J. Cent. South Univ. (2017) 24: 2049−2057
DOI: https://doi.org/10.1007/s11771-017-3614-6

Springer

Permutation-substitution image encryption scheme based on a modified chaotic map in transform domain

Ramadan Noha[1], Ahmed HossamEldin H[1], El-khamy Said E[2], Abd El-Samie Fathi E[1]

1. Faculty of Electronic Engineering, Menofia University, Menof, Egypt;
2. Faculty of Engineering, Alexandria University, Alexandria, Egypt

Abstract: A new chaotic image encryption scheme based on permutation and substitution in the Fourier domain is presented. Fractional Fourier Transform (FRFT) is used before the encryption scheme to get a large degree of randomization. The permutation is achieved by Baker map and the substitution by a key-related-to-plain-image algorithm based on the modified Logistic map. Modification of the Logistic map is developed to increase the space of the encryption key, and hence increase the security. The key of the encryption algorithm dependents on the plain image, and thus, the cipher image is sensitive to both the initial key and the plain image to resist known-plaintext and chosen plaintext attacks. The key space is large and hence the algorithm can effectively resist brute-force attacks. The proposed scheme is examined using different performance evaluation metrics and the results prove that the proposed scheme is highly secure, and it can effectively resist different attacks.

Key words: Backer map; chaotic encryption; fractional Fourier transform (FRFT); modified Logistic map

1 Introduction

Transmission of the images over the Internet has become a very important issue. Thus, the protection of images against illegal access is very important. It is a must to protect images of army emplacements, bank building construction, and images captured by military satellites. Image encryption is used for secure transmission over open channels. Traditional encryption schemes such as Data Encryption Standards (DES) [1], Advanced Encryption Standards (AES) [2] and RC6 [3] are used to encrypt data, but they are not effective for image encryption due to the bulky nature of images, high correlation between pixels, and high redundancy, which complicate the operation and make it time consuming. Chaos-based image encryption algorithms have a better performance than the traditional encryption algorithms in the case of an image encryption [4]. Chaotic systems have many important properties, which meet some encryption requirements such as permutation, substitution, and sensitivity dependence on the initial conditions [5].

In the 19th century, Kerchhoff proposed a famous theory about the security principles of any encryption system. He said “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge” [6]. This theory presented the most important principles for designing cryptosystems. Kerchhoff observed that the encryption algorithms are supposed to be known to the attackers. Thus, the security of an encryption system should rely on the secrecy of the encryption/decryption key instead of the encryption algorithm itself. Even though in the very beginning, the opponent does not know the algorithm, the encryption system will not be able to protect the ciphertext once the algorithm is broken. The security level of an encryption algorithm is measured by the size of its key space. The larger the size of the key space is, the more time the attacker needs to do the exhaustive search in the key space [7].

Chaotic image encryption algorithms with fixed keys are easy to break. Fixed keys mean that the same key stream is used to encrypt different images. Three algorithms were demonstrated in Refs. [8−10]. The common characteristic of these algorithms is that the key in the substitution step only depends on the initial key. LI et al [11] analyzed this kind of algorithms and found some drawbacks such as weak sensitivity to the change of plain images or key stream. In this case, the key stream can be obtained by known-plaintext and chosen-plaintext attacks. Practically, user keys do not frequently change. Consequently, this kind of encryption algorithm is cracked. Under these circumstances, in order to design more secure image encryption algorithms, the key should not be related only to the initial key but also

Received date: 2016−03−08; **Accepted date:** 2017−03−13
Corresponding author: Ramadan Noha; Tel: +86−002−01005115059; E-mail: eng_noharamadan@yahoo.com

to the plaintext [12].

In image encryption, to improve the security and avoid the disadvantage of fixed key stream, the key stream should depend on the plain image. In the proposed key-related-to-plain-image algorithm, a modified Logistic map uses the plain image to generate the initial key. This key is used to encrypt the image, and then the correlation between the initial key and plain image is guaranteed.

In this work, a new image encryption algorithm based on scrambling of the positions and changing the values of image pixels in the Fourier domain is presented. Firstly, the image is rotated using the FRFT with different angles. After that, the rotated image is subjected to two-level encryption with Baker map and a modified Logistic map.

2 Fractional Fourier transform (FRFT)

The FRFT performs a rotation of the signal with an arbitrary angle. The FRFT is defined by generalizing the rotation with an angle that is π/2 in the classical FT to a rotation with an arbitrary angle $\alpha=a\pi/2$ with $a\in\mathbf{R}$. The parameter a is called the fractional order of the transform. The parameter a is limited to the range $0\leq a\leq 1$. Generally, $f_a(u)$ is the FRFT of order a of a signal $f(x)$, and u is a free variable of hybrid time/frequency nature. When $a=0$, it is a time variable, and when $a=1$ it is a frequency variable. As a takes values from 0 to 1, the interpretation of u changes gradually from "time" to "frequency", reflecting the temporal changes in the frequency content of the transformed signal. The FRFT has several equivalent definitions. One of them is a kernel-based integral transformation. It is defined by means of the transform kernel as [13, 14]

$$K_\alpha(t,u)=\begin{cases}\sqrt{\dfrac{1-\mathrm{j}\cot\alpha}{2\pi}}\cdot\exp\left(\mathrm{j}\dfrac{t^2+u^2}{2}\cdot\cot\alpha-\mathrm{j}\dfrac{tu}{\sin\alpha}\right), \\ \quad \text{if } \alpha\neq n\pi \\ \delta(u-t), \quad \text{if } \alpha=2n\pi \\ \delta(u+t), \quad \text{if } \alpha=(2n+1)\pi\end{cases} \tag{1}$$

The FRFT of a function $x(t)$ with an angle α is defined as

$$X_\alpha(u)=\int_{-\infty}^{\infty}x(t)K_\alpha(t,u)\mathrm{d}t \tag{2}$$

In this work, the FRFT is used, because the chaotic encryption in the Spatial Domain (SD) has a drawback that keeps the statistical characteristics of the image intact after scrambling. The FRFT domain provides the ability to transform correlated data patterns into uncorrelated patterns after scrambling in the transform domain. This process can achieve a large degree of randomization when returning back to the spatial domain.

3 Chaotic Baker map

The permutation step in the proposed scheme is performed with Baker map. Encryption using Baker map depends on an invertible two-dimensional chaotic Backer map on a square matrix. The chaotic Baker map is generalized by introducing parameters and then discredited to represent pixels. To encrypt an $N\times N$ image, the ciphering map is iteratively applied to the image. It is shown that the permutations induced by the Baker map behave as typical random permutations.

The Baker map, B, is described by the following equations:

$$\begin{cases}B(x,y)=(2x,y/2), & 0<x<1/2 \\ B(x,y)=(2x-1,y/2+1/2), & 1/2<x<1\end{cases} \tag{3}$$

Since an image is defined by a finite number of pixels, a correspondingly discretized form of the basic map needs to be derived. The discretized map is required to assign a pixel to another pixel in a bijective manner. The discredited generalized Baker map will be denoted B (n_1 ⋯ n_k), where the sequence of k integers, n_1, ⋯, n_k, is chosen such that each integer n_i divides N, and $n_1+\cdots+n_k=N$ [15].

4 Modified chaotic Logistic map

The Logistic map is represented by a simple non-linear dynamic equation. It is used to produce chaotic behaviors. Mathematically, a logistic map has the form [16]:

$$x_n=rx_{n-1}(1-x_{n-1}) \tag{4}$$

where x_n is a number between zero and one, n is the iteration number, r is a positive number between zero and four, and x_0 is the initial value. Figure 1 shows the bifurcation diagram of the Logistic map. This diagram has three regions which are convergence, bifurcation, and chaos, respectively. The convergence region is at $r\in[0,3]$. The bifurcation region is at $r\in[3,3.57]$, where the phenomenon of bifurcation doubling occurs. The chaos region is at $r\in[3.57,4]$, where the chaotic behavior occurs.

The modified chaotic Logistic map is developed to increase the range of r from 0 to 13.8. The modified chaotic Logistic map has the form [17]:

$$x_n=rx_{n-1}(1-x_{n-1})(1-x_{n-1})(1.2-2x_{n-1})(1.2-2x_{n-1}) \tag{5}$$

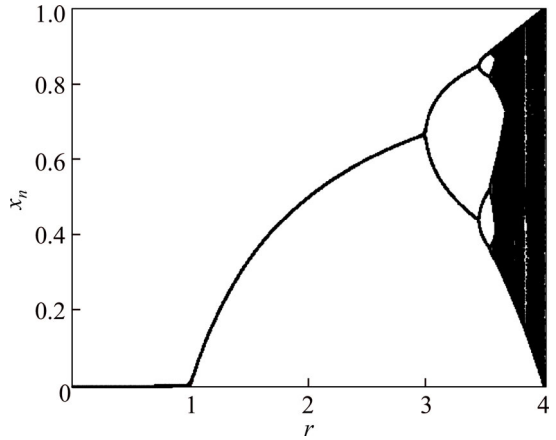

Fig. 1 Bifurcation diagram of Logistic map

The modified chaotic Logistic map is applied under the following conditions:

$$x_n \in [0,1]$$

$$r \in [0,13.8]$$

Figures 2(a), (b) and (c) show the iteration property of the modified Logistic map at different values of r to determine which value is suitable for utilization in encryption. It is clear that the modified Logistic map exhibits chaotic behavior at r=13.8, as shown in Fig. 2(c).

Figure 2(d) shows the bifurcation diagram of the modified Logistic map. This diagram has three regions which are convergence, bifurcation, and chaos, respectively. The convergence region is at $r \in [0, 3.4]$. The bifurcation region is at $r \in [3.4, 5.2]$. The chaos region is at $r \in [5.2, 13.8]$, where the chaotic behavior occurs.

5 Key-related-to-plain-image encryption algorithm

The substitution step in the proposed scheme is done by the key-related-to-plain-image algorithm, which is based on the modified chaotic Logistic map. For a gray-scale image of size $M \times N$, we use a 1-D lexicographically-ordered vector $\boldsymbol{i}=\{i_1, i_2, \cdots, i_L\}$, where $L=M \times N$. Given the initial value of the modified Logistic map x_0=0.02 and the chaotic parameter r=10, the modified Logistic map uses the plain image to generate the current chaotic number, and then takes the generated chaotic number as the next input to the chaotic iterations. This process is repeated and the last output value is used as the initial key. This key is used to encrypt the image. By doing so, the correlation between the initial key and the plain image is created. The flowchart of the encryption algorithm is shown in Fig. 3.

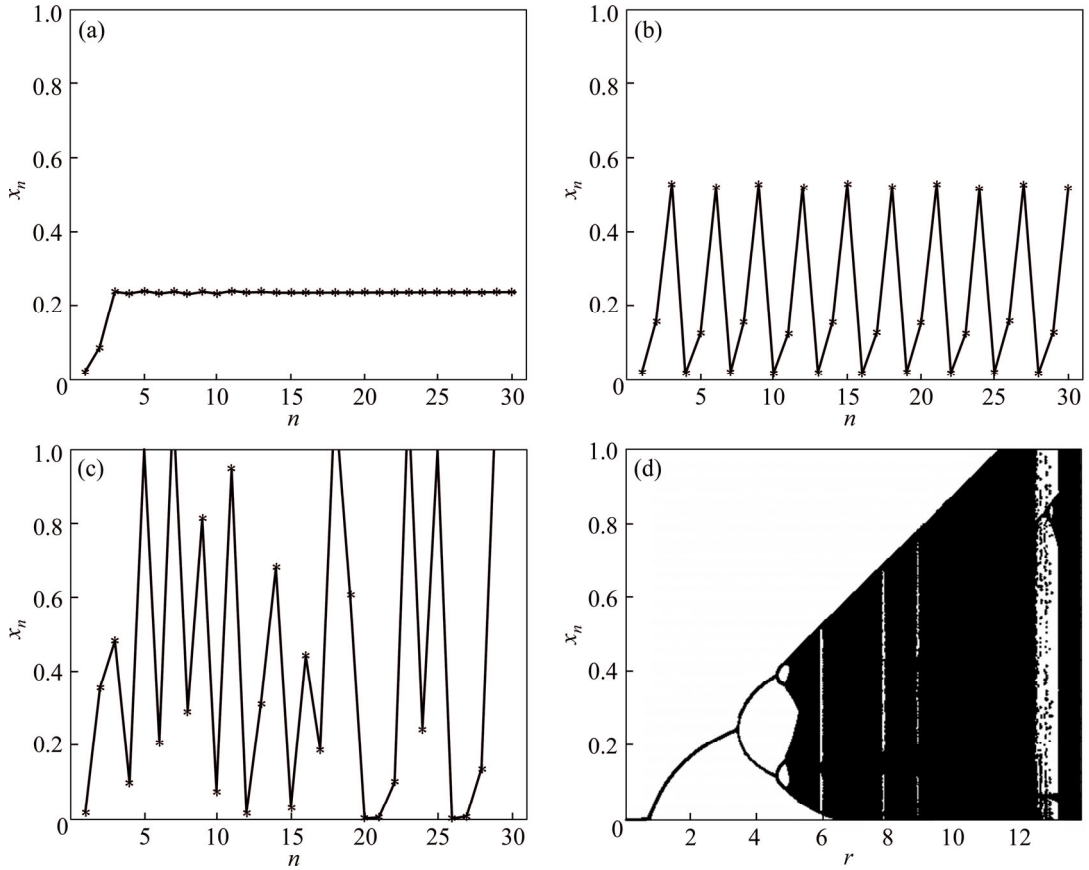

Fig. 2 Analysis of modified Logistic map: (a) Iteration property at r=3.2; (b) Iteration property at r=6; (c) Iteration property at r=13.8; (d) Bifurcation diagram of modified Logistic map

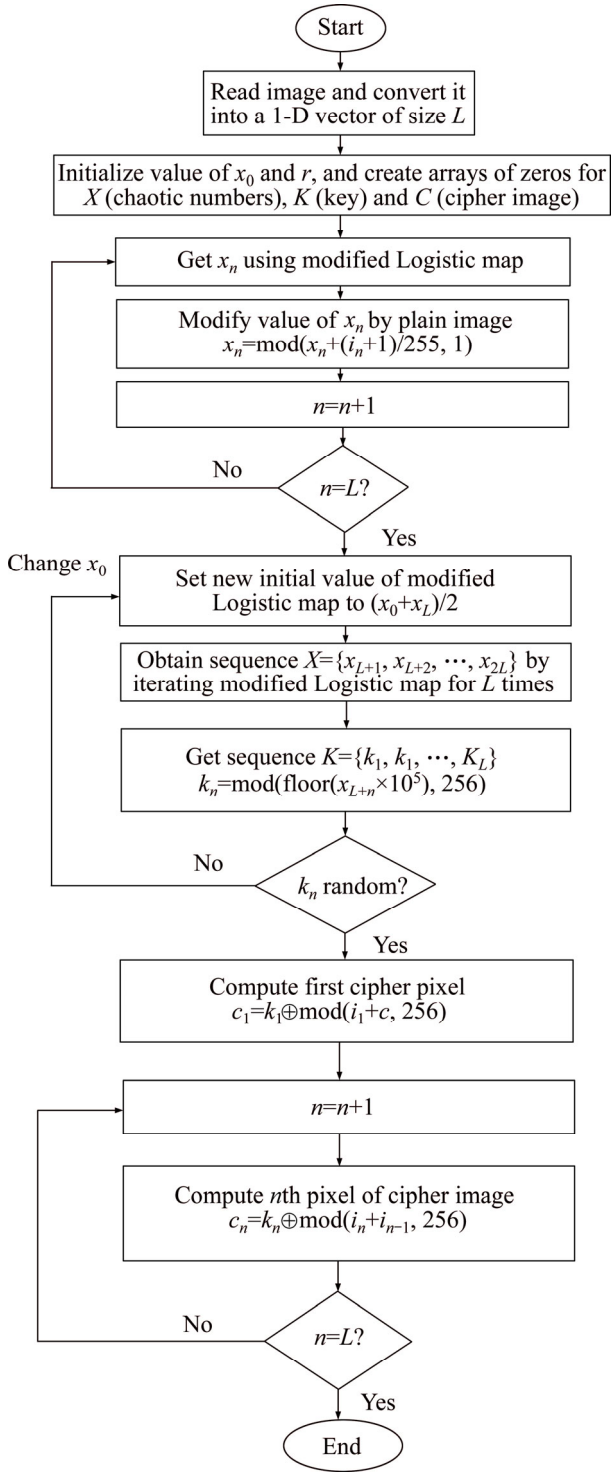

Fig. 3 Encryption flowchart of key-related-to-plain-image algorithm

The decryption algorithm is the reverse of the encryption process as follows:

Step 1: Let the initial value of the modified Logistic map be $(x_0+x_L)/2$.

Step 2: Generate the chaotic sequence $X=\{x_{L+1}, x_{L+2}, \cdots, x_{2L}\}$ by the modified Logistic map using Eq. (5) according to the same value of x_0=0.02, and chaotic parameter r=10.

Step 3: Obtain the key stream $K=\{k_1, k_2, \cdots, k_L\}$ according to sequence X.

Step 4: Decrypt the first pixel as follows:

$$i_1 = K_1 \oplus \mathrm{mod}(c_1 + 256 - c, 256) \tag{6}$$

where i_1 is the decrypted value of the first pixel.

Step 5: Set $n=n+1$

Step 6: Decrypt the nth pixel using the previous pixel of the cipher image and the k_n as follows:

$$i_n = k_n \oplus \mathrm{mod}(c_n + 256 - i_{n-1}, 256) \tag{7}$$

Step 7: Repeat steps 5 and 6, until n reaches L, and hence the decrypted image $\boldsymbol{i}$ is obtained.

6 Proposed scheme

The proposed encryption scheme is based on scrambling the positions and changing the values of image pixels in the frequency domain. The proposed algorithm is divided into two stages. The first stage is applying the fractional Fourier transform with three different values of α; $\pi/10$, $2\pi/10$ and $3\pi/10$ on the plain image. Then, the transformed image is subjected to the second stage, which consists of the permutation and substitution. The permutation process is achieved using the chaotic Baker map. The permuted transformed image is then encrypted with the key-related-to-plain-image algorithm using the modified Logistic map to achieve the substitution, as shown in Fig. 4.

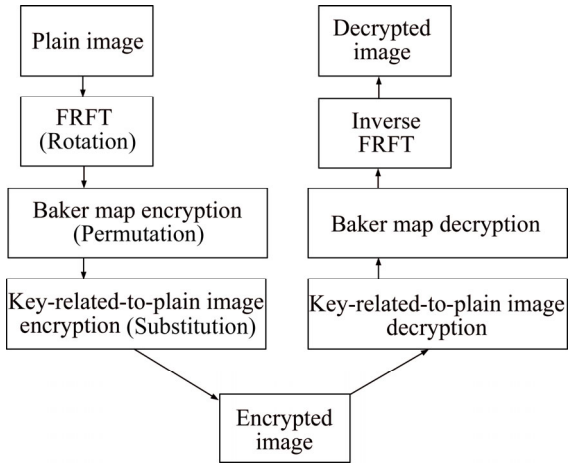

Fig. 4 Proposed scheme

7 Security analysis

A good encryption scheme should resist most kinds of known attacks. The key space should be large enough to resist brute-force attacks. In the proposed scheme, the key space consists of the key space of both the permutation and the substitution processes. The key space of the Baker map (permutation process) for a gray-scale image of size 256× 256 is equal to 10^{63} [18].

The secrete key of the key-related-to-plain-image algorithm (substitution process) depends on (x_0, r, x_L, c), where x_0, x_L and r are double precision numbers and c is a constant integer, $c\in[1, 255]$. The number of different values for x_0, x_L and r is 10^{14}. It gives 14 significant decimal digits precision. So, the key space of the substitution process is $10^{14}\times10^{14}\times10^{14}\times255$ in addition to the value of the parameter α, which represents the angle of rotation of the FRFT. Such a large key space can resist brute-force attacks. Table 1 gives the key space of the encryption schemes.

Table 1 Key space of encryption schemes

Encryption scheme	Key space
Proposed scheme	$10^{63}\times10^{14}\times10^{14}\times10^{14}\times225$
Chaotic Baker map	10^{63}
RC6	2^{128}

In the proposed scheme, the pixel values of the plain image are utilized to change the chaotic numbers generated by the modified Logistic map. This chaotic sequence generated depends not only on the initial key, but also on the plain image. When different plain images are encrypted, the corresponding key streams are not the same. Hence, the attacker cannot obtain useful information by encrypting some special images since the resulting information is related to the chosen images [19, 20]. Therefore, the proposed scheme can resist the known-plaintext and chosen-plaintext attacks.

8 Sensitivity analysis

In general, the encrypted image must be sensitive to small changes in the secret key. In order to resist differential attacks, a small change in the secret key should cause a significant change in the encrypted image. Two parameters are used for differential analysis: net pixel change rate (NPCR) and unified average changing intensity (UACI) [21]. We obtained NPCR and UACI of the encrypted Mandrill image under changes in the values of x_0 and r. We used x_0=0.02 and r=10 as the first set of the key, and then changed them. Table 2 gives the values of NPCR and UACI of the encrypted images with keys (x_0, r) and other slightly different keys ($x_0+\Delta x_0$, $r+\Delta r$). The results show that for the proposed scheme, more than 99% of the pixels in the encrypted image change their gray values, when the key just changes by 10^{-15}. This means the proposed scheme provides high key sensitivity. For a 256 gray level image, the expected UACI value is 33% and the proposed scheme has UACI value equal to 33.4697%. Furthermore, the proposed scheme has the best results for NPCR and UACI among RC6 and chaotic Baker map.

Table 2 NPCR and UACI of encrypted Mandrill images

Encryption scheme	Key	NPCR	UACI
Proposed scheme	$\Delta x_0=10^{-15}$, $\Delta r=0$	99.5697	33.4432
	$\Delta x_0=0$, $\Delta r=10^{-15}$	99.6048	33.4697
Chaotic baker map	One bit change	99.1791	16.8258
RC6	One bit change	99.6014	27.2870

9 Quality metrics of encryption

Fourmetrics will be used to compare between RC6, chaotic Backer map, the key-related-to-plain-image algorithm and the proposed scheme (Baker+key-related-to-plain-imagealgorithm). These metrics are the correlation coefficient, the maximum deviation, the irregular deviation, and the histogram uniformity. Also, the effect of the angle α in the FRFT domain will be studied.

9.1 Correlation coefficient

The closer the value of the correlation coefficient (CC) to zero is, the better the encryption is. The correlation coefficient equals one if the encrypted image is the same as the plain image and the encryption process fails in hiding the details of the plain image. If the correlation coefficient equals zero, then the plain image and its encrypted version are totally different. So, the success of the encryption process means smaller values of the CC. The CC (C_c) is measured by the following equation [22]:

$$C_c=\frac{\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y))}{\sqrt{\left(\sum_{i=1}^{N}x_i-E(x))^2\right)}\sqrt{\left(\sum_{i=1}^{N}y_i-E(y))^2\right)}} \tag{8}$$

where $E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$, and x and y are the gray-scale pixel values of the plain and encrypted images.

9.2 Maximum deviation

The maximum deviation (MD) measures the quality of encryption in terms of how it maximizes the deviation between the plain and the encrypted images. It is calculated as follows [23]:

1) Get the histogram distributions of both the plain and encrypted images;

2) Compute the absolute difference or deviation between the two histogram curves;

3) Count the area under the absolute difference curve, which is the sum of deviations (D):

$$D=\frac{h_0+h_{255}}{2}+\sum_{i=1}^{254}h_i \tag{9}$$

where h_i is the amplitude of the absolute difference curve

at index i. The higher the value of D is, the more the encrypted image is deviated from the plain image.

9.3 Irregular deviation (ID)

This quality metric is based on how much the deviation caused by encryption is irregular. It is measured as follows [24]:

1) Calculate the matrix $\boldsymbol{D}$, which represents the absolute difference between the pixel values at each position before and after encryption. So, $\boldsymbol{D}$ can be represented as

$$\boldsymbol{D}=|I-J| \tag{10}$$

where I is the plain image, and J is the encrypted image.

2) Construct the histogram distribution H of the matrix $\boldsymbol{D}$;

3) Get the average value of this histogram:

$$\overline{H}=\frac{1}{256}\sum_{i=0}^{255}H(i) \tag{11}$$

4) Subtract this average from the deviation histogram, and then take the absolute value of the result.

$$A(i)=\left|H(i)-\overline{H}\right| \tag{12}$$

Estimate the area under the absolute AC curve. ID (D_I) can be represented as

$$D_\mathrm{I}=\sum_{i=0}^{255}A(i) \tag{13}$$

Thus, the lower the ID value, the better the encryption algorithm.

9.4 Histogram analysis

The histogram uses a bar graph to profile the occurrence of each gray level present in an image. The horizontal axis is the gray-level values. It begins at zero and goes to the number of gray levels. Each vertical bar represents the number of times of corresponding gray level occurrence times in the image. This test is made using the MATLAB built in function (imhist).

10 Results and discussion

All the experiments have been carried out with MATLAB R2007a on Windows XP system on a Laptop with Intel Core 2 Duo Processor 1.6 GHz, 2 GB RAM, and 150 GB hard disk. We used the Mandrill 256×256 image as the plain image.

Here, a detailed discussion of the results is obtained in Table 3:

1) Visual inspection

The encrypted Mandrill images using the different encryption schemes in the spatial and FRFT domains are shown in Figs. 5, 6 and 7. All encryption schemes have succeeded in hiding the features of the image in both domains. Visual inspection is not enough for judging the quality of the encryption schemes. So, other metrics are considered to evaluate the quality of encryption.

2) Histogram

The histograms of the plain and encrypted images in spatial and FRFT domains are shown in Figs. 8, 9 and 10. From these figures, one can say that the histograms of the encrypted images are fairly uniform and significantly

Table 3 Encryption evaluation metrics of encrypted images for different encryption schemes in spatial and FRFT domains

Encryption scheme	Domain		CC	MD	ID	Time/s
Proposed scheme	Spatial		0.0030	53300	49630	18.098
	FRFT	$\alpha=\pi/10$	0.0016	53300	42126	20.937
		$\alpha=2\pi/10$	0.0021	53249	42228	20.487
		$\alpha=3\pi/10$	**0.0016**	**56405**	**42126**	20.363
Key-related-to-plain-image algorithm	Spatial		0.00052	55633	49380	17.550
	FRFT	$\alpha=\pi/10$	0.0040	52865	42536	18.063
		$\alpha=2\pi/10$	0.0046	53065	42336	18.783
		$\alpha=3\pi/10$	0.0040	52865	42536	19.660
Chaotic Baker map	Spatial		0.0190	0	72760	1.133
	FRFT	$\alpha=\pi/10$	0.0069	0	62976	1.236
		$\alpha=2\pi/10$	0.0190	0	63474	1.228
		$\alpha=3\pi/10$	0.0069	0	62976	1.264
RC6	Spatial		0.0013	55496	49548	2310
	FRFT	$\alpha=\pi/10$	0.0039	53174	42496	2314
		$\alpha=2\pi/10$	0.0039	53174	42496	2313
		$\alpha=3\pi/10$	0.0039	53174	42496	2316

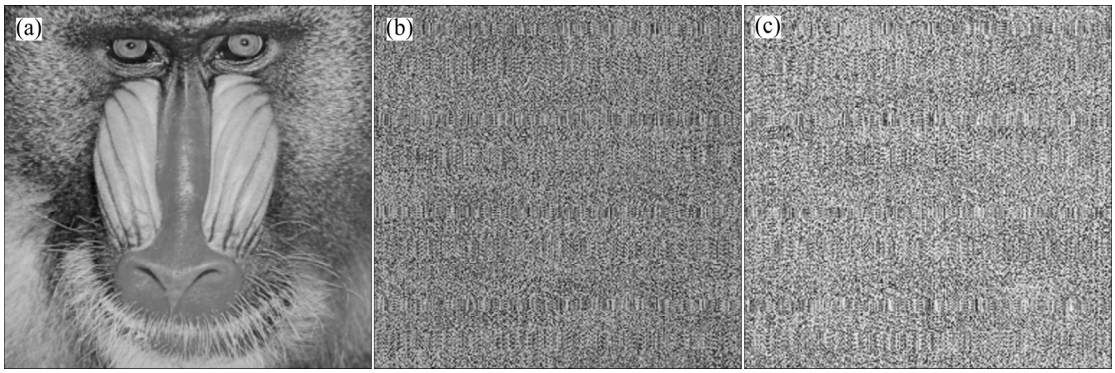

Fig. 5 Encrypted images using chaotic Baker map in spatial and FRFT domains: (a) Mandrill plain image; (b) Spatial domain; (c) FRFT domain, $\alpha=\pi/10$

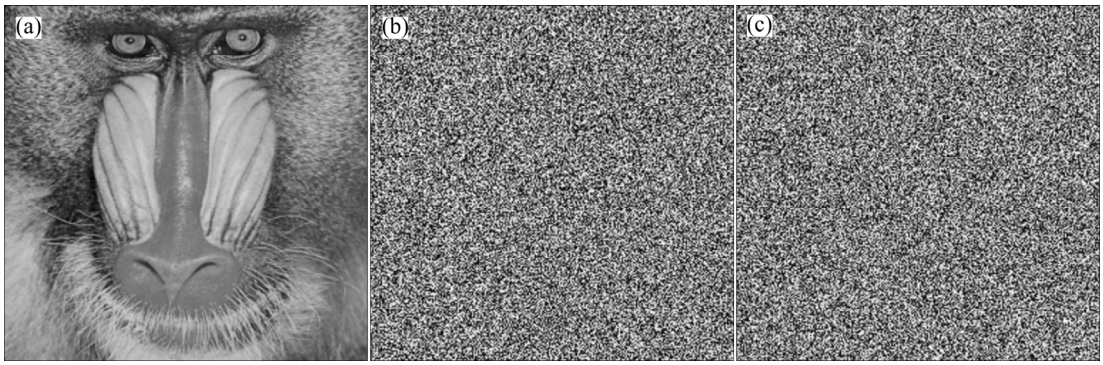

Fig. 6 Encrypted images using key-related-to-plain-image algorithm in spatial and FRFT domains: (a) Mandrill plain image; (b) Spatial domain; (c) FRFT domain, $\alpha=\pi/10$

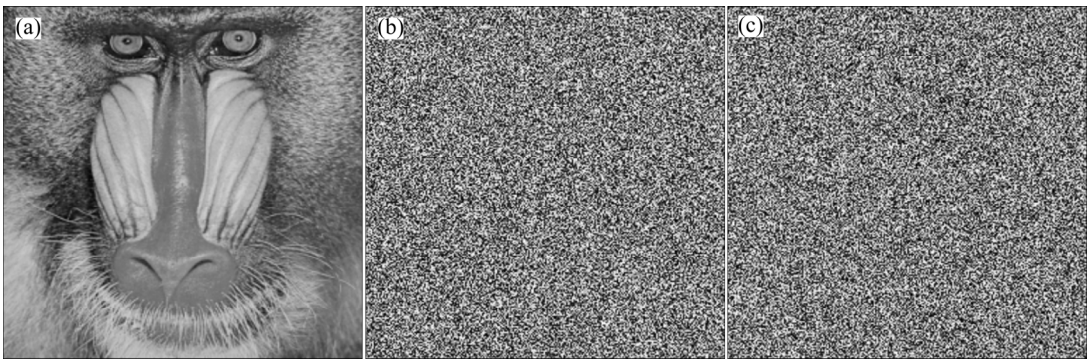

Fig. 7 Encrypted images using proposed scheme in spatial and FRFT domains: (a) Mandrill plain image; (b) Spatial domain; (c) FRFT domain, $\alpha=\pi/10$

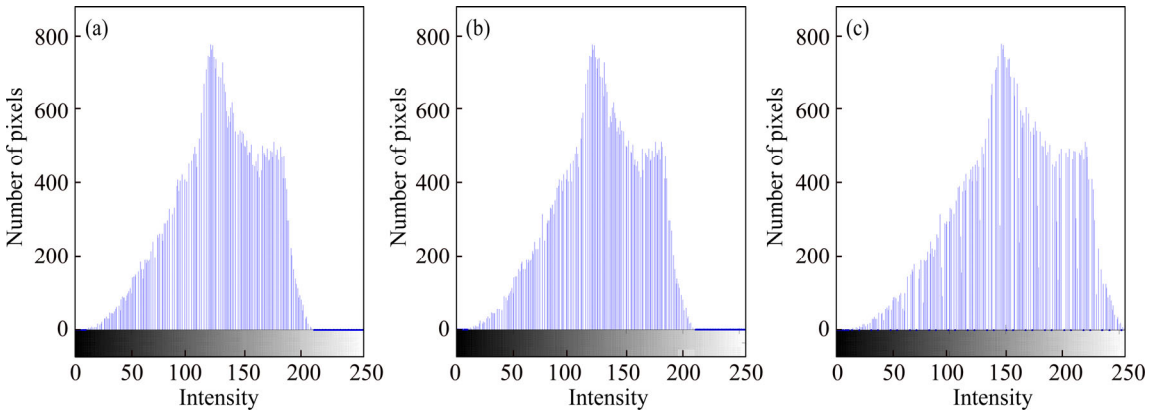

Fig. 8 Histograms of encrypted images using chaotic Baker map in spatial and FRFT domains: (a) Mandrill plain image; (b) Spatial domain; (c) FRFT domain, $\alpha=\pi/10$

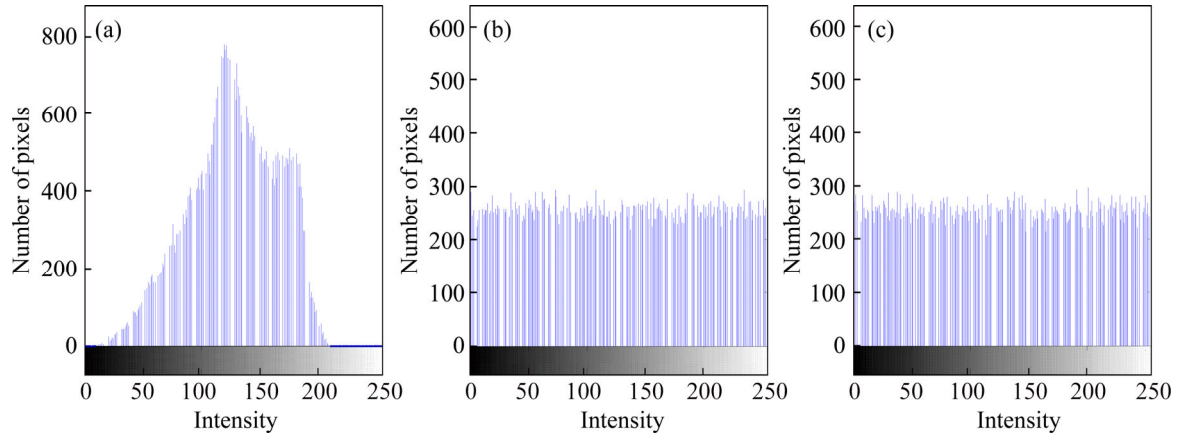

Fig. 9 Histograms of encrypted images using key-related-to-plain-image algorithm in spatial and FRFT domains: (a) Mandrill plain image; (b) Spatial domain; (c) FRFT domain, $\alpha=\pi/10$

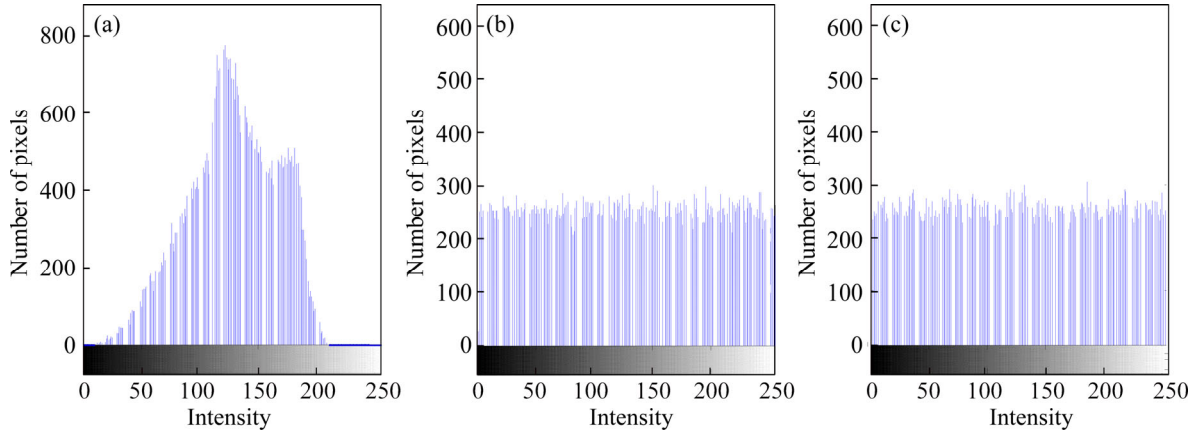

Fig. 10 Histograms of encrypted images using proposed scheme in spatial and FRFT domains: (a) Mandrill plain image; (b) Spatial domain; (c) FRFT domain, $\alpha=\pi/10$

different from that of the plain image except for the Baker map encryption. It is the same as the plain image, because Baker map encryption is based only on permutations.

3) Correlation coefficient

In general, all algorithms have good CC values, but the CC for the proposed scheme has the lowest value for both the spatial and FRFT domains at all values of α. For RC6, the value of CC does not change with the angle α. So, the correlation coefficient between the plain image and the encrypted image has been improved with the proposed scheme.

4) Maximum deviation

The proposed scheme has the highest MD, especially in the FRFT domain at $\alpha=3\pi/10$. The chaotic Baker map has the worst MD in both spatial and FRFT domains, because the Baker map encryption is just a permutation of pixels.

5) Irregular deviation

The proposed scheme has the best result of ID among all algorithms, especially in the FRFT domain at $\alpha=3\pi/10$. Baker map encryption has the worst ID result. In general, the FRFT enhances the ID of all schemes.

6) Speed

The encryption time of RC6 is the longest time. The encryption time of chaotic Baker map is the shortest time. The encryption time of the proposed scheme is greater than that of chaotic Baker map encryption, since it consists of two levels of encryption (permutation and substitution) to achieve a high level of security.

11 Conclusions

A new and efficient image encryption scheme based on a combination of two chaotic encryption maps has been introduced. The permutation is achieved by the chaotic Backer map. The substitution is performed with a proposed key-related-to-plain-image algorithm using the modified Logistic map, which has a wide range of a chaotic parameter to be more robust to attacks. The key of the substitution algorithm depends on the initial key and the plain image, and thus the proposed scheme can resist the known-plaintext and chosen plaintext attacks. The proposed scheme has a very large key space, and hence it can resist brute-force attacks. The FRFT has been studied with different values of the rotation angle. It

has improved the performance of the chaotic cryptosystem. FRFT allowed using a wide range of angles without restrictions to increase the degree of security. Simulation results have shown that the proposed scheme is very sensitive to minor changes in the key. Security and quality measurements have been carried out to demonstrate that the proposed scheme is more secure and resistant to different attacks.

References

[1] BURR W E. Data encryption standard [M]// NIST's anthology. A Century of Excellence in Measurements Standards and Technology: A Chronicle of Selected NBS/NIST Publications, 2000.

[2] FIPS PUB 197. Advanced Encryption Standard (AES) [S]. National Institute of Standards and Technology, U.S. Department of Commerce, 2001.

[3] RIVEST R L, ROBSHAW M J B, SIDNEY R, YIN Y L. The RC6TM Block Cipher [M]. Cambridge, USA: MIT Laboratory for Computer Science, 1998.

[4] PATIDAR V, PAREEK N K, SUD K K. A new substitution–diffusion based image cipher using chaotic standard and logistic maps[J]. Nonlinear Sci Numer Simulat, 2009, 14: 3056−3075.

[5] ZHANG L H, LIAO X F, WANG X B. An image encryption approach based on chaotic maps [J]. Chaos, Solitons & Fractals, 2005, 24: 759−765.

[6] SHANNON C E. A mathematical theory of communication [J]. Bell System Technical Journal, 1948, 27: 379−423.

[7] YANG M, BOURBAKIS N, LI S. Data-image-video encryption [M]. IEEE, 2004.

[8] MAO Y, CHEN G, LIAN S. A novel fast image encryption scheme based on 3D chaotic Baker maps [J]. International Journal of Bifurcation and Chaos, 2004, 14(10): 3613−3624.

[9] SHEN J, JIN X, ZHOU C. A color image encryption algorithm based on magic cube transformation and modular arithmetic operation [J]. Advances in Multimedia Information Processing, Lecture Notes in Computer Science, 2005, 3768: 270−280.

[10] HE X, ZHU Q, GU P. A new chaos-based encryption method for color image [J]. Rough Sets and Knowledge Technology, Lecture Notes in Computer Science, 2006, 4062: 671−678.

[11] LI C, CHEN G. On the security of a class of image encryption schemes [C]// Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '08). Seattle, Wash, USA, 2008: 3290−3293.

[12] CAO Guang-hui, HU Kai, ZHANG Yi-zhi, ZHOU Jun, ZHANG Xing. Chaotic image encryption based on running-key related to plaintext [J]. Hindawi Publishing Corporation the Scientific World Journal, 2014(6): 490179.

[13] OZAKTAS H M, ZALEVSKY Z, KUTAY M A. The fractional Fourier transform [M]. Chichester: Wiley, 2001.

[14] OZAKTAS H M. Fractional Fourier domains [J]. Signal Process, 1995, 46: 119−124.

[15] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps [J]. Int J Bifurcation and Chaos, 1998, 8(6): 1259−1284.

[16] BAKER G L, GOLLUB J P. Chaotic dynamics an Introduction [M]. First Ed. New York: Press Syndicate of the University of Cambridge, 1990.

[17] EL-HOSENY H, AHMED H H, KAZEMIAN H, ABD EL-SAMIE F E, ABBAS A M. Digital image encryption in transform domains [D]. Faculty of Electronic Engineering, Menofia University, Menof, 2014.

[18] FRIDRICH J. Symmetric ciphers based on two-dimensional chaotic maps [J]. Int J Bifurcation and Chaos, 1998, 8(6): 1259−1284.

[19] ZHU Cong-xu, XU Si-yuan, HU Yu-ping. Breaking a novel image encryption scheme based on Brownian motion and PWLCM chaotic system [J]. Nonlinear Dynamics, 2015, 79(2): 1511−1518.

[20] ZHU Cong-xu, LIAO Chun-long, DENG Xiao-heng. Breaking and improving an image encryption scheme based on total shuffling scheme [J]. Nonlinear Dynamics, 2013, 71(1, 2): 25−34.

[21] MERKLE R C, HELLMAN M. On the security of multiple encryption [J]. Communications of the ACM, 1981, 24(7): 465−467.

[22] http://in.mathworks.com/help/images/ref/corr2.html

[23] CURRAN K, BAILEY K. An evaluation of image based steganography methods [J]. International Journal of Digital Evidence, 2003, 2(2): 55−88.

[24] FU Chong, CHEN Jun-jie, ZOU Hao, MENG Wei-hong, ZHAN Yong-feng. A chaos based digital image encryption scheme with an improved diffusion strategy [J]. Optics Express, 2012, 20(3): 2363−2378.

(Edited by YANG Bing)

Cite this article as: Ramadan Noha, Ahmed HossamEldin H, El-khamy Said E, Abd El-Samie Fathi E. Permutation-substitution image encryption scheme based on a modified chaotic map in transform domain [J]. Journal of Central South University, 2017, 24(7): 2049–2057. DOI: https://doi.org/10.1007/s11771-017-3614-6.