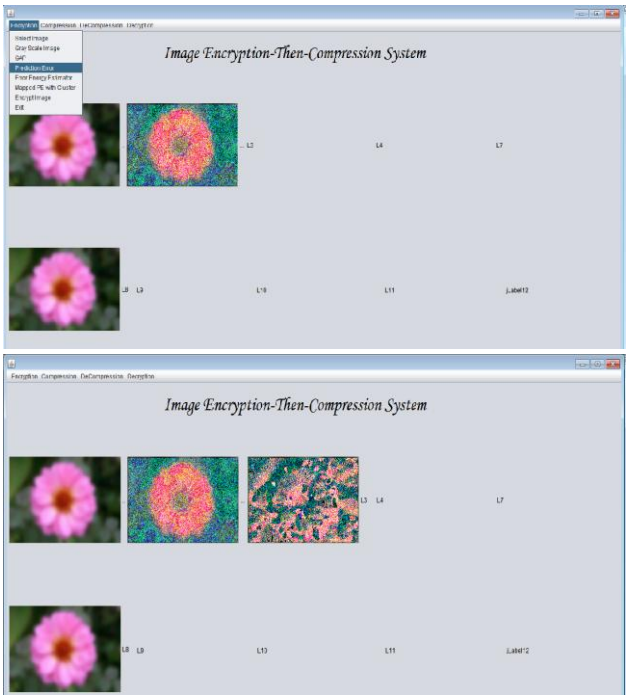


2. Convert it into Grey Scale Image :

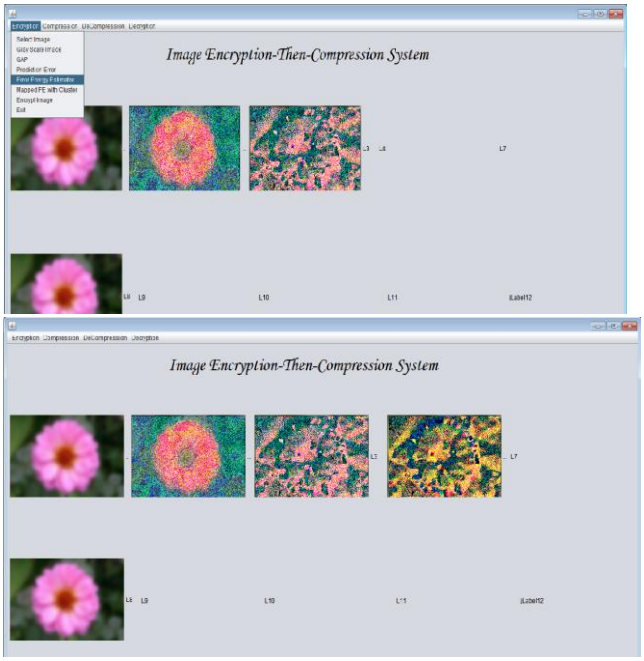
3. Apply GAP Method :



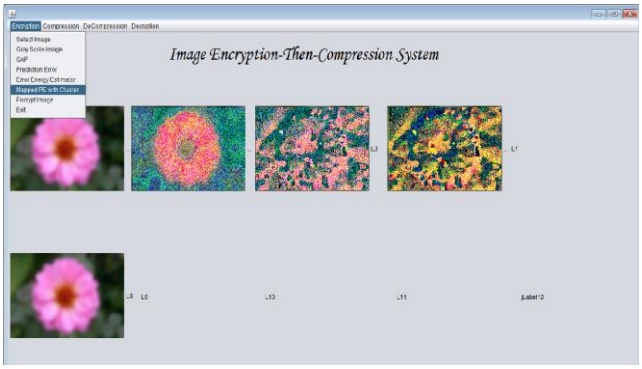
4. Calculate Prediction Error :



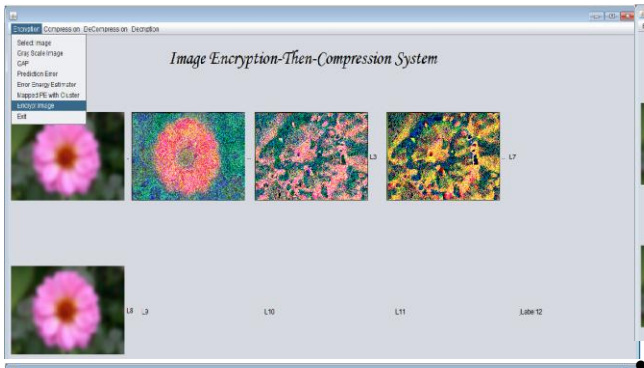
5. Calculate Error energy estimator :

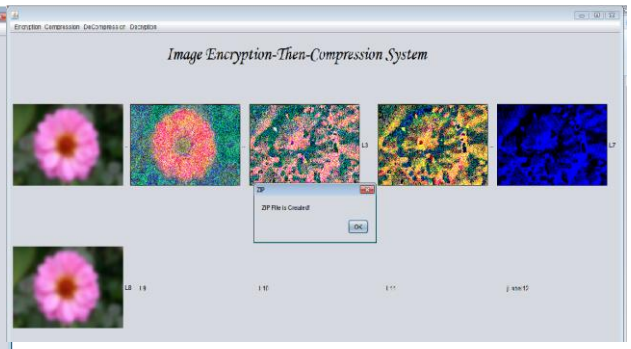


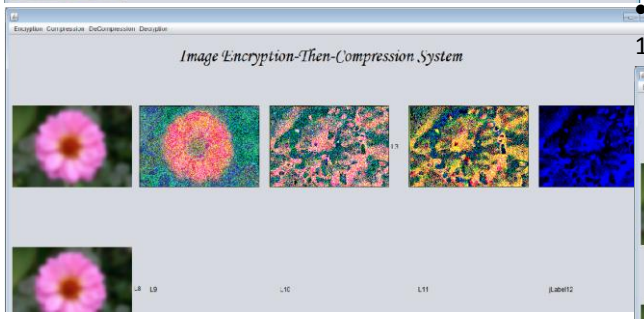
6. Map Prediction error with clusters :



7. Encrypt the image :

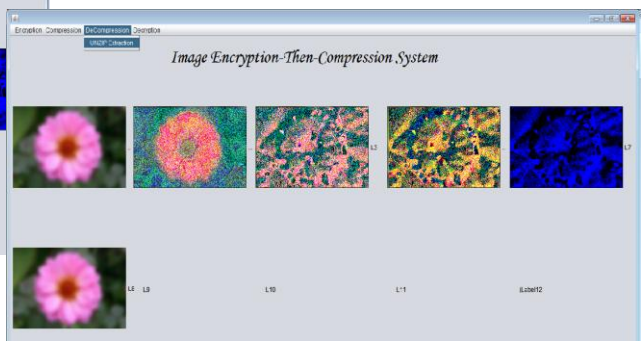






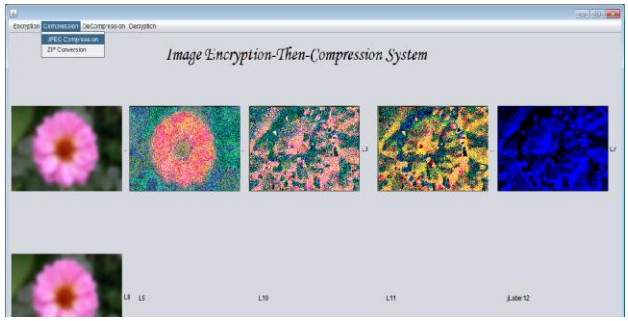
- Decompression

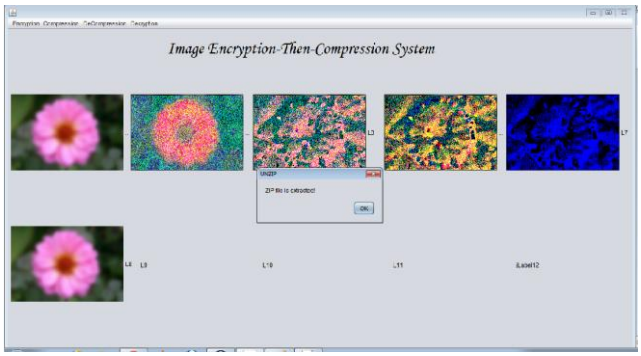
1. UnZIP Extraction :

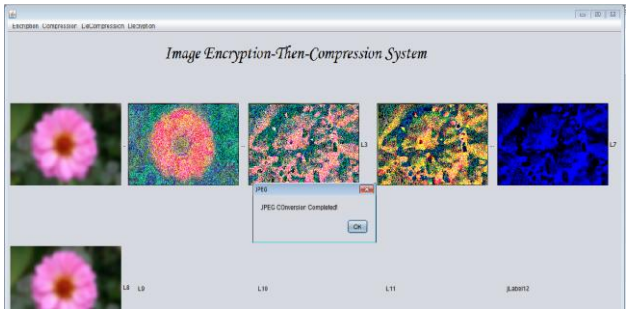


- Compression Process

1. JPEG conversion :

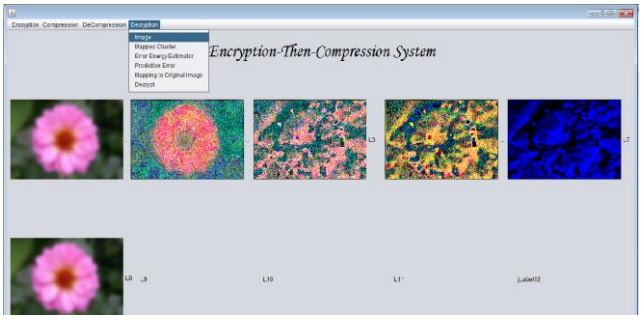




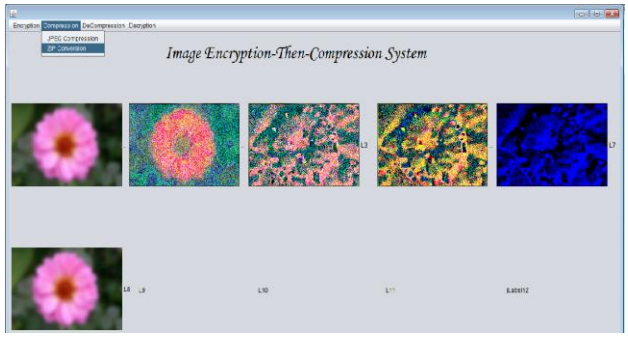


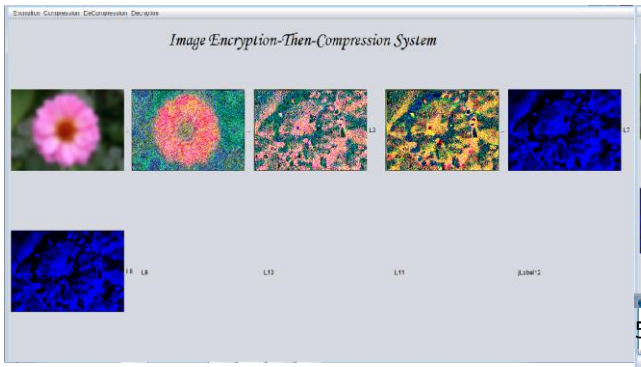
- Decryption

1. It selects the Input image as Encrypted Compressed Image :

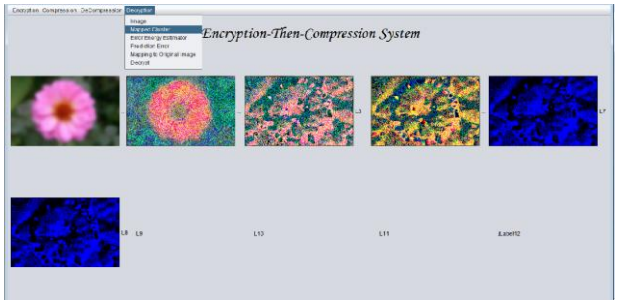


2. ZIP conversion :

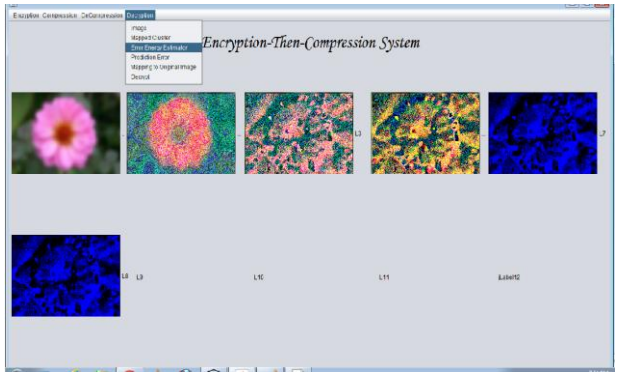


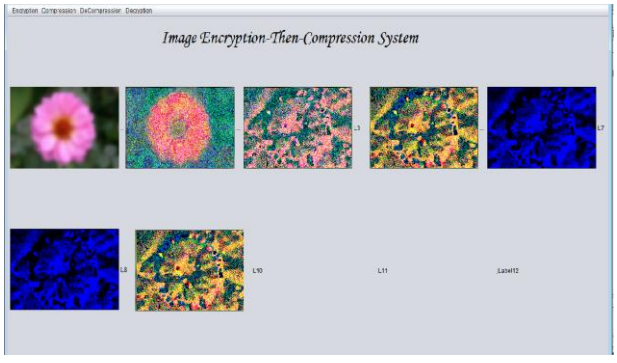


2. Map Prediction error with clusters :

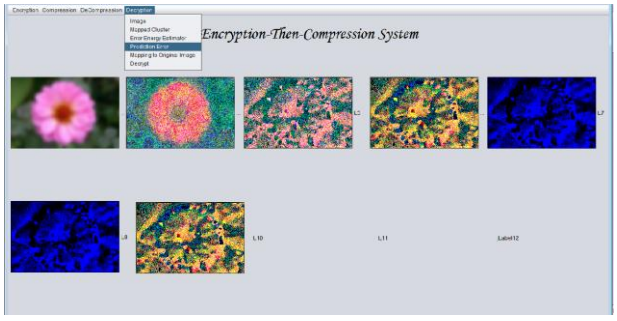


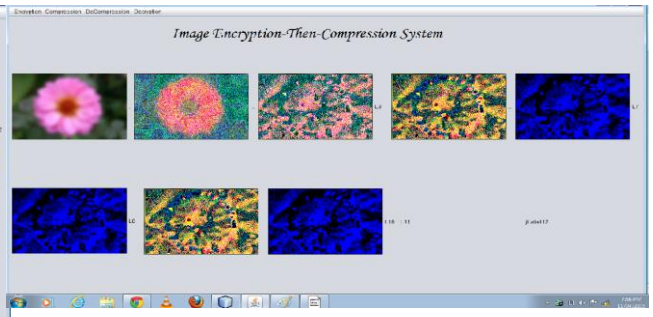
3. Map with Error energy estimator :



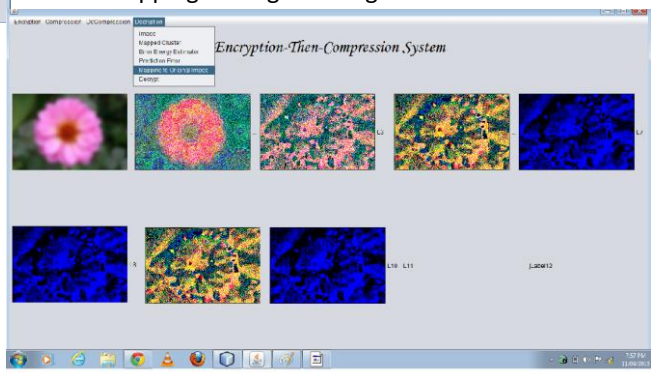


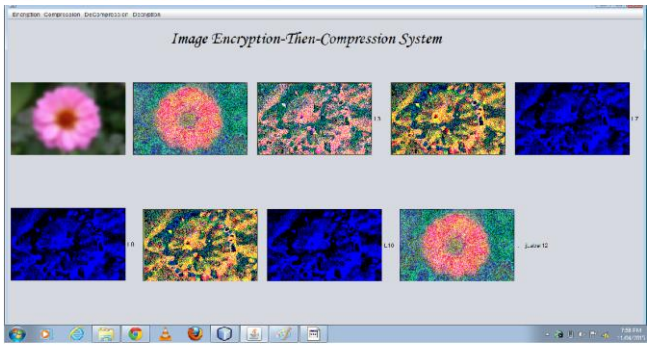
4. Get Prediction Errors :=



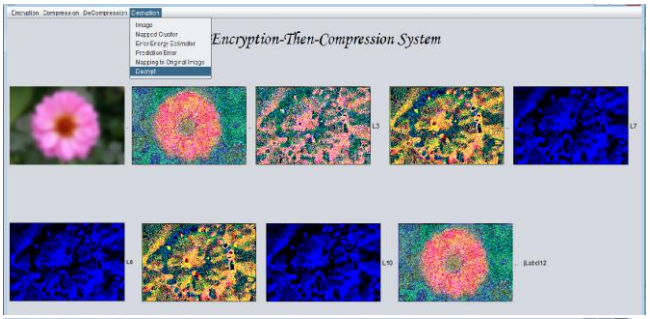


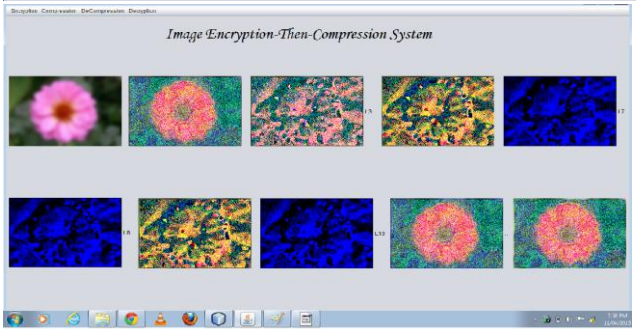
5. Mapping to Original Image :

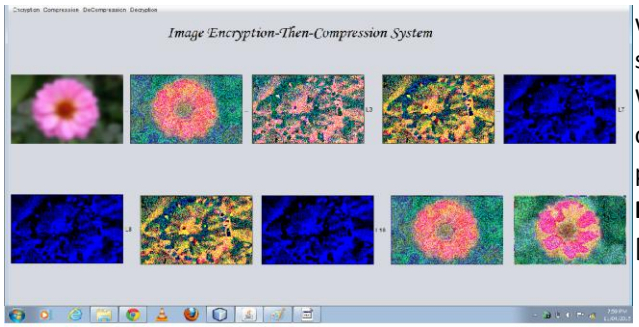


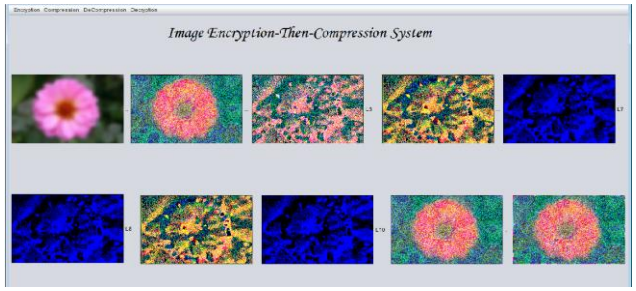


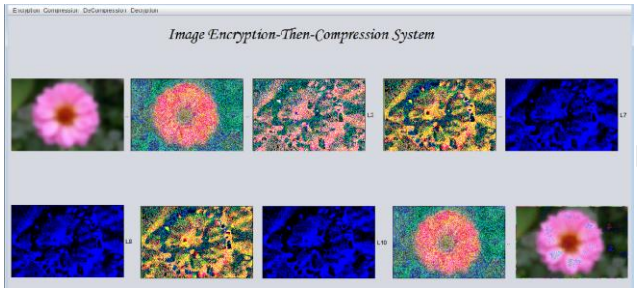
6. Decrypt the Image :











CONCLUSION

This paper gives the idea about an efficient image Encryption-then-Compression (i.e. ETC)system. Through Prediction error clustering and random permutation produces the image encryption within the given framework. A context-adaptive arithmetic coding approach is used to realize highly efficient compression of the encrypted data.

And it has proved that the high level of security has been retained. Important is what, the coding efficiency of proposed compression method on encrypted images is similar to that of the method state of-the-art lossless/lossy image codes in which inputs is received an original, unencrypted images.

ACKNOWLEDGMENT

We take this opportunity to express our sincere thanks to guide Prof. S. A. Shinde and co-guide Prof.R .V. Panchal for their guidance, support, encouragement and advice. We are thankful to our Head of the Department Prof. G. J. Chhajed for their unwavering moral support and motivation during the entire course of the . College and technicians for their help in making this project a successful. We would also like to express our deep gratitude support and motivation during the entire course.

We would like to thank all the staff members of our college and technicians for their help in making this project a successful one.

REFERENCES

[1] Jiantao Zhou, Member, IEEE, Xianming Liu, Member, IEEE, Oscar C. Au, Fellow, IEEE, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation".

[2] X. Wu and N. Memon, "Context-based, adaptive, lossless image codec,"*IEEE Trans. Commun.*, vol. 45, no. 4, pp. 437–444, Apr. 1997.

[3] M. J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," *IEEE Trans. Imag. Process.*, vol. 9, no. 8, pp. 1309–1324, Aug. 2000

[4] 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

[5] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in *Proc. 16th Eur. Signal Process. Conf.*,Aug. 2008, pp. 1–5.

[6] PAUL G. HOWARD and JEFFREY SCOTT VITTER, FELLOW, IEEE "Arithmetic coding for data compression".

[7] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm".

[8] Jolly Shah and Dr.Vikas Saxena, JIIT, July 2011," Performance Study on Image Encryption Schemes".