Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Cilt:36, No: 4 Özel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol. 36, No: 4 Special Issue (2015)
ISSN: 1300-1949

New digital images cryptography algorithm using butterflies and Banyan network-connected

Fariba Dehghani FIROUZABADI[1], Ali Mohammad LATIF[2*]

[1]*Department of Computer, Maybod Branch, Islamic Azad University, Maybod, Iran*

[2]*Department of Electricity and Computer, Yazd University, Yazd, Iran*

Received: 22.03.2015; Accepted: 29.05.2015

Abstract

Information security is a critical issue for data privacy of peoples and organizations. A powerful tool to satisfy this requirement is cryptography. Cryptography is a method of securing which is done by using a reversible mathematical relationship. As images are widely used in digital products and because of its special nature, has its special cryptographic algorithms. In this paper, a new cryptography algorithm for digital images are proposed by using the butterfly and Banyan network connectivity which are one of the tools of parallel processors; In this algorithm, the image are divided into the some blocks and fragmented by using the technique of displacement and a butterfly network is pixels in each block and then some changes are applied to the bits of each pixel. To evaluate different algorithms, we have used some visual test, correlation analysis and histogram analysis error criteria. Experimental results show that the proposed method, besides having good visual quality, error criteria reduced NPCR, MAE and UACI, respectively, at 13.5237, 13.2083 and 0.935. Also proposed algorithm is able to reduce the correlation of pixels in the horizontal, vertical and diagonal average at 0043/0, 0026/0 and 0039/0.

Keywords: scrambling, digital image, network interconnections, butterfly network, Banyan network.

1. INTODUCTION

Information security is a critical issue for data privacy of peoples and organizations. A powerful tool to satisfy this requirement is cryptography. Nowadays cryptography can be considered more as the study of methods and cryptography algorithms that the mathematical issues are behind these methods. Many people use cryptography to protect the confidentiality of information. Cryptography is the conversion of data into a form that reading it without the proper knowledge and key becomes impossible. Because of the dependence of gray adjacent pixels levels in the images, the text cryptography algorithms cannot be used in image (Ding, et al, 2000) and (Wei, et al, 1999). This feature has isolated field of the image cryptography from other cryptography method. Methods that have been proposed for image cryptography technique work based on inserting and scrambling methods. In the inserting technique, a brightness level to be replaced by using reversible mathematical relationships on each image pixel. In the scrambling method, The image pixels in the image would-be scrambled by using the cryptography algorithm (Che, et al, 2008). Due to the large volume of image data and the specific characteristics of the image, using classic cryptography algorithms such as RSA and DES in images cryptography is inefficient; Because these algorithms are time-consuming and are not usable in real-time systems (Pareek, et al,2006; Kanso, Ghebleh,2012). Many cryptography algorithms are presented for digital images cryptography. For example, as an examples, we can note to the algorithms such as Fibonacci (Jiancheng, et al, 200), Arnold transform (Ying, et al, 2007), regular transform (Xiangdong, et al, 2008) and Gray code (Wei, 2001; Wei, et al, 1999). But according to a study that has been carried

* Corresponding author. *Email: Alatif@yazd.ac.ir*

Special Issue: Technological Advances of Engineering Sciences

out, the algorithm performed well in the first Fibonacci and Arnold cannot become tangled wreck image, Fibonacci and Arnold transform algorithm cannot performed well in the first image scrambling. Furthermore, Gray code and regular transforms cannot be performed on the image, because there is a correlation between pixels in many parts of the encrypted image. In this paper, we try to use from Butterfly, Banyan and shift rotation connectivity networks tools to encrypt digital images.

2- Parallel computing systems

Parallel processor is defined for a computer with more than one processor. Systems with thousands of processors such are called as massively parallel systems. Recent multicore processors are ideal for creating parallel systems and there are some parallel processors that are called large particles versus small particles. This divisions will refer to the size of the particles.
There are several types of parallel processors. The differences are between the type of interconnection of the processors or the connection between the processor and memory. Parallel processors can be divided into symmetric Multi-Processing and asymmetric Multi-Processing. In the asymmetric multiprocessor system, one processor for executing operating system and other processors are used to execute user applications. In symmetric multi-processor system, the operating system can run on each processor open or all processors simultaneously. In recent years, various designs and constructions are done for parallel processing that the butterfly network connection is one example for that. This article tries to use this network for image cryptography.

3- Network interconnections between processor and memory

Properties and characteristics of network congestion memory multi-processors depends on the interconnections between the processor and memory. The density and congestion may occur in hardware connection even when the CPU refers to different sectors. Consider a cross-network communication between the 8processor and 8 memory. Each memory can service only one application at one time. Therefore, requests by multiple processors will lead to congestion simultaneously in one memory slot. Cross network has important properties that makes no congestion in the network interconnections. Transverse channels can connect all processors simultaneously to different memory. Each switch can be set to allow each patterns occur at the same-time of the communication processor and memory.

For n processors with n memory, you will need n^2 switches. So it costs $O(n^2)$. Obviously, if the number of processors is large, the cost of $O(n^2)$ isn't affordable. For reducing these costs, some networks with the cost of $O(n \log n)$ such as the butterfly and Banyan network connectivity which are shown in the figures of (1) and (3) are provided. Network Butterfly is derived from the shape of the Butterfly Wings that has appeared in every phase of the network. The butterfly wings are consecutive at each stage. A butterfly networks is built from $(n+1)\times 2^n$ processor in $n+1$ row which has 2^n processor in each row. The proceesor of $p(r, j)$ is connected to the processors of $p(r-1, j)$ and $p(r-1, m)$. To obtain m, j must be written in binary form. Then the r^{th} bot of the binary representation of the j will be inverted. For example, if j=3 and r=2, it means that the second Second row and third column has been choosed. If the binary representation of the number three considered as 0011, by the given value of r, the second bit of the number three should be

changed so that it will become as 0001. So the interconnection betweeen the processors of $p(1,3)$ and $p(1,1)$ will be Will b established to the $p(2,3)$.

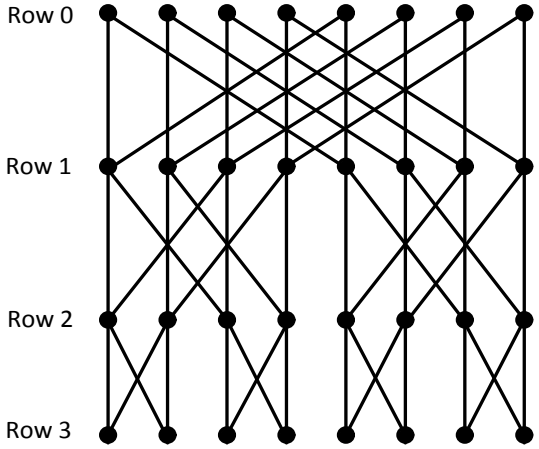


Figure 1: Butterfly Network Connection

4. The proposed algorithm

In the proposed algorithm, we try to encrypt the image in four steps. In the first step, butterfly network connected processors are mapped to the pixels of the image data. For implementation, it is assumed that the image size is 256 × 256; so the whole picture reshape into the 8192 block size of 8 × 1. Then the numbers of 1 to 8192 are placed randomly in a matrix. This matrix is called S-box. There are no duplicated elements in this matrix. This randomly fixed matrix contains the number of blocks that should be sent in the cryptography step. In this paper, a butterfly network connection with n = 3is used; Therefore, this network will have 4 rows Where each row has 8 processors; in the first stage, 4 row of the matrix is called from S-box. These numbers are the number of blocks that must be sent to the butterfly network connection. For example, if the numbers which are read from the matrix was 4-15-100-50, the blocks of 4-15-5-100 are put Below together and an 4 × 8 matrix is obtained. This matrix is called A. Processors can be mapped to pixels. In the mapping and implementation of butterfly network connectivity, vertical lines will not be considered. The fourth row of pixels in matrix-a is displaced with a third row of the matrix on the diagonal lines drawn in Figure 1. A third row of pixels and the pixels of the second row of the matrix diagonal lines in Figure 1 are pasted together and the first and second row of the A matrix pixels, are likewise displaced. With these operations, a 4 × 4 matrix is obtained. This matrix is called B. now the first row of the matrix B is replaced instead of the 4 Blocks. Also the second row of the matrix B will be put in place Block 15. Similarly, the contents of the pixel blocks 100 and 50 are displaced with the third and fourth rows of the matrix B. The above steps are repeated until all the blocks are displaced. The final image of the first stage to the second stage will be considered as the input image. In the second phase, four consecutive are called from S-box matrix. . After calculating the equivalent binary content of pixels, even bit of the each pixel will displaced with the even bit of the bottom pixel. For example, if A(1,1)=107andA(2,1)=0, after replacing the even bits, the content of the pixels will be A(1,1)=48andA(2,1)=65. Then the content of the A (1,1) pixel will displace with A(2,1). This operation is repeated until the entire block will be displaced. In the third stage, four consecutive algorithm numbers called from S-box matrix. The encoded image blocks are put together in the second stage and an 4 × 8 matrix is obtained. In the third phase, rotation shift in a circle is applied as shown in Figure (2) on the

matrix. The user specifies the number of shift rotation. The third step repeat until all the blocks are replaced.

Figure 2. How to shift the pixels in the matrix

In the fourth step, the Banyan network connection is used. As in Figure 3 is specified, the Banyan network connection is made from the butterfly and shuffle network connection. Banyan is a self routing network. Banyan is a multistage network connection where the P memory is connected to P processors. In Banyan networks, we have $\frac{p}{2}\log(p)$ switches. For example, in Figure 3,8 processor is connected to 8 memory unit. It is obvious that in this network, we have $\frac{8}{2}\log(8)=12$ switches. Processors are numbered from zero to 8 and three bits are used in the shuffle of the function. Routing is performed at each stage and the data is sent from a specific memory to a specific processor.

After receiving the encrypted image from the third stage, eight consecutive numbers are called from the S-box matrix. In the third stage the encrypted image blocks are put together and an 8 × 8 matrix is obtained. Then the Banyan network connection is mapped into image pixels which are in this matrix (Fig3). Image pixels are displaced with each other as drawn diagonal lines in Figure 3. These steps are repeated until all pixels blocks are displaced. It is noteworthy that to decode the image, Reverse coding work should be done.

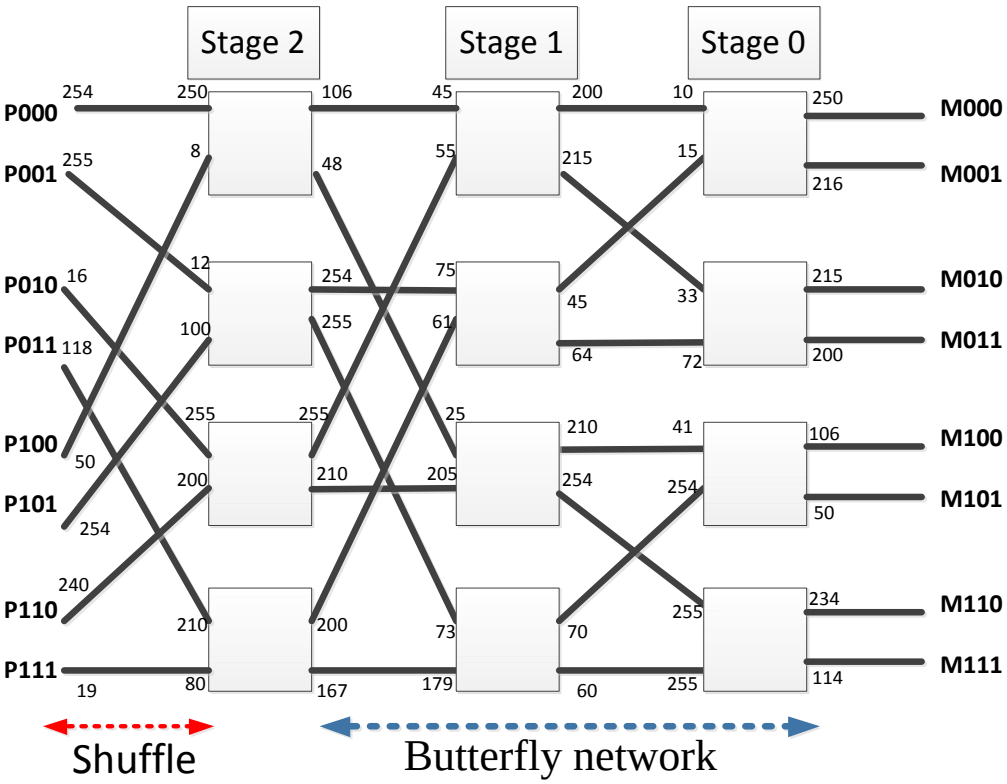


Figure 3. Mapping of the image pixels to the Banyan network

5- Analyzing the proposed algorithm using visual test

The proposed algorithm is performed on standard images of male photographer (Figure 4) and Mickey Mouse (Fig. 5) as well as pictures of coins, the machine and pepper and the results is shown in Figure (6) to (11). According to the results of implementation, the image becomes cluttered so that it cannot be seen in any sense of the original image.

Figure 4 image of the Photographer man

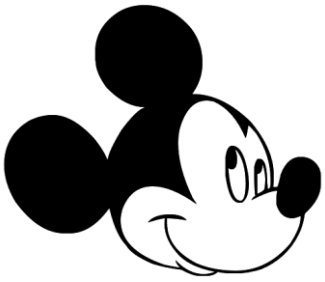
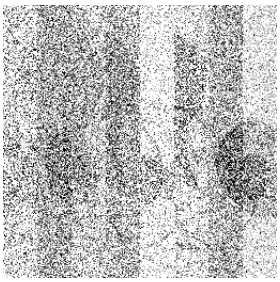
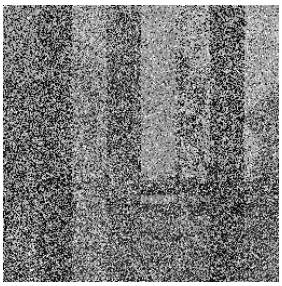


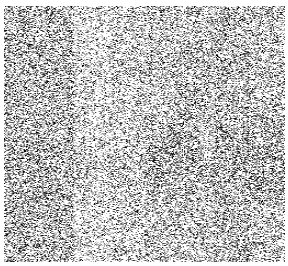
Figure 5.image of Mickey Mouse

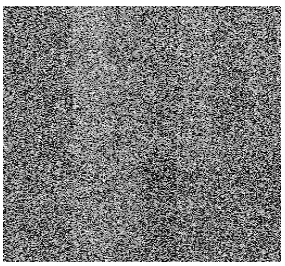




B :Encrypted image of Mickey-Mouse **A :Encrypted image of photographer man**

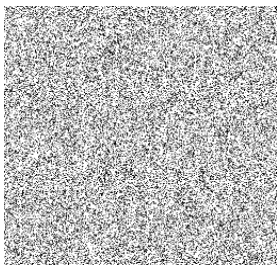
Figure 6: One-step of running the algorithm

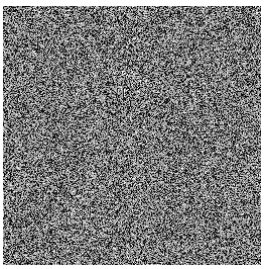




B :Encrypted image of Mickey-Mouse **A :Encrypted image of photographer man**

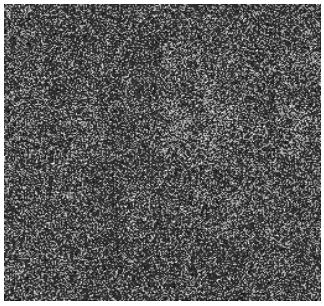
Figure 7 : two-step of running the algorithm





B :Encrypted image of Mickey-Mouse **A :Encrypted image of photographer man**

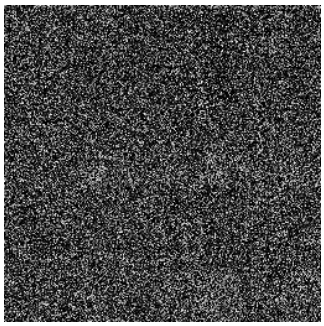
Figure 8 : five-step of running the algorithm



B. The Encrypted Picture

A :Main image of coins

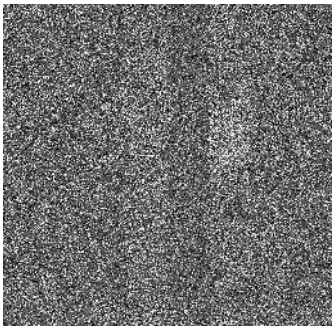
Figure 9 : two-step of running the algorithm



B: The Encrypted Picture

A: The original image machine

Figure 10. Two-step of running the algorithm



B :The Encrypted Picture

A :The original image of pepper

Figure 11 : two-step of running the algorithm

6- Analyzing the algorithm using correlation analysis

In the image data, each pixel is correlated with its neighboring pixels. Ideally an cryptography algorithm should be carefully encrypted images in a way that the correlation between pixels are low (Rakesh, et al, 2012). In the Table 2, the correlation between pixels in the horizontal, vertical and diagonal is provided for photographer man on the image (Fig. 4). The correlation criteria is expressed in equation (1).

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (1)$$

$$\mathrm{Cov(x,y)} = \frac{1}{\mathrm{M\times N}} \times \sum_{\mathrm{j=1}}^{\mathrm{M\times N}} ((\mathrm{x_j} - \frac{1}{\mathrm{M\times N}} \sum_{\mathrm{j=1}}^{\mathrm{M\times N}} \mathrm{x_j})(\mathrm{y_j} - \frac{1}{\mathrm{M\times N}} \sum_{\mathrm{j=1}}^{\mathrm{M\times N}} \mathrm{y_j})) \quad (2)$$

$$D(x) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (x_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} x_j)^2 \quad (3)$$

$$D(y) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (y_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} y_j)^2 \quad (4)$$

In this equation, x and y are lighting of two neighboring pixels in an image and M × N are the pixels of the image. Equation 5 is the minimum absolute error that is the average of the absolute error (Jolfaei, 2010; Hyndman, 2006; Willmott, 2005). $C(i, j)$ and $P(i, j)$ are the values of the encrypt image pixels and the main image.

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C(i, j) - P(i, j)| \quad (5)$$

Equation 6 referred to the calculation of the $NPCR$ that is the average rate of change of the image pixels in the original image for a bit change (Ye, Zhao, 2012; Wong, Kwok, 2009; Wu And et al, 2011). In general, it may be unauthorized user to change a pixel of the encrypted image achieve to a significant relationship between the original image and the encrypted image. Then by changing a pixel of the encrypted image, impair the decryption at the receiver side. The values of $UACI$ and $NPCR$ are used to calculate the degree of dependence between the original image and encrypted image. The better the result of the calculation in the $UACI$ and $NPCR$, the closer relationship between the main image and the encrypted image.

$$NPCR = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i, j)}{M \times N} \times 100\% \quad (6)$$

$$D(i, j) = \begin{cases} 0 & if \quad C(i, j) = \overline{C}(i, j) \\ 1 & if \quad C(i, j) \neq \overline{C}(i, j) \end{cases} \quad (7)$$

In equation 7, C and $\bar{c}$ are two encrypted images that the original images are different only in one bit. The method of calculating the $UACI$ are shown in figure 8 (Wong, 2009; Wu, et al, 2011).

$$UACI = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[\frac{|C(i, j) - \overline{C}(i, j)|}{255} \right] \times 100\% \quad (8)$$

The more the $UACI$, $NPCR$ and MAE, the better performance of the cryptography. The values of the table 1 show that the $UACI$ and $NPCR$ has a better performance than the others. By comparison of the proposed algorithms, the values of the MAE has improved. Also correlation analysis for visual comparison can be seen in Figures 10 to 13.the results of the above sequence of three chaotic image cryptography, logistics, TD-ERCS and the proposed algorithm. By seeing the picture of 10 to 13, the proposed algorithms could scramble the picture in a way that the contents of the encrypted image give no information from the original image.

Table 1. Measurement criteria

NPCR	MAE	UACI	The evaluated Algorithms
33.6855%	49.2416%	13.2441%	The chaotic sequence **(**Gu, 2006)
33.6869%	49.2874%	13.2354%	Logistic sequences **(**Ye, 2010)
33.7050%	49.5926%	13.2424%	TD-ERCS sequence **(**Feng-ying; Cong-xu, 2011)
47.2161%	36.1655%	14.1756%	The proposed algorithm

Table 2. Correlation Analysis

Diagonal	Vertical	Horizontal	Correlation function
0.9373	0.9564	0.9562	Image of photographer man
0.6681	0.6704	0.6693	The chaotic cryptography image
0.6662	0.6671	0.6657	Picture Password Logistics
0.6653	0.6668	0.6675	Picture cryptography of TD-ERCS
0.6626	0.6655	0.6635	Image cryptography algorithm

The cryptography algorithm is a cryptographic key. Key cryptography is a key which is used to decrypt the encrypted data. Good cryptography algorithm is an cryptography algorithm to identify the key or keys that you cannot guess. Some cryptographic algorithms with has the rotation period, i.e. after the replication algorithm can be decoded. Obviously, the larger the length of the key, the higher security of the algorithm. The proposed algorithm has five key. The size of the original image, the number of shift rotation, S-box in Banyan networks, P,N in the Butterfly network are key cryptography algorithm. Thus, given the large key length, the proposed method has good security.

DISCUSSION AND CONCLUSIONS

In this paper, a new algorithm was introduced to encode the gray level images. According to the proposed algorithm, the image will be blocked. Then, by using the butterfly network connection blocks are scrambled. After bits displacement of the image, a circular shift rotation is applied and in the last step, the content of the blocks will be displaced using network connection. The proposed algorithms will be evaluated by the standard tests. The proposed algorithm is able to shed the image so that the image hash is not predictable. Analysis of the test results show that the proposed algorithm has been evaluated with respect to the three algorithms that the encrypted image pixels is reduced in the horizontal, vertical and diagonal average at 0/0043, 0/0026 and 0/0039. To assess the difference between the original and main image, we have used $UACI$, MAE and $NPCR$ as a criterion. Experimental results show that the proposed method, besides having good visual quality, will reduce the error criterion of $UACI$, MAE and $NPCR$ into the 13/5237, 13/2083 and 0/935 respectively. Obtained Numerical results show that the proposed method has good utility.

REFERENCES

Che. S, Che. Z & Ma.B. (2008). An Improved Image Scrambling Algorithm. Second International Conference On Genetic And Evolutionary Computing, Pp.495-499.

Ding.W, Yan.W& Qi. D. (2000). Digital Image Scrambling. Progress In Natural Science, Vol. 11, Pp.7-14.

Feng-Ying. H & Cong-Xu .Z.(2011). An Novel Chaotic Image Encryption Algorithm Based On Tangent-Delay Ellipse Reflecting Cavity Map System. Procedia Engineering, Vol. 23, Pp. 186-191.

Gu. G.S. & Han. G.Q. (2006). The Application Of Chaos And DWT In Image Scrambling. IEEE Conference on Industrial Electronics And Applications, Pp. 3729 – 3733.

Hyndman.R. J. & Koehler. A. B. (2006). Another Look At Measures Of Forecast Accuracy, International Journal Of Forecasting.

Jiancheng. Z, Ward. R.K. & Dongxu.Q. (2004). A New Digital Image Scrambling Method Based On Fibonacci Numbers, In Proceedings Of The International Symposium On Circuits And Systems,Vol 3.

Jolfaei. A & Mirghadri .A. (2010). Survey: Image Encryption Using Salsa20. International Journal of Computer Science Issues, Vol. 5, Pp. 213-220.

Kanso. A & Ghebleh. M. (2012). A Novel Image Encryption Algorithm Based On A 3D Chaotic Map. Nonlinear Science and Numerical Simulation, Vol .17, Pp. 2943-2959.

Pareek. N.K, Vinod .P & Sud.K.K. (2006). Image Encryption Using Chaotic Logistic Map. The Journal Of Image And Vision Computing, Vol .24, Pp. 926-934.

Rakesh. S, Ajitkumar. A .Kaller, Shadakshari. B. C &Annappa .B. (2012). Image Encryption Using Block Based Uniform Scrambling And Chaotic Logistic Mapping. International Journal on Cryptography and Information Security, Vol .2, Pp. 49-57.

Wei. D, Wei-Qi. Y& Dong-Xu. Q. (1999). Digital Image Scrambling Technology Based On Gray Code. International Conference on Computer Aided Design & Computer Graphics, Vol. 3. Pp.900-904.

Wei. D. (2001). Digital Image Scrambling, Progress In Natural Science Journal, Vol 11, P. 454-460.

Willmott. C.J & Matsuura.K. (2005). Advantages Of The Mean Absolute Error (MAE) Over The Root Mean Square Error (RMSE) In Assessing Average Model Performance. Climate Research Clime Res, Vol .30, Pp.79-82.

Wong. K.W & Kwok. B.S.H. (2009). An Efficient Diffusion Approach For Chaos-Based Image Encryption .Chaos Solitons & Fractals, Vol.41, Pp. 2652-2663.

Wu. Y, Noonan. J.P & Agaian. S. (2011). Shannon Entropy Based Randomness Measurement and Test For Image Encryption. Journal of Information Sciences.Pp.1-23.

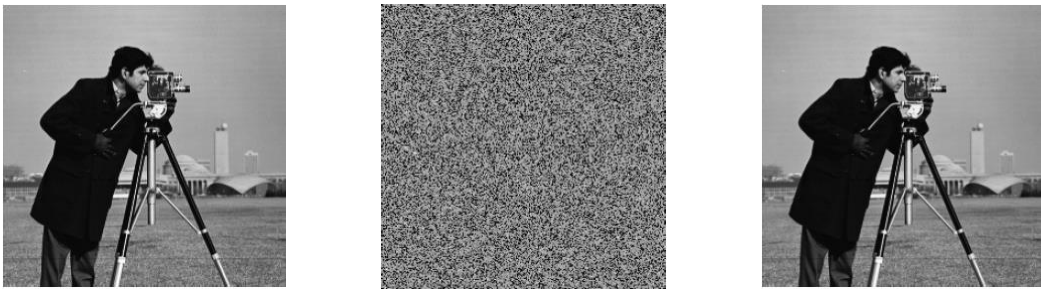
Xiangdong. L, Junxing. Z, Jinhai. Z & Xiqin. H. (2008).Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation, International Journal of Computer Science and Network Security, Vol 8, P. 64-68.

Ye. G. (2010). Image Scrambling Encryption Algorithm Of Pixel Bit Based On Chaos Map. Pattern Recognition Letters, Vol .31, Pp.354-347.

Ye. R & Zhao. H. (2012). An Efficient Chaos Based Image Encryption Scheme Using Affine Modular Maps. International Journal of Computer Network and Information Security, Vol .4, Pp.41-45.

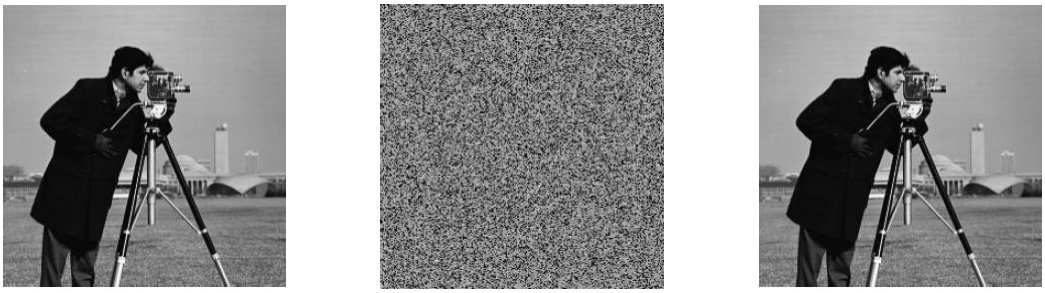
Ying. W, Zhao .Z & Lelin. Z. (2007). A Fault-Tolerable Encryption Algorithm for Two-Dimensional Digital Image, IEEE Conference on Industrial Electronics and Applications, P.2737 - 2741.

APPENDIX



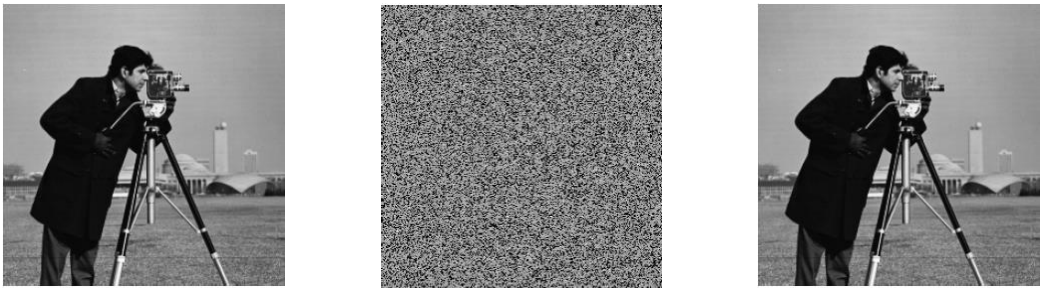
C. Decrypted image **B. Encrypted image** **A. The original image**

Figure 10 Encryption and decryption with the chaotic sequence



C. Decrypted image **B. Encrypted image** **A. The original image**

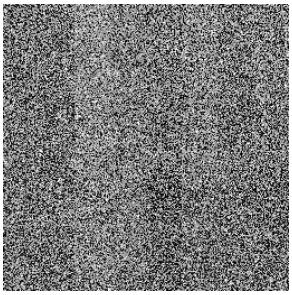
Figure 11: Encryption and decryption sequence Logistics



C. Decrypted image **B. Encrypted image** **A. The original image**

Figure 12: Encryption and decryption sequence TD-ERCS


C. Decrypted image


B. Encrypted image


A. The original image

Figure 13: Encryption and decryption algorithm