ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IMAGE ENCRYPTION USING ADVANCED COMBINATION OF PERMUTATION TECHNIQUE TO REDUCE CORRELATION AMONG NEIGHBORING PIXELS

A.Narmadha*, Dr.G.Velmayil
RESEARCH SCHOLAR, PG AND RESEARCH DEPARTMENT OF COMPUTER SCIENCE,
QUAID-E-MILLATH GOVERNMENT COLLEGE FOR WOMEN (A).
ASSISTANT PROFESSOR, PG AND RESEARCH DEPARTMENT OF COMPUTER SCIENCE,
QUAID-E-MILLATH GOVERNMENT COLLEGE FOR WOMEN (A).

ABSTRACT

Images occupy the most important position in multimedia data. Techniques for transmitting and storing images are increasing to a greater extent. Images that are transferred over the network are confidential and private. Therefore there is a need for protecting these image data from the unauthorized users. This is achieved using Image Encryption. There are many techniques used to protect the image data. Most of the existing Image Encryption and Decryption techniques perform image encryption by scrambling the pixels or by dividing the images into blocks and shuffling them or by permutation. Images are arrangement of pixels and the image information can be predicted from the value of the neighboring pixels. Therefore it is important to decrease the correlation among the neighboring pixels and increase the entropy. The proposed work deals with decomposing the image into block size of very smaller pixels, and the image blocks are scrambled using the proposed permutation technique, which will result in lower correlation and higher entropy. The permuted image obtained is encrypted using RSA algorithm. Pre-processing of the image is carried out, by converting the binary values of the image into Integer which makes easy to work with RSA algorithm for the encryption of the image. Permutation on the smaller blocks of the image itself has provided security to the images, further when encryption is applied on this permuted image a higher level of security has been achieved. Computational Hardness and great security has been provided by RSA algorithm.

KEYWORDS: Permutation, RSA, Neighboring pixels

INTRODUCTION

The increased use of internet in the digital world today has made the security of the digital images more important and attracted much attention [1]. Major part of the transmitted information, either confidential or private, demands for security mechanisms to provide required protection. Therefore, security has become an important issue in the process of storing and transmitting the digital data. In natural images the values of the neighboring pixels are strongly correlated to each other, so that the value of any given pixel can be reasonably predicted from the values of its neighbours [3]. Many encryption algorithms are being developed day by day. Image based data requires more effort during encryption and decryption. According to [4] there are many different types of images and there is no single encryption algorithm which satisfies all the types of images. It has been proved that traditional cryptosystems provide very high security. One of the best traditional algorithms RSA algorithms is used here for encryption it is a widely used Public scheme. Public key cryptography makes use of two keys, Public key which may be known by anybody and can be used to encrypt messages and verify signatures. A Private key known only to the recipient and is used to decrypt messages and create signatures. It is also called as Asymmetric because those who encrypt messages or verify signatures cannot decrypt messages or create signatures. Here the traditional RSA algorithm is slightly modified and is made suitable to work with different types of images.

IMAGE ENCRYPTION

A digital image is defined by an array of individual pixels and each pixel has its own value. Digital images are produced through a process of two steps: *sampling* and *quantization*. Sampling is the process of dividing the original image into small regions called pixels, whereas quantization is the process of assigning an integer value (i.e. color) to each pixel. Image encryption is a technique which transforms the plain images into unreadable format

[4]. Encryption of images can be done using various techniques. Permutation is one of most important technique where images are divided and then permuted or shuffled based on some permutation technique. New encryption algorithms are being developed and used for encryption. **Strong encryption,** secrecy and privacy is the important advantage of Traditional algorithms, hence RSA algorithm is used for the proposed methodology.

PERMUTATION TECHNIQUE

One of the most important techniques is Permutation. The permutation process refers to the operation of dividing and replacing an arrangement of the original image, and thus the generated one can be viewed as an arrangement of blocks [5]. The three basic permutation methods are

i. **Bit permutation:** In bit permutation technique each bit in the image is taken and are permuted with the key chosen from the set of keys by using pseudo random index generator
ii. **Pixel permutation:** In pixel permutation technique group of pixel is taken from the image and the pixel in the gray is permuted using the key that is selected form the set of keys.
iii. **Block permutation:** In block permutation technique group of block is taken from the image and these blocks are permuted as same as the bit and pixel techniques.

The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. Therefore reducing the relationship among the elements by increasing the entropy value of the encrypted images as well as lowering the correlation must be achieved greatly to protect the images from unauthorized access.

EARLIER WORKS ON IMAGE ENCRYPTION USING PERMUTATION AND TRANSFORMATION TECHNIQUE

Image Encryption using Affine Transformation and XOR Operation is based on shuffling the image pixel. It is a two phase process, where the image is encrypted using XOR operation and the pixel value is redistributed using affine transformation with four bit keys [6]. The transformed image is then divided into blocks and encrypted using XOR operation. The result proved that the correlation was decreased significantly [6]. This process is very lengthy and much time consuming. Also chances of mistakes are higher in obtaining the original image since process takes place in two different phases.

Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping is a method where the plain-image is divided into blocks and performs block based shuffling using Arnold Cat transformation. The image is uniformly scrambled after the transformation, where all the pixels in the same block of scrambled image come from different blocks of original image [8], after which the image as a whole is shuffled again by the transformation technique. Finally the shuffled image is encrypted using a chaotic sequence generated using symmetric keys, to produce the ciphered image for transmission [8]. But to synchronize the received chaos sequence with the one generated at the receiver end is a difficult process.

Image Encryption based on the RGB PIXEL Transposition and Shuffling is a technique which is done by developing a cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values [9]. The algorithm ultimately makes it possible for encryption and decryption of the images based on the RGB pixel. In this technique the RGB colors are extracted and the extracted RGB values are transposed and shuffled to obtain ciphered images [8]. Obtaining each values and shuffling it separately and then together is considered to be lengthy and moreover only coloured images can be encrypted using this technique.

Image Encryption Using Advanced Hill Cipher Algorithm generates a self- invertible matrix for hill cipher algorithm. Using this key matrix they encrypted gray scale as well as color image except for the image with background of same gray level or same color [9]. This is matrix based algorithm. It directly encrypts gray scale. It is simple to implement. This algorithm cannot work on image with background of same gray level or same color.

An Enhanced Chaotic Image Encryption, in this technique the image is encrypted pixel by pixel using logistic maps. The advantage of logistic map is that it has a very complex dynamics. Use of two logistic map increases the complexity of algorithm [10]. Only the first few coefficients are encrypted since energy is concentrated in these values. The algorithm uses a coupled logistic map. The first logistic map whose initial parameters are taken from the key generated during user authentication process provides the initial parameters for second logistic map. Chaos based technique has been considered best for their superior properties in security and complexity [10]. The architecture of this method is

not sensitive to changes in the plain text and they are insecure upon chosen and known Plain image attacks.

A New Image Encryption Approach using Combinational Permutation Techniques permute the image using the three basic types of permutation. First the image is permuted using bit permutation technique. Same image is then permuted with the Pixel permutation and finally with the block permutation technique [3]. All the three results are compared with each other and conclusion has been drawn from the comparisons, and has been concluded that the bit permutation has achieved the lower correlation when compared to block permutation and pixel [3]. But only permutation has been carried out where the images have not attained higher entropy and lower correlation, so that the permuted images appear to be easily predictable.

An Image Encryption Approach Using a Combination of Permutation Technique followed by Encryption, in this technique the original image was divided into 4pixel*4Pixel blocks, which were rearranged into a permuted image using a permutation process. The permuted image was then fed into RijnDael encryption algorithm [2]. The final image obtained was a permuted encrypted ciphered image. This resulted in lower correlation between the image elements [2]. Further different encryption techniques can be applied to achieve best encryption and the blocks can also be further divided to achieve less correlation.

PROPOSED TECHNIQUE

The proposed technique decomposes the *plain image* of any size and various formats into smaller block. The blocks may contain a certain number of Pixels. The permutation technique used here is the pixel permutation technique. Here in this proposed technique the image is divided into 2pixel*2pixel block. The decomposed blocks of the plain images can be transformed into new locations by using permutation process. The step involved in the permutation process of the proposed technique is, to load the plain image and identify the height and width of the image in order to divide the images into blocks. The obtained blocks of the plain image are permuted to obtain a permuted image. The binary value is then converted into integer and is fed into the RSA algorithm for Encryption. The general methodology is given in Fig (1).

5.1. Block Diagram

The block diagram of the proposed methodology explains the different process involved in the methodology. It gives an overview of the entire system

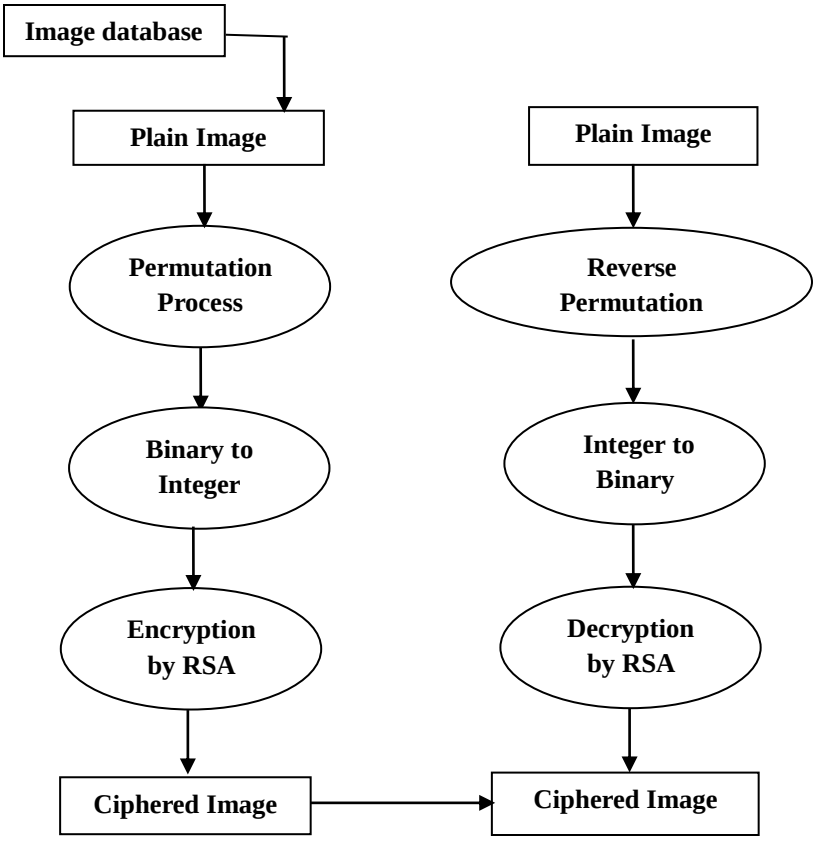

Fig (1): Block diagram of the Proposed Permutation Technique

The permuted image is converted to work with RSA algorithm. The reverse process is carried out on the decryption to get back the original image.

5.2. Algorithm

Algorithm provides the steps for designing the proposed methodology. The algorithm clearly explain the steps involved,

Algorithm for Permutation Technique

1: Load the plain Image
2: Get the Width and Height of the image
3: Identifying the horizontal and vertical number of blocks.
4: Number of Blocks = Horizontal Number of Blocks ×Vertical Number of Blocks
5. Start Permutation
5.1: For I = 0 to Number of Blocks -1
5.2: Get the new location of block I from the permutation table
5.3: Set block I in its new location
5.4: end permutation
6. Generated permuted image

7. Get the Binary Matrix of the image
8. Convert Binary to Integer
9. Apply RSA algorithm to the Integer value of the Image
10. Obtain the encrypted image

The permutation process is based on the combination of image permutation followed by the encryption [4]. The new algorithm is used to encrypt the image files to enhance the security in the communication area for data sending.

BLOCK DIVISION OF IMAGE

This section gives a clear view of how the image division takes place in the proposed methodology. First the original image for which division process is to carried out is taken. The original image is shown in Fig (2.a)

Fig (2.a): Original Image

The original image is divided into two rows and two columns. Fig (2.b) shows the four block view of the original image.

Fig (2.b): 4 block view of Image

Iterate the process for further division. In Fig (2.c) the image is divided into four rows and four columns

Fig (2.c): 16 block view of Image

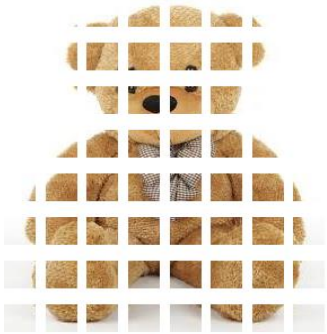

Fig (2.d) 64 Block View of the Image

Each block is further decomposed similarly till we obtain a 2*2 pixel blocks. The images are permuted using pixel permutation process. The 2*2 pixel permuted image obtained is shown in Fig (2.e).

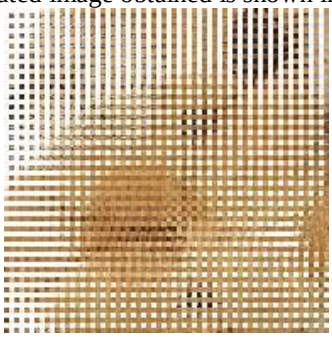

Fig (2.e) Final Permuted Image

The original and permuted image which has been obtained after the division and permutation process is shown in **Fig (3)**.

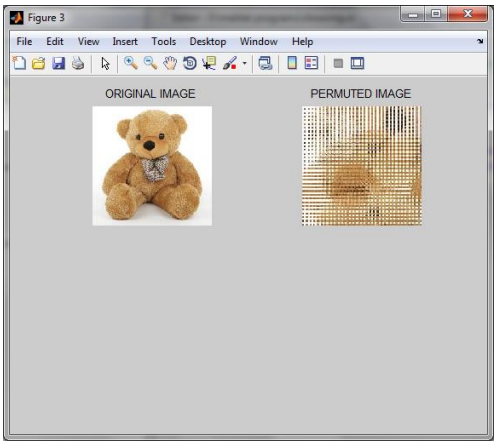

Fig (3): Original and Permuted View of an Image

The image obtained after permutation is permuted to a greater extends and it is significantly different from that of the original image. This shows that the proposed methodology has provided good security to the image

RESULTS AND DISCUSSION

All image encryption techniques will be evaluated on the basis of three important Image Security measures. They are Correlation, entropy and histograms. The measurements of correlation, entropy and histogram will be used to measure and Compare the security level of the original image, permuted and encrypted images. Analysis on these security measures are given one by one below.

Pixel permutation has been carried out in the proposed methodology. Images are divided into 2 pixel*2 pixel blocks in order to achieve lower correlation among the neighboring pixels and higher entropy. The general permutation is a total number of arrangements of a set of objects where order doesn't matter. Permutation is given by

nPr =n! / (n-r)! **..... (1)**

n = total number of objects

r = number of objects we select

Pixel permutation has resulted in lower correlation and higher entropy. Correlation and entropy are calculated using different formulae.

7.1 Entropy Analysis

Entropy is defined as a measure of disorder in an image. The entropy is calculated using the following formulae [10].

$H = -\sum_{k=0}^{G-1} P(k)\log_2(P(k))$ ..... (1)

Where

H: Entropy

G: gray value of input image (0... 255).

P(k): is the probability of the occurrence of symbol k.

The entropy is calculated for the original image and the permuted image. And it has been observed that the image after permutation has achieved higher entropy and shown in **Fig (4).**

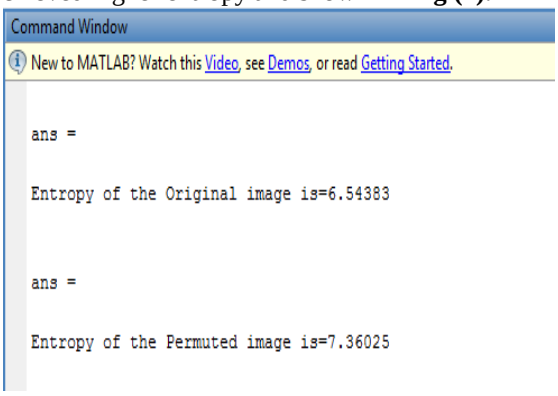

Fig (4): Entropy of the Original and Permuted image.

After calculating the Entropy of the original image is 6.54383 and the permuted image is 7.36025. The difference between the original and permuted entropy is 0.81. Clearly the entropy is increased.

The graphical image of the original and permuted image clearly shows the improved entropy of the permuted image when compared to the original image and is shown in Fig 4.a and 4.b.

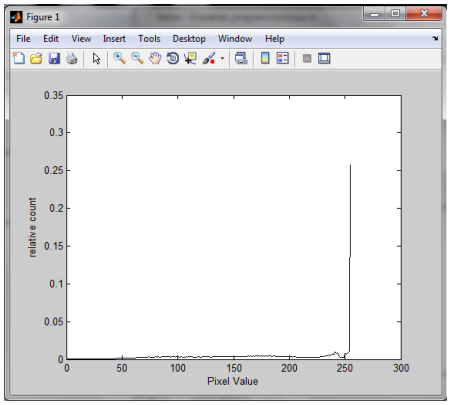

Fig (4.a): Entropy graph of Original Image

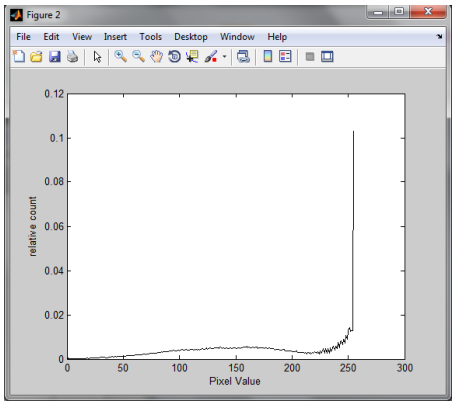

Fig (4.b) Entropy graph of Permuted Image

The graph shows the pixel value and its count. From the graph it has been proved the pixel value and count has been increased.

Entropy calculation performed for original and permuted image of a single image is shown in Fig (4). Table 1 shows the entropy calculation performed for the image data set collected for different size of images.

Table 1: Entropy Calculated for the image sample data.

Name of the Image	Size of the image	Entropy of original Image	Entropy of Permuted Image
Smiley	100 x 100	5.89088	6.76471
Flower	100 x 100	5.56324	6.71034
Fruit	100 x 100	6.04651	6.85099
Bear	225 x 225	6.54383	7.36025
Earth	225 x 225	6.09293	7.40768
Rose	225 x 225	6.53902	6.91106
Design	500 x 500	6.56025	7.46783
Puppies	500 x 500	7.85385	7.03181
Fish	500 x 500	5.78643	7.42027

The table 1 proves that the entropy is increased for all the image samples. The value obtained for permuted image is greater than the original image. Thus the proposed methodology has proved to be secure.

7.2 Histogram Analysis

Histogram is one of the important security measures. Histogram refers to the pixel intensity value. The Histogram of the original image and permuted image has been shown in **Fig (5.a)** and **Fig (5.b)** clearly shows the significant changes between the original and permuted image

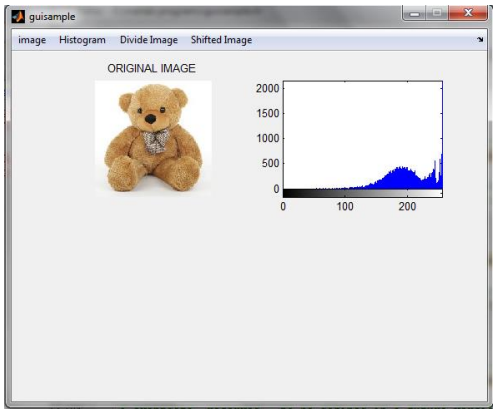

Fig (5.a): Histogram of the Original image

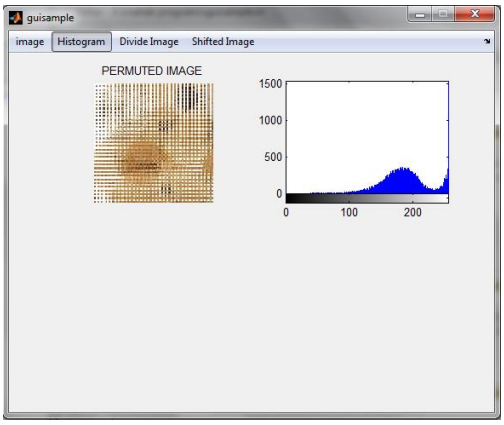

Fig (5.b): Histogram of the Permuted Image

7.3 Correlation Analysis

The correlation between the images is what makes the images compressible; pixels in the images are correlated to their neigh boring pixels. The correlation among the pixels is greatly reduced in the proposed methodology. By dividing the images and then permuting them has achieved the lower correlation. Correlation is calculated using the formulae [10]

$$\mathbf{r} = \frac{n\sum(xy)-\sum x\sum y}{\sqrt{[n\sum(x^2)-(\sum x)^2][n\sum(y)^2-(\sum y)^2]}} \quad \text{..... (2)}$$

Where

r: correlation value

n: the number of pairs of data

$\sum xy$: Sum of the products of paired data

$\sum x$: Sum of x data

$\sum y$: Sum of y data

$\sum x^2$: Sum of squared x data

$\sum y^2$: Sum of squared y data

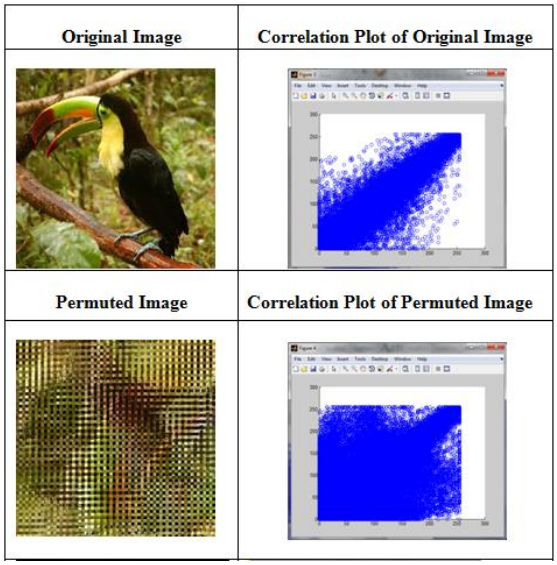

Fig (6) Correlation Plot for Sample Image

The correlation plot for one image sample is given. The correlation has reduced, because the correlation plot of the original image is linear whereas the correlation plot of permuted image is scattered. This shows the low correlation among the pixels.

The correlation is calculated for the same data set for which the entropy is calculated. The correlation is reduced for all the image samples taken.

Table 2: Correlation Calculation for Original and Permuted Image

Image Name	Original Image	Permuted Image
Smiley	0.9657	0.5904
Flower	0.9648	0.8373
Fruit	0.9472	0.6529
Bear	0.9766	0.8160
Earth	0.9586	0.6317
Rose	0.9134	0.7358
Design	0.9845	0.7102
Puppies	0.9821	0.7880
Fish	0.9856	0.5262

Correlation table (2) gives the correlation value of the original and permuted image. Generally the correlation will be reduced only after encryption. In the proposed methodology the correlation has been reduced after the permutation itself. This shows that the proposed methodology is one among the best.

CONCLUSION

This paper suggests a method to achieve higher entropy and lower correlation among the neighboring pixels. Pixel permutation along with block permutation technique is used to achieve the aim of the research. Images are divided into much smaller blocks and permuted using a key which resulted in a permuted image. Entropy analysis and correlation analysis and histogram analysis is calculated for various data sets which contained images of different size and format and it proves lower correlation and higher entropy. To ensure high security finally permuted images is converted to binary to integer and fed into RSA algorithm. Thus high level security is achieved. This algorithm works comparatively well for images of equal height and width. It is very efficient method for smaller and medium sized images. It is a time consuming process for very large size images. Certain images are easily predictable with the help of their predominant color. Their color may sometimes give a clue for the attackers; those images must be handled accordingly. These types of images are rare. In future these types of images can be considered. Various traditional encryption algorithms like DES, AES, IDEA, can be applied on the permuted image in future to achieve high level security.

REFERENCES

1. Avi Dixit, Pratik Dhruve and Dahale Bhagwan, "Image Encryption Using Permutation and Rotational XOR Technique," Department of Electronics and Telecommunication, Thakur College of Engineering and Technology, Mumbai University, Mumbai, India.
2. Mohammad Ali Bani Younes, and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.4, April 2008
3. A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, 2006, p.127, http://www.enformatika.org
4. A.Nag, J.P.SINGH, S.Khan, S.Ghosh, S.Viswas, "Image encryption using affine transformed XOR operation," International Journal of Computer Application Volume 95-no.19 2011.
5. Ravi Shankar Yadav, M.H.D.Rizwan Beg & Manish Madhava Tripathi, "Image Encryption Techniques: A Critical Comparison," International Journal of Computer Science Engineering and

Information Technology Research (IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 1, Mar 2013, 67-74

6. B.Y.Mohammad Ali and J.Aman, "Image Encryption Using Block-Based Transformation Algorithm," IAENG International Journal of Computer Science, Vol. 35, Issue. 1, 2008, pp. 15-23.
7. C. Chan, and Y. Wu, "A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme", International Journal of Computer Science and Network Security, Vol. 8, No. 4, 2008, pp. 128-132.
8. Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B" Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping '" International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.1, March 2012
9. S.K.Panigrahy, B.Acharya, D.Jena," Image Encryption using self-invertible key matrix of Hill cipher algorithm2008", International Conference on Advances in Computing.
10. Rajinder Kaur, Er.Kanwalprit Singh(2013). "Image Encryption Techniques: ASelected Review", IOSR Journal of Computer Engineering (IOSR-JCE) e- ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013)PP 80-83