AN IMAGE ENCRYPTION APPROACH USING CHAOS AND STREAM CIPHER

[1]ALIREZA JOLFAEI, [2]ABDOLRASOUL MIRGHADRI

[1, 2] Faculty and Research Center of Communication and Information Technology, IHU, Tehran, Iran

ABSTRACT

In this paper, a novel image encryption scheme is proposed based on combination of pixel shuffling and W7. Due to sensitivity to initial conditions, chaotic maps have a good potential for designing dynamic permutation map. So a chaotic Henon map is used to generate permutation matrix. An external secret key is used to derive the initial conditions for the chaotic map and W7 secret key. Pixel shuffling is performed via vertical and horizontal permutation. Shuffling is used to expand diffusion in the image and dissipate the high correlation among image pixels. In order to evaluate performance, the proposed algorithm was measured through a series of tests. Experimental results illustrate that the scheme is highly key sensitive and shows a good resistance against brute-force and statistical attacks.

Keywords: *Shuffling, W7, Henon Map, Permutation Matrix, Test.*

1. INTRODUCTION

Along with the fast progression of data exchange in electronic way, it is important to protect the confidentiality of data from unauthorized access. Security breaches may affect user's privacy and reputation. So, data encryption is widely used to confirm security in open networks such as the internet. Due to the substantial increase in digital data transmission via internet, the security of digital images has become more prominent and attracted much attention in the digital world today. Also, the extension of multimedia technology in our society has promoted digital images to play a more significant role than the traditional texts, which demand serious protection of users' privacy for all applications. Each type of data has its own features; therefore, different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are used for text data. However, due to large data size and real time requirement, the algorithms that are appropriate for textual data may not be suitable for multimedia data.

Classical cryptographic algorithms such as RSA, DES, and ... are inefficient for image encryption due to image inherent features, especially high volume image data. Many researchers proposed different image encryption schemes to overcome image encryption problems [1, 2, 3, 4]. In this research we have tried to find a simple, fast and secure algorithm for image encryption using the characteristics of chaotic functions and the LFSR-based stream ciphers. According to key's large space in the chaotic functions, this method is very robust. Finally, this algorithm is very sensitive to small changes in key so even with the knowledge of the key approximate values; there is no possibility for the attacker to break the cipher.

The rest of the paper is organized as follows: In Section 2, we describe the relation between chaos and cryptography. In Section 3, we briefly introduce the methods used in this paper. The new algorithm is proposed in section 4. In section 5, we test the efficiency of algorithm by visual inspection. In section 6, we analyze the security of the proposed image cipher and evaluate its performance through various statistical analysis, key sensitivity analysis, differential analysis, key space analysis, etc and compare the results. Finally, some conclusions are given in section 7.

2. CHAOS AND CRYPTOGRAPHY

Chaos is a phenomenon that occurs in nonlinear definable systems sensitive to initial conditions and has a pseudo-random behavior. Dynamic chaotic systems in case of Liapunov exponential equations meet will remain stable in chaos mode. An important characteristic that has caused this phenomenon to take into consideration for many cryptographic systems is being definable despite of its pseudo-random behavior. Due to pseudo-random behavior, the output of the vision system seems

random in attackers' view, while in receiver's view, the system can be defined and decryption is possible. Many cryptographic algorithms based on chaos theory are presented till now [5, 6, 7] and some of them are somehow employed in way that are capable of image encryption addition to text encryption. Image encryption must have special features such as suitable speed for image massive data ciphering. Text encryption methods are not suitable for implementation on the image. Practically, we need to transmit a reasonable amount of information, which requires a large sample space and that in turn implies a large number of keys. The distribution of a large number of keys is liable to cause horrendous management problems. So, one of the main advantages of chaotic system's realization is facilitated key management approach because this method only needs to protect and secure transmission of secret key (parameters and initial values of chaotic system), which has a little volume and therefore not only a little memory is needed to maintain it but also there is more confidence during its transfer. The unauthorized access to short length keys is significantly less possible than the large length keys during data transmission through the insecure channel.

3. METHODS

We used Henon map and W7 stream cipher for constructing our new approach that are described as follows:

3.1. Henon Map

The Henon map is a prototypical two-dimensional invertible iterated map represented by the state equations with a chaotic attractor and is a simplified model of the Poincare map for the Lorenz equation proposed by Henon in 1976 [8]. The chaotic Henon mapping has been proposed as a method of generating pseudo-random sequences [9]. The two-dimensional Henon map is defined as follows:

$$\begin{cases} x_{n+1} = 1 + y_n - \alpha x_n^2 \\ y_{n+1} = \beta x_n, \end{cases} \qquad (1)$$

with initial point (x_0, y_0). The pair (x, y) is the two-dimensional state of the system. When $\alpha = 1.4$ and $\beta = 0.3$, the system is in chaotic state. Henon showed that if the initial point lies in the area S defined by the four points (-1.33, 0.42), (1.32, 0.133), (1.245, -0.14) and (-1.06, -0.5), then the subsequent points, (x_i, y_i) for $i \geq 1$, also lie in S [8]. The Henon map possesses a strange attractor. For any values of (x_i, y_i) in S, the sequence of points quickly converges to this attractor and remains on it during the iterations that follow.

3.2. Stream Cipher

In cryptography, Stream ciphers are an important class of symmetric encryption algorithms [10]. They encrypt binary digits of a plain-image one at a time, using an encryption transformation which varies with time. A stream cipher is a symmetric key cipher where plain-image bits are combined with a keystream, typically by XOR operation.

3.2.1. W7 Stream Cipher

The W7 stream cipher is a synchronous symmetric encryption designed for efficient hardware implementation at very high data rates [11]. This cipher has been proposed in order to replace A5/1 in GSM security scheme, due to the security problems of A5/1 [12]. W7 algorithm supports key lengths of 128-bit and consists of a control and a function unit. The function unit is responsible for the keystream generation and contains eight similar cells. Each cell contains three LFSRs and one majority function. Fig. 1 shows W7 key stream generator and the detailed design of the block C2 is shown in Fig. 2. Compared with A5/1, the key size is increased from 64 bits to 128 bits; each LFSR sequence is filtered by a cubic Boolean function, 8 parallel identical structures for outputting one byte instead of one bit. W7 is fast and has a cheap and efficient hardware implementation, so the idea to use W7 for image encryption purposes might be tempting. This is additionally motivated by the fact that using existing and tested ciphers instead of designing new ones is advised from a security's viewpoint.

4. THE PROPOSED ALGORITHM

In this section, we propose a new image encryption scheme that consists of a pixel shuffler unit and a stream cipher unit. Fig. 3 demonstrates the block diagram of the proposed algorithm. So far, many researchers suggested using combination of Pixel scrambling and symmetric encryption [2, 3, 13, 14]. Pixel scrambling has two important issues that are useful for image ciphering. It not only rearranges the pixel location (diffusion), but also changes the value of each pixel (confusion). Creating confusion in the image before applying the stream cipher is redundant and not only adds no enhancing property to the system but also increases the computational complexity. Confusion is

performed by stream cipher itself through nonlinear function operation. Pixel location displacement is appropriate before applying encryption, because unlike the text data has only two neighbours, each pixel in the image is in neighbourhood with eight adjacent pixels. For this reason, each pixel has a lot of correlation with its adjacent neighbours. However, it is very important to disturb the high correlation among image pixels to increase the security level of the encrypted images. In order to dissipate the high correlation among pixels, we proposed shuffling operation. Pixel shuffler unit consists of a permutation map that is applied in two different directions: vertical and horizontal, to decrease adjacent pixels correlation. A permutation matrix is an identity matrix with the rows and columns interchanged. It has a single 1 in each row and column; all the other elements are 0. The inverse of a permutation matrix is the same as its transpose, $P^{-1} = P^T$. So, no extra calculation is needed to compute the reciprocal matrix for decryption. This is a valuable property for cryptographic purposes that increases algorithm speed and decreases memory usage.

According to shuffling algorithm, a two-dimensional Henon map is employed as a pseudo-random number generator to build permutation matrix. Let's suppose that the plain-image is an $N \times N$ matrix. The shuffling algorithm is described as follows:

NoIt ← N

For it = 1: NoIt

(x_{n+1}, y_{n+1}) ← Henon (x_n, y_n)

V (it) ← $x_n + iy_n$

D (it) ← $\sqrt{x_n^2 + y_n^2}$

End For

Pmap ← Permutation map that is generated from D,

Pmap elements ∈ {0, 1}.

P ← Plain-image

For it = 1: NoIt

Vertical permutation ← Pmap × P (:, it)

Horizontal permutation ← P (it, :) × Pmap

End For

Fig.4 shows Shuffling in two directions with $(x_0, y_0) = (0.4, 0.3)$ as seed point. It is seen that, as we expected, the shuffling doesn't affect the plain-image histogram. This means that the corresponding statistical information in shuffled image is as same as the plain-image.

According to Shannon information theory, secure encryption systems provide some circumstances on information entropy [15]. So that:

$$H(P \mid C) = H(P), \qquad (2)$$

where C is cipher-image and P is plain-image. In order to satisfy equation (2), C should not give any information about P. To fulfil this desire cipher-image must be as random as possible. Since a plain-image that has history of uncertainty is distributed non-uniformly, an ideal cipher-image histogram has to approximate the uniform balanced distribution. Also each two adjacent pixels should be statistically non-correlated. This purpose cannot be achieved under a limited number of permutations. Permuted image cannot resist against statistical and known plaintext attacks [16, 17]. So after pixel permutation in two directions, the W7 algorithm is deployed. In gray scale image, each pixel has a value between 0-255. $P = \{P(i, j) : i, j = 0, 1, 2, ..., 255\}$, where P is set of pixels and (i, j) denotes pixel location. Hence, each pixel's length is 8 bits in $GF(2)$. Thus, image matrix is a binary sequence of $8 \times H \times W$ length, where H is number of rows and W is number of columns. W7 algorithm generates a pseudorandom cipher bit stream known as keystream, equal length to shuffled image binary sequence. Then these two bit streams are XOR-ed.

$$Shuffled\_image \oplus Keystream = Cipher\_image. \quad (3)$$

For decryption, cipher-image is XOR-ed with keystream then reverse shuffling operation is performed via inverse permutation map, i.e. $P^{-1} = P^T$.

5. VISUAL TESTING

The algorithm is applied with a 256-level gray scale TIF image that has the size of 256×256 and visual test is performed. Plain-image is encrypted by using the W7 secret key '00001000000008000 100002000010000' (in hexadecimal) and (x_0, y_0) = (0.4, 0.3) as the initial point of chaotic map. Fig. 5 demonstrates encryption result. By comparing the plain and cipher-image in Fig. 5, there is no visual information observed in the encrypted image.

6. SECURITY ANALYSIS

A good encryption procedure should be robust against all kinds of cryptanalytic, brute-force and statistical attacks. In this section, the performance of the proposed image encryption scheme is analyzed in detail.

6.1. Key Space Analysis

It is well known that a large key space is very important for an encryption algorithm to repel the brute-force attack. Since the algorithm has a 128-bit key, the key space size is 2^{128}. Furthermore, if we consider the two seed points of shuffler as part of the key, the key space size will be even larger. This means if the precision is 10^{-14}, then the key space can be $2^{128} \times 10^{14\times 2} \approx 2^{221} \approx 3.4\times 10^{66}$. Apparently, the key space is large enough to resist all kinds of brute-force attacks.

6.2. Histogram Analysis

To prevent the leakage of information to attackers, it is important to ensure that encrypted and original images do not have any statistical similarities. The histogram analysis clarifies how pixels in an image are distributed by plotting the number of pixels at each intensity level. Fig.5 shows histogram analysis on test image using proposed algorithm. The histogram of original image contains large sharp rises followed by sharp declines as shown in Fig. 5(c) and the histogram of the encrypted image as shown in Fig. 5(d) has uniform distribution which is significantly different from original image and has no statistical similarity in appearance. Therefore, the proposed algorithm does not provide any clue for statistical attack. The encrypted image histogram, approximated by a uniform distribution, is quite different from plain-image histogram. The uniformity caused by the proposed encryption scheme is justified by the chi-square test [18, 19] as follows:

$$\chi^2 = \sum_{k=1}^{256} \frac{(v_k - 256)^2}{256}, \qquad (4)$$

where k is the number of gray levels (256), v_k is the observed occurrence frequencies of each gray level (0–255), and the expected occurrence frequency of each gray level is 256. With a significance level of 0.05, it is found that $\chi^2_{test} < \chi^2(255, 0.05)$, implying that the null hypothesis is not rejected and the distribution of the encrypted histogram is uniform. Relatively uniform distribution in cipher-image histogram points out good quality of method.

6.3. Information Entropy

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon [20]. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(m) = \sum_{i=0}^{2N-1} P(m_i) \log_2 \frac{1}{P(m_i)}, \qquad (5)$$

where $P(m_i)$ represents the probability of symbol m_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., $m = \{m_1, m_2, ..., m_{2^8}\}$. Truly random source entropy is equal to 8. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. Let us consider the cipher-image in Fig. 5(b), the number of occurrence of each gray level is recorded and the probability of occurrence is computed. The entropy is as follows:

$$H(m) = \sum_{i=0}^{255} P(m_i) \log_2 \frac{1}{P(m_i)} = 7.9904 \approx 8. \qquad (6)$$

The value obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack.

6.4. Correlation Coefficient Analysis

There is a very good correlation between adjacent pixels in the image data [21]. Equation (7) is used to study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations.

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_j)^2) \times (N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}}, \qquad (7)$$

where x and y are intensity values of two neighbouring pixels in the image and N is the number of adjacent pixels selected from the image to calculate the correlation. 1000 pairs of two

adjacent pixels are selected randomly from image to test correlation. Correlation test image is depicted in Fig. 5(a). Fig. 6 shows the correlation distribution of two adjacent pixels in the plain-image and cipher-image. It is observed that neighbouring pixels in the plain-image are correlated too much, while there is a little correlation between neighbouring pixels in the encrypted image. Results for correlation coefficients are shown in table 1.

6.5. Differential analysis

In general, a desirable property for an encrypted image is being sensitive to the small changes in plain-image (e.g., modifying only one pixel). Opponent can create a small change in the input image to observe changes in the result. By this method, the meaningful relationship between original image and encrypted image can be found. If one small change in the plain-image can cause a significant change in the cipher-image, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. Three common measures were used for differential analysis: MAE, NPCR and UACI [22, 23]. MAE is mean absolute error. NPCR means the number of pixels change rate of ciphered image while one pixel of plain-image is changed. UACI which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image.

Let $C(i, j)$ and $P(i, j)$ be the gray level of the pixels at the ith row and jth column of a $W \times H$ cipher and plain-image, respectively. The MAE between these two images is defined in

$$MAE = \frac{1}{W \times H} \sum_{j=1}^{W} \sum_{i=1}^{H} |C(i,j) - P(i,j)|. \quad (8)$$

Consider two cipher-images, C_1 and C_2, whose corresponding plain-images have only one pixel difference. The NPCR of these two images is defined in

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \quad (9)$$

where $D(i,j)$ is defined as

$$D(i,j) = \begin{cases} 0, & if \quad C_1(i,j) = C_2(i,j), \\ 1, & if \quad C_1(i,j) \neq C_2(i,j). \end{cases} \quad (10)$$

Another measure, UACI, is defined by the following formula:

$$UACI = \frac{1}{W \times H} \times \sum_{i,j} \left[\frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times 100\%. \quad (11)$$

Tests have been performed on the proposed scheme on a 256-level gray scale image of size 256×256 shown in Fig. 5(a). The MAE experiment result is shown in table 2. It is illustrated that there is a fluctuation between MAE of row and column-row permuted image. The MAE of Column-row permuted image is about 9 percent more than MAE of row permuted image while the MAE of encrypted image is 21 percent more than MAE of shuffled image. The larger the MAE value, the better the encryption security. The NPCR and UACI test results are shown in table 3. Results obtained from NPCR show that the encryption scheme's sensitivity to small changes in the input image is under 0.01%. The UACI estimation result shows that the rate influence due to one pixel change is very low. The results demonstrate that a swiftly change in the original image will result in a negligible change in the ciphered image. The reason lies in the mode of operation. The function of shuffler and W7 operates in counter mode and does not mangle plaintext in a complicated way.

6.6. Sensitivity analysis

An ideal image encryption procedure should be sensitive with the secret key. It means that the change of a single bit in the secret key should produce a completely different cipher-image. Fig. 7 shows key sensitivity test result. It can be observed that the decryption with a slightly different key (different secret key or initial values) fails completely. Therefore, the proposed image encryption scheme is highly key sensitive.

6.7. Image Sequence Randomness Test

To ensure the security of a cryptosystem the cipher must have some properties such as good distribution, long period, high complexity and efficiency. In particular, the outputs of a cryptosystem must be unpredictable in the absence of knowledge of the inputs. Recently, the NIST designed a set of different statistical tests to justify randomness of binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators. These tests focus on a variety of different types of non-randomness that could exist in a sequence. The mathematical description of each test can be found at [24]. So, we used the NIST test suite in order to test the randomness of the surveyed algorithms. In

all tests if the computed *P*-value is < 0.01, then conclude that the sequence is non-random. Otherwise, conclude that the sequence is random.

Fig. 8 illustrates that the image sequence encrypted by the proposed scheme has no defect and passes all the statistical tests with high *P*-values.

7. CONCLUSION

In this paper, an encryption scheme based on combination of a chaotic map and stream cipher is presented. The proposed encryption system included two major parts, chaotic pixels shuffling and W7. A chaotic map is used to generate a permutation matrix in two orientations to build shuffler. Henon map is a good candidate for permutation matrix generation. Permutation matrix has a desirable property that its inverse is known. Thus, much memory is saved in decryption process. All parts of the proposed chaotic encryption system were simulated using MATLAB. Shuffling expands diffusion property and decreases vertical, horizontal and diagonal correlation of two adjacent pixels. The number of occurrence for each grey level in the image is not changed after pixel shuffling. So shuffled image histogram is the same as plain-image histogram. The proposed schemes key space is large enough to resist all kinds of brute-force attacks. Theoretical and experimental results indicate that the cipher-image histogram of the proposed scheme is so even that the entropy measured is almost equal to the ideal value. The uniformity of cipher-image histogram was justified by the chi-square test. Research results show that the proposed scheme has resistance to statistical attacks. The differential analysis results illustrate that a small change in the original image will result in a negligible change in the ciphered image. The MAE experiment result showed that the MAE value increases through each level of algorithm. Sensitivity analysis shows that the proposed encryption scheme is sensitive to the key; a small change of the key will generate a complete different decryption result and cannot get the correct plain-image. Randomness test results showed that the new scheme has no defect and passes all the statistical tests with high *P*-values. According to latter discussions, it seems that the proposed encryption scheme can be a potential candidate for image encryption.

REFRENCES:

[1] M. Sharma and M.K. Kowar, "Image Encryption Techniques Using Chaotic Schemes: a Review," *International Journal of Engineering Science and Technology*, vol. 2, no. 6, 2010, pp. 2359–2363.

[2] A. Jolfaei and A. Mirghadri, "An Applied Imagery Encryption Algorithm Based on Shuffling and Baker's Map," *Proceedings of the 2010 International Conference on Artificial Intelligence and Pattern Recognition (AIPR-10)*, Florida, USA, 2010, pp. 279–285.

[3] A. Jolfaei and A. Mirghadri, "A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1," *Proceedings of The 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI10)*, Sanya, China, 2010.

[4] L. Xiangdong, Z. Junxing, Z. Jinhai, and H. Xiqin, "Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation," *IJCSNS International Journal of Computer Science and Network Security*, vol. 8, no. 1, 2008, pp. 64–68.

[5] Z.H. Guan, F. Huang, and W. Guan, "Chaos-Based Image Encryption Algorithm," *Physics Letters A*, vol. 346, 2005, pp. 153– 157.

[6] M. Suneel, "Cryptographic Pseudo-random Sequences from the Chaotic Henon Map," *Sadhana*, vol. 34, no. 5, 2009, pp. 689–701.

[7] V. Patidar, N.K. Pareek, G. Purohit, and K.K. Sud, "Modified Substitution–Diffusion Image Cipher Using Chaotic Standard and Logistic Maps," *Commun Nonlinear SciNumer Simulat*, vol. 15, 2010, pp. 2755–2765.

[8] M. Henon, "A Two-Dimensional Mapping with a Strange Attractor," *Communication in Mathematical physics*, vol. 50, 1976, pp. 69–77.

[9] R. Forre, "The Henon Attractor as Key Stream Generator," *Abstracts of Eurocrypt 91*, 1991, pp. 76–80.

[10] R.A. Rueppel, "Analysis and Design of Stream Ciphers," Springer, 1986.

[11] S. Thomas, D. Anthony, T. Berson, and G. Gong, "The W7 Stream Cipher Algorithm," *Internet Draft*, April 2002.

[12] Alex Biryukov, Adi Shamir, David Wagner, "Real time cryptanalysis of A5/1 on a PC," *FSE'2000, LNCS 1978*, Springer, 2001, pp. 1–18.

[13] A.S. Alghamdi, H. Ullah, M. Mahmud, and M.K. Khan, "Bio-Chaotic Stream Cipher-Based Iris Image Encryption," *Proceedings of*

the International Conference on Computational Science and Engineering, 2009, pp. 739–744.

[14] X.Y. Yu, J. Zhang, H.E. Ren, G.S. Xu1, and X.Y. Luo, "Chaotic Image Scrambling Algorithm Based on S-DES," *Journal of Physics: Conference Series*, vol. 48, 2006, pp. 349–353.

[15] D.R. Stinson, Cryptography theory and practice. Chapman and Hall/CRC, pp. 45–70.

[16] J.K. Jan and Y.M. Tseng, "On the Security of Image Encryption Method," *Information Processing Letters*, vol. 60, no. 5, 1996, pp. 261–265.

[17] S. Li, C. Li, G. Chen, N.G. Bourbakis, and K.T. Lo, "A General Quantitative Cryptanalysis of Permutation-only Multimedia Ciphers against Plaintext Attacks," Signal Processing: Image Communication, vol. 23, no. 3, 2008, pp. 212–223.

[18] P. L'ecuyer and R. Simard, "TestU01: A C Library for Empirical Testing of Random Number Generators," *ACM Transactions on Mathematical Software*, vol. 33, no. 4, Article 22, 2007.

[19] A. Jolfaei and A. Mirghadri, "Survey: Image Encryption Using A5/1 and W7," *Journal Of Computing*, vol. 2, no. 8, 2010, ISSN 2151–9617.

[20] C.E. Shannon, "Communication Theory of Secrecy Systems," *Bell Syst Tech J*, vol. 28, 1949, pp. 656–715.

[21] H.H. Ahmed, H.M. Kalash, and O.S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images," *Journal of Optical Engineering*, vol. 45, 2006.

[22] A.N. Pisarchik and M. Zanin, "Image Encryption with Chaotically Coupled Chaotic Maps," *Physica D*, vol. 237, no. 20, 2008, pp. 2638–2648.

[23] G. Chen, Y. Mao, and C. Chui, "A Symmetric Image Encryption Scheme Based on 3d Chaotic Cat Maps," *Chaos, Solitons & Fractals*, vol. 12, 2004, pp. 749–761.

[24] A. Rukhin et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST Special Publication 800-22*, Revision 1a, 2010.

AUTHOR PROFILES:

Alireza Jolfaei received the Bachelor's degree in

Biomedical Engineering in the field of Bio-electric with the honor degree from Islamic Azad University, Science and Research branch, Tehran, Iran in 2007 and Master's degree in Telecommunication in the field of Cryptography with the honor degree from IHU, Tehran, Iran in 2010. He was a chosen student in the first meeting of honor students of Islamic Azad University, Science and Research Branch in 2005. Currently, he is a TA at the faculty and research center of communication and information technology, IHU, Tehran, Iran. His research interest includes: Cryptography, Information Systems Security, Network Security, Image Processing and Electrophysiology.

Abdolrasoul Mirghadri received the B.Sc., M.Sc. and PHD degrees in

Mathematical Statistics, from the faculty of Science, Shiraz University in 1986, 1989 and 2001, respectively. He is an assistant professor at the faculty and research center of communication and information technology, IHU, Tehran, Iran since 1989. His research interest includes: Cryptography, Statistics and Stochastic Processes. He is a member of ISC, ISS and IMS.

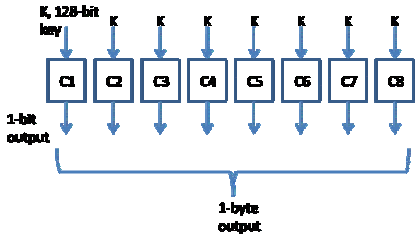


Figure 1. W7 key stream generator.

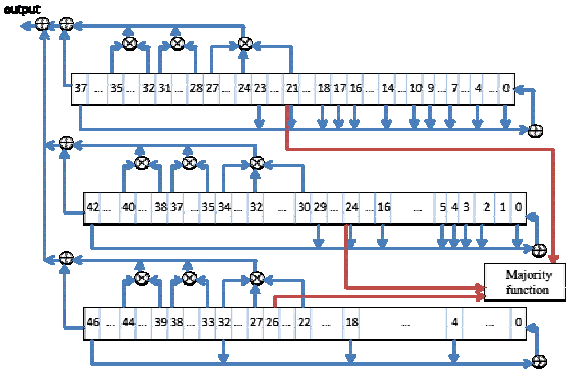


Figure 2. Diagram of C2 Block in W7 stream cipher.

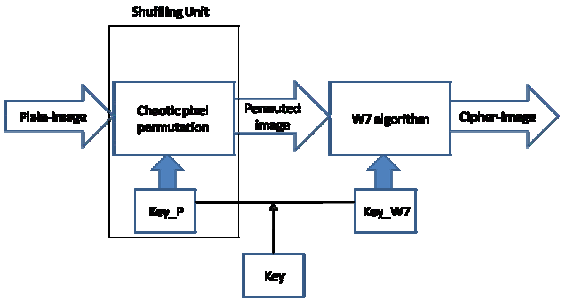
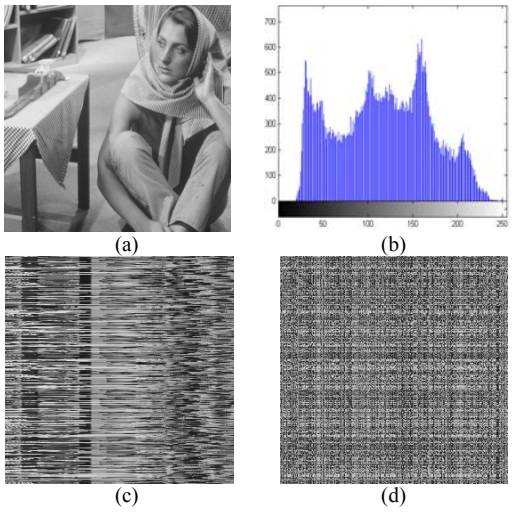


Figure 3. Block diagram of the proposed scheme.



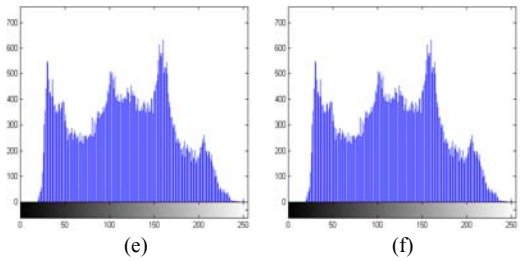


Figure 4. Shuffling using Henon map: (a) plain-image, (b) plain-image histogram, (c) horizontal permutation, (d) vertical and horizontal permutation, (e) horizontal permutated image histogram, (d) histogram of permuted image in vertical and horizontal directions.

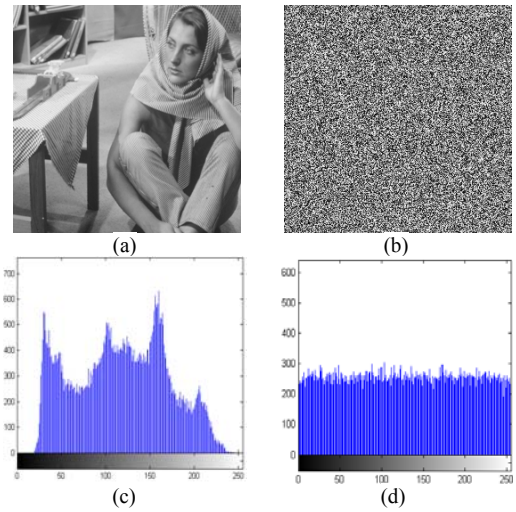
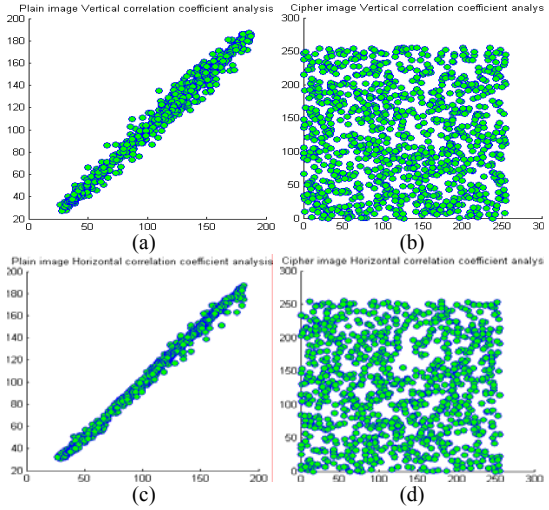
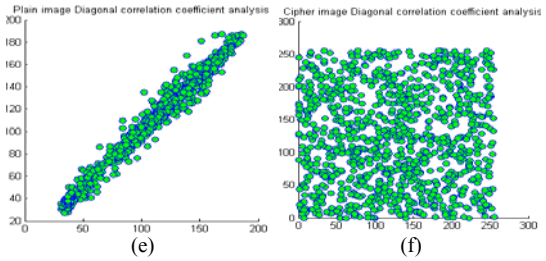


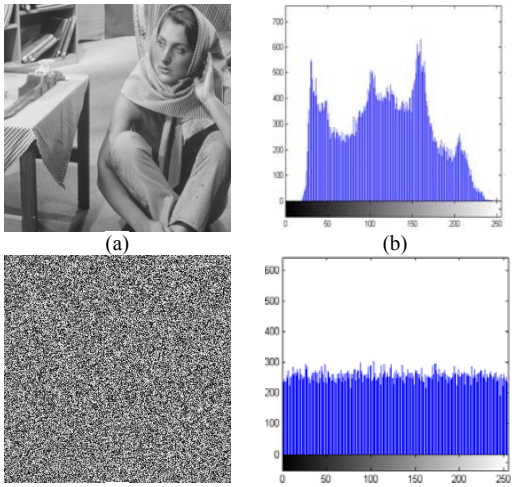
Figure 5. Visual test result: (a) plain-image, (b) encrypted image, (c) plain-image histogram, (d) cipher-image histogram.





(e) (f)

Figure 6. Correlation of two adjacent pixels: (a) distribution of two vertically adjacent pixels in the plain-image, (b) distribution of two vertically adjacent pixels in the cipher-image, (c) distribution of two horizontally adjacent pixels in the plain-image, (d) distribution of two horizontally adjacent pixels in the cipher-image, (e) distribution of two diagonally adjacent pixels in the plain-image, (d) distribution of two diagonally adjacent pixels in the cipher-image.



(a) (b)

(c) (d)

Figure 7. Key sensitivity test: (a) plain-image, (b) plain-image histogram, (c) Decrypted image with wrong key, (d) Decrypted image with wrong key histogram.

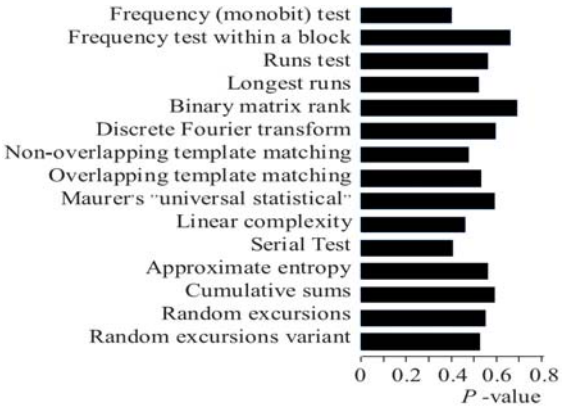


Figure 8. Results of NIST tests for the image sequence encrypted by the proposed scheme.

Table 1. Correlation coefficients of two adjacent pixels in the proposed method.

Correlation Coefficient Analysis		
Image	**Adjacent pixels orientation**	
	Vertical	**Horizontal**
Plain-image	0.9924	0.9976
Cipher-image	0.0038	0.0096

Table 2. A comparison of MAE of methods used in the proposed scheme.

Method	**MAE**
Row permuted image	56.0851
Column-row permuted image	61.4098
Encrypted image after shuffling	74.7693

Table 3. NPCR and UACI of proposed method.

NPCR	**UACI**
0.0015 %	0.0005%