Signal Processing 97 (2014) 172–182

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

A new 1D chaotic system for image encryption

Yicong Zhou *, Long Bao, C.L. Philip Chen

Department of Computer and Information Science, University of Macau, Macau 999078, China

ARTICLE INFO

Article history:
Received 10 August 2013
Received in revised form
21 October 2013
Accepted 25 October 2013
Available online 13 November 2013

Keywords:
Chaotic system
Image encryption
Security analysis
Chosen-plaintext attack

ABSTRACT

This paper introduces a simple and effective chaotic system using a combination of two existing one-dimension (1D) chaotic maps (seed maps). Simulations and performance evaluations show that the proposed system is able to produce many 1D chaotic maps with larger chaotic ranges and better chaotic behaviors compared with their seed maps. To investigate its applications in multimedia security, a novel image encryption algorithm is proposed. Using a same set of security keys, this algorithm is able to generate a completely different encrypted image each time when it is applied to the same original image. Experiments and security analysis demonstrate the algorithm's excellent performance in image encryption and various attacks.

1. Introduction

Information security is an eternal topic. In the ancient time, when people transmitted important text information to the others over a long distant, how to prevent the leakage of original text information became a tough and vital problem. To deal with this problem, many methods of steganography and cryptography were proposed. However, with the development of information technologies, the digital image, a format of information, has been increasingly utilized, stored and transmitted, such as medical images, grayscale images, color images, binary images and so on. Hence, how to protect this type of information becomes an essential and urgent challenge [1–4].

Considering the characteristic of image data, many existing image encryption algorithms have been proposed based on different technologies, such as SCAN [5,6], circular random grids [7,8], elliptic curve ElGamal [9], gray code [10], wave transmission [11], vector quantization [12], fractional wavelet transform [13,14], p-Fibonacci transform [15], and chaos [16–21]. Among these technologies, chaos-based image encryption has become one of efficient and excellent encryption methods. This is because chaotic systems/maps have high sensitivity to their initial values and control parameters, chaotic property, non-convergence, and state ergodicity. Therefore, many chaotic image encryption algorithms have been developed by directly utilizing existing chaotic systems/maps to their encryption processes [22,23]. In general, a chaos-based image encryption algorithm contains two portions: a chaotic system and image encryption.

Chaotic systems/maps in the image encryption algorithms can be divided into two categories: one-dimension (1D) and multi-dimension (MD). The MD chaotic maps have increasing applications in image security [24–26] because of their complex structures and multiple parameters. However, multiple parameters increase the difficulty of their hardware/software implementations and computation complexity [27]. 1D chaotic systems, on the other hand, have a simple structure and are easy to implement [27–31]. But, they also have three problems including: (1) the limited or/and discontinuous range of chaotic behaviors [32,33]; (2) the vulnerability to low-computation-cost analysis using iteration and correlation functions [34]; and (3) the nonuniform data distribution of output chaotic sequences. Hence, developing new chaotic systems with better chaotic performance is needed.

* Corresponding author. Tel.: +86 853 83978458; fax: +86 853 28838314.
E-mail address: yicongzhou@umac.mo (Y. Zhou).

0165-1684/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2013.10.034

For evaluating an image encryption algorithm, security should be the first and vital principle. Many chaos-based image encryption algorithms have been shown to have the security weakness by cryptanalysis [35–37]. For example, they are unable to withstand the chosen-plaintext attacks.

To address these above-mentioned problems, this paper introduces a new chaotic system with a simple structure. It integrates two existing 1D chaotic maps to generate a number of new chaotic maps. They have excellent chaotic properties, including a wide range of parameter settings and the uniform-distributed variant density function. These can be verified by simulations and analysis of three specific examples of the proposed chaotic system. To demonstrate its applications, we then introduce a novel image encryption algorithm which has the excellent confusion and diffusion properties for withstanding different attacks, especially the chosen-plaintext attacks. Every time the algorithm is applied to an original image with the same set of security keys, it generates a new encrypted image which is completely different from any previous one. This ensures that the proposed algorithm is able to withstand the chosen-plaintext attacks.

This paper is organized as follows. Section 2 briefly reviews several existing chaotic maps. They will be used in the new chaotic system and its three examples are proposed in Section 3. Section 4 introduces the novel image encryption algorithm. Simulation results are presented in Section 5. Section 6 provides a detailed security study and various attacks to the proposed image encryption algorithm. Section 7 reaches a conclusion.

2. Background

In the group of chaotic maps, the 1D chaotic maps have lots of applications because of their simple structures. In this section, we briefly review three 1D chaotic maps: the Logistic, Tent and Sine maps. They will be used for our new chaotic system.

2.1. Logistic map

The Logistic map is one of famous 1D chaotic maps. It is a simple dynamical equation with complex chaotic behavior. The mathematical definition can be expressed in the following equation:

$$X_{n+1} = \mathcal{L}(r, X_n) = rX_n(1-X_n) \tag{1}$$

where r is a parameter with range of $(0,4]$ and X_n is the output chaotic sequence.

To observe its chaotic behaviors, its bifurcation diagram and Lyapunov Exponent are presented in Figs. 2(a) and 3(a). In the bifurcation diagram shown in Fig. 2(a), the dotted line shows its good chaotic behavior and the solid line represents its non-chaotic property. There are two problems in the Logistic map. First, its chaotic range is limited only within $[3.57, 4]$. Even within this range, there are some parameters which make the Logistic map to have no chaotic behaviors. This is verified by the blank zone in its bifurcation diagram and plot of the Lyapunov Exponent in Fig. 3(a). For the Lyapunov Exponent, a positive value means a good chaotic property of a chaotic map. As shown in Fig. 3(a), the Lyapunov Exponents of the Logistic map are smaller than zero when parameter $r < 3.57$. Second, the data range of the chaotic sequences is smaller than $[0, 1]$, showing the non-uniform distribution in the range of $[0, 1]$. These narrow down the applications of the Logistic map.

2.2. Tent map

The Tent map is known as its tent-like shape in the graph of its bifurcation diagram. It can be defined by the following equation:

$$X_{n+1} = \mathcal{T}(u, X_n) = \begin{cases} uX_n/2 & X_i < 0.5 \\ u(1-X_n)/2 & X_i \geq 0.5 \end{cases} \tag{2}$$

where parameter $u \in (0, 4]$.

Its chaotic property is shown in bifurcation analysis in Fig. 2(b) and Lyapunov Exponent analysis in Fig. 3(b). Both analysis results prove that its chaotic range is $[2, 4]$. The Tent map has the same problem as the Logistic map: the limited chaotic range and nonuniform distribution of the variant density function.

2.3. Sine map

The Sine map has a similar chaotic behavior with the Logistic map. The definition can be described by the following equation:

$$X_{n+1} = \mathcal{S}(a, X_n) = a \sin(\pi X_n)/4 \tag{3}$$

where parameter $a \in (0, 4]$.

As shown in Figs. 2(c) and 3(c), its bifurcation diagram and Lyapunov Exponent are similar with those of the Logistic map in Figs. 2(a) and 3(a). Thus they have the same problems as discussed in Section 2.1.

3. New chaotic system

In this section, a new chaotic system will be proposed to solve the problems discussed in Section 2. To evaluate its performance, three examples are then introduced.

3.1. System structure

The new chaotic system is shown in Fig. 1. It is a nonlinear combination of two different 1D chaotic maps which are considered as seed maps. The system is defined by the following equation:

$$X_{n+1} = \mathcal{A}_{FG} = (F(a, X_n) + G(b, X_n)) mod\ 1 \tag{4}$$

where $F(a, X_n)$ and $G(b, X_n)$ are two 1D chaotic maps (seed maps) with parameters a and b; *mod* is the modulo operation, and n is the iteration number.

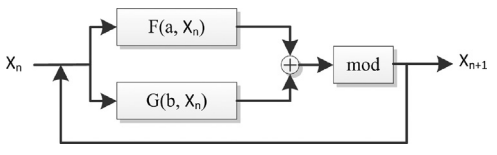

Fig. 1. The new chaotic system.

Combining outputs of two seed maps, the new chaotic system shows a mixed chaotic property. Here, the '*mod*' operation is to ensure its output data with in range of [0, 1].

Using different seed maps, this system is able to generate many new chaotic sequences. Compared with its corresponding seed maps, this system has more complex chaotic properties. When one of its seed maps is out of the chaotic range, this chaotic system can still have excellent chaotic behaviors.

3.2. Examples of the proposed chaotic system

To show the excellent performance of the proposed chaotic system, three examples will be introduced and analyzed here.

3.2.1. The Logistic-Tent system

The first example utilizes the Logistic and Tent maps as seed maps. The system is called the Logistic-Tent system (LTS). To simplify its chaotic complexity, we combine the parameter settings for each seed map, as defined in the following equation:

$$X_{n+1} = \mathcal{A}_{\mathcal{LT}}(r, X_n) = (\mathcal{L}(r, X_n) + \mathcal{T}((4-r), X_n)) mod\ 1 = \begin{cases} (rX_n(1-X_n) + (4-r)X_n/2) mod\ 1 & X_i < 0.5 \\ (rX_n(1-X_n) + (4-r)(1-X_n)/2) mod\ 1 & X_i \geq 0.5 \end{cases} \quad (5)$$

where parameter $r \in (0, 4]$.

The bifurcation diagram and Lyapunov Exponent of the LTS are shown in Figs. 2(d) and 3(d), respectively. Its chaotic range is within (0, 4], which is much larger than these of the Logistic or Tent maps. Its output sequences uniformly distribute within [0, 1] (see Fig. 2(d)). Hence, the LTS has better chaotic performance than the Logistic and Tent maps.

3.2.2. The Logistic-Sine system

The Logistic-Sine system (denoted as LSS) is the second example of the proposed chaotic system, defined in Eq. (6). Its parameters are also unified for simplicity.

$$X_{n+1} = \mathcal{A}_{\mathcal{LS}}(r, X_n) = (\mathcal{L}(r, X_n) + \mathcal{S}((4-r), X_n)) mod\ 1 = (rX_n(1-X_n) + (4-r)\sin(\pi X_n)/4) mod\ 1 \quad (6)$$

where parameter $r \in (0, 4]$.

Figs. 2(e) and 3(e) show its bifurcation diagram and Lyapunov Exponent results. The chaotic behaviors of the LSS exist in the whole range of parameter settings and its chaotic sequences have a uniform-distribution within [0, 1].

3.2.3. The Tent-Sine system

Using the Tent and Sine maps as seed maps, the proposed chaotic system in Eq. (4) becomes a new chaotic system called the Tent-Sine system (TSS). Its definition can be described in Eq. (7) after unifying its parameter settings.

$$X_{n+1} = \mathcal{A}_{\mathcal{TS}}(r, X_n) = (\mathcal{T}(r, X_n) + \mathcal{S}((4-r), X_n)) mod\ 1$$

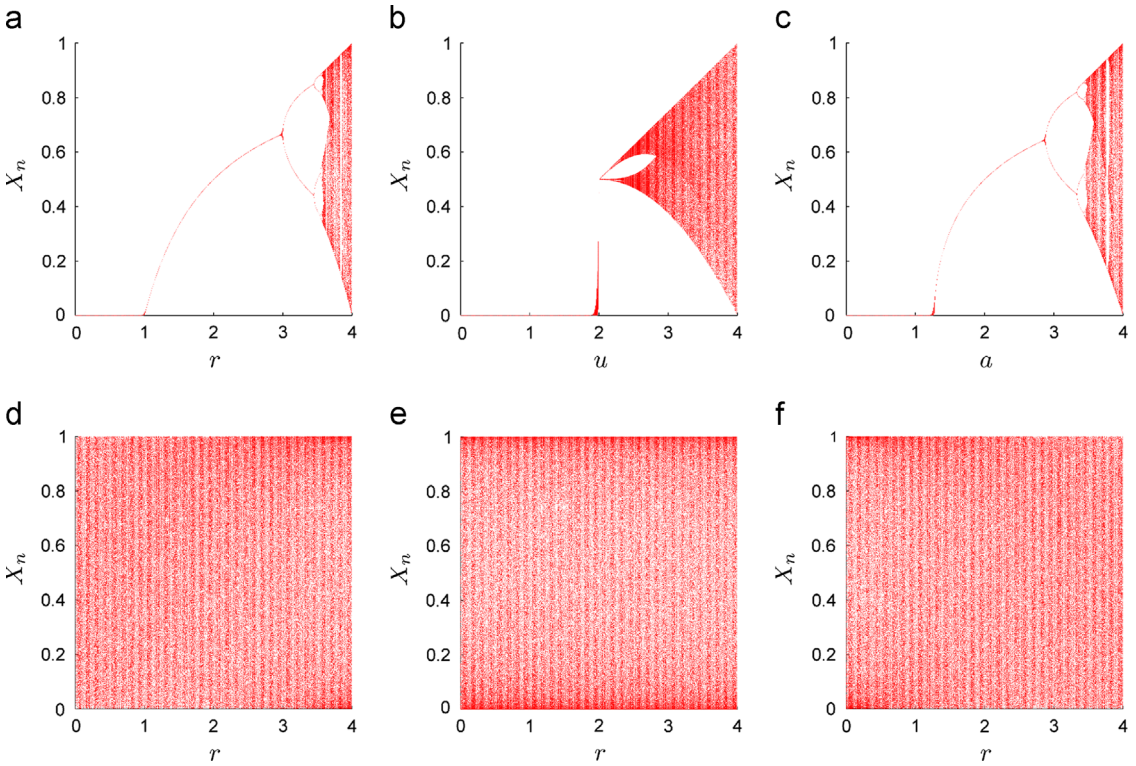

Fig. 2. The Bifurcation diagrams of the (a) Logistic map; (b) Tent map; (c) Sine map; (d) LTS; (e) LSS; and (f) TSS.

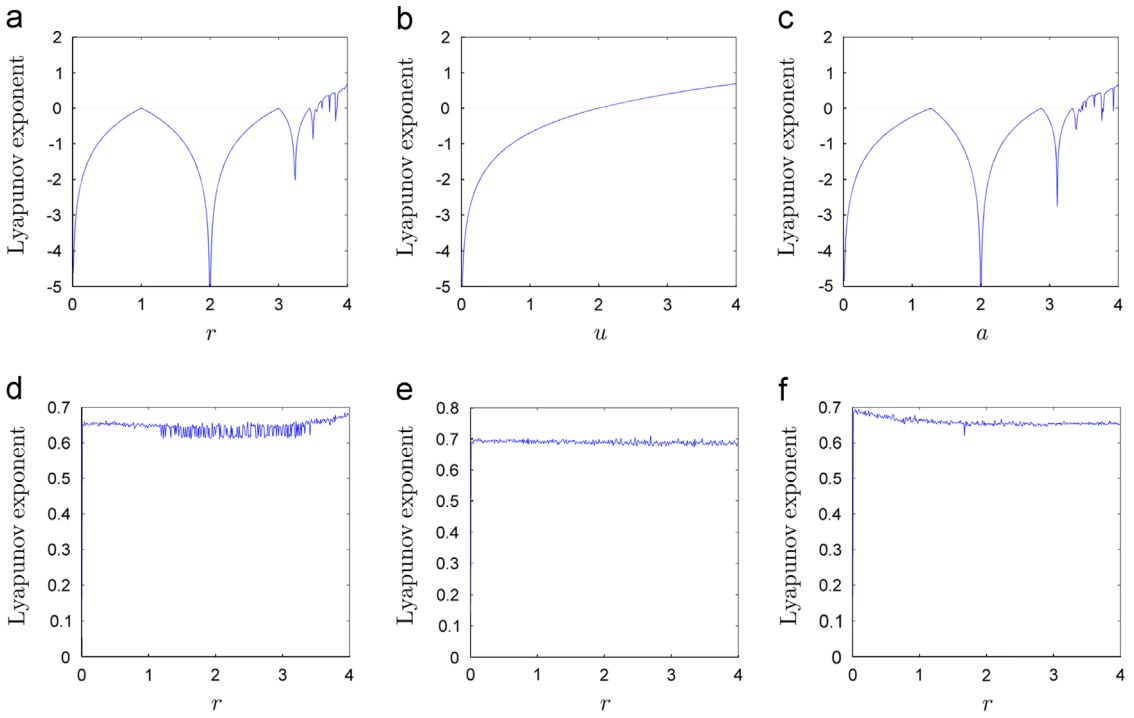

Fig. 3. The Lyapunov Exponent of the (a) Logistic map; (b) Tent map; (c) Sine map; (d) LTS; (e) LSS; and (f) TSS.

$$= \begin{cases} (rX_n/2+(4-r)\sin(\pi X_n)/4) mod\ 1 & X_i < 0.5 \\ (r(1-X_n)/2+(4-r)\sin(\pi X_n)/4) mod\ 1 & X_i \geq 0.5 \end{cases} \quad (7)$$

where parameter $r \in (0, 4]$.

As shown in Figs. 2(f) and 3(f), the TSS has excellent chaotic properties similar with the LTS and LSS.

3.2.4. Discussion

The proposed chaotic system has at least three advantages compared with its corresponding seed maps.

First, the distribution of its density function is more uniform than its corresponding seed maps. As shown in Fig. 2, all seed maps have the limited data ranges within [0, 1]. As can be seen from its three examples (LTS, LSS and TSS), the output sequences of the new chaotic system spread out in the entire data range between 0 and 1. This property ensures the proposed system well suitable for different applications such as information security.

Second, the proposed chaotic system has a wider chaotic range. Even if one seed map is out of the chaotic range, the proposed system still keeps chaotic behaviors. This can be demonstrated by the results shown in Fig. 3. The Lyapunov Exponents of three examples are greater than 0 in the entire range of the parameter settings $r \in (0, 4]$. However, their seed maps have positive values of Lyapunov Exponents only within limited ranges.

Lastly, the proposed system has better chaotic behaviors. As shown in Fig. 3, the Lyapunov Exponents of three examples are all larger than their corresponding seed maps, indicating better chaotic performance. Furthermore, the Lyapunov Exponents of the LTS, LSS, and TSS have similar distributions and are close to 0.7 in the entire parameter range $r \in [0, 4]$. This indicates that they all have the similar properties and excellent chaotic performance.

4. New image encryption algorithm

To investigate the applications of the proposed chaotic system in information security, using the LTS as its example, we introduce a new image encryption algorithm in this section.

The proposed algorithm is shown in Fig. 4. It has a 4-round-encryption structure. Each encryption round includes five steps: the random pixel insertion, row separation, 1D substitution, row combination and image rotation. The algorithm first inserts a random pixel in the beginning of each row in the original image, separates each row into a 1D data matrix, applies a substitution process to change data values in each 1D matrix, combines all 1D matrices back into a 2D data matrix according to their row positions in the original image, and then rotates the 2D matrix 90 degrees counterclockwise. Repeating these processes four times obtains the final encrypted image. An illustrative example is shown in Fig. 5. The proposed algorithm is able to transform original images randomly into different noise-like encrypted images with excellent confusion and diffusion properties.

4.1. Random pixel insertion

The random pixel insertion aims at inserting one pixel with a random value in the beginning of each row in the

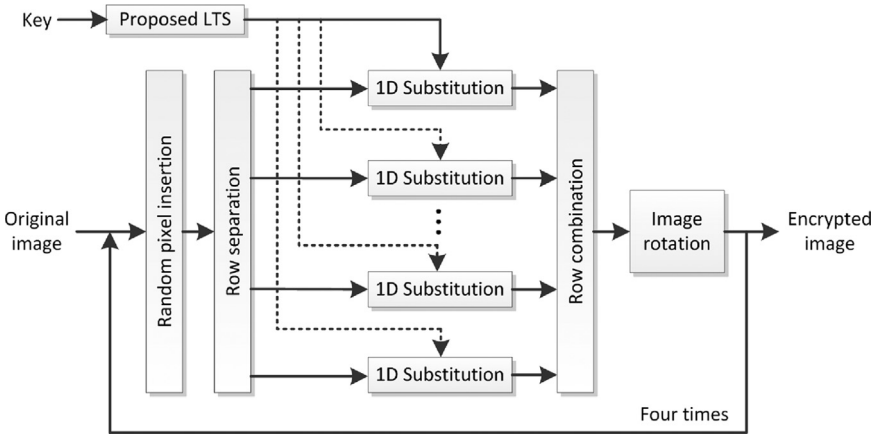

Fig. 4. The new image encryption algorithm.

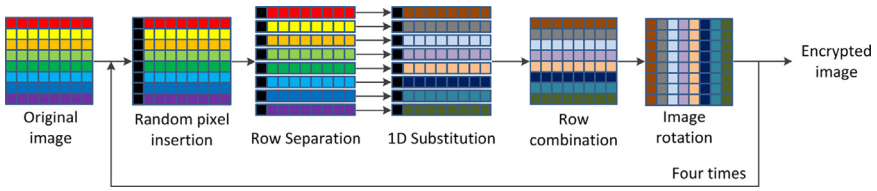

Fig. 5. An illustrative example of the proposed algorithm.

original image. It is defined by the following equation:

$$I(i,j)=\begin{cases} Rand(i) & \text{if } j=1 \\ O(i,j-1) & \text{otherwise} \end{cases} \tag{8}$$

where O is the original/input image with size of $M\times N$; $I(i,j)$ is the processed image with size of $M\times(N+1)$, $1\le i\le M$, $1\le j\le(N+1)$; $Rand(i)$ is a random function that produces random numbers.

$Rand(i)$ could use any random generator to produce random numbers which are one-time-used and unpredictable. The underlying fundamental is to generate a completely random and different image $I(i,j)$ for each encryption round. The resulting encrypted images (even in different rounds) are completely different, non-repeated and unpredictable.

4.2. Row separation

The row separation is to transfer the image $I(i,j)$ row by row into 1D matrices, as shown in the following equation:

$$R_i(j)=I(i,j) \tag{9}$$

where R_i stands for the ith1D row matrix with length of $(N+1)$.

4.3. 1D substitution

The 1D substitution process is designed to change data values in each 1D matrix R_i. It is defined by the following equation:

$$B_i(j)=\begin{cases} R_i(j) & \text{if } j=1 \\ B_i(j-1)\oplus R_i(j)\oplus(\lfloor S_k(i,j)\times 10^{10}\rfloor mod\ 256) & \text{otherwise} \end{cases}. \tag{10}$$

where $\oplus$ denotes the bit-level XOR operation, $\lfloor\cdot\rfloor$ is the floor function, and $S_k(i,j)$ is the random sequence for the kth $(k=1,2,3,4)$ encryption round, which is generated by the proposed LTS $(\mathcal{A}_{\mathcal{LT}})$ as defined by the following equation:

$$S_k(i,j)=\begin{cases} S_1(0,0) & \text{for } i=0,j=0,k=1 \\ S_2(M,0) & \text{for } i=0,j=0,k=3 \\ S_{k-1}(N,0) & \text{for } i=0,j=0,k=2,4 \\ \mathcal{A}_{\mathcal{LT}}(r_0,S_k(i-1,0)) & \text{for } i>1,j=0 \\ \mathcal{A}_{\mathcal{LT}}(r_k,S_k(i,j-1)) & \text{for } i>1,j>0 \end{cases} \tag{11}$$

where r_k and $S_k(0,0)$ are the parameter and initial value in the kth encryption round, respectively; $S_1(0,0)$, r_0 and r_k are defined by users.

4.4. Row combination

After changing data values in each row matrix in the 1D substitution process, the row combination is an inverse process of the row separation and random insertion. It combines all 1D matrices back into a 2D image matrix, and removes the first pixel in each row. The process is defined in the following equation:

$$C(i,j)=B_i(j+1) \tag{12}$$

where C is the 2D image matrix with size of $M \times N$ and $j \le N$.

4.5. Image rotation

The image rotation is to rotate the 2D image matrix 90 degrees counterclockwise defined by the following equation:

$$E(i,j) = C(j, N-i+1) \tag{13}$$

After the first encryption round, E is the feedback to the input of the random pixel insertion process. After four encryption rounds, E is the final encrypted image.

In this algorithm, security keys are composed of six portions: the LTS parameter (r_0) and initial value ($S_1(0,0)$), the LTS parameters in each encryption round (r_1, r_2, r_3, r_4) in Eq. (11).

In image decryption, the authorized users should have correct security keys and follow the inverse procedures of image encryption described in Fig. 4. The inverse 1D substitution is defined in the following equation:

$$R_i(j) = B_i(j-1) \oplus B_i(j) \oplus (\lfloor S_k(i,j) \times 10^{10} \rfloor mod\ 256) \tag{14}$$

4.6. Discussion

Following the confusion and diffusion principles, the proposed image encryption algorithm designs five above-mentioned processes. It has at least four advantages. Namely, the algorithm is able to

(1) generate a random and unpredictable encrypted image every time when it is applied to the same original image with the same set of security keys. A new encrypted image is completely different from any previous one;
(2) encrypt images with a high speed. This is because its 1D substitution process can be implemented in parallel, and it does not contain any permutation process which may require a high computation cost;
(3) encrypt images with excellent confusion and diffusion properties, achieving a high level of security; and
(4) withstand the chosen-plaintext, data loss, and noise attacks.

5. Simulation results

The proposed image encryption algorithm can provide a high level of security to different types of images, such as grayscale images, color images, biometrics, and binary images. For color images, we use the proposed algorithm to encrypt each color component individually and then combine them to obtain the encrypted color images. From the results shown in Fig. 6, all encrypted images are noise-like ones. These can prevent the original information from leakage. Because the binary image has huge data redundancy containing only two pixel values, it is often a difficult case for image encryption. As can be seen in Fig. 6(d), the proposed algorithm transfers the binary image into a noise-like encrypted image with a uniform-distributed histogram.

6. Security analysis

When a new encryption algorithm is being developed, its security should be first taken into consideration. This section analyzes the security issues of the proposed image encryption algorithm. For simplicity, all parameters and initial values in the security keys are set to 14 decimals for our simulations in this paper unless specified. However, the users are flexible to choose any other settings by considering the tradeoff between the security level and computation cost.

6.1. Security key analysis

An encryption algorithm should have a security key space large enough to withstand the brute force attack, and should be high sensitivity to any change of its security keys.

6.1.1. Security key space

As mentioned in Section 4.5, the security keys of the proposed image encryption algorithm are composed of five parameters (r_0, r_1, r_2, r_3, r_4) and the initial value ($S_1(0,0)$). Here, r_0, r_1, r_2, r_3, r_4 are in range of $[0,4]$ and $S_1(0,0) \in [0,1]$. If the length of each parameter and the initial value is set to 14 decimals, the key space of the proposed algorithm is 10^{84}. It is sufficiently large to resist the brute force attack.

6.1.2. Key sensitivity

In the key sensitivity test shown in Fig. 7, an initial key set (denoted as K_1) is $r_0 = 3.997, r_1 = 3.99, r_2 = 3.96, r_3 = 3.77, r_4 = 3.999, S_1(0,0) = 0.6$. We use K_1 to encrypt the original image in Fig. 7(a) to obtain the encrypted image (denoted as E_1) in Fig. 7(b). And then a small change is applied to $r_0 = 3.99700000000001$ while keeping others unchanged. This generates another key set denoted as K_2. Using K_2 to encrypt the same original image in Fig. 7(a) will generate another encrypted image (E_2) in Fig. 7(c). The pixel-to-pixel difference $|E_1 - E_2|$ in Fig. 7(d) proves that a tiny change (10^{-14}) in the security key will result in a significant change in the encrypted image.

In the decryption process, a small change is applied only to $r_1 = 3.99000000000001$ to obtain the third security key set denoted as K_3. We use K_1 and K_3 to reconstruct the original image from the encrypted image E_1 in Fig. 7(b), individually. The decryption results are shown in Fig. 7(e) and (f). As can be seen, using only the correct key (i.e. K_1) can completely reconstruct the original image. However, even a tiny change in the security key (i.e. K_3) will lead to the failure of image decryption as shown in Fig. 7(f). Thus, the proposed algorithm has high key sensitivity in both the encryption and decryption processes.

6.2. Statistical analysis

The main effect of this new image encryption algorithm is to transform the visually meaningful images into

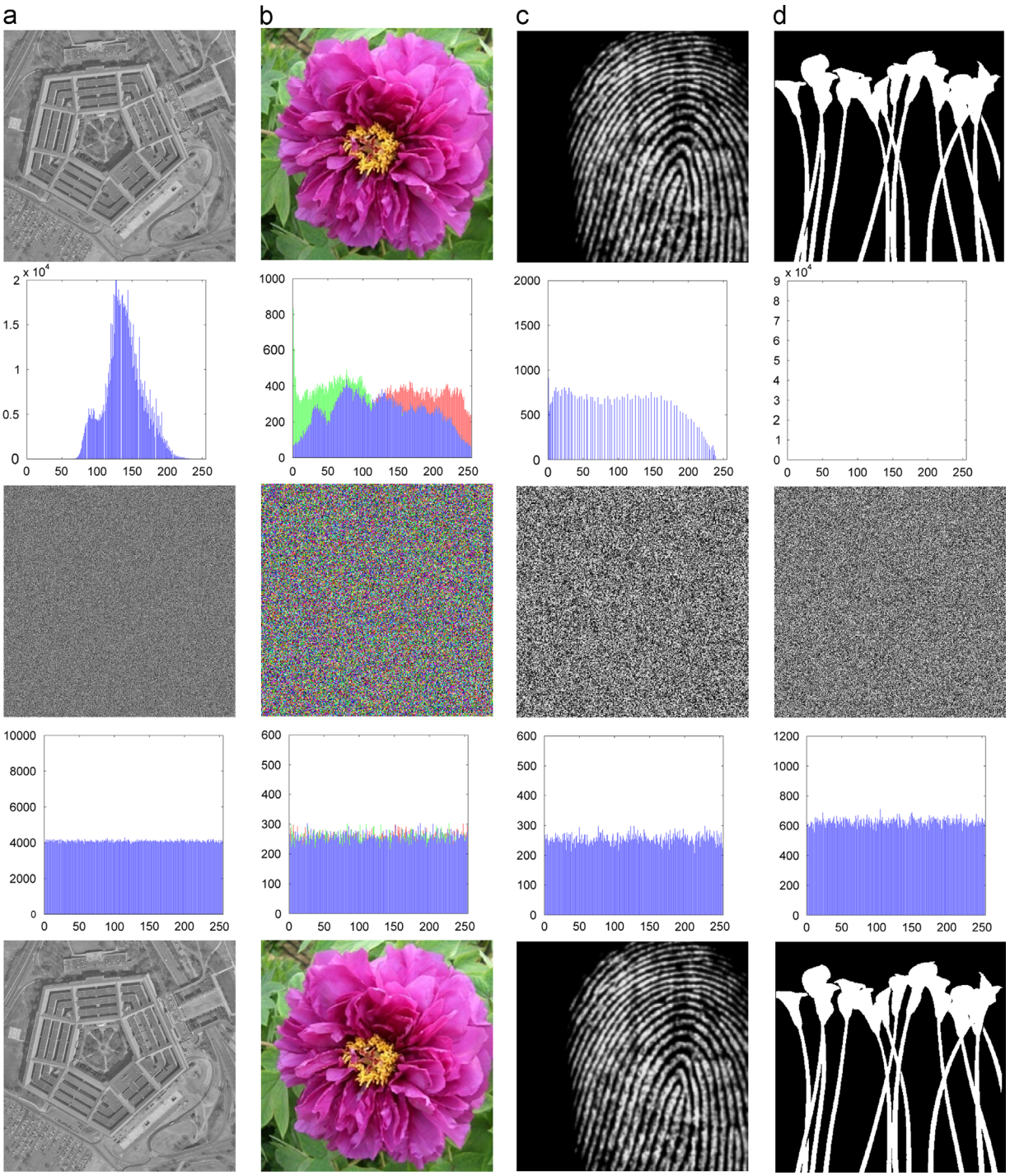

Fig. 6. The proposed algorithm encrypts different types of images. The first, third, and fifth rows show the original, encrypted, and reconstructed images, respectively; The second and forth rows show histograms of the corresponding original and encrypted images. (a) Grayscale image; (b) color image; (c) fingerprint (biometrics); and (d) binary image. (For interpretation of the references to color in this figure caption, the reader is referred to the web version of this article.)

noise-like encrypted images. There are several statistical methods for evaluating the noise-like encrypted images, including the information entropy and correlation analysis.

6.2.1. Information entropy

Information entropy (IFE) is designed to evaluate the uncertainty in a random variable as shown in the following

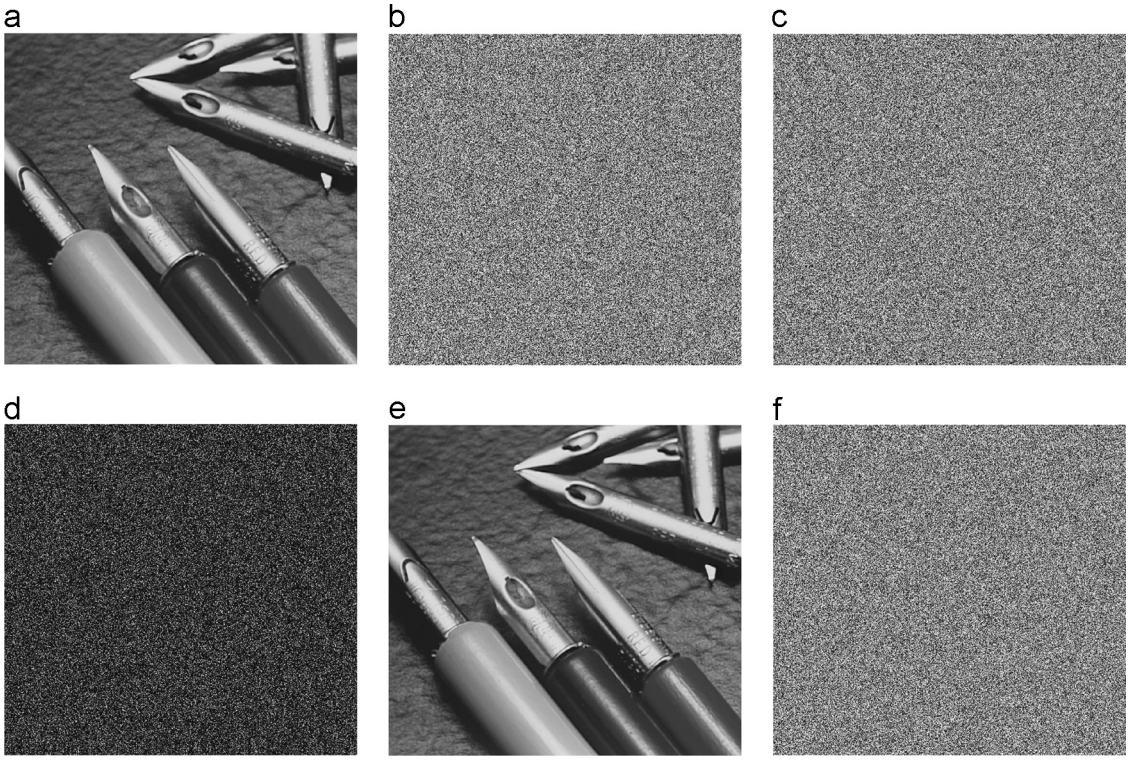

Fig. 7. The key sensitivity test for the encryption and decryption processes. (a) The original image; (b) the encrypted image E_1 with the security key set K_1; (c) the encrypted image E_2 with the security key set K_2; (d) the pixel-by-pixel difference $|E_1-E_2|$; (e) the decrypted image from E_1 using the correct security key set K_1; and (f) the decrypted image from E_1 using an incorrect security key set K_3.

equation:

$$H_L = \sum_{l=0}^{F-1} P(L=l)\log_2 \frac{1}{P(L=l)} \tag{15}$$

where F is the gray level and $P(L=l)$ is the percentage of pixels of which the value is equal to l.

The IFE can be used for evaluating the randomness of an image. An IFE score of an image close to the maximum IFE value means the excellent random property. For a grayscale image with a data range of $[0,255]$, its maximum IFE is 8. Table 1 shows the IFE scores of images before and after applying the proposed encryption algorithm. From these results, the IFE scores of all encrypted images with different sizes are close to 8. Furthermore, compared with the Liao's algorithm [11], the IFE scores of this proposed algorithm are slightly higher. This means that the encrypted images of this proposed algorithm have better random distributions.

Table 1
Information entropy analysis.

File name	Image size	Original image H_O	Encrypted image by proposed algorithm H_E^1	Encrypted image by Liao's algorithm [11] H_E^2
fingerprint.bmp	256×256	5.19634	7.99763	7.99722
fruit.png	512×512	7.45159	7.99931	7.99929
5.2.03.tiff	1024×1024	6.83033	7.99983	7.99982

6.2.2. Correlation analysis

The obvious characteristic of visually meaningful images is redundancy. There are high correlations between pixels and their neighboring pixels at horizonal, vertical and diagonal directions. The image encryption algorithm aims at breaking these pixel correlations in the original images, and transforming them into noise-like encrypted images with little or no correlations. The correlation values can be calculated by the following equation:

$$C_{xy} = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x\sigma_y} \tag{16}$$

where μ and σ are the mean value and standard deviation, respectively; $E[\cdot]$ is the expectation value.

Hence, a good encrypted image should be unrecognized and have the correlation values close to zero. Table 2 compares correlations of the original image with its encrypted versions generated by different encryption algorithms. The original image is the image shown in Fig. 6(a). As can be seen, the original image has high correlation values in all directions while all encrypted images have very low correlation values. These show their excellent performance in image encryption. Furthermore, compared to the Chen's and Liao's algorithms, the proposed

Table 2
Correlation values at the horizonal, vertical and diagonal directions.

Image	Encryption algorithm	Horizonal	Vertical	Diagonal
Original image in Fig. 6(a)		0.8652	0.8593	0.7957
Encrypted images	Chen's algorithm [39]	0.0053	−0.2088	0.0036
	Liao's algorithm [11]	-9.9847×10^{-4}	0.0018	-8.0539×10^{-4}
	Proposed algorithm	$\mathbf{-0.9750 \times 10^{-5}}$	$\mathbf{-5.7066 \times 10^{-6}}$	$\mathbf{-7.2484 \times 10^{-4}}$

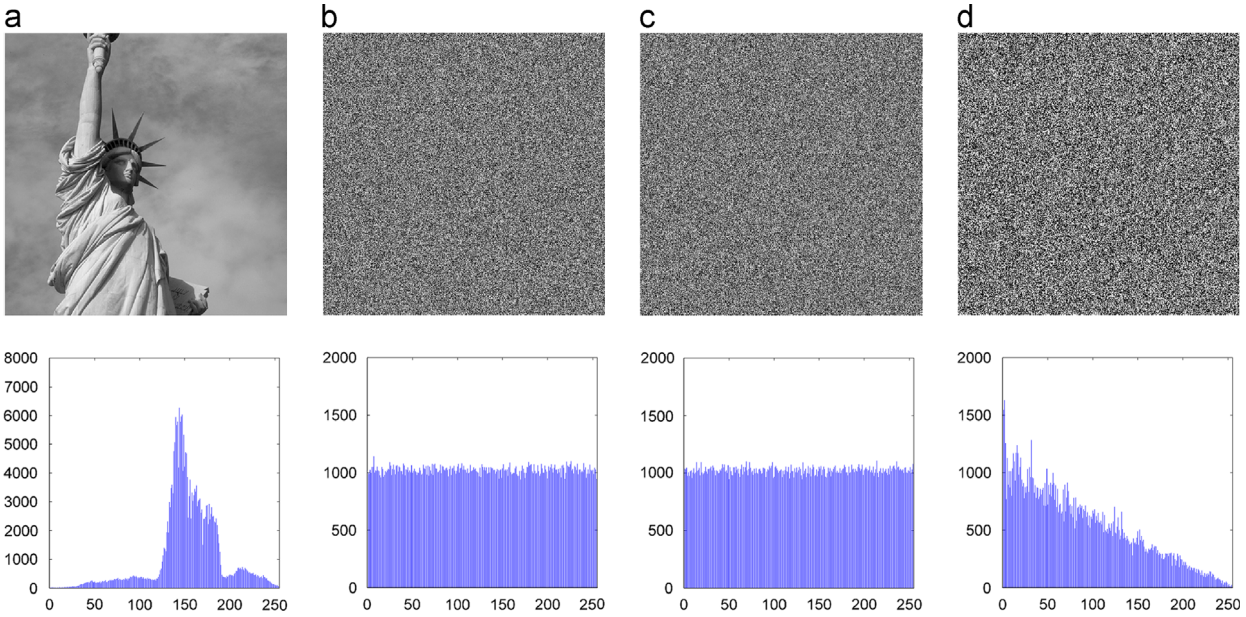

Fig. 8. The proposed algorithm encrypts an image twice using the same set of security keys. (a) The original image and its histogram; (b) the encrypted image (C_1) after the first encryption run and its histogram; (c) the encrypted image (C_2) after the second encryption run and its histogram; and (d) the pixel-to-pixel difference ($|C_1 - C_2|$) and its histogram.

algorithm obtains the smallest correlation values in all directions. It outperforms these two algorithms with respect to performance of image encryption.

6.3. Chosen-plaintext attack

An image encryption algorithm with the excellent diffusion property is able to resist the chosen-plaintext attack. However, when many existing image encryption algorithms use the same security keys to encrypt an original image, their encrypted image are duplicate. This security weakness provides the opportunity for attackers to break the encryption algorithms using the chosen-plaintext attack.

To address this problem, our proposed image encryption algorithm designs a random pixel insertion process. It allows our algorithm to generate a totally different encrypted image each time when our algorithm is applied to the same original image with the same set of security keys. This can be verified by the experiment results shown in Fig. 8. Using the same set of security keys, the proposed algorithm is applied to the original image (Fig. 8(a)) twice. Two encrypted images C_1 (Fig. 8(b)) and C_2 (Fig. 8(c)) are obtained in the first and second encryption runs, respectively. Their pixel-to-pixel difference $|C_1 - C_2|$ (Fig. 8(d)) shows that two encrypted images are completely different. Theoretically, for each set of security keys and a specific original image with size of $M \times N$, the proposed algorithm is able to generate $2^{16(M+N)}$ different encrypted images. This ensures that the proposed algorithm is able to withstand the chosen-plaintext attack.

6.4. Data loss and noise attacks

In real applications, images will inevitably experience the data loss and noise during transmission. An image encryption algorithm should resist the data loss and noise attacks.

Fig. 9 shows the simulation results of these two attacks. An image is first encrypted by our proposed algorithm. The encrypted image is applied with a data cut with size of 70×70 (Fig. 9(a)) and with 1% 'Salt & Pepper' noise (Fig. 9(b)), individually. The decryption process is then applied to these two images. As can be seen, the reconstructed images contain most of original visual information even if there are limited data losses and noise. These demonstrate the excellent performance of the proposed algorithm in against the data loss and noise attacks.

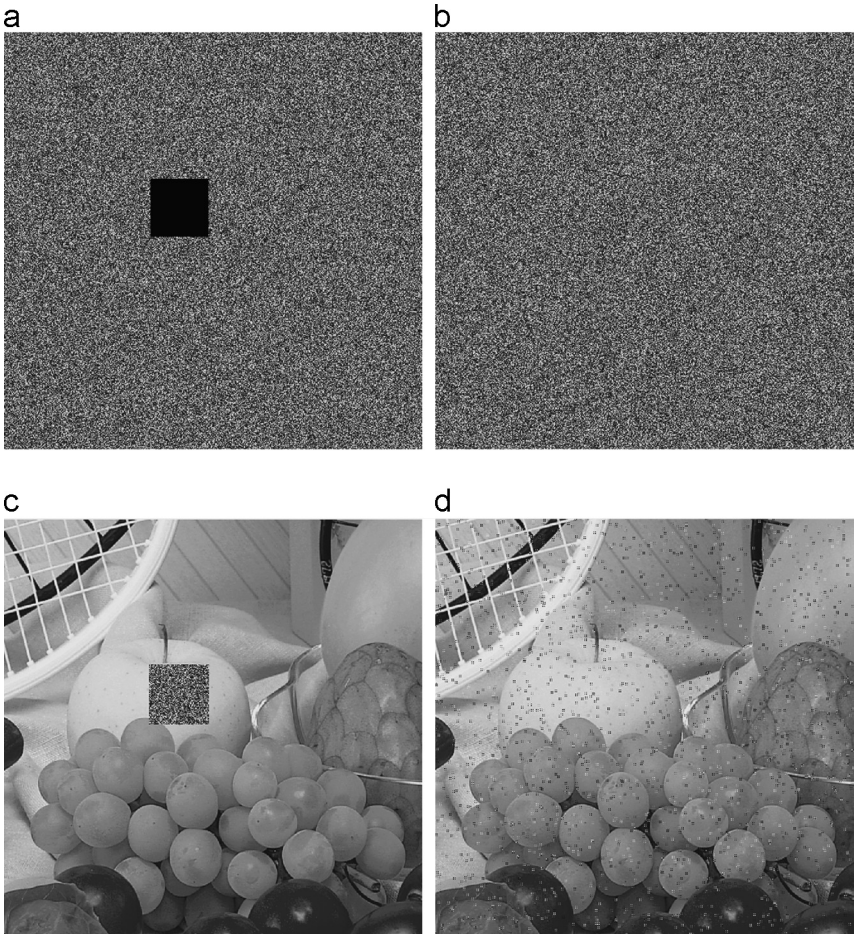

Fig. 9. Data loss and noise attacks. (a) The encrypted image with a 70×70 data loss; (b) the encrypted image added with 1% 'salt & pepper' noise; (c) the decrypted image of (a); and (d) the decrypted image of (b).

Table 3
Comparison of the encryption time of different algorithms.

File name	Image size	Proposed algorithm (s)	Liao's algorithm [11] (s)	Wu's algorithm [38] (s)
fingerprint.bmp	256×256	**0.1789**	0.5699	7.6418
fruit.png	512×512	**0.6639**	2.2516	34.7684
5.2.03.tiff	1024×1024	**3.1426**	8.9864	151.7092

6.5. Speed analysis

To analyze the computation cost of the proposed image encryption algorithm, in this section, we compare the encryption speed of the proposed algorithm to two state-of-art algorithms, the Liao's algorithm [11] and Wu's algorithm [38]. Our experiments have been conducted under MATLAB 7.1.10 (R2010a) in a computer with the Windows 7 operating system, Intel(R) Core(TM) i7-2600 CPU @ 3.40 GHz and 4 GB RAM. Table 3 shows the encryption time of three algorithms for different image sizes. As can be seen, the proposed algorithm performs faster than the two existing ones. Furthermore, the encryption speed of our algorithm can be further improved by performing the 1D substitution processes in parallel. These demonstrate that the proposed algorithm is suitable for real applications.

7. Conclusion

In this paper, we have proposed a new chaotic system. Combining existing chaotic maps, the proposed chaotic system is able to produce a large number of new chaotic maps. They all have similar properties including excellent chaotic behaviors, large chaotic range and uniform distributed density function. Three examples were introduced and discussed to demonstrate the excellent performance of the proposed chaotic system.

To investigate applications of the proposed chaotic system in multimedia security, we have introduced a new image encryption algorithm. It has been shown to have excellent diffusion and confusion properties and can resist the chosen-plaintext attack. Particularly, encrypted images of the proposed algorithm are random, non-repeated and unpredictable, even using the same set of security keys and the same original image. The algorithm can also withstand the data loss and noise attacks.

Acknowledgments

This work was supported in part by the Macau Science and Technology Development Fund under Grant 017/2012/A1 and by the Research Committee at University of Macau under Grants SRG007-FST12-ZYC, MYRG113(Y1-L3)-FST12-ZYC and MRG001/ZYC/2013/FST.

References

[1] A.A. Abd El-Latif, L. Li, N. Wang, Q. Han, X. Niu, A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, Signal Process. 93 (11) (2013) 2986–3000.
[2] C.K. Volos, I.M. Kyprianidis, I.N. Stouboulos, Image encryption process based on chaotic synchronization phenomena, Signal Process. 93 (5) (2013) 1328–1340.
[3] X. Zhang, X. Wang, Chaos-based partial encryption of SPIHT coded color images, Signal Process. 93 (9) (2013) 2422–2431.
[4] Y.-C. Hou, Z.-Y. Quan, C.-F. Tsai, A.Y. Tseng, Block-based progressive visual secret sharing, Inf. Sci. 233 (0) (2013) 290–304.
[5] R.-J. Chen, S.-J. Horng, Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata, Signal Process.: Image Commun. 25 (6) (2010) 413–426.
[6] S.S. Maniccam, N.G. Bourbakis, Image and video encryption using SCAN patterns, Pattern Recognit. 37 (4) (2004) 725–737.
[7] S.J. Shyu, Image encryption by multiple random grids, Pattern Recognit. 42 (7) (2009) 1582–1596.
[8] T.-H. Chen, K.-C. Li, Multi-image encryption by circular random grids, Inf. Sci. 189 (0) (2012) 255–265.
[9] L. Li, A.A. Abd El-Latif, X.M. Niu, Elliptic curve Elgamal based homomorphic image encryption scheme for sharing secret images, Signal Process. 92 (4) (2012) 1069–1078.
[10] Y. Zhou, K. Panetta, S. Agaian, C.L.P. Chen, (n, k, p)-gray code for image systems, IEEE Trans. Cybern. 43 (2) (2013) 515–529.
[11] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (2010) 2714–2722.
[12] T.-H. Chen, C.-S. Wu, Compression-unimpaired batch-image encryption combining vector quantization and index compression, Inf. Sci. 180 (9) (2010) 1690–1701.
[13] G. Bhatnagar, Q.M.J. Wu, B. Raman, A new fractional random wavelet transform for fingerprint security, IEEE Trans. Syst. Man Cybern. Part A: Syst. Hum. 42 (1) (2012) 262–275.
[14] G. Bhatnagar, Q.M.J. Wu, B. Raman, Discrete fractional wavelet transform and its application to multiple encryption, Inf. Sci. 223 (0) (2013) 297–316.
[15] Y. Zhou, K. Panetta, S. Agaian, C.L.P. Chen, Image encryption using P-Fibonacci transform and decomposition, Opt. Commun. 285 (5) (2012) 594–608.
[16] C.-K. Chen, C.-L. Lin, C.-T. Chiang, S.-L. Lin, Personalized information encryption using ECG signals with chaotic functions, Inf. Sci. 193 (0) (2012) 125–140.
[17] S.M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Process. 92 (2012) 1202–1215.
[18] X. Tong, M. Cui, Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator, Signal Process. 89 (2009) 480–491.
[19] Y. Zhang, D. Xiao, Y. Shu, J. Li, A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations, Signal Process.: Image Commun. 28 (3) (2013) 292–300.
[20] C.-J. Cheng, C.-B. Cheng, An asymmetric image cryptosystem based on the adaptive synchronization of an uncertain unified chaotic system and a cellular neural network, Commun. Nonlinear Sci. Numer. Simul. 18 (10) (2013) 2825–2837.
[21] L. Bao, Y. Zhou, C.L.P. Chen, H. Liu, A new chaotic system for image encryption, in: 2012 International Conference on System Science and Engineering (ICSSE), 2012, pp. 69–73.
[22] G.A. Sathishkumar, K. Bhoopathy bagan, N. Sriraam, Image encryption based on diffusion and multiple chaotic maps, International Journal of Network Security & Its Applications, 3 (2) (2011) 181–194.
[23] A. El-Latif, L. Li, N. Wang, X. Niu, Image encryption scheme of pixel bit based on combination of chaotic systems, in: 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011, pp. 369–373.
[24] A. Kanso, M. Ghebleh, A novel image encryption algorithm based on a 3D chaotic map, Commun. Nonlinear Sci. Numer. Simul. 17 (7) (2012) 2943–2959.
[25] S.-J. Xu, X.-B. Chen, R. Zhang, Y.-X. Yang, Y.-C. Guo, An improved chaotic cryptosystem based on circular bit shift and XOR operations, Phys. Lett. A 376 (10–11) (2012) 1003–1010.
[26] S. Behnia, A. Akhshani, H. Mahmodi, A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps, Chaos Solitons Fractals 35 (2) (2008) 408–419.
[27] G. Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognit. Lett. 31 (5) (2010) 347–354.
[28] X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, Signal Process. 92 (2012) 1101–1108.
[29] Z.-L. Zhu, W. Zhang, K.-W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Inf. Sci. 181 (6) (2011) 1171–1186.
[30] G. Bhatnagar, Q.M. Jonathan Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digit. Signal Process. 22 (4) (2012) 648–663.
[31] V. Patidar, N. Pareek, K. Sud, A new substitution–diffusion based image cipher using chaotic standard and Logistic maps, Commun. Nonlinear Sci. Numer. Simul. 14 (7) (2009) 3056–3075.
[32] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, G. Chen, On the security defects of an image encryption scheme, Image Vis. Comput. 27 (9) (2009) 1371–1381.
[33] D. Arroyo, J. Diaz, F.B. Rodriguez, Cryptanalysis of a one round chaos-based substitution permutation network, Signal Process. 93 (5) (2013) 1358–1364.
[34] M.I. Sobhy, A.E.R. Shehata, Methods of attacking chaotic encryption and countermeasures, in: Proceedings of 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '01), 2001, pp. 1001–1004.
[35] R. Rhouma, S. Belghith, Cryptanalysis of a new image encryption algorithm based on hyper-chaos, Phys. Lett. A 372 (38) (2008) 5973–5978.
[36] X. Ge, F. Liu, B. Lu, W. Wang, Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem and its improved version, Phys. Lett. A 375 (5) (2011) 908–913.
[37] C. Li, S. Li, G. Chen, W.A. Halang, Cryptanalysis of an image encryption scheme based on a compound chaotic sequence, Image Vis. Comput. 27 (8) (2009) 1035–1039.
[38] Y. Wu, G. Yang, H. Jin, J.P. Noonan, Image encryption using the two-dimensional Logistic chaotic map, J. Electron. Imaging 21 (1) (2012). 013014-1.
[39] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solitons Fractals 21 (3) (2004) 749–761.