International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-12)

Research Article | **December 2015**

X-OR and Arnold Cipher Based Double Phase Image Encryption Technique

Gajendra Singh Chandel, Vinod Sharma
SSSIST, Sehore, Madhya Pradesh,
India

Abstract—

Image encryption is a suitable method to protect image data. Image and text data has their unique features. The available encryption algorithms are good for text data. They may not be suitable for multimedia data. In fact the pixels of natural images are highly correlated to their neighboring pixels. Due to this strong correlation any pixel can be practically predicted from the values of its neighbors. In this work, 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 Arnold transformation 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 very meaningless. The proposed encryption method in this study has been tested on different gray images of 256*256 and showed good results.

Index Terms— Arnold Transformation, Scrambling, XOR Operation.

I. INTRODUCTION

Image encryption is necessary for future multimedia Internet applications. Password codes to Identify individual users will likely be replaced are biometric images of fingerprints and retinal scans in the future. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper might duplicate or reroute the information. By encrypting these images, a degree of security can be achieved. Furthermore, by encrypting noncritical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information [1]. Encryption is also used to protect data in transit, as an Example data being transferred via networks (e.g. the web, e-commerce), mobile telephones, wireless microphones, wireless communication systems, Bluetooth devices and bank automatic teller machines [2]

The main idea in the image encryption [3] is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. The image information has special properties such as bulk capability, high redundancy and high correlation among the pixels that imposes special requirements on any encryption technique.

Image encryption can also be used to protect privacy. As an example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the price and to improve service, electronic forms of medical records have been sent over networks from laboratories to medical centers. According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks [4].

Unlike text messages, image data have their special features such as high redundancy, and high correlation among pixels. Also, they are usually huge in size, which together makes traditional encryption methods difficult to apply and slow to process. Sometimes, image applications have their own requirements like real-time processing, fidelity reservation, image format consistence, and data compression for transmission, etc. Simultaneous fulfillment of these requirements along with high security and high quality demands has presented great challenges to real-time imaging practice [5-6].

Now, there are many types of methods available that can do Image Encryption [5-9], and the majority of them are scrambling algorithms based on pixel shuffling. In 2011 Zhang et al. proposed an image encryption method based on total shuffling scheme [7]. This method is characterized in that the secret code stream used in encryption is not only associated with the key, but also related to the plain image. This plain image related encryption method is strongly against chosen plaintext attacks [8]. However, the first secret code is not safe enough to resist the chosen plaintext attack, which is pointed out and crypt analyzed in [9].

In 2013, Eslami et al. suggested an improved algorithm [10] over these shortcomings described in [9]. Two major improvements, such as using previous cipher image pixels to execute “add modulus and xor” operations instead of plain image pixels, and enlarging the iteration times of chaotic system in every round, make the image encryption scheme proposed in [7] higher security against the chosen plaintext attacks with slower encryption speed as a trade off. Yong zhang [11] proposed a lookup table based encryption improvement on the schemes proposed in [7, 10] to improve the encryption speed.

Pixels shuffling based image encryption techniques have one problem that it cannot change the histogram of an image. Hence, their security performances are not good. The encryption method that combines the pixel exchanging and gray level changing can handles reach a good chaotic effect. our proposed method do this job. The latter chapters are arranged as follows: various image encryption techniques are briefly introduced in Section 2. Arnold transformation is presented is

section 3.Section 4 describes our proposed method based on the permutation and substitution. Section 5 presents some representative parameters to describe encryption quality. Section 6 shows the result of our method and The comparative performance analyses of our method with other methods. Section 7 concludes the paper.

II. VARIOUS IMAGE ENCRYPTION METHODS

There are various types of image encryption methods. The image encryption algorithms can be categories into three major groups.

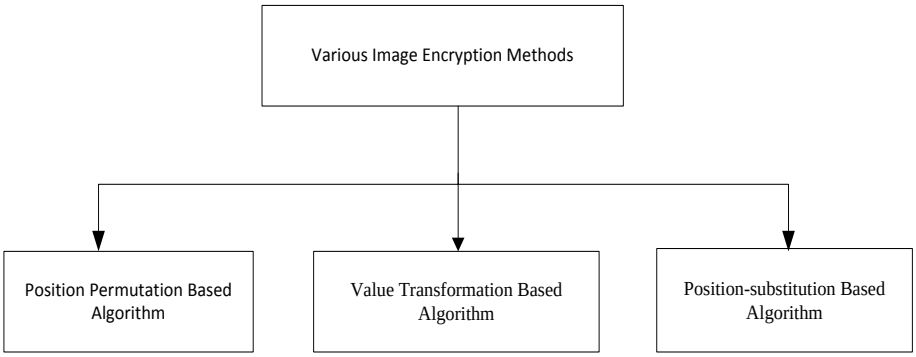


Figure 3.1 Various Image Encryption Methods.

- Position Permutation (Transposition) Based Algorithm.
- Value Transformation (Substitution) Based Algorithm.
- Position- Substitution Based Algorithm

A. Position Permutation (Transposition) Based Algorithm

Transposition means rearranging elements in the plain image. the rearrangement of element can be done by bit, pixel, and block wise . The permutation of bits decreases the perceptual information, whereas the permutation of pixels and blocks produce high level security. In the bit permutation technique, the bits in each pixel are permuted using the permutation keys with the key length equal to 8. In the pixel permutation, 8 pixels are taken as a group and permuted with the same size key. In this investigation the combination of block, bit, and pixel permutation are used respectively. The Position Permutation Based Algorithm is use for the various techniques.

B. 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 . Value Transformation Based Algorithm are Digital Signatures and Lossless Image Compression and Encryption Using SCAN, Image Cryptosystems, Color Image Encryption Using Double Random Phase Encoding, Image Encryption Using Block-Based Transformation Algorithm and affine Transform etc

C. Position- Substitution Based Algorithm

This technique is combination of both position permutation and value transformation. Position permutation and value transformation can be combined. In this technique first pixels are reordered and then a key generator is used to substitute the pixel values. The Position-Substitution Based Algorithm is use for the various techniques

III. ARNOLD TRANSFORM

Arnold transform has periodicity and the transform is simple, but the periodicity depends on image size. The time of image recovery will be much long according to the periodicity.

Arnold transform is used widely in information hiding technology, but because of its long transform periodicity, it costs large time and computation memory.

Arnold transform, also called cat map transform, is only suitable for encrypting N×N images. It is defined as [12].

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\, M)$$

Where (x, y) and (x', y') are the pixel coordinates of the original image and the encrypted image, respectively. Let A denote the left matrix in the right part of equation (1), I(x, y) and I(x', y') (n) represent pixels in the original image and the encrypted image obtained by performing Arnold transform n times, respectively. Thus, image encryption using n times Arnold transforms [38] can be written as.

$$I(x', \quad y')(k) = AI(x, \quad y)(k-1)(\mathrm{mod}\, N)$$

Where k = 1, 2, … , n, and I(x', y') (0) = I(x, y). Obviously, one can multiply the inverse matrix of A at each side of equation (2) to obtain I(x, y) (k −1). In other words, the encrypted image can be decrypted by iteratively calculating the following formula n times.

$$J\left(x,\quad y\right)\left(k\right)=A-IJ\left(x',\quad y'\right)\left(k-1\right)\left(\mathrm{mod}\,N\right)$$

Where J(x', y') (0) is a pixel of the encrypted image, and J(x, y) (k) is a decrypted pixel by performing k iterations.

IV. PROPOSED METHODOLOGY

Proposed methodology divided into two phases i.e image encryption and image decryption.

A. Image Encryption

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

a) Input Image

Image encryption process starts with 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.

b) 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.

Encrypt the input 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.

$$\begin{pmatrix} x' \\ y' \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}\ \mathrm{mod}\ N$$

c) Block Level XOR Operation

Use the Scrambled image X_S as the input for block level XOR operation and encrypt it using equation below to generate the final encrypted image X_C.. The Scrambled image X_S is divided into 2 pixels × 2 pixels blocks. The image pixel contained by every block $B_{i,j}$ of X_T is encrypted using block level XOR operation by four eight bit sub key K1 K2 K3 and K4. as given below Respectively.

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

$$P'_{1.2}=P_{1.2}\oplus K_2$$

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

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

Where $P_{i,j}$ is the pixel value at ith and jth location in block inside pixel of image .the encrypted image by using the XOR operation is called by cipher image X_C and it is ready to be sent to receiver site. The total size of key in our algorithm is 32 bit long which proves to be strong enough.

B. Image Decryption

A Reverse process of encrypted image is called as image decryption. Decryption is also systematic or step-by-step procedure to convert cipher image into original image. The decryption process is divided into different steps.

a) Input encrypted image

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

b) Block Level X-OR Operation

Next Step is to performs the block level X-OR operation of encrypted image X_C by using the X-OR operation. Again we divided Cipher image X_C in to 2 pixels × 2 pixels blocks. Then image pixel contained by every pixel Bij of X_C is Decrypted using block level X-OR operation by Same four eight bit keys (K1,K2,K3,K4) as :

$$\mathrm{Decryption\,P'}_{1.1}\ as P_{1.1}\oplus K_1$$

$$\mathrm{Decryption\,P'}_{1.2}\ as P_{1.2}\oplus K_2$$

$$\mathrm{Decryption\,P'}_{2.1}\ as P_{2.1}\oplus K_3$$

$$\mathrm{Decryption\,P'}_{2.2}\ as P_{2.2}\oplus K_4$$

c) Anti Scrambling by using inverse Arnold transform

The Next step is to applying anti scrambling on decrypted image X_D . The decryption is achieved by applying Inverse Arnold transformation to the encrypted image. The corresponding two dimensional Inverse Arnold transformation matrix is as follows:

$$\begin{pmatrix} x \\ y \end{pmatrix}=\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}\ \mathrm{mod}\ N$$

after antiscrambling has been done by using Anti- Arnold's Transformation, the resultant image is our desired image X .

Figure 1 shows the block diagram of proposed methodology.

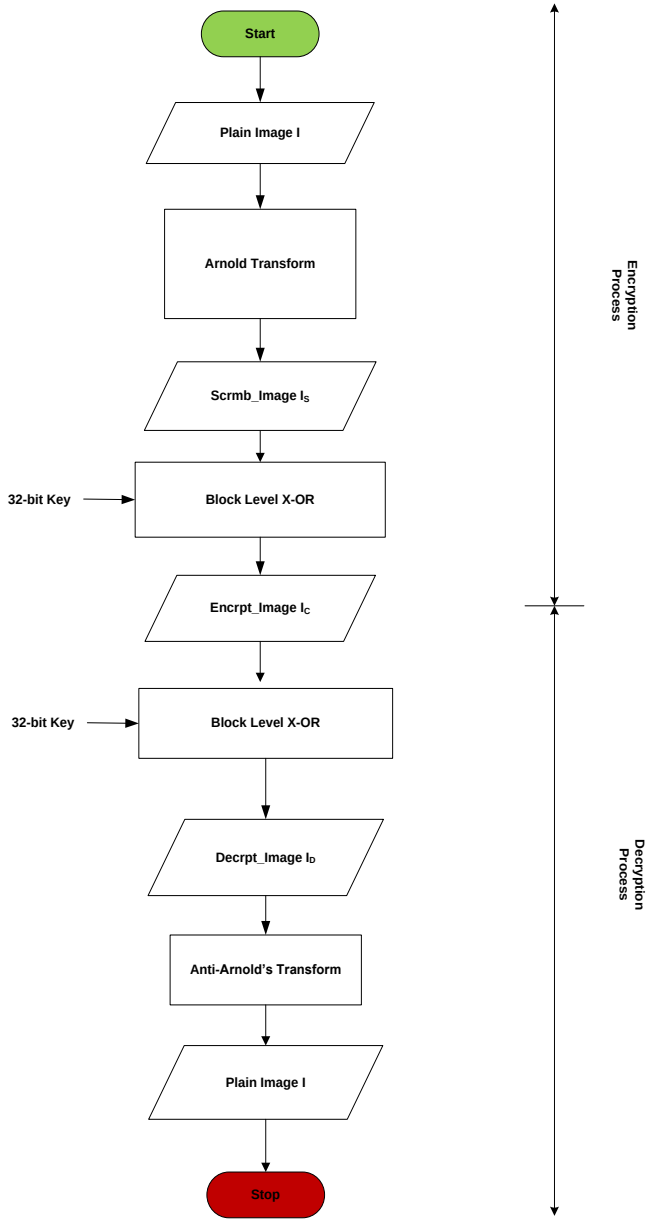


Fig. 1. Block diagram of the proposed image encryption system working

V. ENCRYPTION QUALITY MEASUREMENTS

The Correlation between plain and cipher images, the irregular deviation and the correlation coefficient quality metric were used to test the quality of each cipher.

A. Irregular deviation

This measure will be done by calculating the 'X' matrix which represents the absolute values of the deviation between each pixel values before and after encryption. Next, present the results graphically (histogram distributions). After that, compute the average value of how many pixels are deviated at every deviation value 'D'. This is followed by computing the absolute value of subtracting this average from the deviation histogram 'S'. Finally, count the area 'AS' under the absolute curve 'S' (sum of variations of the deviations histogram from the uniformly distributed histogram.) .

The followed steps summarize this measure:

X=|I-E|

H=Histogram(X);

$$D = \frac{1}{256}\sum_{i=0}^{255} h_i$$

S(i)=|H(i)-D|

$$AS = \sum_{i=0}^{255} S_i$$

I: the Plain Image
E: Encrypted Image
H: Histogram Distribution
hi :the amplitude of the absolute difference histogram at the value i

B. Correlation Coefficient

Statistical analysis such as correlation coefficient factor is used to measure the relationship between two variables; the image and its encryption. This factor demonstrates to what extent the proposed encryption algorithm strongly resists statistical attacks. Therefore, encrypted image must be completely different from the original one .the correlation coefficient is measured by the following equation:

$$C.C = \frac{\sum_{i=1}^{N} (x_i - E(x))\ (y_i - E(y))}{\sqrt{\sum_{i=1}^{N} (x_i - E(x))^2}\ \sqrt{\sum_{i=1}^{N} (y_i - E(y))^2}}$$

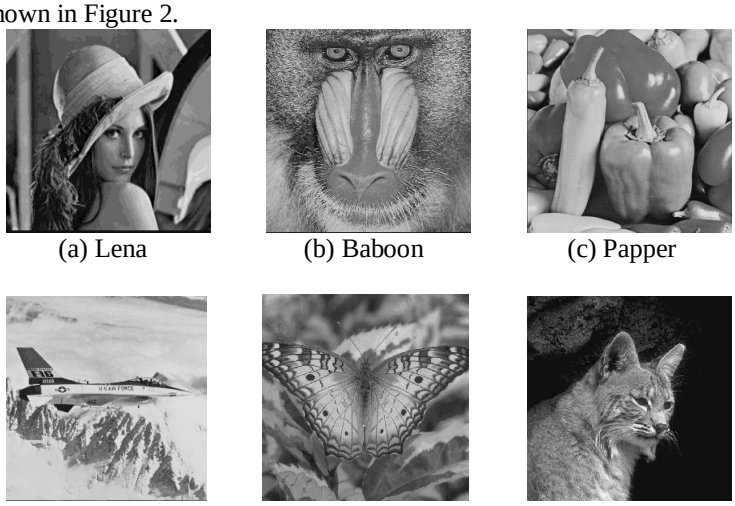
C.C: Correlation Coefficient

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i$$

x and y: gray-scale pixel values of the original and encrypted images.

VI. RESULT AND ANALYSIS

In the experiment, we do image encryption using permutation and substitution technique and we are taken different images of size 512× 512 shown in Figure 2.

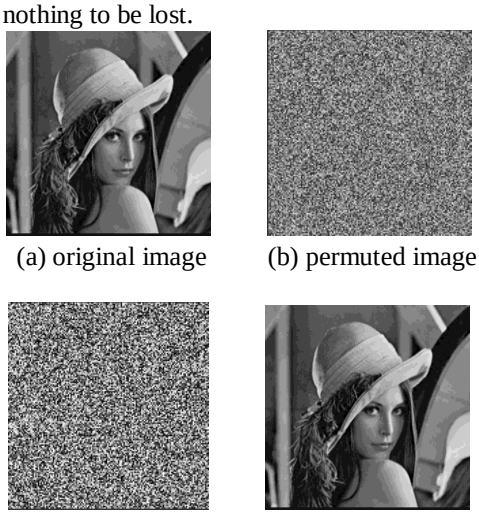


(a) Lena (b) Baboon (c) Papper

(d) Plane (e) Butterfly (f) Cat

Fig. 2. Test Images of size 512×512

To demonstrated our method we used the gray image Lena as Shown in Fig. 3(a), The results after permutation and substitution are shown as in Fig. 3(b) and 3(c) respectively. Figure 3(d) is the result of decryption, comparing with original image as shown in Figure 3(a), there is nothing to be lost.



(a) original image (b) permuted image

(c) substituted permuted image (d) Decrypted image

Fig. 3. Results after image encryption and Decryption system for Lena

The Average quality parameters between the corresponding proposed method and among different methods are tabulated in Table I. figure 4 shows average Irregular Deviation between each pixel values before and after encryption and comparison with different image Encryption Methods . Figure 5 Shows average Correlation between pixel values and comparison with different image Encryption Methods

TABLE I. THE ENCRYPTION QUALITY TEST RESULTS FOR EACH CIPHER.

Proposal Algorithm	Irregular Deviation	Correlation Coefficient
RC6 algorithm	0.7050	0.0023
Chaotic Baker map scrambling	0.9790	0.0032
Encryption using SCAN patterns	1.539	1.72e-4
CKBA	3.917	0.0044
Affine transformation	0.8526	0.5088
Tent map	0.9690	0.0079
Proposed method	**0.8239**	**0.0019**

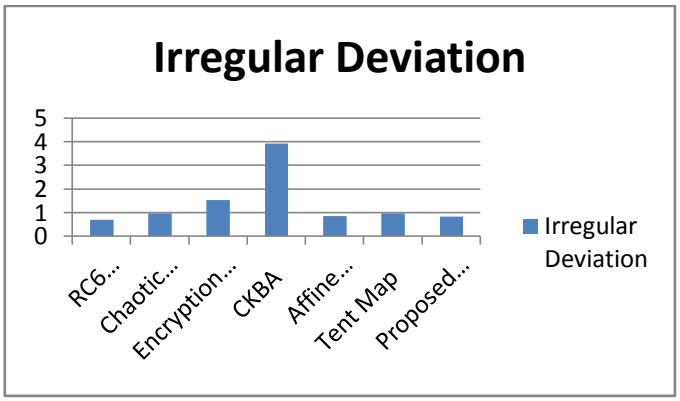


Fig 4.Average Irregular deviation comparison graph

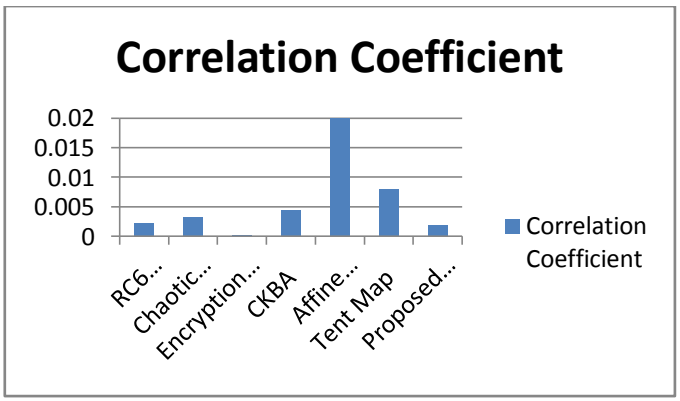


Fig 5.Average correlation coefficient comparison graph

VII. CONCLUSION

In this work, the design and implementation of an encryption algorithm that provides both high security and performance were presented. Also, other features such as flexibility, simplicity and easiness of implementation are taken into account when designing the algorithm.

In this work, we proposed a symmetric key image encryption technique that first scramble the locations of the pixels using 4 8-bit sub keys and then encrypt the pixel values by XOR the selected 8-bit key. The scrambling operation is done using Arnold transformation 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 very meaningless. The proposed encryption method in this study has been tested on different gray images of 256*256 and showed good results.

To accomplish this research work, we have designed our image Encryption and Decryption System using Matlab 7.8.0. We have evaluated our proposed image Encryption and Decryption System on gray Scale image.

REFERENCES

[1] W. Xiao, J. Zhang and W. Wu, " A Watermarking Algorithm Based on Chaotic Encryption" , Proceedings of IEEE TENCON, pp. 545-548, 2002.

[2] 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.

[3] John Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[4] 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.
[5] 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.
[6] 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.
[7] G. Zhang, and Q. Liu, "A novel image encryption method based on total shuffling scheme," Opt. Commun. vol. 284, pp. 2775-2780, 2011.
[8] Y. Zhang, J. Xia, P. Cai, and B. Chen, "Plaintext related two-level secret key image encryption scheme," TELKOMNIKA. vol. 10, pp. 1254-1262, 2012.
[9] X. Wang, and G. He, "Cryptanalysis on a novel image encryption method based on total shuffling scheme," Opt. Commun. vol. 284, pp. 5804-5807, 2011.
[10] Z. Eslami, and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling," Opt. Commun. vol. 286, pp. 51-55, 2013.
[11] Yong Zhang," Encryption Speed Improvement on "An Improvement over An Image Encryption Method Based on Total Shuffling" International Conference on Sensor Network Security Technology and Privacy Communication System, 2013.
[12] W. Ding, W. Q. Yan, D. X. Qi, "Digital Image Scrambling Technology Based on Arnold Transformation.

