Image Encryption Using Chaos and Block Cipher

Alireza Jolfaei (Corresponding author)
Faculty and Research Center of Communication and Information Technology
IHU Tehran, Iran
E-mail: Jolfaei@yahoo.com

Abdolrasoul Mirghadri
Faculty and Research Center of Communication and Information Technology
IHU, Tehran, Iran
E-mail: Amrghdri@ihu.ac.ir

The research is financed by Cryptography Research Center (CRC).

Abstract

In this paper, a novel image encryption scheme is proposed based on combination of pixel shuffling and new modified version of simplified AES. Chaotic baker's map is used for shuffling and improving S-AES efficiency through S-box design. Chaos is used to expand diffusion and confusion in the image. Due to sensitivity to initial conditions, chaotic baker's map has a good potential for designing dynamic permutation map and S-box. In order to evaluate performance, the proposed algorithm was measured through a series of tests. These tests included visual test and histogram analysis, randomness test, information entropy, encryption quality, correlation analysis, differential analysis and sensitivity analysis. Experimental results show that the new cipher has satisfactory security and is more efficient than AES which makes it a potential candidate for encryption of multimedia data.

Keywords: Image encryption, Shuffling, Simplified AES, Chaos, Baker's map, S-box

1. Introduction

Visual information and imagery play an important role in almost all areas of our lives. Due to the substantial increase in use of computers, there is an increasing tendency to security and image fidelity verification. Transmitted images may have different applications, such as commercial, military and medical applications. So it is necessary to encrypt image data before transmission over the network to preserve its security and prevent unauthorized access. However, compared to text, much more processing power and bandwidth for processing is required. In recent years a number of different image encryption schemes have been proposed in order to overcome image encryption problems (Lv, Zhang, & Guo, 2009) (Akhshani et al., 2010) (Jolfaei & Mirghadri, 2010a). Due to desirable properties of non-linear dynamical systems such as pseudo-random behavior, sensitivity to initial conditions and ergodicity, the chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption.

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 possibility of creating very long length keys. 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 analyze the security of the proposed image cipher and evaluate its performance through various tests such as statistical analysis, differential analysis, key sensitivity analysis, etc and compare the results. Finally, some conclusions are given in section 6.

2. Chaos and cryptography

Cryptography is the knowledge of protecting the privacy of information during communication under antagonistic situations. Nowadays, cryptography plays an important role in the developing information technologies and proliferating computer network communications. Current cryptographic methods are based on

number theoretic or algebraic concepts. Chaos is another paradigm, which seems promising. Chaos is one of the possible behaviors associated with evolution of a nonlinear dynamic system and occurs for specific values of system parameters. The chaotic behavior is a delicate behavior of a nonlinear system, which apparently looks random. The discovery of this pseudo-random behavior happening as a result of deterministic systems turned out to be quite revolutionary leading to many issues interconnecting stability theory, new geometrical features and new signatures characterizing dynamical performances. The chaotic state can be observed by the existence in the phase space of a chaotic attractor or fractal in which all the system trajectories evolve following a certain pattern but are never the same. In a more analytical approach the chaotic state can be very well studied by the Lyapunov exponents that globally characterize the behavior of dynamical systems (Kocarev et al., 2006). Chaos will be observed only when there is at least one positive Lyapunov exponent and the total sum of all exponents is negative, i.e. the dynamical system has a stable but random like state called chaotic state.

In the last two decades, Chaos theory has received a great deal of attention from the cryptographic community. So, a remarkable number of chaotic systems, both physical and mathematical, were designed for realizing encryption and decryption of messages in both hardware and software equipments (Patidar, Pareek & Sud, 2009) (Etemadi Borujeni & Eshghi, 2009) (XiaoJun & MingGen, 2010).

Chaos based cryptography is still in its childhood and may not have exact parallelism to concepts and notions of traditional cryptographic and cryptanalysis approaches. However, chaotic maps and cryptographic algorithms have some similar properties: Pseudo-random behavior, sensitivity to initial conditions and parameters and unstable orbits with long periods, depending upon the precision of the numerical implementation. Encryption rounds of a cryptographic algorithm lead to diffusion and confusion properties. In a similar manner, iterations of the chaotic map spread the initial region over the entire phase space.

3. Methods

We used baker's map and S-AES algorithm to construct our new approach that are described as follows:

3.1 Baker's map

The baker's map, invented by Eberhard Hopf in 1937, is an intuitively accessible, two-dimensional chaos-generating discrete dynamical system (Fridrich, 1998) (Machado, Baptista & Grebogi, 2004). This is a simple example of a map similar to a horseshoe, although it is a discontinuous map (Lichtenberg & Lieberman, 1992). Consider the map F for the half-open square $[0,1)\times[0,1)$ onto itself where

$$F(x,y)=(\sigma(x),g(a,x,y)), \tag{1}$$

$$\sigma(x)=2x \mod 1,\ 0\le\sigma(x)<1, \tag{2}$$

$$g(a,x,y)=\begin{Bmatrix}\frac{1}{2}ay & 0\le x<\frac{1}{2}\\ \frac{1}{2}(ay+1) & \frac{1}{2}\le x<1\end{Bmatrix}\mod 1,\ 0\le g<1. \tag{3}$$

Note that (0, 0) is the only fixed point of F, and it is unstable. The Jacobian matrix of F is $J=\begin{bmatrix}2 & 0\\ 0 & \frac{1}{2}a\end{bmatrix}$ for almost all x, so $\det(J)=a$. Therefore F is area preserving if and only if $a=\pm1$.

Consider first the case $a=1$. Then the geometrical nature of the map is depicted in figure 1(a), where it is seen that the map is equivalent to a horizontal stretching and vertical contraction, followed by a vertical cutting and stacking. This resembles the preparation of dough, so F is often called the baker's transformation (Lichtenberg & Lieberman, 1992). When $0<a<1$, areas are contracted by F. We show $F(S)$ in figure 1(b), where S is the unit square.

The iterative relation of the baker's map used in the proposed scheme is as follows (Otto & Denier, 2005):

$$x_{n+1}=(x_n+y_n)\,|\,1,\ y_{n+1}=(x_n+2y_n)\,|\,1. \tag{4}$$

Figure 2 demonstrates the pseudo-random number sequence generated by baker's map for the initial points of x_0 = 0.5 and y_0 = 0.4 for 100 iterations.

3.2 Simplified AES

Simplified AES was developed by Musa in 2003, as an educational tool to explain the Advanced Encryption Standard properties. It was designed so that the two primary attacks on symmetric-key block ciphers of that time, differential cryptanalysis and linear cryptanalysis, are not trivial on simplified AES. S-AES is simplified version of AES algorithm (Mansoori & Khaleghei Bizaki, 2007) and has similar properties and structure to AES with much smaller parameters. It operates on 16-bit plaintexts and generates 16-bit cipher texts, using the expanded key $k_0, k_1, \ldots, k_{47}$. It has 2 ciphering rounds. Both the key expansion and encryption algorithms of S-AES depend on an S-box that depends on the finite field with 16 elements. Figure 3 depicts the overall structure of S-AES. In comparison with AES, S-AES has less number of rounds and operates faster. So, using S-AES for image encryption purposes might be tempting. We also recommend the article (Musa, Schaefer & Wedig, 2003) for an excellent and accessible explanation of the S-AES algorithm.

4. The proposed algorithm

In this paper, a new image encryption scheme is proposed that consists of a pixel shuffler unit and a block cipher unit. So far several different cryptographic systems have been presented for image ciphering. Many researchers suggested using combination of Pixel scrambling and symmetric encryption (Chen, Mao & Chui, 2004) (Yang, Bourbakis & Li, 2004) (Jolfaei & Mirghadri, 2010b). 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 private key encryption is redundant and not only adds no enhancing property to the system but also increases the computational complexity. The computational complexity is a big concern due to the limited bandwidth in wireless data networks, processing limitations, memory limitations and time constraints. So there should be a tradeoff between speed, security and flexibility. Perturbation is performed by block cipher itself through S-box operation. Pixel location displacement is appropriate before applying encryption, because unlike the text data that has only two neighbors, each pixel in the image is in neighborhood with eight adjacent pixels. For this reason, each pixel has a lot of correlation with its adjacent neighbors. Thus, it is important to disturb the high correlation among image pixels to increase the security level of the encrypted images. In order to resist against cryptanalyst's correlation and statistical attack, correlation is dissipated using chaotic permutation matrix. 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. Permutation map is applied in three different directions vertical, horizontal and diagonal to decrease adjacent pixels correlation. Let's suppose that the plain-image is an $N \times N$ matrix. The shuffling algorithm is described as follows:

Algorithm 1. Shuffling algorithm

NoIt ← N
For it = 1: NoIt **do**
    (x_{n+1}, y_{n+1}) ← baker (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 $\in \{0, 1\}$.
P ← Plain-image
For it = 1: NoIt **do**
    Vertical permutation ← Pmap × P (:, it)
    Horizontal permutation ← P (it, :) × Pmap
End For
For it = 2: NoIt **do**
    Shiftsize ← The shift amount for the it-*th* row of plain-image, that is (NoIt-it+1)
    C ← Circularly right shifted pixels in it-*th* row of plain-image, by Shiftsize elements
End For

17: VC ← Vertical permutation in C

18: **For** it = 2: NoIt **do**

19: Shiftsize ← The shift amount for the it-*th* row of VC, that is (NoIt-it+1)

20: Diagonally permuted image ← Circularly left shifted pixels in it-*th* row of VC, by (-Shiftsize) elements.

21: **End For**

Figure 4 shows the pixels spatial permutation in Tehran's satellite image using baker's map. It is seen that, as we expected, the image histogram is not affected by pixels shuffling.

According to Shannon information theory, secure encryption systems provide some circumstances on information entropy (Shannon, 1949). So that:

$$H(P \mid C) = H(P). \tag{5}$$

According to equation (5), C (cipher-image) should not give any information about P (plain-image). To fulfill 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 (Li et al., 2008**)**. So after pixel shuffling in three directions, the S-AES cryptosystem is implemented. Figure 5 illustrates the block diagram of the proposed algorithm. The only nonlinear element in the S-AES algorithm is S-box. Therefore, the scheme security essentially relies on the S-box. In fact, the S-box design is heart of block cipher design. The S-box can be defined as a Boolean mapping $B_2^m \rightarrow B_2^n$, where $B_2 = \{0, 1\}$.

So far, the S-box design criteria for one of the most famous block ciphers, *DES*, after several decades was dubious. On the other hand, designers of new block ciphers usually express hypothetical conditions for S-box design. The S-box in AES was selected through mathematical calculations. AES divides the input block into a four by four array of bytes, while S-AES divides it into a two by two array of nibbles, which are four bits long. In the first and second round of S-AES algorithm, an S-box is used to substitute each nibble into a new nibble. In computer, the S-box substitution is performed using a lookup table. We used baker map to generate dynamic S-boxes as the replacement of the S-box of S-AES to attain chaos-based block cipher. The chaotic baker mapping has good level of unpredictability and irregularity. We quantized its outputs to make dynamic S-box as follows:

Algorithm 2. S-box generation algorithm

1: NoIt ← number of iterations that is 16

2: **For** it1 = 1: NoIt **do**

3: (x_{n+1}, y_{n+1}) ← baker (x_n, y_n)

4: V (it1) ← x_n+iy_n

5: D (it1) ← $\sqrt{x_n^2 + y_n^2}$

6: **End For**

7: **For** it1 = 1: NoIt **do**

8: M ← Max {D}

9: **For** it2 = 1: NoIt **do**

10: **If** D (it2) == M **do**

11: D (it2) ← -16 + it1

12: **End If**

13: **End For**

14: **End For**

15: S-box ← |D|

Table 1 shows a generated S-box using x = 0.2 and y = 0.3 as seed points of chaotic mapping. In this table, the intermediary output of the inversion is not shown.

So, an equivalent replacement block for the S-box is built using two-dimensional chaotic baker's map. The new generated S-box is reversible and has random properties. According to the proposed scheme, each time that the cryptographic algorithm runs, a new S-box is generated according to a seed point derived from an external secret key. Hence, encrypting the same plain-images leads to different cipher-images. Using dynamic S-box increases schemes resistance against differential and linear cryptanalysis and causes an increase in the system security. Since the structure of the S-boxes is completely hidden from the cryptanalyst, these attacks have a more difficult time exploiting that structure. Moreover, these S-boxes can be created on demand, reducing the need for large data structures stored with the algorithm. The essential cryptographic characteristics and requirements for obtaining good S-box have been checked and results showed the satisfactory level of them.

5. Security analysis

In this section we performed a series of test to justify the efficiency of the proposed image encryption scheme and compared the results with AES. The evaluation consisted of theoretical derivations and practical experimentation. A good encryption scheme should resist all kinds of known attacks, such as known plaintext attack, ciphertext-only attack, statistical attack, differential attack and various brute-force attacks. We used the following quantitative measures to evaluate the security of the proposed image encryption scheme (Jolfaei & Mirghadri, 2010c).

5.1 Visual test and histogram analysis

The algorithm is implemented on a computer with processor Intel Pentium V, 2.00GHz Dual. Input test plain-image is a 256-level gray scale image with the size of 128×128. In figure 6, (a) input image, (b) shuffled image and (c) cipher-image is shown. Plain-image, shuffled image and cipher-image histograms are depicted in figures 6(d), 6(e) and 6(f), respectively. The histogram of shuffled image is similar to the histogram of plain-image. This means that the corresponding statistical information in shuffled image is as equal as the plain-image. The encrypted image histogram, approximated by a uniform distribution, is quite different from plain-image histogram. Uniformity caused by encryption algorithm is justified by the chi-square test (L'Ecuyer & Simard, 2007) described as follows:

$$\chi^2 = \sum_{k=1}^{256} \frac{(v_k - 64)^2}{64}, \tag{6}$$

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 64. Assuming a significant level of 0.05, $\chi^2(255, 0.05) = 293$, chi-square value for the final encrypted image of the proposed system is 216. This implies that the null hypothesis is not rejected and the distribution of the encrypted histogram is uniform, $\chi^2_{test} < \chi^2(255, 0.05)$.

Relatively uniform distribution in cipher-image histogram points out good quality of method. 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 that, how the pixel values of image are distributed. Figure 7 shows histogram analysis on several images having different contents and sizes using proposed algorithm. The histogram of original images contains large sharp rises followed by sharp declines as shown in figure 7(c). And the histogram of the encrypted images as shown in figure 7(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. Plain-images and cipher-images are shown in figures 7(a) and 7(b), respectively.

5.2 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 test 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 (Rukhin et al., 2010). So, we used the NIST test suite in order to test the randomness of the surveyed algorithm. 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.

Figure 8 depicts the NIST tests results and illustrates that the image sequences encrypted by the AES and the proposed scheme have no defect and pass all the statistical tests with high *P*-values.

5.3 Information entropy

Information theory is the mathematical theory of data communication and storage founded in 1949 by Shannon (Stinson, 1995). Modern information theory is concerned with error-correction, data compression, cryptography, communications systems, and related topics. It is well known that the entropy $H(s)$ of a message source s can be calculated as:

$$H(s) = \sum_{i=0}^{2N-1} P(s_i) \log_2 \frac{1}{P(s_i)}, \tag{7}$$

where $P(s_i)$ represents the probability of symbol s_i and the entropy is expressed in bits. Let us suppose that the source emits 2^8 symbols with equal probability, i.e., $s = \{s_1, s_2, ..., s_{2^8}\}$. After evaluating equation (7), we obtain its entropy $H(s) = 8$, corresponding to a truly random source. 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 ciphertext of the plain-image shown in figure 4(a). The number of occurrence of each gray level is recorded and the probability of occurrence is computed. The entropy is as follows:

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)} = 7.9902 \approx 8. \tag{8}$$

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.

5.4 Measurement of encryption quality

Image encryption quality measure is a figure of merit used for the evaluation of image encryption techniques. With the application of encryption to an image a change takes place in pixels values as compared to those values before encryption. Such change may be irregular. This means that the higher the change in pixels values, the more effective will be the image encryption and hence the encryption quality. So the encryption quality may be expressed in terms of the total changes in pixels values between the original image and the encrypted one. A measure for encryption quality may be expressed as the deviation between the original and encrypted image (Ahmed, Kalash & Farag Allah, 2006) (Jolfaei & Mirghadri, 2010d). The quality of image encryption may be determined as follows:

Let P and C denote the original image and the encrypted image respectively, each of size $H \times W$ pixels with L grey levels. $P(x, y), C(x, y) \in \{0, ..., L-1\}$ are the grey levels of the images P and C at position (x, y), $0 < x < H-1$, $0 < y < W-1$. We will define $H_L(P)$ as the number of occurrence for each grey level L in the original image (plain-image), and $H_L(C)$ as the number of occurrence for each grey level L in the encrypted image (cipher-image). The encryption quality represents the average number of changes to each grey level L and it can be expressed mathematically as:

$$Encryption \quad Quality = \frac{\sum_{L=0}^{255} |H_L(C) - H_L(P)|}{256}. \tag{9}$$

The encryption quality test was performed using the input image of size 128×128 shown in figure 4(a). The encryption quality of the proposed scheme is 70.6250 while the encryption quality of AES is 69.5250.

5.5 Correlation coefficients analysis

In the image data each pixel is highly correlated with its adjacent pixels (Pisarchik & Zanin, 2008). An ideal encryption algorithm should produce the cipher-images with no such correlation in the adjacent pixels. Following equations are used to study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations.

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{10}$$

$$D(x) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N}x_j)^2, \tag{11}$$

$$Cov(x,y) = \frac{1}{N}\sum_{j=1}^{N}(x_j - \frac{1}{N}\sum_{j=1}^{N}x_j)(y_j - \frac{1}{N}\sum_{j=1}^{N}y_j). \tag{12}$$

x and y are intensity values of two neighboring pixels in the image and N is the number of adjacent pixels selected from the image to calculate the correlation. Figure 9 illustrates results for analysis of correlation coefficients for a gray-scale image of size 1000×1000 shown in figure 7(a). 1000 pairs of two adjacent pixels are selected randomly from image to test correlation. It is observed that neighboring pixels in the plain-image are correlated too much while there is a little correlation between neighboring pixels in the encrypted image.

5.6 Difference between cipher and plain-images

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. To test the influence of one-pixel change on the whole image encrypted by the proposed algorithm, three common measures were used: MAE, NPCR and UACI (Chen, Mao & Chui, 2004) (Alvarez & Li, 2006). 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 $H \times W$ cipher and plain-image, respectively. The MAE between these two images is defined in

$$MAE = \frac{1}{H \times W}\sum_{i=0}^{H-1}\sum_{j=0}^{W-1}|C(i,j) - P(i,j)|. \tag{13}$$

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

$$NPCR = \frac{\sum_{i,j} D(i,j)}{H \times W} \times 100\%, \tag{14}$$

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

$$D(i,j) = \begin{cases} 0, & if \quad C_1(i,j) = C_2(i,j), \\ 1, & if \quad C_1(i,j) \neq C_2(i,j). \end{cases} \tag{15}$$

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

$$UACI = \frac{1}{H \times W} \times \sum_{i,j}[\frac{|C_1(i,j) - C_2(i,j)|}{255}] \times 100\%. \tag{16}$$

Tests have been performed on the proposed scheme, about the one-pixel change influence on a 256 gray-scale image of size 128×128. The MAE experiment result is shown in table 2. It is illustrated that there is a slight fluctuation between MAE of row, column-row and diagonal-column-row permuted image. The MAE of shuffled image is about 32 while the MAE for encrypted image is about 84. The MAE of encrypted image is 159 percent more than MAE of shuffled image. The larger the MAE value, the better the encryption security. Also, the MAE value of proposed scheme is about 1 percent higher than AES's. The NPCR and UACI test results are shown in table 3. Results obtained from NPCR show that the encryption scheme is not sensitive to small changes in the input image. 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.

5.7 Key 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. For testing the key sensitivity of the encryption schemes under study, the test image shown in figure 4(a) is encrypted using the proposed algorithm. The seed points used for chaotic S-box are $(x_1, y_1) = (0.1, 0.6)$ and $(x_2, y_2) = (0.11, 0.6)$. Figure 10 shows key sensitivity test result. It is not easy to compare the encrypted images by simply observing these images. So for a better comparison, the cipher-images histograms are depicted in figure 10. It can be observed that two encrypted images with a slightly different key are quite different.

6. Conclusion

In this paper, an image encryption scheme based on combination of chaotic baker's map and modified version of S-AES is presented. Baker's map is used to generate a permutation matrix, which is in turn used to generate S-box in the S-AES algorithm. All parts of the proposed chaotic encryption system were simulated using computer code. Pixel shuffling expands diffusion property and dissipates 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. Theoretical and experimental results indicate that the cipher-image histogram distribution of the proposed scheme is so even that the entropy measured is almost equal to the ideal value. The histogram uniformity was justified by the chi-square test. According to NIST randomness tests the image sequence encrypted by the proposed algorithm and AES have no defect and pass all the statistical tests with high *P*-values. The measured encryption quality showed that the proposed scheme has a better encryption quality than the AES. Correlation analysis showed that correlation coefficients between adjacent pixels in the plain-image are significantly decreased after applying encryption function. To quantify the difference between encrypted image and corresponding plain-image, three measures were used: MAE, NPCR and UACI. The MAE experiment result showed that the MAE value of proposed scheme rises through each level of algorithm. Also, the new algorithm has a bigger MAE value than AES. Differential analysis showed that a swiftly change in the original image will result in a negligible change in the ciphered image. Consequently, the proposed scheme has a high security which is due to characteristics of baker's chaotic system.

References

Ahmed, H.H., Kalash, H.M., & Farag Allah, O.S. (2006). Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images. *Journal of Optical Engineering*, 45.

Akhshani, A., Behnia, S., Akhavan, A., Abu Hassan, H., & Hassan, Z. (2010). A Novel Scheme for Image Encryption Based on 2D Piecewise Chaotic Maps. *Optics Communications,* 283, 3259-3266.

Alvarez, G., & Li, S. (2006). Breaking an Encryption Scheme Based on Chaotic Baker Map. *Phys Lett A*, 352(1-2), 78-82.

Chen, G., Mao, Y., & Chui, C.K. (2004). A Symmetric Encryption Scheme Based on 3D Chaotic Cat Map. *Chaos, Solitons & Fractals*, 21, 749-761.

Etemadi Borujeni, S., & Eshghi, M. (2009). Chaotic Image Encryption Design Using Tompkins-Paige Algorithm. *Hindawi Publishing Mathematical Problems in Engineering*, doi: 10.1155/2009/762652.

Fridrich, J. (1998). Symmetric Ciphers Based on Two Dimensional Chaotic Maps. *International Journal of Bifurcat Chaos*, 8(6), 1259-1284.

Jolfaei, A., & Mirghadri, A. (2010a). A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1. In *Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence (AICI 2010)*, Sanya, China.

Jolfaei, A., & Mirghadri, A. (2010b). An Image Encryption Approach Using Chaos and Stream Cipher. *Journal of Theoretical and Applied Information Technology*, 19(2), 117-125.

Jolfaei, A., & Mirghadri, A. (2010c). Survey: Image Encryption Using Salsa20. *International Journal of Computer Science Issues*, 7(5).

Jolfaei, A., & Mirghadri, A. (2010d). A New Approach to Measure Quality of Image Encryption. *International Journal of Computer and Network Security*, 2(8), 38-44.

Kocarev, L., Stczepanski, J., Amigo, J.M., & Tomovski, I. (2006). Discrete Chaos—I: Theory. *IEEE Transactions on Circuits and Systems,* 53(6), 1300-1309.

L'Ecuyer, P., & Simard, R. (2007). TestU01: A C Library for Empirical Testing of Random Number Generators. *ACM Transactions on Mathematical Software*, 33(4), Article 22.

Li, S., Li, C., Chen, G., Bourbakis, N.G., & Lo, K.T. (2008). A General Quantitative Cryptanalysis of Permutation-only Multimedia Ciphers against Plaintext Attacks. *Signal Processing: Image Communication*, 23(3), 212-223.

Lichtenberg, A.J., & Lieberman, M.A. (1992). *Regular and Chaotic Dynamics*. Springer, New York.

Lv, Z., Zhang, L., & Guo, J. (2009). A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System. In *IEEE Proceedings of the Second International Symposium on Computer Science and Computational Technology (ISCSCT '09)*, China, 191-194.

Machado, R.F., Baptista, M.S., & Grebogi, C. (2004). Cryptography with Chaos at the Physical Level. *Chaos, Solitons and Fractals*, 21(5), 1265-1269.

Mansoori, S.D., & Khaleghei Bizaki, H. (2007). On the vulnerability of Simplified AES Algorithm Against Linear Cryptanalysis. *International Journal of Computer Science and Network Security*, 7(7), 257-263.

Musa, M., Schaefer, E., & Wedig, S. (2003). A Simplified AES Algorithm and its Linear and Differential Cryptanalyses. *Cryptologia*, 27, 148-177.

Otto, S.R., & Denier, J.P. (2005). *An Introduction to Programming and Numerical Methods in MATLAB*. Springer-Verlag, ISBN: 1852339195.

Patidar, V., Pareek, N.K., & Sud, K.K. (2009). A New Substitution–Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. *Commun Nonlinear SciNumer Simulat*, 14, 3056-3075.

Pisarchik, A.N., & Zanin, M. (2008). Image Encryption with Chaotically Coupled Chaotic Maps. *Physica D*, 237(20), 2638-2648.

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

Shannon, C.E. (1949). *Communication Theory of Secrecy Systems*. Bell Syst Tech J, 28, 656-715.

Stinson, D.R. (1995). *Cryptography: Theory and Practice*. CRC Press LLC, ISBN: 0849385210.

XiaoJun, T., & MingGen, C. (2010). Feedback Image Encryption Algorithm with Compound Chaotic Stream Cipher Based on Perturbation. *SCIENCE CHINA Information Sciences*, 53(1), 191-202.

Yang, M., Bourbakis, N., & Li, S. (2004). Data-Image-Video Encryption. *IEEE Potentials*, 23(3), 28-34.

Table 1. A generated S-box using baker's map with x = 0.2 and y = 0.3 as seed points

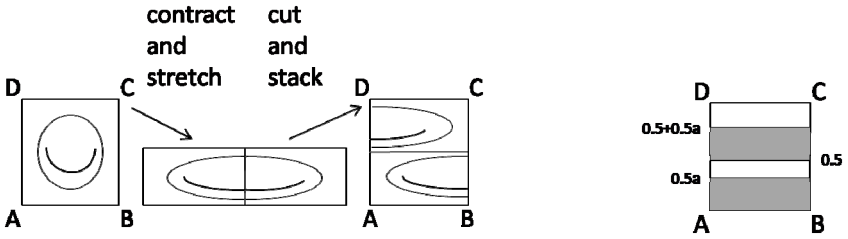
Nibble	S-box	Nibble	S-box
0	b	8	4
1	0	9	d
2	5	a	3
3	c	b	9
4	7	c	a
5	6	d	f
6	8	e	e
7	1	f	2

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

Proposed method	MAE
Row permuted image	31.8358
Column-row permuted image	32.4899
Diagonal-column-row permuted image	32.4308
Encrypted image after shuffling (proposed scheme)	84.0504
AES	83.9937

Table 3. NPCR and UACI value of AES and the proposed method

Method	NPCR	UACI
AES	$<10^{-3}$%	$<10^{-3}$%
Proposed scheme	$<10^{-3}$%	$<10^{-3}$%



(a) (b)

Figure 1. Baker's map: (a) geometrical nature of the baker's map, (b) area contraction by the map *F*

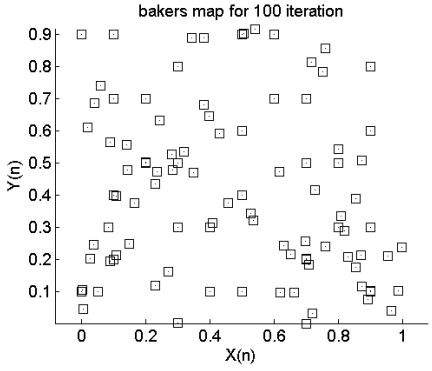


Figure 2. Pseudo-random number sequence generated by baker's map

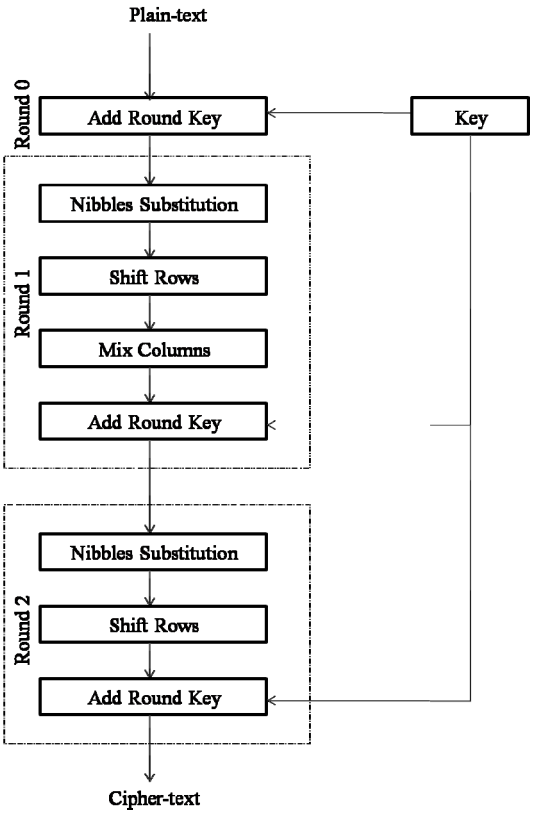


Figure 3. S-AES encryption overview

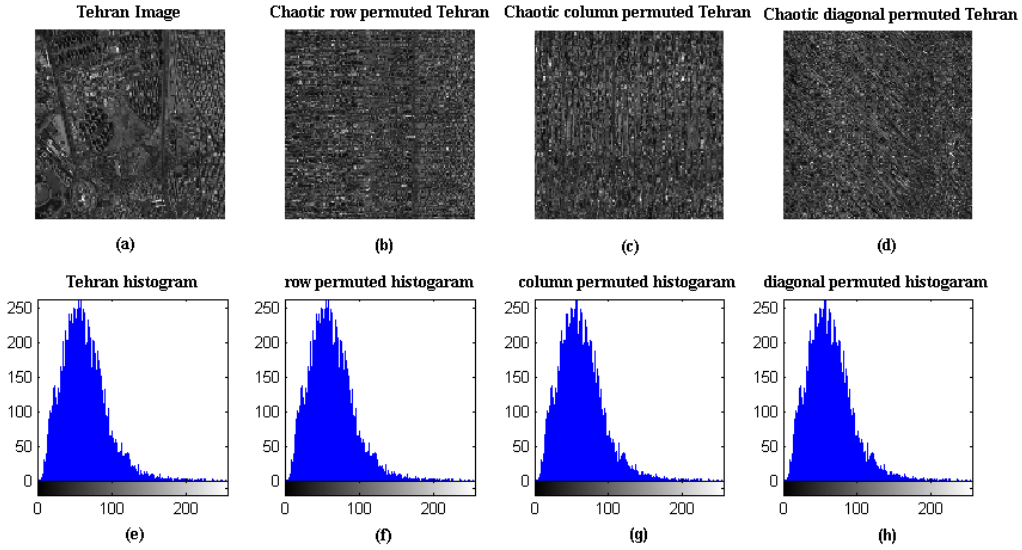


Figure 4. Permuting Tehran's aerial image pixel location using baker's map: (a) Tehran's aerial image, (b) chaotic row permutation, (c) chaotic column permutation, (d) chaotic diagonal permutation, (e) Tehran's aerial image histogram, (f) chaotic row permutation histogram, (g) chaotic column permutation histogram, (h) chaotic diagonal permutation histogram

ISSN 1913-8989 E-ISSN 1913-8997

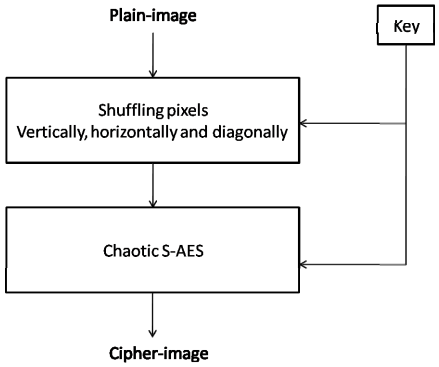


Figure 5. The proposed encryption algorithm

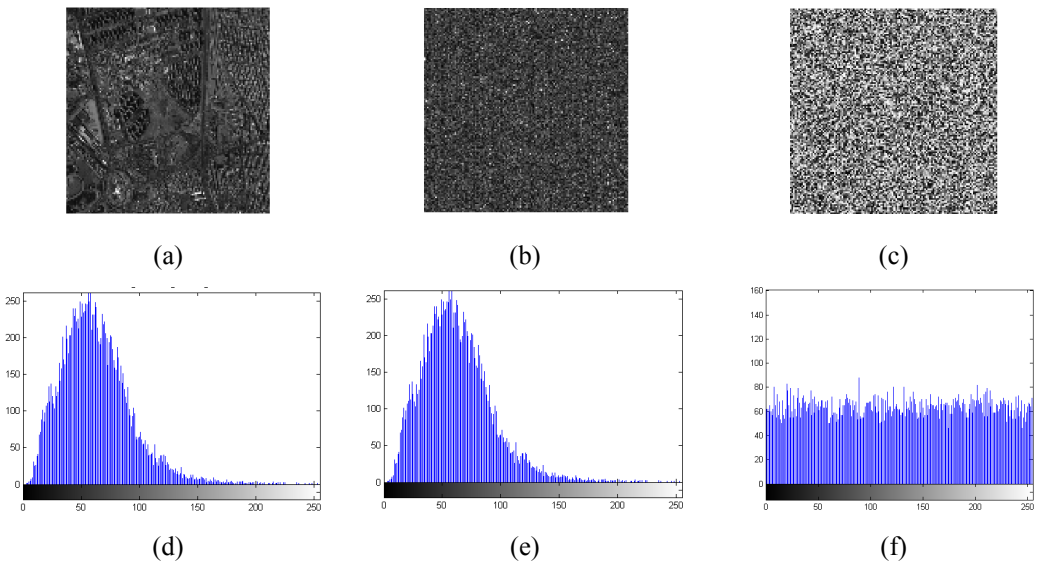


Figure 6. Implementation of the proposed algorithm on a 256 gray-scale plain-image of size 128×128: (a) Tehran's aerial image (plain-image), (b) shuffled image, (c) ciphered image using chaotic S-AES algorithm after pixel shuffling, (d) plain-image histogram, (e) shuffled image histogram, (f) cipher-image histogram

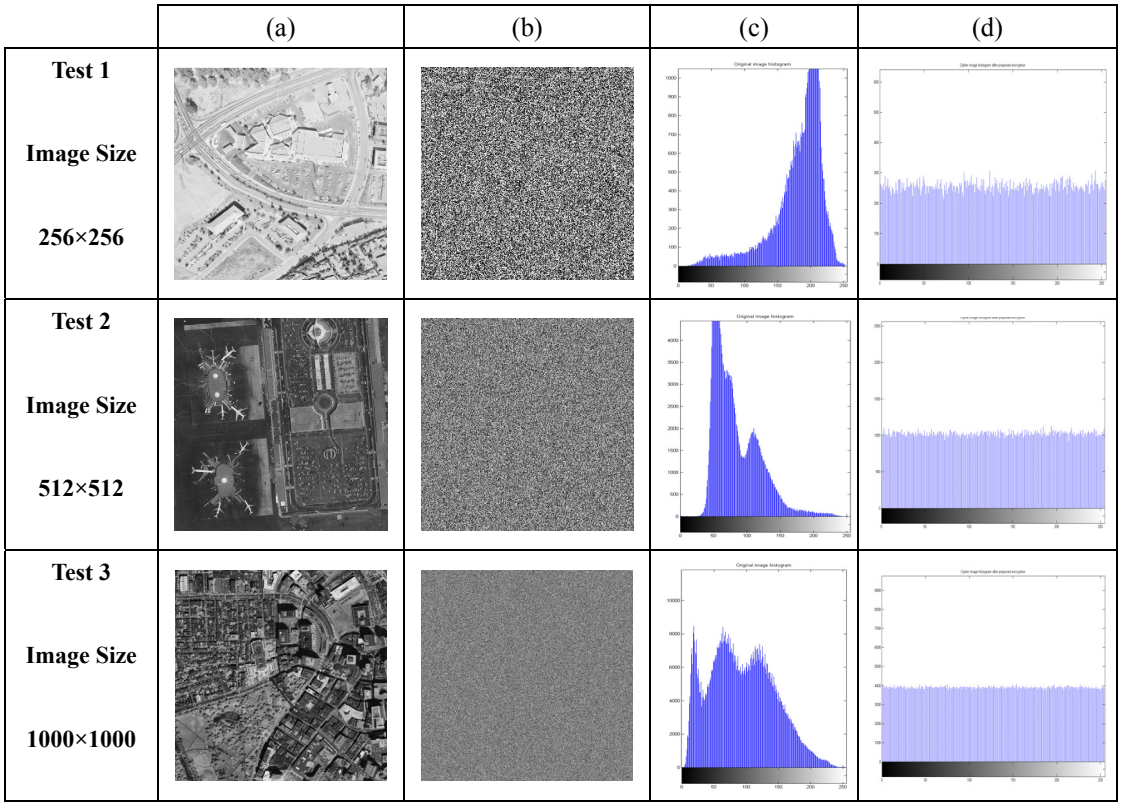


Figure 7. Histogram analysis for three test images with different sizes: (a) plain-image, (b) cipher-image, (c) plain-image histogram, (d) cipher-image histogram

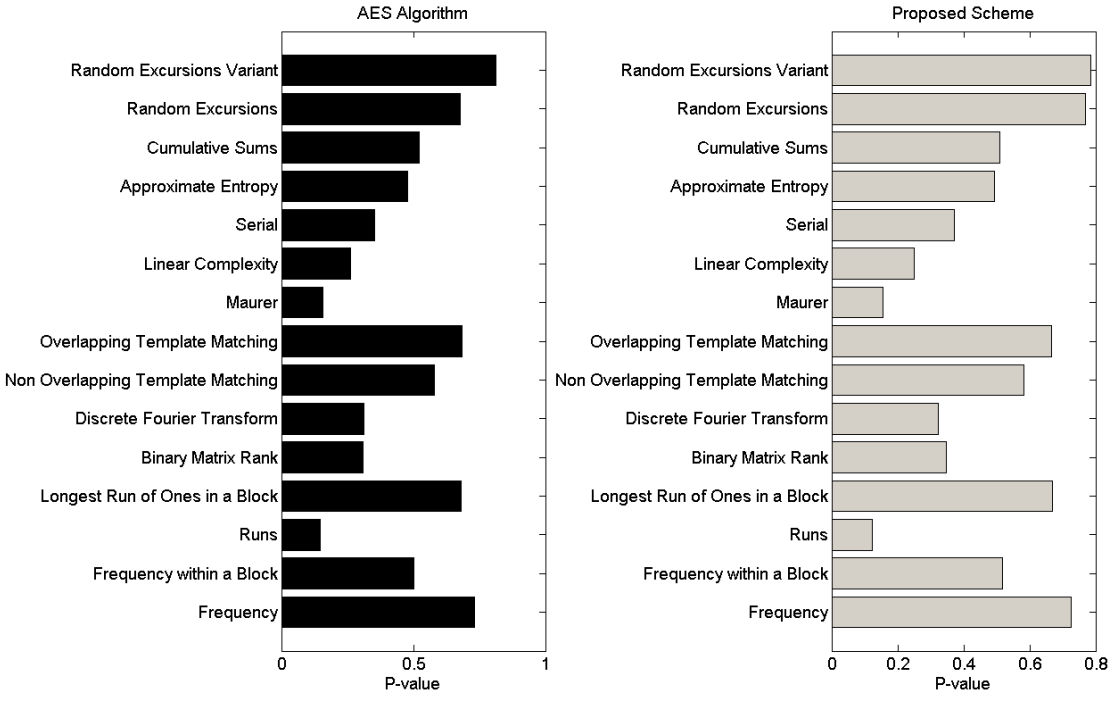


Figure 8. Randomness test results

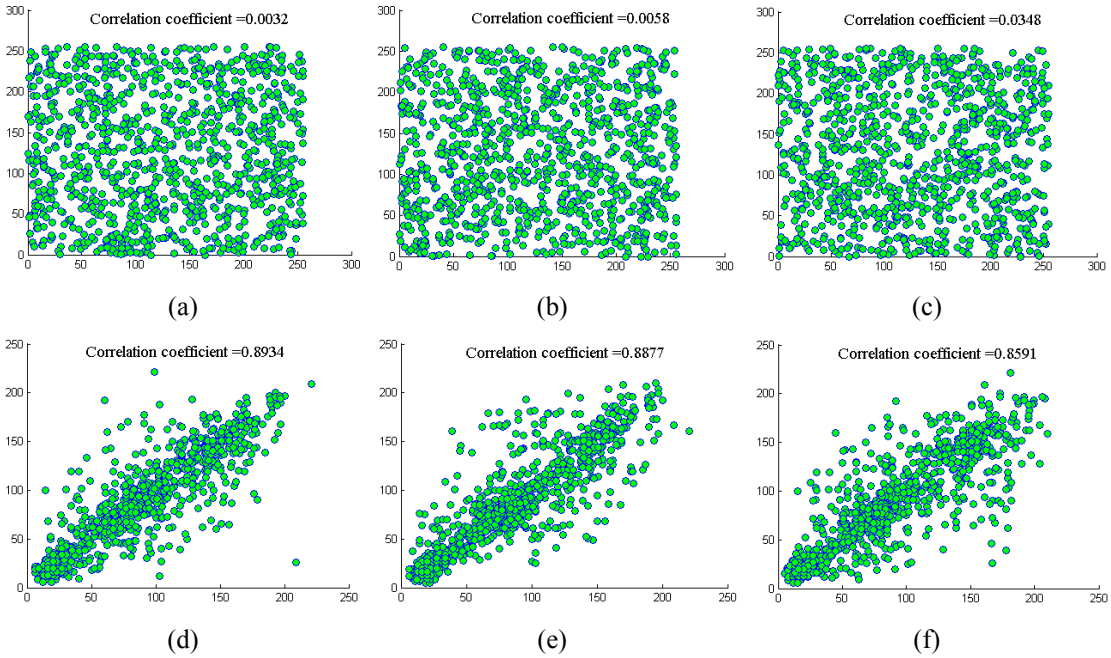


Figure 9. Correlation of two adjacent pixels: (a) distribution of two vertically adjacent pixels in the cipher-image with correlation coefficients = 0.0032, (b) distribution of two horizontally adjacent pixels in the cipher-image with correlation coefficients = 0.0058, (c) distribution of two diagonally adjacent pixels in the cipher-image with correlation coefficients = 0.0348, (d) distribution of two vertically adjacent pixels in the plain-image with correlation coefficients = 0.8934, (e) distribution of two horizontally adjacent pixels in the plain-image with correlation coefficients = 0.8877, (d) distribution of two diagonally adjacent pixels in the plain-image with correlation coefficients = 0.8591

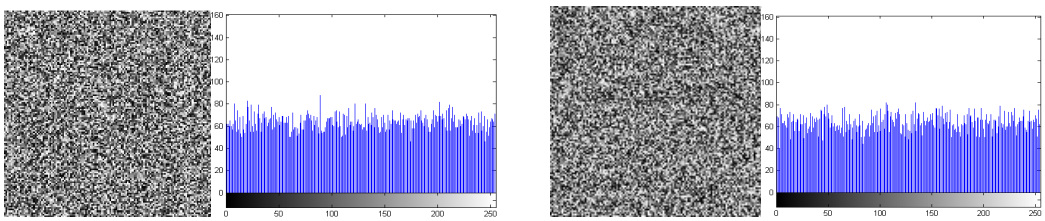


Figure 10. Key sensitivity test: Figures (a) and (b) show the encrypted image with its corresponding histogram using proposed scheme with two different secret keys with slight differences