Image Encryption Using Random Scrambling and XOR Operation.

Rinki Pakshwar [1], Asst Prof. Vijay Kumar Trivedi [2], Prof.& HOD Vineet Richhariya [3]

[1]*Dept. of Computer Science*
Lakshmi Narain College of Technology, Bhopal(India)

[2]*Asst. Prof. Dept. of Computer Science*
Lakshmi Narain College of Technology, Bhopal(India)

[3] *Prof. & HOD Dept. of Computer Science*
Lakshmi Narain College of Technology, Bhopal(India)

***Abstract* -This paper aims at improving the level of security and secrecy provided by the digital gray scale image encryption. The image encryption and decryption algorithm is designed and implemented to provide confidentiality and security in transmission of the image based data as well as in storage. Since the pixel of image is 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. Hence we used Scrambling technique that Shuffles the pixels of image .This Scrambled image is called transformed image. The transformed 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 size of key in our algorithm is 32 bit long which proves to be strong enough. The proposed encryption algorithm in this study has been tested on some Gray Scale images and showed good results.**

Keywords-Image encryption, image reconstruction, Bit-Plane Decomposition, Random Scrambling X-OR.

I. INTRODUCTION

Image Encryption is the process of encoding messages 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 [1]. 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 [2].

Image encryption techniques try to convert an image to another one that is hard to understand [2]. 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 [3]. Asymmetric key algorithm [3] 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 [3].

Nearly all the available encryption algorithms like .DES, AES [4], RSA [4] and IDEA [4] are used for text data. Act of them DES [4], AES[4], RSA[4] and IDEA[4] can achieve high security, it is not be suitable for images and videos encryption

IJERT

due to the intrinsic characters of images and videos .So we need some other technique for encrypt image and videos. For large data size and high redundancy, encryption special requirements and different encryption algorithms [5, 6] is needed. The image encryption algorithms divided into three major groups: (i) position permutation based algorithm [7, 8], (ii) value transformation based algorithm [9, 10, 11, 12] (iii) visual transformation based algorithm [7].several encryption algorithms are based on chaotic maps. In this paper, we propose image encryption using Random Scrambling and XOR operation . Affine transform that is based on shuffling the image pixels and they encrypting the resulting image using XOR operation. We used 32 bit key that is good for practical purposes.

II. BIT-PLANEDECOMPOSITIONAND RECONSTRUCTION

A. Bit-plane Decomposition of Image

The gray level of every pixel of an image explained by multi-bits, in which all bits the same in the level are created of a binary plane, so it is called bit-plane [13]. Let X is an M × N digital image with L bits. After decomposing it, we can get L bit-plane images, which are described by $X^{(l)}$ (l = 0, 1,………,1). Let $B^{(l)}(\cdot)$ be the operator of bit-plane decomposition, then the decomposition of l^{th} bit-plane is expressed by.

$$X^{(l)} = B^{(l)}(X)$$

If X (*m*, *n*) is a pixel located at (*m* , *n*), then the l^{th} bit of *X* (*m* , *n*) is:

$$X^{(l)}(m,n) = B^{(l)} = \begin{Bmatrix} 1 \ \ if \left(x(m,n)/2^{(l)} \right) \bmod 2 = 1 \\ 0 \qquad\qquad\qquad otherwise \end{Bmatrix}$$

B. Reconstruction of Image.

Suppose $B^{-1(l)}(\cdot)$ are the image reconstruction operator, we have,

$$X_T = \sum_{l=0}^{L-1} B^{-1(l)}\left(X^{(l)}\right)$$

For a pixel at position (*m*, *n*), we also have

$$X_T(m,n) = \sum_{l=0}^{L-1} 2^{(l)} \times X^{(l)}(m,n)$$

C. Random Scrambling and Anti-scrambling of Image.

The random scrambling method and anti-scrambling gives in the reference [14] is easy as well as, more stable and safer than the classical method – Arnold transforms [15].We describe it our algorithm .The method transforms an *M*×*N* digital image *X* into a 1-D vector *V*. Then it uses a random natural number generator and select a couple of different seeds to produce two random sequences R_S and R_D with the same length as *V*, and scrambles the 1-D vector *V* as follows [14]:

$$V\left(R_S(i)\right) \leftrightarrow V\left(R_D(i)\right) i = 0,1,\ldots,(M \times N - 1)$$

Where the sign " ↔" denotes the interchanging of two relevant elements in sequences $\boldsymbol{R}_S$ and $\boldsymbol{R}_D$.

Due to the interchanging rule is reversible. There for, when two random sequences $\boldsymbol{R}_S$ and $\boldsymbol{R}_D$ in anti-scrambling are same as that of in scrambling, the anti-scrambling can also be completed by the rule , namely, equation is the rule of anti-scrambling as well as the rule of scrambling.

D. Bit-plane Scrambling and Anti-scrambling.

For bit-plane scrambling and anti-scrambling, in which we transform the bit-plane image $\boldsymbol{X}^{(l)}$ into a 1-D vector $\boldsymbol{V}^{(l)}$ firstly. Relative to Eq. 5, the rule of bit-plane scrambling and anti-scrambling will be rearrange as.

$$V^{(l)}\left(R_S(i)\right) \leftrightarrow V^{(l)}\left(R_D(i)\right) i = 0,1,\ldots.(M \times N - 1); l = 0,1,\ldots.L-1$$

III . PROPOSED ALGORITHM

Algorithm 1: Encryption Algorithm at Sender Side

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

Input: A Gray scale image X.
Output: Cipher image X_C.

1. Input a gray scale image X of M × N size with L bits per pixel.
2. Then we decomposed a gray image into *l* bit-plane images.

$$X^{(l)} = B^{(l)}(X) \text{……..(1)}$$

If *X (m, n)* is a pixel located at *(m, n),* then the l^{th} bit of *X (m,n)* is:

$$X^{(l)}(m,n) = B^{(l)} = \begin{Bmatrix} 1 \ \ if \left(x(m,n)/2^{(l)} \right) \bmod 2 = 1 \\ 0 \qquad\qquad\qquad otherwise \end{Bmatrix}$$

.. …………(2)

3. We transform the bit-plane image $X^{(l)}$ into a 1-D vector $V^{(l)}$.

IJERT

4. Then it uses a random natural number generator and chooses a couple of different seeds to produce two random sequences R_S and R_D with the same length as V. and scrambles the 1-D vector V.

$$V\left(R_S\left(i\right)\right) \leftrightarrow V\left(R_D\left(i\right)\right) i = 0,1,...,\left(M \times N - 1\right)$$

………(3)

We merged the scrambled bit-plane images according to their original levels on bit-planes and gained a Transformed image $X_{T.}$

$$X_T = \sum_{l=0}^{L-1} B^{-1(l)}\left(X^{(l)}\right)$$

For a pixel at position (*m*,*n*) ,we also have

$$X_T\left(m,n\right) = \sum_{l=0}^{L-1} 2^{(l)} \times X^{(l)}\left(m,n\right)$$

……….(4)

5. The transformed image then divided into 2 pixels × 2 pixels blocks.
6. Each block $B_{i,j}$ of X_T is encrypted using XOR operation by four 8-bit keys (K_1,K_2,K_3,K_4).

$$P'_{1.1=}P_{1.1} \oplus K_1$$

$$P'_{1.2=}P_{1.2} \oplus K2 ....(5)$$

$$P'_{2.1=}P_{2.1} \oplus K_3$$

$$P'_{2.2=}P_{2.2} \oplus K_4$$

Where $P_{i,j}$ is the pixel value at i^{th} and j^{th} location in block resulted image called by cipher image X_C is ready to be sent to receiver site.

7. End**.**

IJERT

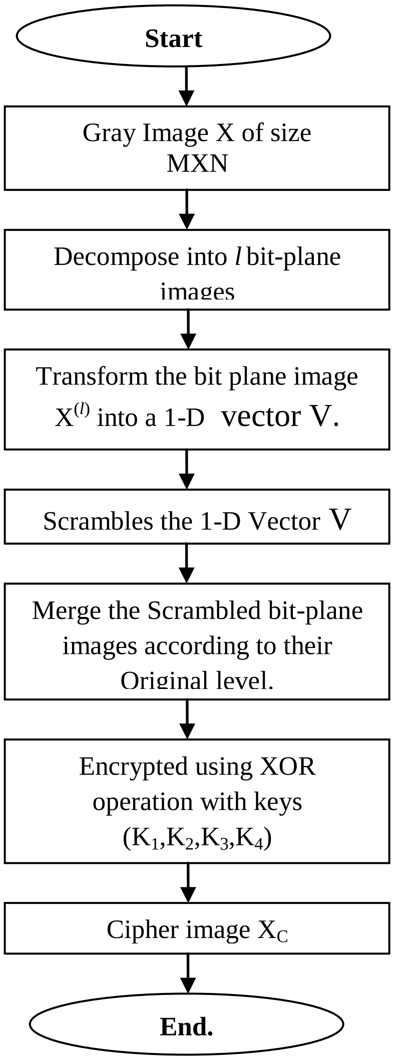

Start
Gray Image X of size MXN
Decompose into *l* bit-plane images
Transform the bit plane image $X^{(l)}$ into a 1-D vector V.
Scrambles the 1-D Vector V
Merge the Scrambled bit-plane images according to their Original level.
Encrypted using XOR operation with keys (K_1,K_2,K_3,K_4)
Cipher image X_C
End.

Figure 1: Flowchart of Encryption Algorithm at Sender side.

Algorithm 2: Decryption Algorithm at Receiver Side:

The input is a gray scale encrypted image X_C of *M* × *N* pixel size with *L* bit per pixel.Which is to be converted in to its original form as before sending.

Input: Cipher image $X_{C.}$

Output: A Gray scale image X.

1. For Decryption, the cipher image X_C is first divided into 2 pixels × 2 pixels blocks.
2. Each pixel of every block is decrypted using XOR operation with keys (K_1, K_2, K_3, K_4) .

$$\text{Decrypt } P'_{1\cdot 1} \text{ as } P_{1.1}=P'_{1.1}\oplus K_1$$

$$\text{Decrypt } P'_{1\cdot 2} \text{ as } P_{1.2}=P'_{1.2}\oplus K_2 \quad \text{.....(6)}$$

$$\text{Decrypt } P'_{2.1} \text{ as } P2.1=P'_{2.1}\oplus K_3$$

$$\text{Decrypt } P'_{2.2} \text{ as } P_{2.2}=P'_{2.2}\oplus K_4$$

3. The decrypted image X_D is then decomposed again into *l* bit-plane images by using the formula used in eq. (2).
4. We then transform the bit-plane image $X_D^{(l)}$ into a 1-D vector $V^{(l)}$ .Then we use again random natural number generator and use the same a couple of seeds used at encryption time to produce same random sequences R_S and R_D with the same length as V. and antiscrambles the 1-D vector V .

$$V^{(l)}\left(R_S\left(i\right)\right)\leftrightarrow V^{(l)}\left(R_D\left(i\right)\right) i=0,1,....\left(M\times N-1\right); l=0,1,....L-1 \quad \text{...........(7)}$$

5. Lastly, we merged the antiscrambled bit-plane images according to their original levels on bit-planes and gained an Original image X.
6. End.

IJERT

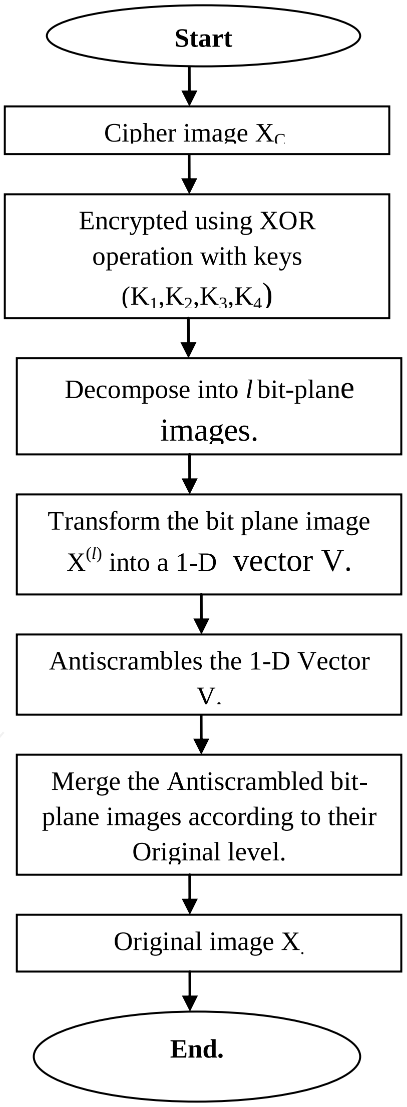
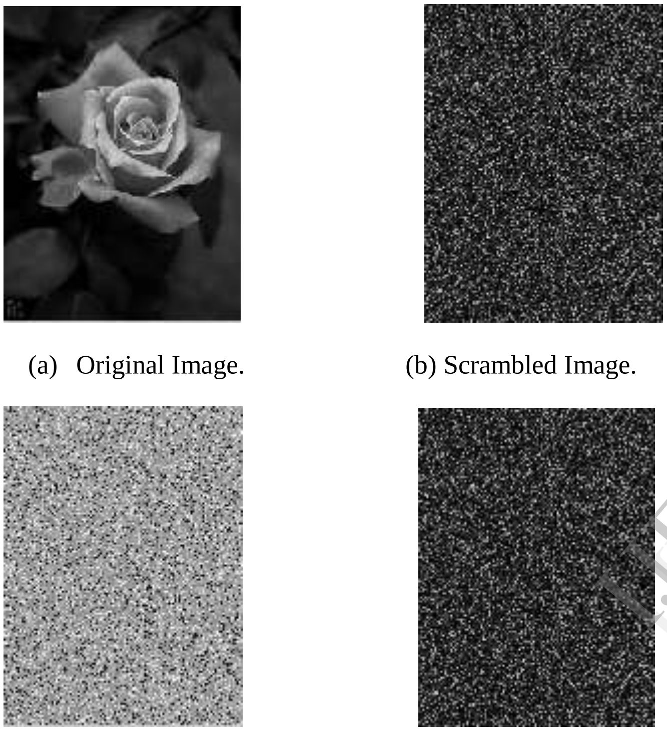

Start
Cipher image X_C
Encrypted using XOR operation with keys (K_1,K_2,K_3,K_4)
Decompose into *l* bit-plane images.
Transform the bit plane image $X^{(l)}$ into a 1-D vector V.
Antiscrambles the 1-D Vector V.
Merge the Antiscrambled bit-plane images according to their Original level.
Original image X.
End.

Figure 2: Flowchart of Decryption Algorithm at Receiver side.

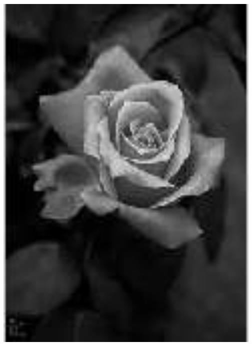
IV. SIMULATION RESULTS

Our Proposal we implement our algorithm in Mat lab 7.8.0 running on windows XP platform. we have used Seven 8- bit gray scale image of size 256×256.One such image of 8-bit gray image of Rose flower of size 256×256 is shown in figure 3. The encrypting process of the Image by taking the initial condition, the encrypted image hides the totality of the information contained therein, as seen in figure 3(a) and figure 3(c), Here the random scrambling and X-OR operation condition is treated as the key for the encryption of the image. The distribution of intensities of the encrypted image varies when changing the value of the initial condition. When the decryption process is done with the same initial condition, we recover the original image, as shown in figure 3(e).If the keys used in the decryption process are equal to the keys used in the encryption process, the image will be recovered. Shown figure 3 in image Encryption and Decryption.



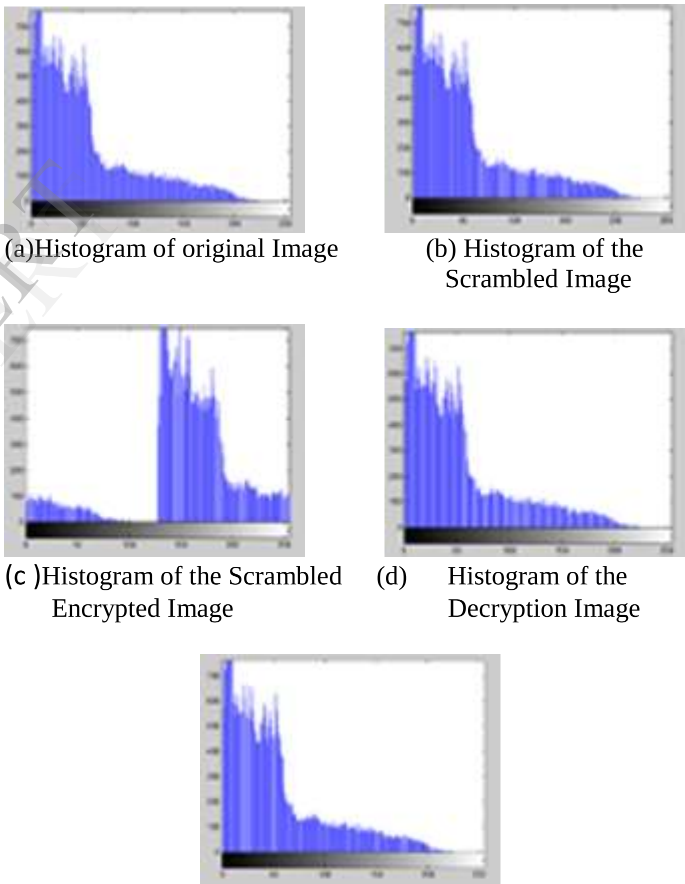
(a) Original Image. (b) Scrambled Image.

(c) Scrambled Encrypted Image. (d) Decryption Image.



(e) Image after Antiscrambling

Figure 3: Encrypted and Decrypted Image.



(a)Histogram of original Image (b) Histogram of the Scrambled Image

(c)Histogram of the Scrambled Encrypted Image (d) Histogram of the Decryption Image

(e) Histogram of the Antiscrambled Decrypted Image.

Figure 4: Histograms of the Encrypted and Decrypted image.

IJERT

Histogram Deviation Calculation.

The Histogram Deviation calculation of the Seven Gray scale encrypted images Flower, Bird, Lena, Hours, Nature, X-Plane and Airplane X-Plane and Airplane are tabulated in Table1, from which it can be said that the Histogram Deviation than that obtained using Random Scrambling and X-OR operation .

Image Name	Histogram Deviation
Flower	1.5716
Bird	1.4615
Lena	0.7257
Hours	0.7165
Nature	0.6895
X-Plane	0.6103
Airplane	0.8335

Table 1: Show Histogram Deviation Calculation

Average Correlation Coefficient between pixel values.

The Average correlation coefficients between the corresponding pixels values of the three encrypted images Lena, X-Plane and Airplane are tabulated in Table 2, from which it can be said that the correlation coefficients are worse than that obtained using secret key of an image X-OR operation and Compare average correlation coefficient between pixel values on three different images encryption method.

IJERT

Image Name	Chaotic Baker map [16]	Affine Transformed X-OR [3]	Proposed Method.
Lena	0.3247	0.5088	0.14
X-plane	0.8762	0.4983	0.28
Airplane	0.2877	0.2873	0.04

Table 2: Show average Correlation between pixel values and compare different image Encryption Methods.

V. CONCLUSION

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 scheme presented in this paper has a simple implementation module. The proposed encryption algorithm can ensure multiple criteria such as lossless, maximum distortion, maximum performance and maximum speed. The proposed encryption method in this study has been tested on different gray images and showed good results. Future work will be focused on the development of this algorithm to get color image.

ACKNOWLEDGMENT.

The author would like to express their thanks & gratitude to all those who gave suggestions and valuable contributions to this work. The authors would also like to thank the reviewers for their comments to improve this paper. Our special thanks to Prof Vineet Richaria, Head, Computer Science and Engg Dept.,LNCT, Bhopal, India. And Asst Prof Vijay Kumar Trivedi Computer Science and Engg Dept., LNCT, Bhopal, India whose help, stimulating suggestions, experience and encouragement helped us in all the times of study and analysis of this work.

REFERENCES

[1] 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, sMenouf-32952, Egypt, 2006.

[2] Li. Shujun, X. Zheng “Cryptanalysis of a chaotic image encryption method”,Inst. of Image Process. Xi'an ssJiaotong Univ, Shaanxi, This paper appears in: Circuits and Systems, ISCAS 2002. *IEEE* International Symposium on Publication Date: 2002, Vol. 2, page(s):708,711, 2002.

[3] 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 on Signal processing communication Computing and Networking Technologies,* 2011.

[4] National Institute of Standards and Technology, “Data EncryptionStandard(DES),” http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.

[5] M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," *in Proceedings of Advanced Concepts for Intelligent Vision Systems, pp 9-11,2002.*

[6] S.Changgui , B. K Bharat, "An efficient MPEG video encryption algorithm," *Proceedings of the symposium on reliable distributed systems, pp. 38 I -386,1998.*

[7] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", *Pattern Recognition and Image Analysis, vol.IO, no.2, pp.236-247, 2000*.

[8] Jui-Cheng Yen and J. I. Guo, "A New Chaotic Image Encryption Algorithm,"*Proc. 1998 National Symposium on Telecommunications,pp. 358-362, Dec, 1998.*

[9] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", *Optics Communications, Vol-2 18 (2203), 229-234.*

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

[11] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems", *The Journal of Systems and Software 58 , 83-91,2001.*

[12] 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.*

[13] 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.*

[14] 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.*

[15] W. Ding, W. Q. Yan, D. X. Qi, “Digital Image Scrambling Technology Based on Arnold Transformation*,” Journal of Computer-aided Design & Computer Graphics, vol. 13, no. 4, pp. 338-341, 2001.*

[16] Ibrahim Fathy El-Ashry, “Digital Image Encryption”, Master Thesis Report in *Menofia University*, 2010 .

IJERT
IJERT