International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# Hueristic Approch for Image Encryption and then Compression by Tree Pattern Approach

**Devashri Anil Vyawahare[1], Anil Gujar[2]**

[1]Computer Department, TSSM'S BSCOER Narhe, Pune, India

[2]Professor, Computer Department, TSSM'S BSCOER Narhe, Pune, India

**Abstract:** ***Most of the times while any message is transferring across the network for security reasons they are normally encrypted directly to make user visibly unreadable or it will be encrypted (hidden) in an image. And now a day's data hacker becomes too intelligent to break the encrypted images to get the original contents. So many systems are designed to combine the encryption and compression in single mould to provide greater security. So we are presenting a novel approach of encryption by maintaining run time LSB (least significant bit) using image decomposition method. This actually enhances the encryption processes by converting image into small blocks of hierarchical cluster of the LSB's. These blocks can be holding the user's message in many different patterns which is actually highly difficult to predict by the hackers. And then all individual blocks can be put in a tree to compress in the same hierarchy of decomposition. Numbers of techniques are proposed to do so. Image encryption is one of them; it provides a high level security to the image. Larger images are difficult to process hence image compression can be done after encryption process. Proposed approach designs the image encryption and then compression (ETC) which is suitable for both lossy and loss less images. Also the proposed scheme is operated on the prediction error domain. An arithmetic code based approach is used for the compression of the image because it performs well than any others.***

**Keywords:** Encryption, Compression, normalization, byte tree.

## 1. Introduction

With the advanced development in multimedia and network technologies the chances of threats in security of multimedia applications increases. So when the multimedia data is transmitting over the network, threat of being attacked or data loss is also increasing. Hence a more efficient and reliable security mechanism is necessary to preserve the privacy of such data. Thus encryption technologies are emerged as one of the best method to accomplish the task. Encryption plays a very important role in maintaining the security of such data. There are lots of applications such as government and private businesses, military area, hospitality services, in such area huge information is need to be transferred over the network. Often this information is stored on electronic computers and then it transferred over the network. Image encryption techniques are widely classifieds in three categories.

- position permutation based algorithm
- value transformation based algorithm
- visual transformation based algorithm

While the cryptography comes with two categories.

- Secret key cryptography
- Public key cryptography

Secret key cryptography is also called as symmetric key cryptography while public key cryptography is known as asymmetric key cryptography.

In order to reduce the size of the image before sending it over the network or to other destination image compression techniques are used. Image compression techniques reduce the size to the great extent so that resources are used to the minimum ratio. Normally in case of image three data redundancies are presents that increase the image size unnecessarily.

- Coding Redundancy
- Interpixel Redundancy
- Psychovisual Redundancy

In image compression techniques number of bits required to presents the image are reduced by taking these redundancies into the scenario. A care is to be taken while compressing the image as resolution of the image should not get reduced. Mainly there are two image compression techniques

1. Lossless image compression.
2. Lossy image compression.

The name of these techniques itself revealed the concept of the techniques.

**1. Lossy image compression techniques**

In this scheme the reconstructed image is not 100% identical to the original image as it induce some sort of loss while compressing image. In spite of inducing the loss, this scheme is beneficial in most of the applications where less accuracy with the more security is required. Figure 1 elaborates the diagram of Lossy image encryption technique. Here prediction, transformation and decompression steps are can be done without introducing any loss, but the next step quantization induces great loss in the method.

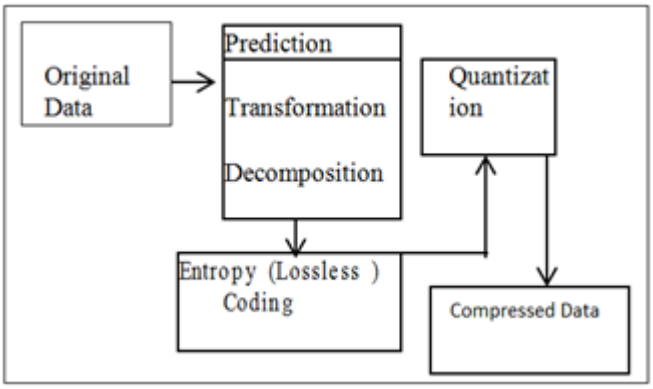



**Figure 1:** Lossy image encryption technique.

Lossy image compression techniques include the following techniques.
1. Transformation coding
2. Vector quantization
3. Fractal coding
4. Block Truncation Coding
5. Sub band coding

**2. Lossless image compression technique.**

In this technique complete information of original image can be easily reconstructed after compression. This method is also known as noiseless compression as it does not introduce any noise while accomplishing the task. This type schemes are widely used in applications like medical.
Lossless image compression techniques include the following techniques.
1. Run length encoding
2. Huffman encoding
3. LZW coding
4. Area coding

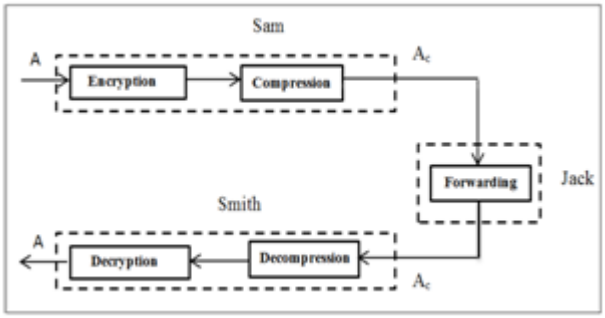



**Figure 2:** Encryption-then-Compression (ETC) system.

Figure 2 illustrates the working of image Encryption and then compression techniques which are much better than the traditional compression and then encryption method as the later one provide more secure and lossless way for image security.
The rest of the paper is organized as follows. Section 2 discusses some related work and section 3 presents the design of our approach. The details of the results and some discussions we have conducted on this approach are presented in section 4 as Results and Discussions. Sections 5 provide hints of some extension of our approach as future work and conclusion.

## 2. Literature Survey

This section represents all the related works of technologies used in our project

[1] Presents a good survey on different encryption techniques. Here author makes use of 25 different study papers to represent the things more clearly. All the given papers are form 1999 to 2012. In advanced author states that these all papers are dealing with the correlation between the pixels of the image. The less the correlation among the pixels the more will be the efficiency of encryption.

The main motto of authors behind this comparison is to differentiate the methods accurately so that the core part of individual method will get exposed. In [2] authors did another survey on different cryptography techniques where difference between different cryptographic approaches is properly differentiated with the help of existing encryption techniques.

3] Explains study on selection of best algorithm for the purpose of image encryption. Now a days chaos based image encryption gaining a lots of attention as these encryption algorithms gives better result when security is at first position. Here authors represent a deep survey on two famous image encryption algorithms i.e. Rubik's cube principle based secure image encryption algorithm and chaos based Fast image encryption algorithm which uses NPCR (Number of pixel change rate), UACI, entropy and correlation coefficient. So after studying these two techniques author conclude that second image encryption technique has higher edge over first technique.

[4] States a PCA based image compression approach. To do this task the process is divided into two steps i.e. PCA Statistical Approach & PCA Neural Network Approach. PCA (Principle component analysis) techniques are basically used to reduce the complexity of dataset. So we can say that PCA used as a data reduction technique.

As PCA is able to extract the information from the complex datasets, it has been applied in number of application from neuroscience to computer graphics. In PCA classical approach Eigen values are used to find Eigen vector between the complex datasets. Here covariance matrix is used as supporting techniques. In PCA neural network approach things are accomplished by finding the interconnection between the different computational elements. So finally author concludes that PCA can be used as a best method for the image compression with the two different alternatives.

[5] Presents a survey on different image lossless encryption techniques. An experimental evaluation is done on the different techniques by using 25 different publically available datasets. In this paper compression efficiency of different techniques are calculated so that it can be easy to conclude the best lossless compression technique. So author finally came to conclusion that the best compression efficiency can be achieved by using CALC.

[6] In this study author combines the different existing image compression techniques to develop the new one. The

work is carried in two steps. In the first step well known algorithm Lempel-Ziv-Welch (LZW) is applied on the input image. The output of the first step is applied to the second step where BCH algorithm is used. BCH acronym as Bose, Chaudhuri and Hoc- quenghem (BCH) error correction and detected algorithm. The second step is continues until inflation is detected. Because of the combining nature of the algorithm it gives a great efficiency if it compared with the traditional image compression methodology.

[7] States the new approach for efficient image compression to improve the system performance linear prediction, A fastest prediction error algorithm and corrected Golomb-Rice code is used by the author. Because of all these used methodology it speeds up the compression operation. Authors conclude that the algorithm is best suit for the big images, noisy images and for those images having high depth.

[8] Presents a novel approach for the image encryption and compression which makes use of biometric characteristics such as fingerprints. A nondestructive spectral fusion is carried out preserve the originality and security of the image. Here author used a popular transformation technique called Discrete Cosine Transformation.

[9] Elaborates a brand new algorithm for the purpose of image encryption then compression. Here in first step author did the encryption of the image by using very famous random permutation method.

The reason behind using of this permutation is that it provides a very high level of security compare to the other methods of the queue. The output of the image encryption is fed to the image compression. Here image compression is carried out by using HAAR and Daubechies Wavelet Transform. This transform provides good compression ratio, Mean square error, and Peak signal to noise ratio all these experiments are carried by using image processing tool available under MATLAB software.
[10] Abdul provides a good overview on the different image ETC algorithms used by the researchers. He mainly focuses on those studies where both the encryption and compressions are carried out simultaneously. In this overview author gives tabular representation of 27 research papers for the better understanding of performance evaluation of each paper.
This eventually elaborates the summary of methodology used by the each of these methods. This study is carried out by dividing the papers in three categories like CE (Compression followed by encryption) , EC (Encryption followed by compression) , JCE (Joint compression and encryption) .The performance is evaluated by using PNSR ratio and coding and decoding time required for the image compression.

[11] Proposed an efficient approach for image encryption using wavelet transform. This technique belongs to Lossy compression as it induces some sort of loss while doing transformation. First image is decomposed to prepare it for the purpose of image compression. Thresholding is used to do image compression. Only those pixels which meet the criterion of threshold are allowed to enter in compressed image. Once image compression is done, image is forwarded to the image encryption method. This paper makes use of HAAR as a wavelet transform.

## 3. Proposed Methodology

In this section, we describe our framework for image encryption and then compression techniques using decomposition and hierarchical pattern manner techniques with the below mentioned steps as shown in figure 3.

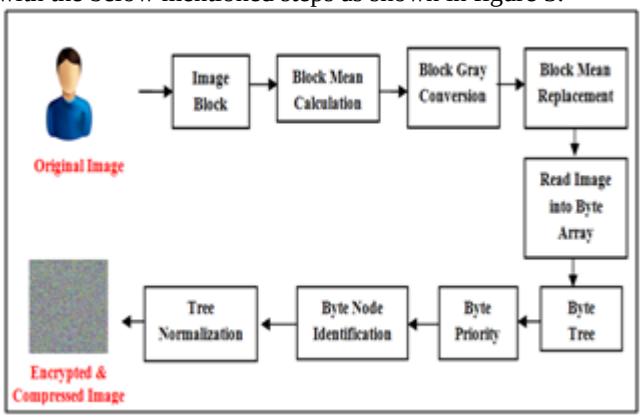



**Figure 3:** Overview of our approach

*Step 1*: In this step image will be read into java buffered Image object and then it is been divided into various blocks and then these blocks will be stored in a vector.

*Step 2:* Here in this step for all the image blocks which are stored in the vector mean values are calculated and then these values are stored in the index position of each vector.

*Step 3:* Here all the Means are replaced with one another based on the random distribution theory , Then every blocks are painted with new replaced mean values to get the Encrypted image.

*Step 4:* Here in this step encrypted image is read into byte and all bytes are stored in a byte vector. Then all the bytes from the byte vector are store in tree based on the priority of byte size.

*Step 5:* In this final step of compression all the bytes are been traverse from its tree to find the normalized compressed values. The they are written in file format to compress the tree. The complete compression technique is shown in the below algorithm

ALGORITHM 1: IMAGE COMPRESSION

Input: Image File
Output: Encrypted file
Step 0: Start
Step 1: Get ByteArray B[ ] of File F
Step 2: Assign sequence of positive integer.{ l1, l2,,,,,,, lk}
Step 3: Summation all as

$$\sum_{i=1}^{k} 2^{-l_i} \leq 1$$

,where each l represents a node
Step 4: Define a queue Q
Step 5:Add all nodes into the priority queue
Step 6:Set the priority according to highest probability of bits.
Step 7:Calculate average probability as L(avg)
Step 8:Set bounds as H(s) _ L(avg) < H(s) + 1 , where H(s) is the entropy.
Step 9: Remove first two nodes of higher priority from queue.
Step 10:Create a new node called Nn
Step 11: Add two nodes from step 10 into Nn unmatched probability
Step 12:Repeat steps 10 to 12 till queue is empty
Step 13:Convert tree into ByteArray
Step 14: Write the ByteArray into file.
Step 15:Stop

## 4. Results and Discussions

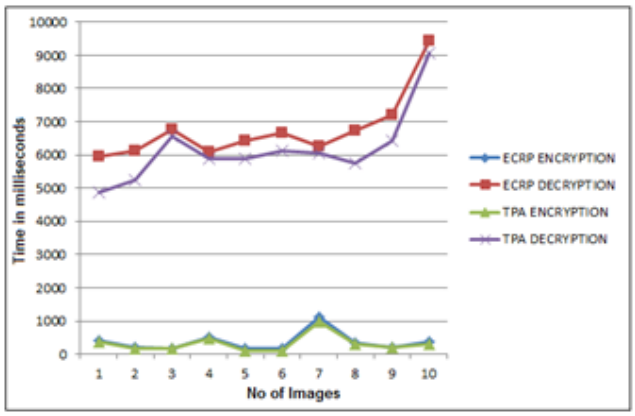
To show the effectiveness of proposed system some experiments are conducted on java based windows machine using netbeans as IDE. To measure the performance of the system we set the bench mark by conducting many tests as follows.

### 4.1 Encryption Time Performance

Proposed model is tested on many images for its encryption time performance by implementing module of the methods mentioned in the Error Clustering and Random permutation (ECRP) [12] System with our model of Tree pattern Approach (TPA). So as a result of this we get the following results which is plotted in the below graph.
Figure 4: Encryption and Decryption performance Time

The above plot clearly indicates that our approach of TPA clearly over performs in the encryption performance time .

### 4.2 Compression Time Performance:




Proposed model is tested on many images for its Compression and decompression time performance with ECRP System with our model of Tree pattern Approach (TPA). So as a result of this we get the following results which is plotted in the below graph.

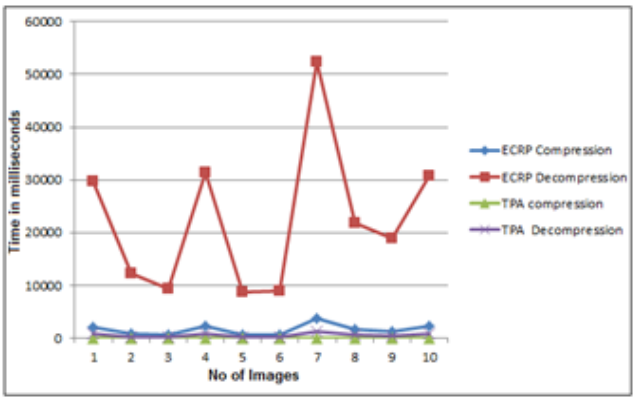



**Figure 5:** Compression and Decompression time Ratio Comparisons

The above plot clearly indicates that our approach of TPA clearly over performs in the compression and decompression performance time .

## 5. Conclusion and Future Scope

Our proposed method of Image encryption using image colour model parameter like RGB enhances the complexity in breaking the encrypted data. As our system extract the colour codes of the pixel to mix and merge pixels values to give highly complex structure of encrypted image. Proposed system is using compressed tree format for calculating byte probability of the pixels to compress the image in more advance format. Our System is lossless where the recovery of the original image is up to 100%. The proposed system can be enhance to reach more accuracy in compression so that compression ratio can be increase to the $1/10^{th}$ of the original image. This can be good contribution over the image compression techniques.

## References

[1] "A Survey On Different Image Encryption and Decryption Techniques" Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya . Rinki Pakshwar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 113 – 116
[2] "Image Encryption Using Different Techniques: A Review" Komal D Patel, Sonal Belani International Journal of Emerging Technology and Advanced Engineering
[3] "Secure Image Encryption Algorithms: A Review" Lini Abraham, Neenu Daniel . INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 4, APRIL 2013
[4] "A STUDY OF VARIOUS IMAGE COMPRESSION TECHNIQUES" Sonal, Dinesh Kumar
[5] "Lossless image compression techniques" BC vemuri, S.sahni.
[6] "Lossless Image Compression Technique Using Combination Methods" A. Alarabeyyat1, S. Al-Hashemi1, T. Khdour1, M. Hjouj Btoush1, S. Bani-Ahmad1, R. Al-Hashemi2 Journal of Software Engineering and Applications, 2012, 5, 752-763

[7] "Simple Fast and Adaptive Lossless Image Compression Algorithm" Roman Starosolski∗ December 20, 2006 Software—Practice and Experience, 2007, 37(1):65-91, DOI: 10.1002/spe.746
[8] "Enhanced System for image's compression and encryption by addition of biometric characteristics" A. Loussert, A. Alfalou, R. El Sawda, A. Alkholidi ISEN-BREST Laboratory L@BISEN 20 rue cuirasse Bretagne C.S. 42807, 2922
[9] "Designing an Efficient Image Encryption-Then-Compression System with Haar and Daubechies Wavelet" Harmanpreet Kaur Aujla, Rajesh Sharma, Harmanpreet Kaur Aujla et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7784-7788
[10] "**Image Compression and Encryption: An Overview** " Abdul Razzaque International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181
[11] " A Novel Image Encryption Supported by Compression Using Multilevel Wavelet Transform" Ch. Samson1 *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 9, 2012*
[12] Jiantao Zhou, Xianming Liu, Oscar C. Au, Yuan Yan Tang ," Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation " ,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014 39