International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 2 Issue 6 June 2016

An Advanced Approach of Partial Image Encryption Technique using Chaotic Map

Aditi Singh Rathore
M.Tech Scholar
SSSIST, Sehore
aditirthr@yahoo.co.in

Kailash Patidar
Head, Dept of CSE
SSSIST, Sehore
kailashpatidar123@gmail.com

Gajendra Singh Chandel
Asst. Prof., Dept of CSE
SSSIST, Sehore
gajendrasingh86@gmail.com

Abstract— **To protect image data, image encryption is an appropriate way. There is a unique feature of image and text data. The available encryption algorithms are good for text data. But it is not suitable for multimedia data because the characteristic of multimedia data is totally different from text data. All multimedia data has got a lot of redundancy but text data does not possess any redundancy. The pixel value of a location is highly correlated to values of its neighboring pixels. Like, a sound sample is correlated to its next sample and its previous samples. This correlation proves to be attack points to any standard encryption algorithm. Because they can predict the values of neighboring pixels or next sound sample by finding out pixel value at a location or one sound sample with reasonable accuracy. In this paper we recount some of the saga undergone by this field; we review the main achievements in the field of chaotic cryptography, starting with the definition of chaotic systems and their properties and the difficulties it has to outwit. According to their intrinsic dynamics, chaotic cryptosystems are classified depending on whether the system is discrete or continuous. Due to their simplicity and rapidity the discrete chaotic systems based on iterative maps have received a lot of attention. In this paper we have presented an advanced method of encryption using chaotic map.**

Keywords— **Chaotic Cryptosystem, Iterative Map, Encryption Algorithms, Neighboring pixels.**

I. INTRODUCTION

Image Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, however that authorized parties. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. As a result, different security techniques have been used to provide the required protection [5].

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 [6].

Image encryption techniques try to convert an image to another one that is hard to understand [6]. On the other hand, image decryption retrieves the original image from the encrypted one.

There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. They protect the secret information by converting the secret information to some unintelligible form using a key. By using a key, we protect the secret information by converting the secret information to some incomprehensible form. We get back information through encrypted information should be converted back to original information. On the Basis of key, the encryption algorithm can be classified into two categories. They are (i) Symmetric key encryption-This algorithm uses same key for both encryption and decryption and (ii) Asymmetric key encryption-This algorithms uses different keys for encryption and decryption [7].

1.1. Symmetric Encryption Method

Symmetric key cryptography is referred to by various other terms, such as secret key cryptography or private key cryptography .In this scheme only one key is used and the same key is used for both encryption and decryption of messages.

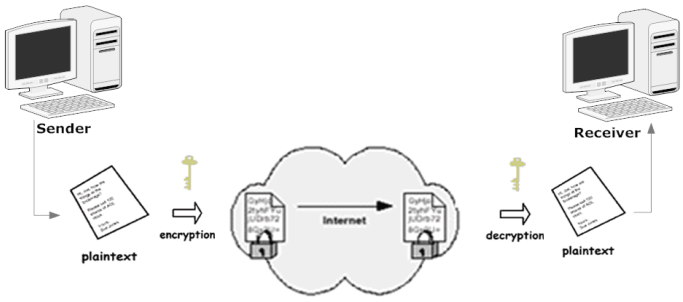


Figure 1.1 Symmetric Encryption Method.

Obviously, both the parties must agree upon the key before any transmission begins and nobody else should know about in figure 1.3 shows symmetric key cryptography works. Basically at the senders end, the key transforms the plain text message in to a cipher text form .At the receivers end, the same key is used to decrypt the encrypted message, thus deriving the original message out of it. The requirement is that both the parties have access to the secret key is one of the main drawbacks of symmetric key encryption, as compared to public-key encryption. There are different types of symmetric-key algorithms. Symmetric-key encryption can use either stream ciphers or block ciphers.

Common symmetric encryption algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA).

1.2 Asymmetric Encryption Method

In Asymmetric key cryptography, also called as public key cryptography two different keys (which form a key pair) are used .one key is used for encryption and only the other corresponding key must be used for decryption. No other key can decrypt the message not even the original key used for encryption .The beauty of this scheme is that every communicating party needs.Just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, she can communicate with anyone else.

There is a simple mathematical basis for this scheme. if you have an extremely large number that has only two factors ,which are prime number, you can generate a pair of key. One of the two keys is called as public key and the other is the private key. Algorithms that use public key encryption methods include RSA and Diffie-Hellman.

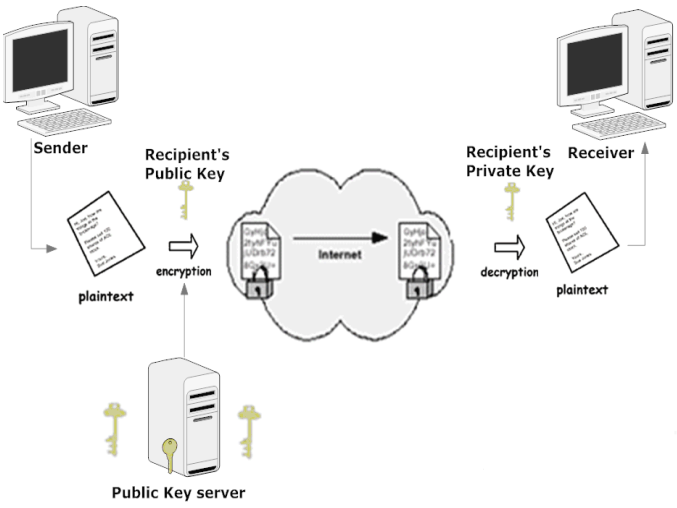


Figure 1.2 Asymmetric Encryption Method.

1.3 Symmetric-key Encryption VS. Asymmetric-key Encryption

Asymmetric algorithms [9] work much slowly then the symmetric algorithm, because they use a lot of complicated mathematics to perform their functions, which require more processing time. With public key, you can just transmit your public key to all of the people whom you need to communicate with, instead of keeping track of a unique for each one of them. The advantage and disadvantage of symmetric and Asymmetric key systems.

- Symmetric key is much faster than asymmetric systems. On the other side asymmetric key Works much more slowly.
- In symmetric key the security is dependent on the length of the key, if using a large key size the algorithm will be hard to break, because symmetric algorithms carry out relatively simplistic mathematical functions on the bits during the encryption and decryption processes.
- Symmetric key requires a secure mechanism to deliver keys properly. While, asymmetric key provide a better key distribution than symmetric systems.
- Symmetric key provides confidentiality but not authenticity, because the secret key is shard. However, asymmetric key can provide authentication and confidentiality.

Asymmetric key algorithm [7] has very higher computational costs than Symmetric key encryption algorithms which have comparatively lower cost. Asymmetric key algorithms are most time prohibitive for multimedia data. But the characteristic of multimedia data is totally different from text data. All multimedia data has got a lot of redundancy but text data does not possess any redundancy. The pixel value of a location is highly correlated to values of its neighboring pixels. Like, a sound sample is correlated to its next sample and its previous samples. This correlation proves to be attack points to any standard encryption algorithm. Because they can predict the values of neighboring pixels or next sound sample by finding out pixel value at a location or one sound sample with reasonable accuracy [7].

Nearly all the available encryption algorithms like .DES, AES, RSA and IDEA are used for text data. Act of them DES, AES, RSA and IDEA can achieve high security, it is not be suitable for images and videos encryption due to the intrinsic characters of images and videos. So we need some other technique for encrypt image and videos. Next section describes some image encryption techniques.

There are different-different types of image encryption methods. The image encryption algorithms can be classified into three major groups.

- Position Permutation Based Algorithm.
- Value Transformation Based Algorithm.
- Visual Transformation Based Algorithm.

1.1.1 Position Permutation Based Algorithm

In Position Permutation Based Algorithm, the given image is divided in to M × N pixel blocks, then each is rearranged in to a permuted image using a given permutation process .The Position Permutation Based Algorithm is use for the various techniques.

- The position permutation algorithm is use for mirror-like image encryption Method.

 The position permutation algorithm is use for chaotic image encryption Method.

1.1.2 Value Transformation Based Algorithm

Values Transformation Based algorithm is based on the technique in which the value of each pixel is change to some other value. The new value of pixel is evaluated by applying some algorithm on pixel .Basically algorithm is mathematical computation where we take input as a pixel value compute it, with some formulas and produce a new value for that pixel . Values transformation based algorithm works for pixel by pixel. Values transformation algorithm is used for different method.

 Digital Signatures method.
 Lossless Image Compression and Encryption Using SCAN.
 Image Cryptosystems techniques.
 Color Image Encryption Using Double Random Phase Encoding techniques.

1.1.3 Visual Transformation Based Algorithm

Visual Transformation is the process of transforming an input image of some format to an output image comprised of gray scale information. Input sources range from images taken in the visual spectrum (e.g. photographs) to non-visible images (e.g. x-rays). Visual representation (of an object or scene or person or and transform it in another visual expression.

Image Encryption has many advantages in field of Medical Application., Face Detection, Remote Sensing Microscope Image Processing, Computer Vision , Registration Techniques Image Compression Technique, Machine Vision Pattern Recognition, Restorations and Enhancements.

II. RELATED WORK

The analysis that has been done after the literature survey is that Image Encryption has many techniques that are broadly approved. But these techniques are mostly applied for particular applications. Thus there is a need for a technique that can be implemented on all types image file formats and on all types of applications.

The work called "A New Encryption Algorithm for Image Cryptosystems" By Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen proposed a [11] efficient cryptosystem for images, this Method is based on vector quantization that is one of the popular image compression techniques. This method is divided to carry out the work in two ways. One is to design a high security image cryptosystems and other is to reduce computational complexity of the encryption and decryption algorithm. In addition, the cryptosystems which they have used can compress image data and additionally speed up the encryption processes. The proposed cryptosystem is very suitable for real application to image storage and transmission. The characteristics of image cryptosystems and some criteria for evaluating the security of image cryptosystem.

In "A Technique for Image Encryption using Digital Signature" By Aloka Sinha , Kehar Singh [12] presented a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. The encoding of the image is completed using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver end, after the decryption of the image, the digital signature may be used to verify the authenticity of the image. Elaborated simulations have been carried out to test the encryption technique. An optical correlator, in either the JTC or the Vander Lugt geometry, or a digital correlation technique, will be used to verify the authenticity of the decrypted image. This encryption technique provides three layers of security. Within the first step, an error control code is used which is determined in time period, based on the size of the input image. Without the data of the particular error control code, it is very difficult to get the original image and tamper with it. The dimension of the image also changes due to the added redundancy. This poses an additional problem to decrypt the image. Also, the digital signature is added to the encoded image in a specific manner. This information can be protected to make the system more secure. At the receiver end, the digital signature can be used to verify the authenticity of the transmitted image. This clearly solves the problem of image recovery and image degradation, unlike the previous methods. The advantage is that there is no need to transmit the keys separately.

In "A New Digital Image Scrambling Method Based on Fibonacci number" By Jiancheng Zou , Rabab K. Ward , Dongxu Qi [13] presented a method for new digital image scrambling method based on Fibonacci numbers. The standardization and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: Encoding and decoding is very simple and they can be applied in real-time situations. The scrambling effect is very sensible, the data of the image is re-distributed randomly across the whole image. The method can endure common image attacks, like compression, noise and loss of data packet .They developed a method to study video scrambling and probe corresponding embedding algorithms for digital watermarks.

The work called "Image Encryption Using Block-Based Transformation Algorithm" By Mohammad Ali Bani Younes and Aman Jantan [14] knowledge about block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blow fish. The initial image was divided into blocks, that were rearranged into a transformed image using a transformation algorithm presented here, then the transformed image was encrypted using the Blowfish algorithm. The results also show that correlation between image elements was significantly decreased by using the proposed technique. The results additionally show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. The proposed technique show's that an inverse relationship exists between number of blocks and correlation, and an immediate relationship between number of blocks and entropy. When compared to several normally used algorithms.

In "A Random Scrambling Method for Digital Image Encryption: Comparison with the Technique Based on Arnold Transform" By Q. D. Sun, W. X. Ma, W. Y. Yan, H. Dai [15]

proposed to expand the use of direct methods in real-time technique a simple one-dimensional random scrambling method and applied it to image encryption. First, they tend to transform the image into a one-dimensional vector. So they did the one-dimensional random scrambling for this vector. Finally, they tend to did reverse transformation on this scrambled vector and got the encrypted image. Compared with Arnold transform, this technique is incredibly straightforward for realizing by software or hardware. It doesn't need iterative computation, and might bring an improved result once being executed one time or twice. The experimental results show the algorithm is effective and has better efficiency and steady scrambling degree than Arnold transform. Additionally the scrambled image has no security problem of periodically.

In " Image Encryption Based on Chaotic Maps" By Jiri Fridrich [16] proposed image encryption based on chaotic 2D maps on a torus or on a square to create new symmetric block encryption schemes. The schemes are unit particularly useful for encryption of large amounts of data, like digital pictures or electronic databases. A chaotic map is initial generalized by introducing parameters and then discretized to a finite square lattice of points which represent pixels or some other data items. Though the discretized map is a permutation and thus cannot be chaotic, it shares certain sensitivity and combining properties with its continuous counterpart as long as the number of iterations remains small. It's shown that for the 2D baker map the permutations behave as typical random permutations. The discretized map is additional extended to 3D and composed with a simple diffusion mechanism. As a result, a block product encryption scheme is obtained. To encrypt an N×N image, the ciphering map is iteratively applied to the image.

In A new chaotic key-based design for image encryption and decryption By J.Cheng, J.1, Guo develope [17] an image encryption and decryption algorithm and its VLSI designed are proposed. Consistent with a chaotic binary sequence, the gray level of every pixel is XORed or XNORed bit-by-bit to one of the two predetermined keys. Its features are as follows: low computational complexity, high security, and no distortion. So as to implement the algorithm, its VLSI design with low hardware price, high computing speed, and high hardware utilization efficiency is also designed. Moreover, the designer of integrating the scheme with MPEG2 is proposed.

2.8 A Survey of Digital Image Scrambling Techniques

By H. Zhao, W. Y. Wen [15] presented a survey of the Internet technique; communication privacy and the information security are attracting a lot of attention recently. The development of image encryption techniques is surveyed.Some techniques, like pixel permutation technique, image secret segmentation technique, image secret sharing technique, and trendy cryptography mechanism-based and chaotic dynamics-based image encryption techniques.

2.9 Image Scrambling Based on Bit Shuffling of Pixels

By Z. J. Tang, X. Lu, W. M. Wei, S. Z. Wang, et al [19] proposed a method to solve a problem image-scrambling scheme based on bit shuffling of individual pixels, which doesn't need reiterative computation .Bits of each pixel are divided into even and odd groups .Those in the even group are swapped so that the original higher bits become lower and vice versa, while bits within the odd group are exchanged with the odd bits in an uncorrelated pixel with a certain offset from the current pixel. The latter is done to reduce the probability of pixel-value being unchanged after bit shuffling.

"Image Encryption Using Affine Transform and XOR Operation" By Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh and Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar [7] consider the problem of image encryption using affine transform and XOR Operation a new location transformation based encryption technique. They redistribute the pixel values to different location using affine transform technique with four 8-bit keys. The remodeled image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The total key size utilized in our algorithm is 64 bit which proves to be strong enough. The experimental results proved that after the affine transform the correlation between pixel values was significantly decreased. The scrambling operation is done using affine cipher techniques that breaks the correlations of the neighboring pixels and make the image unidentifiable .The XOR operation then change the pixel values making the image every meaningless. The encryption and decryption process are simple enough to be carried out on any large sized image or video files, but provides enough security.

III. PROPOSED WORK

Image Encryption

Image Encryption process of a given image is divided in to the following steps.

Input Gray Scale Image

This phase of Image encryption process starts by selecting a gray scale image X of N×N pixel size with L bit per pixel, which is to be converted into encrypted form before transmitting to the other end.

Image Decomposition

Gray level of a pixel of an image is composed by multiple bits, their all bits in same level creates a binary plane ,called bit plane .second step of our image encryption method based on decomposition of the input gray image X into B*B blocks . Since every block is form by B*B pixels. Hance length(L) and width(W) must be divisible by B and when we decompose it, we can get $L*W/B*B$ blocks in image which is described by $B(i,j)$ .where i and j denotes the block number.

Decomposition of image X into Block of B*B is computed by the formula expressed as below.

$$Blk(i,j) = X(\ (i-1)*B+1:i*B,\ (j-1)*B+1:i*B\ )$$

for $1 \le i \le L/B$ and $1 \le j \le W/B$

Where *Blk*(i,j) is block location, X is input image L and W is length and Width of image and B is Block size . in out method we used block size of 4*4 ,8*8, 16*16, upto L/2*W/2.

Scrambling by using Arnold transforms

Since pixel of image are highly correlated to their neighboring pixels. Due to this strong correlation any pixel can be practically predicted from a value of its neighbors. So there is a need of a technique that can shuffle the pixels to reduce the correlation between the neighbor pixels. Pixel Scrambling do this thing to overcome the problem. So Next step is to applying pixel Scrambling by using Arnold transform.
Shuffles the every block Blk(i,j) of gray scale image X with Arnold's Transformation with the help of equation (listed below) up to the Arnold's key which is calculated on the basis of size of the image.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \text{.....}$$

Some conditions for the map is that p and q are positive integers and
=1, which makes the map area-preserving. Here N is the size of the image. in our system we choose the value of p and q is equal to 1.so our cat map would be:
A Reverse process of encrypted image is called as image decryption. Decryption is also systematic or step-by-step procedure to convert cipher image back into original image. The decryption process is divided into different steps.
Input encrypted image
The input is a gray scale encrypted image Y of N × N pixel size with L bit per pixel. Which is to be converted in to its original form as before sending.

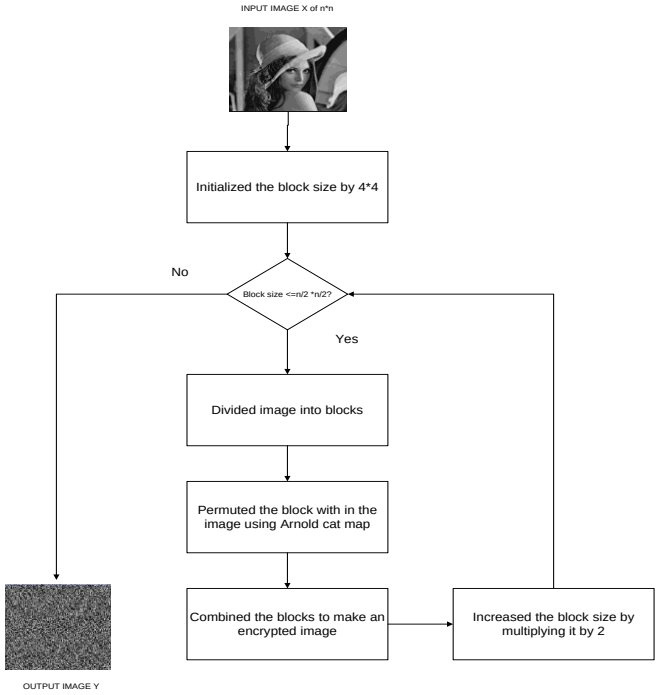


Figure 3.1 : Flowchart of proposed algorithm for embedding process and extracting process

Decomposition of Encrypted Image
Decomposition of the Encrypted image Y into Block of B*B is computed by the same formula used at encryption time and expressed as below.

$$B(i,j) = X(\ (i-1)*B+1:i*B,\ (j-1)*B+1:i*B\ )$$

.....

for $1 \le i \le L/B$ and $1 \le j \le W/B$

Where B(i,j) is block location, X is input image L and W is length and Width of image and B is Block size . in out method we used block size of 4*4 ,8*8, 16*16, upto L/2*W/2.

Anti Scrambling by using inverse Arnold transform
The Next step is to applying anti scrambling on every block of encrypted image Y . The decryption is achieved by applying Inverse Arnold transformation to the encrypted image. The corresponding two dimensional Inverse Arnold transformation matrix is as follows. After antiscrambling has been done by using Anti- Arnold's Transformation, the resultant image is our desired image X .

IV. RESULTS

Evaluation Metrics

The quality of the encrypted image is measured by calculation of certain evaluation measurement metrics. These metrics gives the comparison ratio between the original image and the modified image. The quality may be assessed on the basis of these values. The metrics used in this paper are as follows: Mean Square error (MSE),peak signal- to-noise ratio (PSNR),

Number Of Pixel Change Rate(NPCR),Unified Average Change Intensity(UACI),Universal Image Quality index(UIQ).

Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE [40] can be defined as the measure of average of the squares of the difference between the intensities of the Encrypted image and the original image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-C'(i,j))^2$$

Where C(i, j) is the original image and C' (i, j) is the encrypted image. A large value for MSE means that the image is of poor quality.

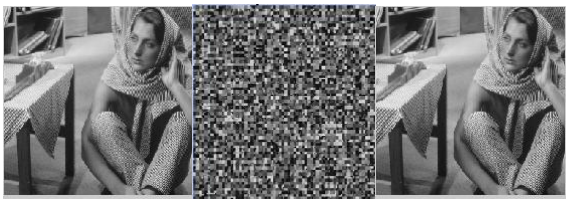
Peak signal to noise ratio (PSNR)

The PSNR [40] depicts the measure of reconstruction of the encrypted image. This metric is used for discriminating between the cover and encrypted image. The easy computation is the advantage of this measure. It is formulated as:

$$PSNR = 20\log 255^2 / MSE$$

A low value of PSNR shows that the constructed image is of poor quality.

To demonstrated our method we used the gray image Lena as Shown in Figure 2 (a), The result after encryption is shown as in Figure 2(b). the block shuffling effect is very good and the encrypted image is very like the salt and paper noise. Figure 2 (c) is the result of decryption, comparing with original image as shown in Figure2(a), there is nothing to be lost.



(a) (b) (c)

Figure 2 Results after image encryption and Decryption system for Lena.

Figure 2 (a) is the histogram of original image Lena. Figure 2 (b)is the histogram of the encrypted image permuted by the proposed method .fig 3 shows that the histogram of the both image are same so we can say that in encrypted image all the gray value remain same only it permuted within the image.

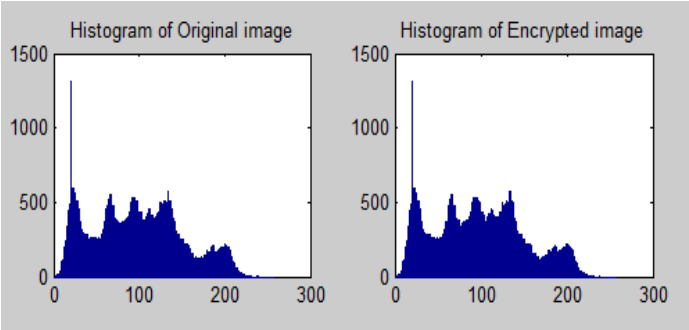


Fig. 3 Histograms of the image Encryption and Decryption system for Lena

Table 1 MSE and PSNR Calculation of proposed method on different images.

Image Name	MSE	PSNR
Lena	5575.067	21.3366
Baboon	3589.8239	25.1601
Fish	9851.0722	16.3919
Boat	3654.9044	25.0041
Man	6754.8723	19.6693
Baby in womb	5946.1824	20.7768
Jet	1943.6871	30.4891
Airplane	4036.7759	24.1409

	Proposed Method		Method[2]	
Parameter / Image	MSE	PSNR	MSE	PSNR
Leena	**5575.067**	**21.3366**	106.5086	27.8570
Baby in Womb	**5946.1824**	**20.7768**	47.1727	31.3939

Table 2: Comparison between proposed method and method in with respect to different quality parameters.

V. CONCLUSION

We proposed a symmetric key image encryption technique that first scramble the locations of the pixels using four 8-bit sub keys and then encrypt the pixel values by XOR the selected 8-bit key. The scrambling operation is done using one dimensional Vector techniques that breaks the correlations of the neighboring pixels and make the image unidentifiable. The XOR operation then change the pixel values making the image very meaningless. The application of keys so that the security level is further increased. The encryption and decryption process are simple enough to be carried out on any large sized image or video files, but provides enough security. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the gray image based data as well as in storage. The proposed encryption algorithm can ensure multiple criteria such as lossless, minimum distortion, maximum performance and maximum speed. The proposed encryption method in this study has been tested on different

gray images and showed good results. The security level of image encryption and decryption is further increased.
We have designed our image Encryption and Decryption System using Matlab 7.8.0 to accomplish this research work. We have evaluated our proposed image Encryption and Decryption System on gray Scale image. The experimental result proved that after Histogram Deviation and Correlation Coefficient between pixel values was significantly decreased.

Future Work

We present a two phase Image Encryption and Decryption algorithm by using Random Scrambling and X-OR Operation of the only for gray scale image, This is based on Shuffled the image pixels and correlation between adjacent pixels of image using Random Scrambling and encrypting the resulting image using X-OR operation Hence, our method can be used to image encryption and decryption of different types of gray scale image. we will future investigate in our proposed algorithm also can be applying to color image.

VI. REFERENCES

[1] Michael Eziashi Osadebey , " Integrated Content-Based Image retrieval Using Texture, Shape And Spatial Information ", Master Thesis Report in Media Signal Processing, pp. 3-5 February 2006.
[2] Image, Richard E. Woods, "Digital Image Processing", Prentice Hall Processing in IDL", IDL Publication Version 7.1 May 2009.
[3] National Institute of Standards and Technology, "Data Encryption Standard (DES)," http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.
[4] National Institute of Standards and Technology, "Advanced Encryption Standards (AES)," http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[5] H. El-din. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption quality analysis of the RC5 block cipher algorithm for digital images", Menoufia University, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia-32952, Egypt, 2006.
[6] Li. Shujun, X. Zheng "Cryptanalysis of a chaotic image encryption method", Inst. of Image Process. Xi'an Jiaotong Univ, Shaanxi, This paper appears in: Circuits and Systems, ISCAS, IEEE International Symposium on Publication, Vol. 2, and page: 708,711, 2002.
[7] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh and Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar, "Image Encryption Using Affine Transform and XOR Operation," IEEE International Conference on Signal Processing, Communication Computing and Networking Technology, 2011.
[8] P.Vijayram Reddy, K.Venkatesh Sharma and Dr.P. Mall sham, P.Radha Devi, "Secure Image Transmission through Unreliable Channels", IJCSE , Vol. 02, No. 06, 2053-2058, 2010.
[9] M. Abomhara, Omar Zakaria, Othman O. Khalifa ,"An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 1793-8201, February, 2010.
[10] San Diego, California, USA "Applications of Digital Image Processing", Part of the SPIE International Symposium on Optical Engineering and Applications, 10-14 August 2008.
[11] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A New Encryption Algorithm for Image Cryptosystems", The Journal of system and Software 58, 83-91, 2001.
[12] Aloka Sinha , Kehar Singh, "A Technique for Image Encryption using Digital Signature", Optics Communications,Vol-218 ,229-234 ,2003.
[13] Jiancheng Zou , Rabab K. Ward , Dongxu Qi, "A New Digital Image Scrambling Method Based on Fibonacci Number", Proceeding of the IEEE Inter Symposium On Circuits and Systems, Vancouver ,Canada ,Vol .03 , PP .965-968 , 2004.
[14] Mohammad Ali Bani Younes and Aman Jantan ," Image Encryption Using Block-Based Transformation Algorithm", lAENG International Journal of Computer Science, 35: I, 2008.
[15] Q. D. Sun, W. X. Ma, W. Y. Yan, H. Dai , "A Random Scrambling Method for Digital Image Encryption: Comparison with the Technique Based on Arnold Transform", Journal of Shanghai Second Polytechnic University, vol. 25, no. 3, pp. 159-163, 2008.
[16] Jiri Fridrich, "Image Encryption Based on Chaotic Maps", Proceeding of IEEE Conference On Systems, Man, and Cybernetics, pp. 1 105-II 10, 1997.
[17] J. Cheng; J.1. Guo, "A new chaotic key-based design for image encryption and decryption", IEEE International Symposium on Circuits and Systems, vol A, no. 4, pp. 49 - 52, May. 2000.
[18] H. Zhao, W. Y. Wen, "A Survey of Digital Image Scrambling Techniques," Fujian Compute, No. 12, pp. 10, 12. 2007.
[19] Z. J. Tang, X. Lu, W. M. Wei, S. Z. Wang, et al, "Image Scrambling Based on Bit Shuffling of Pixels," Journal of Optoelectronics Laser, vol. 18, no. 12, pp. 1486- 1488, 1495, 2007.
[20] Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma, "Image Encryption Based on Bit-plane Decomposition and Random Scrambling", Journal of Shanghai Second Polytechnic University , vol. 09 , 2012.
[21] W. Xiao, J. Zhang and W. Wu, " A Watermarking Algorithm Based on Chaotic Encryption" , Proceedings of IEEE TENCON, pp. 545-548, 2002.
[22] S. Li and X. Zheng, "On The Security of An Image Encryption Method", In Proceedings IEEE Int. Conference on Image Processing (ICIP), Vol. 2, pp. 925 928,2002.
[23] John Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[24] M. Ashtiyani, P. M. Birgani, and H. M. Hosseini, "Chaos-Based Medical Image Encryption Using Symmetric Cryptography", 3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA), pp. 1-5, 7-11 April 2008.
[25] L. Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", Proceedings of the 4th ACM International Conference on Multimedia, pp. 219 229, 1996.
[26] W. Zheng, M. Luttrell, J. Wen, M. Severa and W. Jin, "A Format Complain Configurable Encryption Framework for Access Control of Multimedia Proceedings", International Workshop on Multimedia Signal Processing, pp. 435-440, 2001.
[27] R. Karri, K. Wu, P. Mishra, and Y. Kim, " Concurrent Error Detection Schemes for Fault-Based Side-Channel Cryptanalysis of Symmetric Block Ciphers", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 21, No. 12, pp. 1509- 1517, Dec. 2002.
[28] Z. H. Guan, F. Huang and W. Guan, " Chaos-Based Image Encryption Algorithm", Physics Letters A, Vol. 346, No. 1-3, pp. 153-157, 10 October 2005.
[29] H. Gao, Y. Zhang, S. Liang and D. Li, "A New Chaotic Algorithm for Image Encryption", Chaos, Solitons & Fractals, Vol. 29, No. 2, pp. 393-399 , July 2006.
[30] X. Li, J. Knipe, and H. Cheng, ," Image Compression and Encryption Using Tree Structures" , Pattern Recognition Letters, Vol. 18, No. 8, pp. 2439 2451, 1997.
[31] J. I. Guo, J. C. Yen, and J. C. Yeh, "The Design and Realization of A New Hierarchical Chaotic Image Encryption Algorithm", In Proceedings Int. Symposium on Communications (ISCOM 99), pp. 210 214, 1999.
[32] L. Zhang, X. Liao and X. Wang, "An Image Encryption Approach Based on Chaotic Maps ", Chaos, Solitons & Fractals, Vol. 24, No. 3, pp. 759-765, May 2005.
[33] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image Encryption algorithm and its VLSI architecture",Pattern Recogition and image Analysis,Vol.10,no.2pp.236-247,2000.
[34] Jui-Cheng Yen and J. I. Guo, "A New Chaotic Image Encryption Algorithm", Proc.National Symposium on Telecommunications, pp.358-362, Dec, 1998.
[35] S.S.Maniccam, N.G. Bourbakis, "Lossless image compression and encryption using SCAN", Pattern Recognition 34, 1229-1245, 2001.
[36] Shuqun Zhang and Mohammed A Karim, "Color image encryption using double random phase encoding", Microwave And Optical Technology Letters Vol. 21, No. 5, 318-322, June 5 1999.
[37] Zhenjun Tang and Xianquan Zhang, "Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies", Department of Computer Science, Guangxi Normal University, Journal of multimedia, Vol. 6, NO. 2, APRIL 2011.
[38] T.Ashok kumar, S. Priya and M.G. Mini, "Optic disc localization in ocular fundus images", IJCA Proc. of ICVCI (5) International Conference ,pp. 20-22, India 2011.
[39] S. Priya , T. Ashok Kumar and Varghese Paul , "Fabric Defect Detection using Bitplane Decomposition and Mathematical Morphology", European Journal of Scientific Research ISSN 1450-216X Vol.80 No.3 , pp.322-330 , 2012.

[40] Qiudong Sun, Ping Guan, Yongping Qiu, Yunfeng Xue, "A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling", IEEE, 2012.
[41] D E Newton, "Encyclopedia of Cryptology", ABC-CLIO Inc, California, USA, 1997.
[42] Ibrahim Fathy El-Ashry , "Digital Image Encryption ", Master Thesis Report in Menofia University, 2010 .