International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 6 (2015) pp. 13775-13788

http://www.ripublication.com

A Novel Image Encryption Approach Using Block Based Transformation and Random Phase Encoding

S.Suresh Raja
Associate Profesor,MCA
K.L.N.College of Engineering
Pottapalaya - 630611
Sivagangai District,
Tamil Nadu,
India

2. Dr.V.Mohan,
Dean and Head of the Department,
Dept. of Math ,
Thiagarajar College of Engineering,
Madurai
Tamil nadu, India

3. Dr.S.Vijayalakshmi
Assistant Professor,
Dept. Of Computer Applications
Thiagarajar College of Engineering,
Madurai
Tamil nadu, India

Abstract

Security is the major concern of transmitting the data in open networks. Each type of data has its own features and different techniques should be followed to protect confidential data from unauthorized access. Considering the security in transmitting the image in open network, a new image encryption algorithm is proposed. In this paper we introduce a block based transformation algorithm on the combination of image transformation associated with a known encryption and decryption algorithm called blowfish. The original image was divided into eight blocks, and the pixels of each block are then shuffled with different function of each. The transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased by using the proposed technique and

higher entropy is achieved. At the receiver side these blocks are retransformed in to their original position and performed a decryption process which gives the original image. Advantage of this approach, is that it reproduce the original image with no loss of information for the encryption and decryption process using blowfish algorithm.

Keywords: Image Encryption, Image Correlation and Entropy, Blowfish

Introduction

Many transmission services require reliable service in digital images. Due to fast growth of internet [1] data encryption is extensively used to make sure the security. However, most of the offered encryption algorithms are used for text data. Due to huge data size and real time constrains, algorithms that are good for textual data may not be appropriate for multimedia data in open network [2]-[4]. In most of the normal images, the values of the adjacent pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors) [5]-[7]. In demand to disperse the high correlation among pixels and increase the entropy value, we have introduced a transformation algorithm that divides the image into eight blocks. All these blocks are shuffled with an indivual function each, then the blocks shuffles their positions before it passes them to the encryption (Blowfish) algorithm. By this time the correlation, histograms and entropy has used to measure the security level of the images are majorly concerned. The variable secret key of the transformation process determines the seed, which is used to build the secret transformation table with a variable number of blocks. If the key has changed, another seed will be generated, and a different secret transformation table is obtained. The variable secret key of the Blowfish algorithm is used to encrypt the transformed image. This encryption process decreases the mutual information among the encrypted image variables (i.e. high contrast) and thus increasing the entropy value. In this paper we propose a block-based transformation algorithm in order to increase the security level of the encrypted images.

Background

Image Encryption can become an integral part of the image delivery process if encryption is the process of transforming the information to insure its security with the huge growth of computer networks and the latest advances in digital technologies. As a result, different security techniques have been used to provide the required protection [8]-[9]. Each type of data has its own characteristics include high correlation among pixels, bulk data capacity and high redundancy. Hence, many different techniques should be used to protect confidential image data from unauthorized access. The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these

images [9]. The security level of digital images over network has attracted much attention recently, and many different image encryption methods have been proposed to enhance the security of these images [8]. According to the image encryption scheme try to convert an image to another one that is hard to understand only. On the other side, image decryption retrieves the original image from the encrypted one. We believe that by proposing block based encryption and decryption algorithm, it will reduce to increasing the entropy value of the encrypted images as well as lower correlation.

Related Work

A Novel Image Encryption Algorithm Based on Hash Function, 2010[10]
The authors Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki proposed a new algorithm using SHA-512 hash function for image encryption. The algorithm comprise of two key sections: The first one shuffles half of the given where the positions of the pixels are relocated. The second generates a random number mask by using SHA-512 hash function. The random number mask is XORed with the remaining part of the given image which knows to be encrypted.

A New Approach for Fast Color ImageEncryption Using Chaotic Map
[11] The authors Kamlesh Gupta, and Sanjay Silakari proposed a new method that uses the basic operations like confusion and diffusion by replacing the straight complex system into friendly one. They used a better encryption method, the 3D cat map and standard 3D. The proposed technique generate diffusion models using a 3D map rotation of the image using vertical and horizontal planes by shuffling red, green and blue using the card and 3D Cat Map. At last the image is encrypted by performing XOR operation on the shambled image and the diffusion model. The new algorithm eliminates the possibility of brute force attack and is very fast in encrypting the image. This has been proven by simulations of statistical analysis, histogram analysis, Entropy and correlation analysis. The experimental result shows that the proposed algorithm is high speed and fast encryption.

Permutation based Image Encryption Technique, 2011 [12]
Sesha Pallavi Indrakanti and P.S.Avadhani[16] proposed a new image encryption techniques based on random pixel permutation with the motivation to maintain the quality of the image. The proposed scheme uses the three types of classification like changing the pixel position, generating the key and visual transformation. The first phase is the image encryption where the images are splits into blocks and the blocks are interchanged. The second phase generates a key by the used in the encryption process. The third phase is the identification process involves the numbering of the shares that are generated by the secret image. The proposed technique provides confidentiality to color image with less computations by strong correlation among the adjacent pixels.

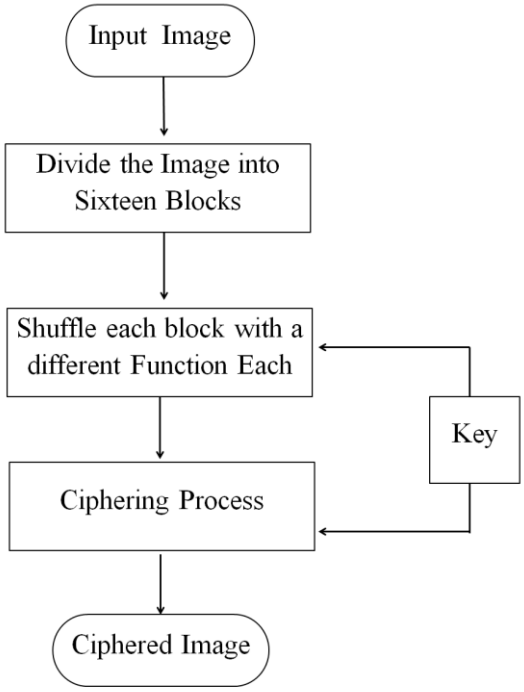
Image encryption using permutation and rotational xor technique, 2012[13]
Avi Dixit, Pratik Dhruve and Dahale Bhagwan proposed an algorithm "**Image encryption using permutation and rotational xor technique"**. The proposed method permutated the binary code of the pixel values of a color image with a 8 bit key which is followed by the transformation of every 8 consecutive pixels. The transformed images are further divided into blocks and the blocks are shifted accordingly. The proposed technique has flaws, where the key size for per mutating the binary code is very small. The algorithm is further appended with 43 digit key and the encryption takes a total of 10 rounds. The experimental results of the proposed technique showed that the correlation between adjacent elements was significantly decreased.

Image Encryption Using Random Pixel Permutation by Chaotic Mapping
G.A.Sathishkumar, Srinivas Ramachandran and Dr.K.Bhoopathy Bagan [14] proposed a new image ciphering technique using random pixel permutation based on chaos logistic maps and prime modulo multiplicative linear generators. The random-like nature of chaos is effectively spread into the encrypted image through permutation and transformation of pixels in the plain image. Simulation results show high sensitivity to key, plaintext and cipher text changes. From a point of image ciphering, the scheme is highly resistive to known/chosen plaintext and cipher text attacks.

Image Encryption Using Shuffling Technique, August 2013[15]
Mohammad Ali Bani Younes proposed a new algorithm "**Image Encryption Using Shuffling Technique",** for image encryption. The proposed method shuffles and rearranges the pixels of the original image randomly within the original image. The original image is permutated using a transformation technique presented. The transformed image is XORed eith a random variable key to produce a ciphering image.

The Proposed Technique
The block-based shift algorithm is based on the combination of image Shifting followed by encryption. The shift algorithm and the Blowfish algorithm use the original image to produce four output images; (a) an original image (b) a transformed image using a Shifting process and (c) a transformed image encrypted using Blowfish (d) a decrypted image. The correlation and entropy of the three images are computed and compared with each other. This technique aims at enhancing the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value. Image measurements (correlation and entropy) will be carried out on the original image and the encrypted images with and without shift algorithm the results are then analyzed.

The general block diagram of shifting method is shown in fig. 1



Algorithm Description
The creation of blocks from the image is presented below.

Algorithm Create_Blocks

1. Load Image
2. For I=1 to size of the image
   2.1: Divide the image
   (Horizontal number of blocks * Vertical number of blocks) 2.1: Get the new location of block I from the image.
   2.2: Set the block I in its new location
   2.3: Next I
3. Output the blocked image

The shifting algorithm is presented below.

Algorithm Perform_Shifting

1. Load Image
2. Input Secure Key
3. Divide the original image to
   (Horizontal number of blocks * Vertical number of blocks)
4. Shift the blocks of images
5. Shift the rows of image
   5.1 For I=1 to horizontal number of blocks
   5.2: circshift (block number, row array value)
   5.3: next I

6. shift the columns of image
    6.1: For I=1 to vertical number of blocks
    6.2: circshift (block number, column array value)
    6.3: next I
7. Output the shifted image

The algorithm of image transformation is presented below.

Algorithm Perform_Transformation

1. For I=1 to Shifting no of blocks
    1.1: Get the location I from the shifting no of blocks 1.2: Set the block I in its new location
    1.3: Next I
2. Output the transformed image

The image encryption algorithm is presented below.

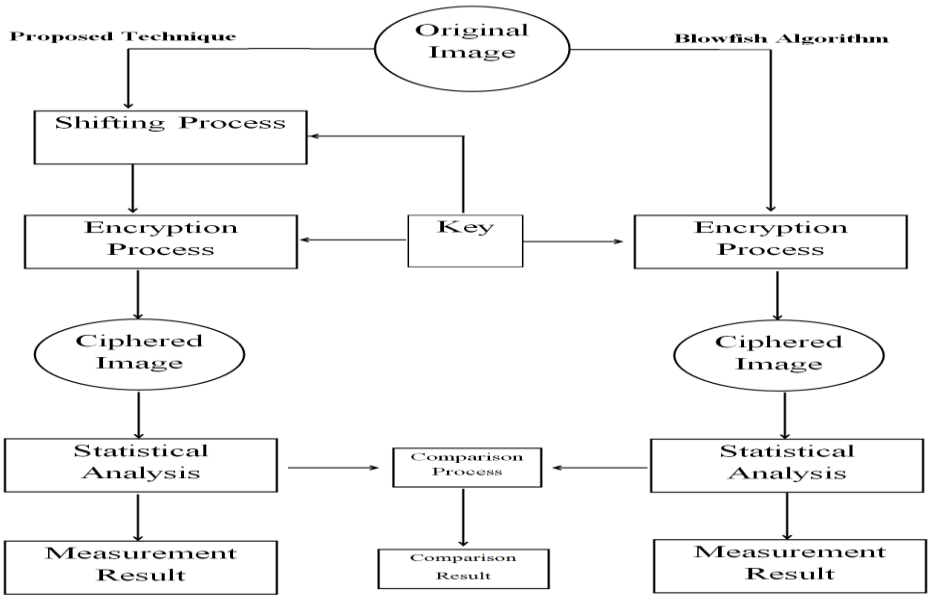
Algorithm Perform_Encryption

1. Load the image
2. Input secure key
3. Get the size of the image
4. Get the length and the breath of the image
5. For ind=1 to length of the image
    5.1: For ind=1 to breath of the image
    5.2: perform the bitxor between the original image and the input secure
    5.3 End
6. Output the encrypted image.

B. Description of combination technique

The block-based transformation algorithm is based on the combination of image transformation followed by encryption (i.e. transformation algorithm followed by the Blowfish algorithm). The transformation algorithm and the Blowfish algorithm use the original image to produce three output images; (a) a transformed image encrypted using Blowfish (b) a transformed image using a shifting process and (c) a ciphered image using Blowfish, The correlation and entropy of the three images are computed and compared with each other. This technique aims at enhancing the security level of the encrypted images by reducing the correlation among image elements and increasing its entropy value. Image measurements (correlation and entropy) will be carried out on the original image and the encrypted images with and without transformation algorithm the results are then analyzed.

The overview model of the proposed technique is shown in Fig.2.



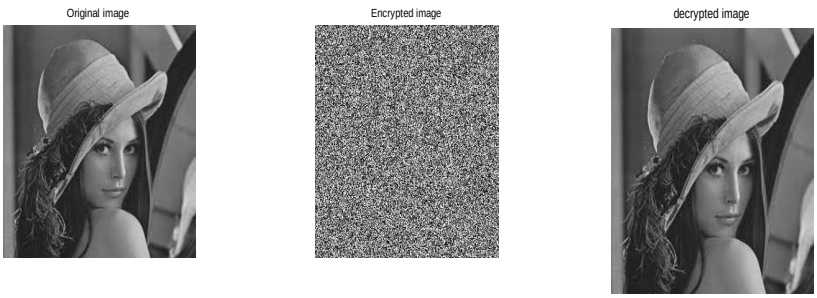
Correlations are computed for each case according to equation (1).

$$r = \frac{n\sum(xy) - \sum x \sum y}{\sqrt{[n\sum(x^2) - (\sum x)^2][n\sum(y^2) - (\sum y)^2]}} \quad (1)$$

Where

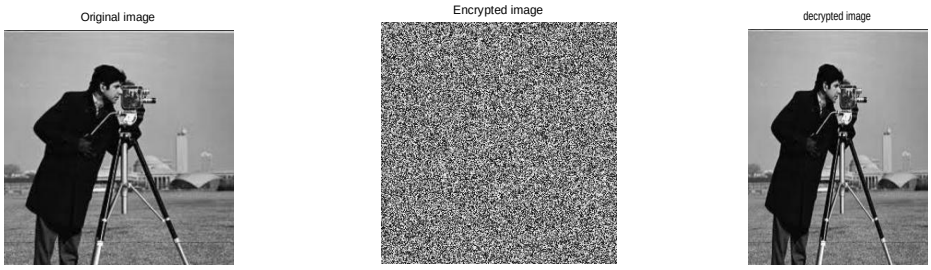
r	:	correlation value
n	:	the number of pairs of data
$\sum xy$	:	sum of the products of paired data
$\sum x$	:	sum of x data
$\sum y$	:	sum of y data
$\sum x^2$	:	sum of squared x data
$\sum y^2$	:	sum of squared y data

Experimental Results



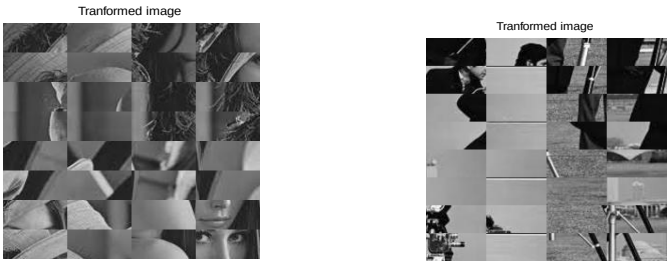
(a) (b) (c)

Figure 2: (a) Original Image (b) Encrypted Image (c) Decrypted



(a) (b) (c)

Figure (3): (a) Original Image (b) Encrypted Image (c) Decrypted Image



(a) (b)

Figure (4): (a) Transformed Image of lena, (b) Transformed Image Cameraman

A high-quality encryption algorithm should be strong against all kinds of attacks, statistical and brute force attacks. Some experimental results are given in this section to demonstrate the efficiency of our algorithm. All the experiments are performed on a laptop Intel® Core™ i3, 3G RAM with Windows Vista. The compiling environment is MATLAB R2009a.

Statistical Analysis

In order to resist the statistical attacks, which are quite common nowadays, the encrypted images should possess certain random properties. To prove the robustness of the proposed scheme, we have performed statistical analysis by calculating the histograms, the entropy, the correlations and differential analysis for the plain image and cipher image. Different images have been tested, and we have found that the intensity values are good.

Histogram Analysis

Histograms may reflect the distribution information of the pixel values of an image. An attacker can analyze the histograms of an encrypted image by using some attacking algorithms and statistical analysis on the encrypted image to get some useful information of the original image. It is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies how pixels in an image are distributed by plotting the number of pixels at each intensity

level.

In the experiments, the original image and its corresponding encrypted image and their histograms are shown in Figure (5) a. and b. The histogram of the original images illustrates how the pixels are distributed by graphing the number of pixels in every gray level. It is clear that the histogram of the encrypted image is nearly uniformly distributed, and significantly different from the respective histograms of the original image. Therefore, the encrypted image does not provide any trace to utilize any statistical attack on the proposed encryption of an image procedure, which makes statistical attacks difficult. The encrypted image histogram approximated uniform distribution; hence it is very different from the plain image histogram.

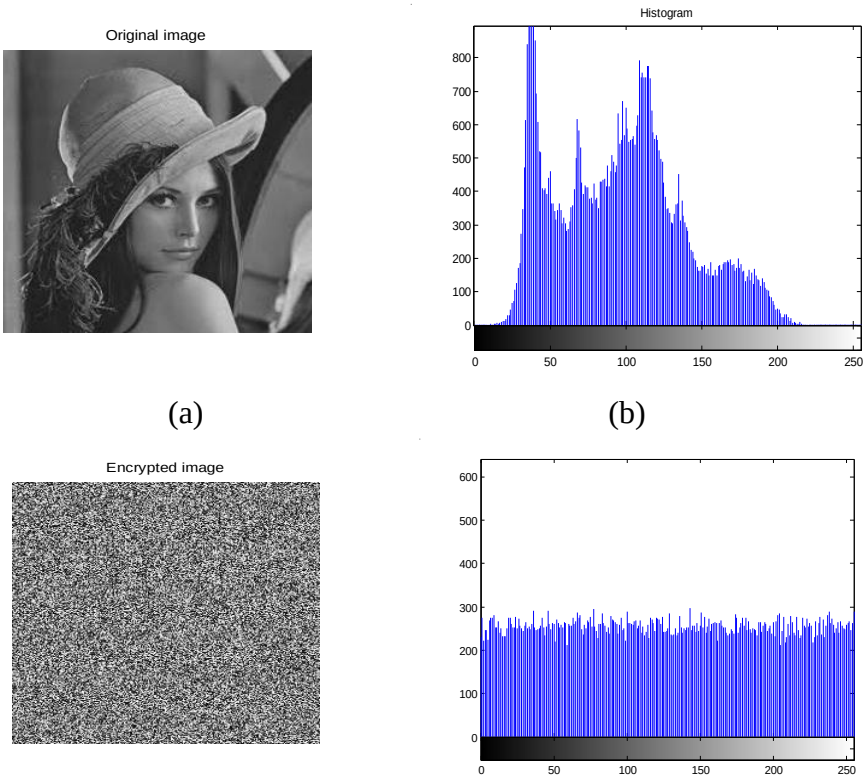
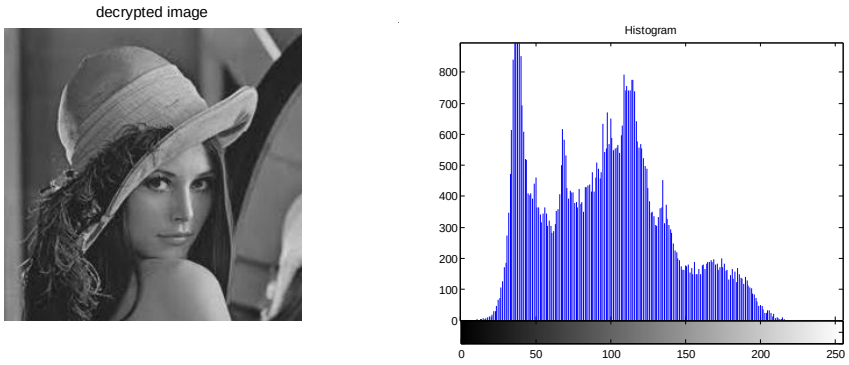


Figure 5: (a) Original Image, (b) Histogram of original Image, (c) Encrypted Image, (d) Histogram of Encrypted Image



(a) (b)

Figure (6): (a) Decrypted Image, (b) Histogram of Decrypted Image

Correlation Factor

In addition to the histogram analysis, we have also analyzed the correlation factor. We find the correlation between the original image and the decrypted image. If the correlation coefficient equals to zero or very near to zero, then the original image and its encryption are totally different i.e., the encryption image has no features and the highly independent from the original image. If the correlation coefficient equals to -1, this means encrypted image is negative of the original image. Equation to find the correlation factor is

correlation_factor = corr2(Y,I)

Information Entropy

Information Entropy of grayscale images

$$H_e = \sum_{k=0}^{G-1} P(k) \log_2 (P(k)) \quad (2)$$

Where:

H_e: entropy.

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

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

E = entropy(I)

E = entropy(I) returns E, a scalar value representing the entropy of grayscale image I. Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image. Entropy is defined as

-sum(p.*log2(p))

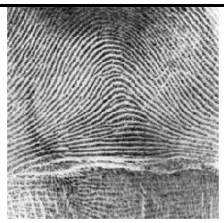
where p contains the histogram counts returned from imhist. By default, entropy uses two bins for logical arrays and 256 bins for uint8, uint16, or double arrays.

I be a multidimensional image. If I has more than two dimensions, the entropy function treats it as a multidimensional grayscale image and not as an RGB image.

Differential Analysis

In general, a desirable property for an encrypted image is about its sensitivity to small changes in plain image (e.g. modifying only one pixel). Opponent can create a small change in the input image to observe the changes in the result. By this scheme, the meaningful relationship between original image and the encrypted image can be simply found. If one small change in the plain image can cause a significant change in the cipher image, with respect to the diffusion and theconfusion, then the differential attack actually loses its efficiency and become practically useless. Three common measures have been used for differential analysis. PSNR, MSE, RMSE. PSNR stands for peak to signal ratio. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image. MSE stands for mean square error. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error. To compute the PSNR, the block first calculates the mean-squared error. RMSE stands for root mean square error. RMSE, is a matrix of root mean square errors (RMSE) associated with the output forecast array MeanForecast. That is, each element of MeanRMSE is the conditional standard deviation of the corresponding forecast error (that is, the standard error of the forecast) in the MeanForecast matrix.

Tested Images and Their Corresponding Entropy, Psnr Ratio and Correlation

Images	Entropy Value (original image)	Entropy Value (decrypted image)	PSNR Ratio	MSE	Correlation	RMSE	Elapsed Time
	7.6448	7.6448	11.1746	5.0006e+003	0.0480	70.7150	0.029809 Seconds.
	7.4722	7.4722	11.3096	4.8476e+003	-0.0490	69.6244	0.012554 Seconds.
	7.1047	7.1047	7.9550	1.0495e+004	-0.3501	102.4454	0.012548 Seconds

Conclusion

In this paper a simple and strong method has been proposed for image security using a combination of blocks based shifting and encryption techniques. The cases showed that the correlation was decreased when the proposed algorithm was applied to them before the Blowfish algorithm. Experimental results of the proposed technique showed that an inverse relationship exists between number of blocks and correlation, and a direct relationship between number of blocks and entropy. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy.

Reference

[1]. M. A. Bani Younes and Aman Jantan, "Image Encryption Using Block-Based Transformation Algorithm" IAENG, 35:1, IJCS_35_1_03, February 2008.

[2]. Kamlesh Gupta and Sanjay Silakari "A Choase Based Image Encryption Using Block-Based Transformation Algorithm" IJCNS, Dec 2009.

[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]. Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom

[5]. S.S.Maniccam, N.G. Bourbakis, "A Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), 1229-1245

[6]. Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China

[7]. Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm" Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

[8]. 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, p.127, 2006, Available: http://www. enformatika.org

[9]. I. Ozturk, I.Sogukpinar, "Analysis and comparison of image encryption algorithm," *Journal of transactions on engineering, computing and technology, December*, http://www.enformatika.org/.

[10]. Guosheng Gu, **"**An Enhanced Chaos Based Image Encryption Algorithm", *School of Computer Science and Engineering, South China University of Technology,* Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) © 2006 IEEE

[11]. Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, "Novel Image Encryption Algorithm Based on Hash Function", 2010 proposed a novel algorithm for image encryption based on SHA-512 hash function.

[12]. Kamlesh Gupta, Sanjay Silakari, " New Approach for FastColor Image Encryption Using Chaotic Map " *Journal of Information Security*, 2011, 2, PP 139-150 doi:10.4236/jis.2011.24014 October 2011 (http://www.SciRP. org/journal/jis)..

[13]. Sesha Pallavi Indrakanti and P.S.Avadhani, "Permutation based Image Encryption Technique", 2011.

[14]. Avi Dixit, Pratik Dhruve and Dahale Bhagwan, " Image encryption using permutation And rotational xor technique" Natarajan Meghanathan, et al. (Eds): SIPM, FCST, ITCA, WSE, ACSIT, CS & IT 06, pp. 01–09, 2012.

[15]. G.A.Sathishkumar, Srinivas Ramachandran and Dr.K.Bhoopathy Bagan, " Image Encryption Using Random Pixel Permutation by Chaotic Mapping", IEEE Symposium on Computers and Informatics,2012.

[16]. Mohammad Ali Bani Younes Department of computer Science National University of Ajloun, Irbid, Jordan, " Image Encryption Using Shuffling Technique" International Journal of Computer Science Research & Technology (IJCSRT) Vol. 1 Issue 3, August - 2013

[17]. Nidhi Sethi and Sandip Vijay, "Comparative Image Encryption Method Analysis Using New Transformed - Mapped Technique". Conference on Advances in Communication and Control Systems 2013

[18]. Blowfish, 12 December 2007, http://en.wikipedia.org/wiki/ Blowfish_%28cipher%29.

[19]. M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems, 2002.

[20]. C. Ratael, gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.

[21]. M. Sonka, V. Hlavac. and R. Boyle, "Digital image processing," in: image Processing, Analysis, and Machine Vision, 1998, 2nd ed. http://www.pws.com