Arab J Sci Eng (2014) 39:1039–1047
DOI 10.1007/s13369-013-0713-z

RESEARCH ARTICLE - ELECTRICAL ENGINEERING

Image Encryption Using Random Bit Sequence Based on Chaotic Maps

**Himan Khanzadi · Mohammad Eshghi ·
Shahram Etemadi Borujeni**

Received: 22 January 2012 / Accepted: 9 July 2013 / Published online: 5 September 2013

Abstract The paper proposes an algorithm for image encryption using the random bit sequence generator and based on chaotic maps. Chaotic Logistic and Tent maps are used to generate required random bit sequences. Pixels of the plain image are permuted using these chaotic functions, and then the image is partitioned into eight bit map planes. In each plane, bits are permuted and substituted according to random bit and random number matrices; these matrices are the products of those functions. The pixels and bit maps permutation stage are based on a chaotic random Ergodic matrix. This chaotic encryption method produces encrypted image whose performance is evaluated using chi-square test, correlation coefficient, number of pixel of change rate (NPCR), unified average changing intensity (UACI), and key space. The histogram of encrypted image is approximated by a uniform distribution with low chi-square factor. Horizontal, vertical, and diagonal correlation coefficients of two adjacent pixels of encrypted image are calculated. These factors are improved compared to other proposed methods. The NPCR and UACI values of encrypted image are also calculated. The result shows that a swift change in the original image will cause a significant change in the ciphered image. Total key space for the proposed method is (2^2,160), which is large enough to protect the proposed encryption image against any brute-force attack.

Keywords Chaotic map · Image encryption · Permutation · Substitution

الخلاصة

تقترح هذه الورقة العلمية خوارزمية لتشفير الصورة باستخدام مولد تسلسل القطعة العشوائي على أساس خرائط الفوضى. وقد استخدمت خرائط الفوضى اللوجستية وخرائط الخيمة لتوليد متواليات القطعة العشوائية المطلوبة. وتم تبديل بكسل الصورة الجلية باستخدام دالات الفوضى هذه، ومن ثم تم تقسيم الصورة إلى مستويات خريطة ذات ثماني قطع. وتمت - في كل مستوى - مبادلة القطع واستبدالها وفقا لمصفوفات القطع والرقم العشوائية، وهذه المصفوفات هي المنتجات من هذه الوظائف. وتستند مرحلة مبادلة خرائط القطعة والبكسل إلى مصفوفة فوضى أرجوديك العشوائية.

إن طريقة تشفير الفوضى هذه تنتج صورة مشفرة يتم تقييمها باستخدام اختبار مربع خي، ومعامل الارتباط، وعدد بكسل لمعدل التغير (NPCR)، ومتوسط كثافة التغيير الموحد (UACI)، ومساحة الأداء الرئيسية. وتم تقريب الرسم البياني للصورة المشفرة بوساطة التوزيع الموحد مع معامل مربع خي منخفض. وتم حساب معاملات الارتباط الأفقية والرأسية والقطرية لبكسلين متجاورين من الصورة المشفرة، وتحسنت هذه العوامل بالمقارنة مع الطرق الأخرى المقترحة. وحسبت أيضا قيم NPCR وUACI من الصورة المشفرة. وتظهر النتيجة أن تغييرا سريعا في الصورة الأصلية يؤدي إلى تغيير كبير في الصورة المشفرة. وإجمالي المساحة الرئيسية للطريقة المقترحة هو (2 ^ 2160)، وهي كبيرة بما يكفي لحماية صورة التشفير المقترحة ضد أي هجوم قوة قاهرة.

1 Introduction

The trend for the transmission of digital images through computer network, especially Internet, has been increasing in recent years. Many applications like military image databases, confidential video conferencing, medical imaging system, online personal photograph album, etc., require reliable, fast, and robust security system to store and transmit digital images [1,9,14,17]. Therefore, the security and

H. Khanzadi (✉) · M. Eshghi
Electrical Engineering Department, Shahid Beheshti University, Evin 1983963113, Tehran, Iran
e-mail: khanzadi.h@gmail.com

M. Eshghi
e-mail: m-eshghi@sbu.ac.ir

S. E. Borujeni
Computer Engineering Department, University of Isfahan, 8174673441 Isfahan, Iran
e-mail: etemadi@eng.ui.ac.ir

privacy of digital images have become major issues. Digital images have special characteristics like data redundancy and strong correlation between adjacent pixels, which make it difficult for traditional ciphers like IDEA, AES, DES, RSA to deal with real-time digital image encryption as these ciphers require high computational power [1]. Many image encryption methods have been proposed in the literature based on different principles. Chaos-based encryption techniques have been preferred compared to other methods, because they provide a good combination of speed and high security [2].

In general, chaotic systems have some properties such as randomness, sensitivity to initial condition, and ergodicity. These properties are essential in building cryptosystems. Chaotic systems generate long-period, random-like chaotic sequence in a deterministic way. A tiny difference in initial values or system parameters leads a major change in the generated chaotic sequences. A chaotic state variable goes through all states in its phase space; these states are usually distributed uniformly. These properties of chaotic systems make them a good candidate for cryptography [8,9].

Fridrich proposed a first work on image encryption based on chaotic maps. In his papers, it is shown how to adapt certain invertible chaotic 2D maps on a torus or on a square to create new symmetric block encryption schemes [21].

A number of chaos based image encryption scheme have been developed recently.

Mao et al. [15] suggested a novel fast image encryption scheme based on 3D chaotic Baker maps and Chen et al. [10] proposed a symmetric image encryption scheme based on 3D chaotic cat maps.

An image encryption scheme based on chaotic systems is introduced by Zhang et al. [5]. They improve the properties of confusion and diffusion in terms of discrete exponential chaotic maps, and design a key scheme for the resistance to statistic attack, differential attack, and grey code attack. Guosheng and Guoqiang proposed an enhanced chaos-based image encryption algorithm. The focus of the work presented in their paper is to incorporate permutation and substitution methods, to present a strong image encryption algorithm. An optimized treatment and a cross-sampling disposal are introduced for enhancing the irregular and pseudorandom characteristics of chaotic sequences [4]. Behnia et al. [6] present a novel algorithm for image encryption based on the mixture of chaotic maps. In their algorithm, a typical coupled map was mixed with a 1D chaotic map and used for high degree security image encryption while its speed is acceptable. Kwok and Tong present a fast image encryption system based on chaotic maps with finite precision representation. The major core of the encryption system is a pseudo-random key stream generator based on a cascade of chaotic maps, serving the purpose of sequence generation and random mixing. Tong and Cui present an image encryption with compound chaotic sequence cipher shifting dynamically. They design a new 2D chaotic function using two 1D chaotic functions, and then prove the chaotic properties to a new function based on a strict Devaney definition [7]. Etemadi and Eshghi present a new permutation-substitution image encryption architecture using chaotic maps and Tompkins–Paige algorithm [9]. In their work, a logistic map is used to generate a bit sequence, which is used to generate pseudo random numbers in Tompkins–Paige algorithm, for pixel permutation and a tent map is used for substitution. A fast image encryption scheme based on a nonlinear chaotic map is proposed by Shujiang et al. [22]. We present an image encryption algorithm based on chaotic maps and gyrator transform. We use chaotic logistic and tent maps to generate random bits and the plain image is encrypted by employing gyrator transform; then the output of gyrator transform is encrypted by the generated random bits of the chaotic functions [23].

In this paper, we propose an algorithm for image encryption using the random bit sequence generator (RBSG) based on chaotic maps. Logistic and tent maps are used as chaotic maps to generate required random bit sequences. The encrypted image is evaluated and compared to other method's encrypted image. The result shows a major improvement in these figures of merit.

The rest of the paper is organized as the following. In Sect. 2, RBSG along with random number matrix and random bit matrix is explained. Proposed image encryption algorithm including pixel permutation, pixel decomposition, bit map permutation, bit map substitution, and bit map composition are presented in Sect. 3. Section 4 provides system simulation and performance evaluation. Section 5 is the comparison of the proposed method to other methods. Finally, the conclusion is presented in Sect. 6.

2 Random Number Matrix and Random Bit Matrix

Random number/bit matrix has two important parts of the scheme. These are generated via RBSG. In the following, first random bit sequence is explained and then RBM and RNM are defined.

2.1 Random Bit Sequence Generator

A new RBSG algorithm is introduced using chaotic functions. Figure 1 shows the structure of this generator. The generator produces chaotic real numbers in a determined range, based on its initial state and selected chaotic function. Then, the generated real numbers are converted to the binary numbers, to be used as a random bit stream. Decimal to the binary converter does this operation. The parameter m shows the length of produced random bit stream. All the above operations are done using the second selected chaotic function, simultaneously. Finally, the output of the system is generated

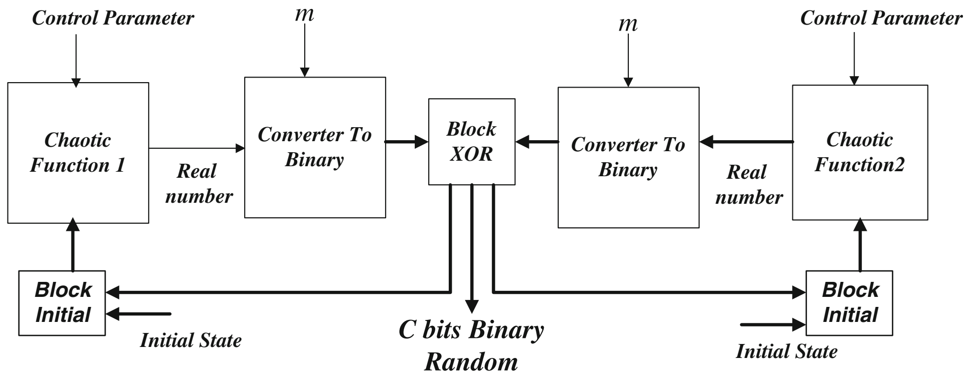


Fig. 1 Design of a random generator using chaotic functions

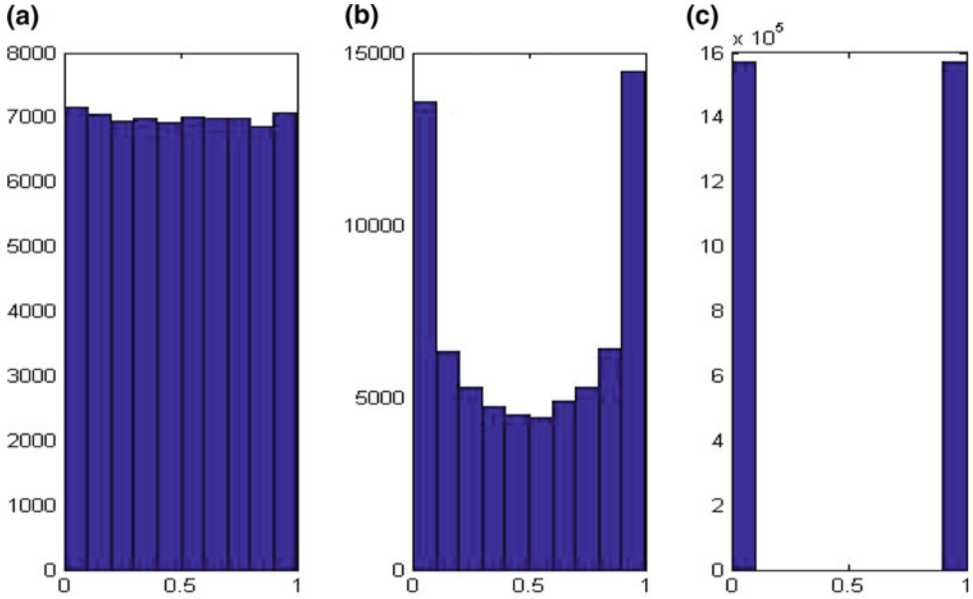


Fig. 2 **a** Histogram of Tent map, **b** histogram of Logistic map, **c** histogram of final output

through an EX-OR block. The chaotic functions, which are used for generating random bits, are Tent and Logistic maps [24]:

$$\text{Tent map: } x'_{i+1} = \begin{cases} px'_i, & x'_i < 1/2 \\ px'_i(1-x'_i), & x'_i > 1/2 \end{cases} \qquad (1)$$

$$\text{Logistic map: } x_{i+1} = \mu(x_i(1-x_i)) \qquad (2)$$

in which, $x \in [0, 1]$, $3.99465 \leq \mu \leq 4$ and $x'(0)$ is initial state. p and μ are control parameters.

The histogram of output of chaotic functions is shown in Fig. 2a, b and the final output is depicted in Fig. 2c. According to Fig. 2c, the distribution of random bits is uniform. The proposed RBSG passes the NIST and FIPS140-1 [18] tests. The C parameter of Fig. 1 is considered to be 48 bits [24].

2.2 Random Bit Matrix (RBM)

To produce a random bit matrix, sufficient numbers of C bits from output of RBSG are put together to produce a binary string. These strings are ordered as a $m \times n$ matrix. Figure 3 summarizes the process of generating RBM matrix.

2.3 Random Numbers Matrix (RNM)

In order to produce a $m \times n$ RNM matrix, each C bits output from the output of RBSG is stored as a new element of the RNM matrix. This work is repeated $m \times n$ times, and each time a new number or C bits output is stored in RNM matrix. This process to generate a RNM matrix is shown in Fig. 4.

3 Proposed Chaotic Image Encryption System

The process encryption system consists of five major stages, pixel permutation, pixel decomposition, bit map permutation, bit map substitution, and bit map composition. These major stages are shown in Fig. 5. The following sub-sections describe these stages.

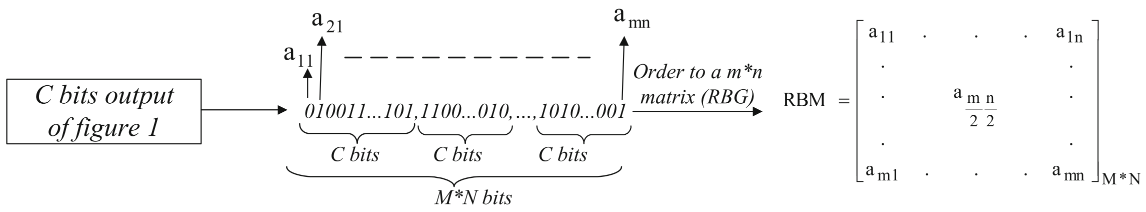


Fig. 3 Generate the RBM matrix

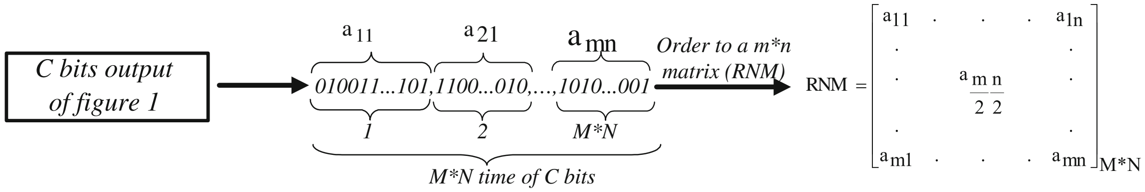


Fig. 4 Generate the RNM matrix

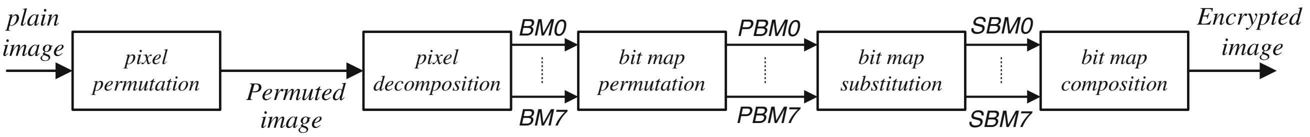
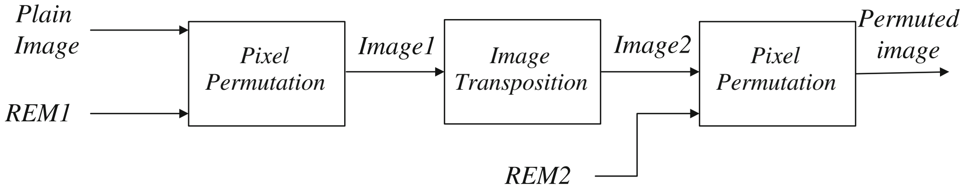


Fig. 5 Block diagram of the proposed encryption system

Fig. 6 The pixel permutation stage



3.1 Pixel Permutation Stage

There are three phases in this stage. In each phase, a RNM is used to produce the required random Ergodic matrix (REM). The positions of pixels of the plain image are permuted using the first REM to produce image 1. Then the pixels of the image 1 are transposed to produce image 2. The image 2 is again permuted with another REM with different initial condition. Each pixel of image is obtained from permutation stage, called permuted image, and has a gray level (0–255) that can be presented with 8 bits.

Although the encrypted permuted image seems invisible after the permutations stages, its histogram is the same as plain image histogram. Three phases of pixel permutation stage are shown in Fig. 6 and they are explained in the following. That is, only the positions of pixels of original image are changed.

3.2 Random ERGODIC Matrix (REM)

An $M \times N$ Ergodic matrix is a matrix whose elements are natural numbers from 1 to $M \times N$, without any repetition [8,19]. The arrangement of elements of a REM is determined using the RNM.

When an Ergodic matrix is reordered based on the values of a random matrix then a REM is produced. Elements of the REM are determined using the order of the elements of the random matrix.

3.3 Pixel Permutation

In this phase, the pixels of the image are permuted using REM. This image which is used to permute, is a M × N matrix with 256 gray scales. All pixels of the image are permuted using REM matrix. Since, the REM has better random specification than the permuted image. REM is applied on an image and the orders of the pixels are changed according to the values of this random matrix. That is, the positions of the pixels are determined based on the values in the REM. REM contains the indices of the pixels. In the next phase, the rows are exchanged with the columns of the matrix of the image. Therefore positions of the pixels of image are changed. And the final phase of the pixel permutation is the decomposition stage; permuted image is decomposed to 8-bit map images

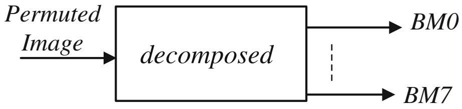


Fig. 7 The decomposition stage

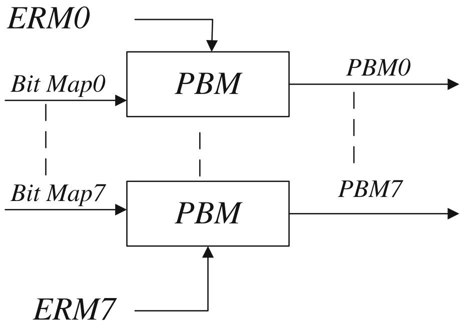


Fig. 8 The block diagram of Permutation Bit Map stage

called BM0–BM7. BM0 consists of a bit map image using the least significant bit of pixel values of permuted image. Other BMs use the other bits of the pixels of permuted image, respectively. The decomposition stage is explained in Fig. 7.

3.4 Bit Map Permutation Stage

The histogram of the permuted image is similar to the histogram of the plain image. The permuted image however cannot resist against deferent attacks. Its histogram needs to approximate the uniform distribution. This improvement is done using a substitution scheme. Actually, bit map permutation stage performs the pixel substitution.

In the bit map permutation stage, these BMs are permuted using other eight different REMs, with eight different initial conditions. The result of this stage is eight permuted bit maps (PBMs), called PBM0–PBM7. The block diagram of permutation bit map stage is shown in Fig. 8.

3.5 Bit Map Substitution Stage

In the substitution stage, a random generator is used to produce eight RBMs, which also have different initial conditions. Each bit of PBM is EX-ORed with corresponding bit in RBMs, respectively. The EX-OR decreases the correlation between the bits. The results of this stage are eight substitute bit maps (SBM0-SBM7), called SBMs. Equation number 3 shows the formula (3).

$$\mathrm{SBM_k}(i,j) = xor(\mathrm{RBG_k}(i,j), \mathrm{BM_k}(i,j)) \tag{3}$$

Where k is natural number from 1 to 8. The block diagram of substitution bit map is shown in Fig. 8.

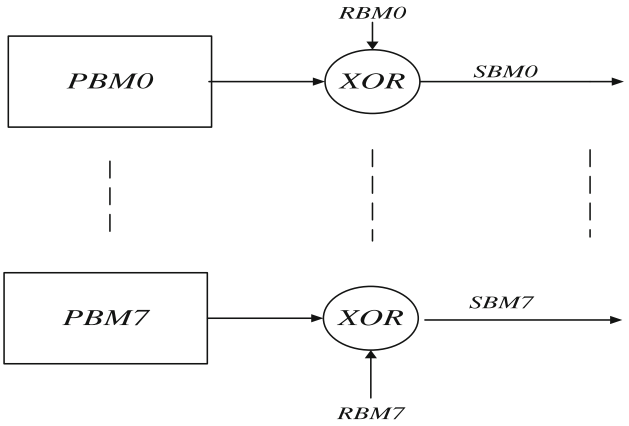


Fig. 9 The block diagram of substitution bit map

3.6 Bit Map Composition

In the composition stage, eight BMs will put together to obtain the image. The BM0 is least significant pixel bit of the image and BM1 is 2th pixel bit of the image, and BM7 is most significant pixel bit of the image. In this section, These SBMs of substitution stage are put together and encrypted image is obtained (Fig. 9).

4 Simulation and Performance Analysis

The proposed algorithm for image encryption along with individual pixel permutation, bit map permutation and substitution, image composition and decomposition are simulated using MATLAB tools. In order to verify the exact operation of the proposed encryption algorithm, a 256 × 256 Lena image with 256 gray scales is used as a plain image.

In this section, the performance of the proposed chaotic image encryption is analyzed. The first criterion for this security analysis is the chi-square test of histogram of encrypted image. The second criterion is the correlation coefficients of pixels in the encrypted image in the vertical, horizontal, and diagonal direction. The third criterion is the difference between encrypted and corresponding plain image, which is measured by mean absolute difference, number of pixel change rate, and unified average changing intensity. Finally, the fourth criterion in this security analysis is key space.

The results of the plain image, bit map permutation, and encryption image and histogram of three images are illustrated in Fig. 10.

4.1 Histogram

The histogram is approximated by a uniform distribution. The uniformity is justified by chi-square test in equation

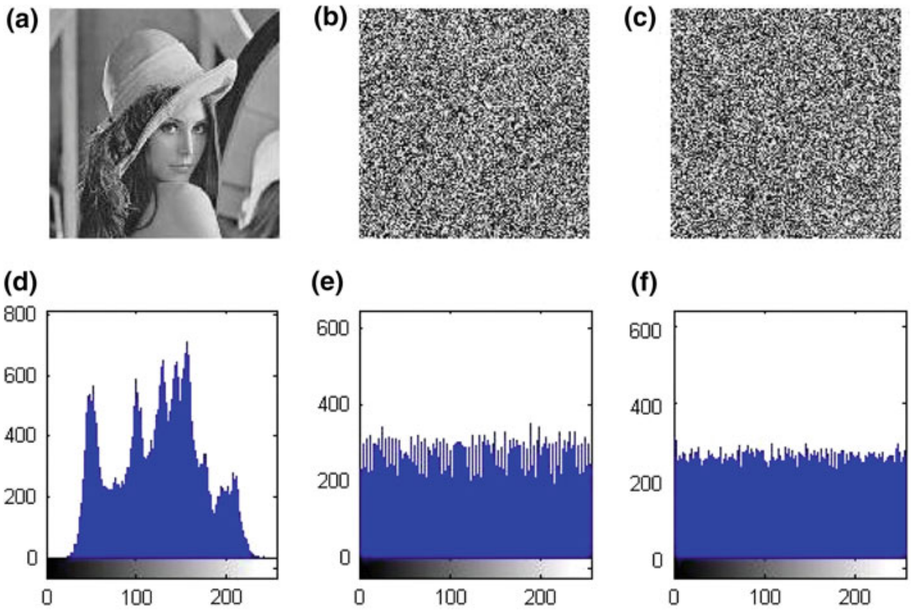


Fig. 10 **a** Plain image, **b** bit map permutation, **c** encrypted image, **d** histograms of plain image, **e** histograms of permutation image, **f** histogram of encrypted image

(4) [9].

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

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. Chi-square value for the final encrypted image of the proposed system is 243, χ^2 test = 243 [9]. The result of this test demonstrated that the histogram of the encrypted image is uniform.

4.2 Correlation Coefficient

The proposed chaotic image encryption system should be resistant to statistical attacks. Correlation coefficients of pixels in the encrypted image should be as low as possible [9]. Horizontal, vertical, and diagonal correlation coefficients r_{xy} of two adjacent pixels can be calculated using the following equations (5):

$$\text{r}_{xy} = \frac{\text{COV}(x, y)}{\sqrt{D(x)D(y)}},$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - \frac{1}{N} N \sum_{i=1} x_i\right)^2,$$

$$\text{COV}(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{5}$$

$$E(z) = \frac{1}{N}\sum_{i=1}^{N} z_i$$

Where x and y are gray-scale values of two adjacent pixels in the image. The following procedure is performed to test the correlation between two adjacent pixels in plain image and ciphered image. First, randomly select 10,000 pairs of two adjacent (in horizontal, vertical, and diagonal direction) pixels from an image. Then, calculate the correlation coefficient of each pair using the above formulas. The results are shown in Table 1. It is clear that the correlation coefficients of the proposed encrypted image of Fig. 10 in all three directions are smaller than the correlation coefficients plain image. The correlation distributions are shown in Fig. 11.

Table 1 The correlation coefficients of the proposed methods

Positions	Plain-image	Ciphered-image
Horizontal	0.9439	0.00059387
Vertical	0.9709	0.0041
Diagonal	0.9136	0.0048
Average (H, V, D)	0.9428	0.003164

4.3 NPCR and UACI Analysis

NPCR means the change rate of the number of pixels of the cipher image when only one pixel of the plain image is modified. The unified average changing intensity (UACI) measures the average intensity of differences between the plain image and ciphered image [2,9]. The NPCR and UACI of these two images are defined in equations 6–8.

$$\text{NPCR} = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\,\% \tag{6}$$

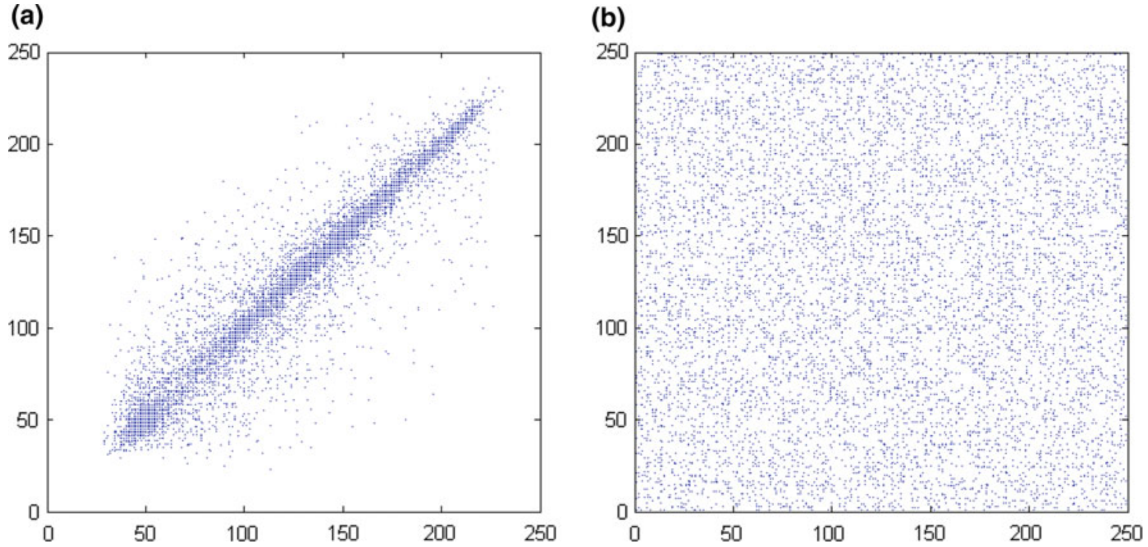


Fig. 11 Correlations of two adjacent pixels in (**a**) diagonal direction of the plain image, (**b**) diagonal direction of the cipher image

Table 2 Comparison of correlation coefficient of the proposed method and the other methods

Methods	Horizontal	Vertical	Diagonal	Average (H, V, D)
Huang et al. [5]	0.02086	0.02458	0.0096668	0.01837
Guanrong Chen 5th round [10]	0.01183	0.00016	0.01480	0.00893
Gao et al. [13]	0.01589	0.06538	0.03231	0.03786
Mao et al. 1st round [15]	0.045	0.028	0.021	0.0313
Zhang et al. 2nd round [11]	0.082	0.040	0.005	0.0423
Zhou et al. 2nd round [12]	0.012	0.027	0.007	0.015
Etemadi et al. [9]	0.005	0.011	0.023	0.013
Wang [3]	0.000707	0.00216	0.014886	0.0059194
Khanzadi et al. [23]	0.0014	0.0055	0.000146	0.002388
Proposed method	0.00059387	0.0041	0.0048	0.003164

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100 \tag{7}$$

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

$$D(i,j) = \begin{cases} 0, & \text{if } (C_1(i,j) = \mathrm{C}_2(i,j)) \\ 1, & \text{if } (C_1(i,j) \neq \mathrm{C}_2(\mathrm{i,j})) \end{cases} \tag{8}$$

W and H are the width and height of encrypted image.

A plain image is first encrypted and then, a pixel in that image is randomly selected and toggled. The modified image is encrypted again using the same keys so as to generate a new cipher image. Finally, the NPCR and UACI values are calculated.

Table 3 Comparison of NPCR and UACI criteria of proposed method and the others

Methods	NPCR %	UACI %
Huang et al. [5]	NA	NA
Guanrong Chen 5th round [10]	50.20	25.20
Gao et al. [13]	NA	NA
Mao et al. 1st round [15]	37	9
Zhang et al. 2nd round [11]	21.50	2.50
Zhou et al. 2nd round [12]	25.00	8.50
Etemadi et al. [9]	99.70	29.30
Khanzadi et al. [23]	99.52	33.14
Wang [3]	97.62	32.90
Proposed method	99.61	33.35
Expected value [9]	99.61	33.46

Table 4 Comparison of key length of proposed method and the others

Methods	Mao et al. [15]	Gao et al. [13]	Zhou et al. [20]	Etemadi et al. [9]	Proposed algorithm
Length (Bin)	2^{128}	2^{150}	2^{112}	2^{218}	2^{2160}
Length (Dec)	10^{38}	10^{45}	10^{33}	10^{65}	10^{650}

A computer simulation shows that NPCR of the proposed system is 99.61 %, where the ideal value of it is 99.61 % [9]. This simulation also shows that the UACI of the proposed algorithm is 33.35 [9], where the ideal value of it is 33.46 % [9].

4.4 Key Space

Key space is total number of different keys that is used in the encryption system. The proposed algorithm encryption consists of 18 RBSG, where each of RBSG is different initial condition. The RBSG has four keys with 48 bits of length. Total length of the key is 4 (keys) × 18 (number of RBSG) ×30 (keys of length) = 2160, key space becomes 2^2,160, which is large enough to protect the proposed encryption systems against brute-force attack. A key space of 2^100 is sufficient for a safe encryption system [9,16]. Therefore, the proposed encryption systems have a large key space and resist against any brute-force attack.

5 Comparison

In this section, the performance of the proposed method is compared to ten other reported research results. The chi-square of our method is about 243, which is 17 % less than the chi-square of method proposed in [9]. The other researchers are not reported the chi-square of their encrypted image.

The correlation coefficient of the proposed method is compared to the others and is shown in Table 2. It is shown that the average correlation coefficient of the proposed system *has one of the best performance among other proposed methods.* Comparison of NPCR and UACI of our proposed method and the others is shown in Table 3. It is shown that NPCR is exact to the expected value and UACI criteria with a difference of about 0.3 % to its expected value.

The key space of our encryption system is also compared to the key space of the other published methods. Table 4 shows this comparison.

As a result, the proposed algorithm has a good ability to encrypt an image against any attack.

6 Conclusion

The proposed algorithm for image encryption along with individual pixel permutation, bit map permutation and substitution, image composition and decomposition are simulated using computer tools. The RBSG is based on chaotic map. Logistic and tent map are used as chaotic maps to generate some random bits sequence. Pixels of plain image are permuted first. Then the permuted image is first partitioned into eight-bit plane. In each plane, bits are permuted and substituted according to random bit and random number matrix. Bit map plane images are decomposed to pixel image.

In order to verify the exact operation of the proposed encryption algorithm, a 256 × 256 Lena image with 256 gray scales is used as a plain image. The results obtained by the Lena Gray scales image are demonstrated.

The histogram of bit map permutation and final encrypted image is calculated and justified by chi-square test. The histogram of encrypted image is approximated by a uniform distribution with low chi-square factor.

The correlation coefficients of pixels in the encrypted image should be as low as possible. Horizontal, vertical, and diagonal correlation coefficients of two adjacent pixels are calculated. As it is shown in Table 3, the average correlation coefficient of the proposed system has one of the best performance among other proposed methods, reviewed in the paper. Correlation co-efficient of a pure noisy image is close to zero. Therefore, the correlation coefficient of the pixels of an image shows the similarity of the image to a pure noise image. The less the correlation coefficient, the more noisy the image. As a result, the proposed method which as a low correlation co-efficient value, compared to the other reported methods in the literature, has a noisy image at its output.

The NPCR and UACI values are calculated. The results shows that a swift change in the original image will result in a significant change in the ciphered image, therefore the algorithm proposed has a good ability to differential attack.

Total key space is (2^2,160), which is large enough to protect the proposed encryption algorithm against brute-force attack.

References

1. Pareek, N.; Patidar V.; Sud, K.: Image encryption using chaotic logistic map. Image Vision Comput. **24**(9), 926–934 (2006)

2. Kwok, H.S.; Tang, W.K.S.: A fast image encryption system based on chaotic maps with finite Precision representation. Chaos Solitons Fractals **32**(4), 1518–1529 (2007)
3. Wang, Y.; Wong, K.W.; Liao, X.; Chen, G.: A new chaos-based fast image encryption algorithm. Appl. Soft Comput. **11**, 514–522 (2009)
4. Gu, G.; Han, G.: An enhanced chaos based image encryption algorithm. In: Proceedings of the first international IEEE conference on innovative computing information and control (ICICIC'06) 1, pp. 492–495 (2006)
5. Zhang, L.; Liao, X.; Wang, X.: An image encryption approach based on chaotic maps. Chaos Solitons Fractals **24**(3), 759–765 (2005)
6. Behnia, S.; Akshani, A.; Mahmodi, H.; Akhavan, A.: A novel algorithm for image encryption based on mixture of chaotic maps. Chaos Solitons Fractals **35**(65), 408–419 (2006)
7. Tong, X.; Cui, M.: Image encryption with compound chaotic sequence cipher shifting dynamically. Image Vision Comput. **26**(6), 843–850 (2008)
8. Alligood, K.T.; Sauer, T.D.; Yorke, J.A.; Chaos: An introduction to Dynamical Systems, Textbooks inMathematical Sciences. Springer, New York (1997)
9. Borujeni, S.E.; Eshghi, M.: Chaotic image encryption design using tompkins-paige algorithm. Hindawi Publishing Corporation Mathematical Problem in Engineering vol. 200, p. 22 (2009)
10. Guarnong, C; Mao, Y.; Chui, C.K.: A symmetric image encryption scheme based on 3D chaotic Cat maps. Chaos Solitons Fractals **21**(3), 749–761 (2004)
11. Linhua, Z; Liao, X.; Wang, X.: An image encryption approach based on chaotic maps. Chaos Solitons Fractals **24**(3), 759–765 (2005)
12. Zhou, Q.; Wo Wong, K.; Liao, X.; Xiang, T.; Hu, Y.: Parallel image encryption algorithm based ondiscretized chaotic map. Chaos Solitons Fractals **38**(4), 1081–1092 (2008)
13. Gao, H.; Zhang, Y.; Liang, S.; Li, D.: A new chaotic algorithm for image encryption. Chaos Solitons Fractals **29**(2), 393–399 (2006)
14. Furhtand, B.; Kirovski, D.: Multimedia Security Handbook. CRC Press, Boca Raton (2005)
15. Mao, Y.; Chen, G.; Lian, S.: A novel fast image encryption scheme based on 3D chaotic bakermaps. Int. J. Bifurcation Chaos **14**(10), 3613–3624 (2004)
16. Alvarez, G.; Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcation Chaos **16**(8), 2129–2151 (2006)
17. Stinson, D.R.: Cryptography: Theory and Practice, CRC Press Series on Discrete Mathematics and Its Applications, 2nd edn. Chapman & Hall/CRC, Boca Raton (2002)
18. Runkin, et al.: Statistical test suite for random and pseudo random numbergenerators for cryptographic applications. NIST special publication, pp. 800–822 (2001)
19. Bollob′as, B.; Fulton, W.; Katok, A.; Kirwan, F.; Sarnak, P.; Simon, B.; Totaro, B.: Mathematical Tools for One-Dimensional Dynamics, Textbooks in Cambridge Studies in Advanced Mathematics. Cambridge University Press (2011)
20. Zhou, F.; Cao, G.; Li, B.: Design of digital image encryption algorithm based on compound chaotic system. J. Harbin Inst. Technol. **14**(Supplement 2), 30–33 (2007)
21. Fridrich, J.: Image encryption based on chaotic maps. In: IEEE International Conference on Systems, Man, and Cybernetics, Computaional Cybernetics and Simulations pp. 1105–1110 (1997)
22. Xu, S.; Wang, Y.; Wang, J.; Guo, Y.: A fast image encryption scheme based on a nonlinear chaotic map. In: Signal Processing Systems (ICSPS), 2010 2nd International Conference on, vol. 2, pp. V2-326-V2-330 (2010)
23. Khanzadi, H.; Omam, M.A.; Lotfifar, F.; Eshghi, M.: Image encryption based on gyrator transforms using chaotic maps. In: Signal Processing (ICSP), 2010 IEEE 10th International Conference on 2608–2612 (2010)
24. Khanzadi, H.; Borujeni, S.E.; Eshghi, M.: Design and FPGA Implementation of a Pseudo Random Bit Generator using Chaotic Maps. Ready to publish in IETE Research Journal