Hindawi
Security and Communication Networks
Volume 2018, Article ID 8402578, 11 pages
https://doi.org/10.1155/2018/8402578

Research Article

An Effective Framework for Chaotic Image Encryption Based on 3D Logistic Map

Guodong Ye, Kaixin Jiao, Chen Pan, and Xiaoling Huang

Faculty of Mathematics and Computer Science, Guangdong Ocean University, Zhanjiang 524088, China

Correspondence should be addressed to Guodong Ye; guodongye@hotmail.com

Received 6 May 2018; Accepted 8 October 2018; Published 21 October 2018

Academic Editor: Angelos Antonopoulos

In this paper, an effective framework for chaotic encryption based on a three-dimensional logistic map is presented together with secure hash algorithm-3 (SHA-3) and electrocardiograph (ECG) signal. Following the analysis of the drawbacks, namely, fixed key and low sensitivity, of some current algorithms, this work tries to solve these two problems and includes two contributions: (1) removal of the phenomenon of summation invariance in a plain-image, for which SHA-3 is proposed to calculate the hash value for the plain-image, with the results being employed to influence the initial keys for chaotic map; (2) resolution of the problem of fixed key by using an ECG signal, that can be different for different subjects or different for same subject at different times. The Wolf algorithm is employed to produce all the control parameters and initial keys in the proposed encryption method. It is believed that combining with the classical architecture of permutation-diffusion, the summation invariance in the plain-image and shortcoming of a fixed key will be avoided in our algorithm. Furthermore, the experimental results and security analysis show that the proposed encryption algorithm can achieve confidentiality.

1. Introduction

In recent years, there has been a rapid development of multimedia including video, images, and audio. Computer science and network technology also promote the wide use of digital information. Among these categories of multimedia, images as an effective way to understand the colors play an important role in our daily life. However, because of illegal wiretapping, revision, or interception, there is an apparent lack of security for communicating images over the network, particularly some private images such as medical and military image. Structurally, cryptography is categorized into two classes [1, 2], namely, symmetric cryptography and asymmetric cryptography. It has supplied numerous effective ciphers for user information, particularly in the form of textual content. Owing to less computation requirement and high efficiency, we prefer symmetric cryptosystems in coding.

An image has some inherent characteristics and is different from textual content, for example, enormous data, high correlation, long redundancy, and bulk data capacity. Therefore, traditional methods such as advanced encryption standard (AES), data encryption standard (DES), or international data encryption algorithm (IDEA) are not effective options for image encryption [3, 4]. Chaos-based methods have recently become attractive for protecting image content. We can employ their superior properties such as control parameter, sensitivity to the initial condition, and nonconvergence in a chaotic system (or map). Numerous image encryption algorithms using chaos have been proposed [5–7], and their efficiency has been partially exhibited. Normally, two processes are adopted by the current image encryption algorithms: pixel permutation and pixel diffusion. First, to reduce the high correlation existing between adjacent pixels, permutation to the pixel positions is considered, for example, Arnold map transformation [8, 9]. However, the exchange of pixel positions alone cannot ensure security because of the nonvariance of the gray distribution in a plain-image. Thus, pixel diffusion is performed as a second step to reformulate the statistical distribution for pixels. It is more important to make a minor change in the plain-image such that it results in an entirely different cipher-image, i.e., realizing an avalanche effect. Compressive sensing was also introduced into the encryption process, and it exhibits a good effect [10].

As early as 1989, Matthews [11] proved that a chaotic sequence of random numbers can be obtained from a simple nonlinear iterative function and applied it for cryptographic use. In [12], the authors presented a symmetrical image encryption algorithm using a one-dimensional (1D) skew tent map, in which a bit-level permutation for pixels was employed. Instead of byte-permutation, a structure of diffusion layer followed by a bit-permutation layer was proposed by El Assad and Farajallah [13]. Although bit-level permutation operation can introduce double diffusion effects, it also leads to a longer time consumption. Logistic map is simple and widely used in performing image encryption with less computation [14]. However, it was shown to have some drawbacks such as a small key and weak security. To overcome these disadvantages of logistic map, Wang and Luan [15] proposed a three dimensional (3D) coupled logistic map. Additionally, various new and improved encryption schemes for images have been reported [16–18], which drives the development of chaos-based encryption methods. Chai et al. [19] proposed a new encryption scheme to resist common attacks using DNA sequence. This scheme is very sensitive to the plain-image after applying secure hash algorithm- (SHA-) 256. However, the time cost will be high because of the exchange between the decimal and binary systems. The same problem can be seen in DNA-based method [20]. In [21], a new hyper-chaos based algorithm has been proposed for image encryption. It computed a larger Lyapunov exponent in the new chaotic system. However, it did not consider the summation invariance in the plain-image. A plaintext-related image encryption system was designed in [22], which also employed a hyper-chaotic system to generate a random sequence. Although this system exhibits a good performance, it only uses fixed secret keys.

Unfavorably, various image encryption algorithms provide a low security. For example, Fu et al. [23] proposed a bit-level permutation scheme to encrypt an image, in which the diffusion effect can be achieved by a two-stage process of bit-level shuffling function using an Arnold map and chaotic sequences. Compared with some other image encryption algorithms with a permutation-diffusion structure, the algorithm has less computational complexity. However, Jolfaei et al. [24] pointed out that a permutation-only scheme for image encryption can be broken if a chosen-plaintext attack is applied. For a plain-image of size $m \times n$, the number of plain-images required to be chosen is $\log_L(mn)$ (where L is the number of different color intensities). One cycle of permutation-diffusion architecture was suggested in [25] for image encryption; the row and column permutations were used in the first stage, and an affine cipher was applied to modify the gray values in the diffusion stage. However, by a strategy of divide-and-conquer [26], a chosen-plaintext can efficiently attack this algorithm having a complex linear relation. In addition, there are numerous other cryptanalysis methods [27–30].

After conducting a detail analysis of the breaking methods, it can be concluded that the drawbacks of the image encryption algorithms are follows: (1) permutation-only structure, (2) diffusion-only structure, (3) one cycle of permutation-diffusion architecture, (4) key-dependence, and (5) fixed keys. To overcome these limitations, a new image encryption model employing both electrocardiograph (ECG) signals and SHA-3 is proposed in this paper. In this model, an ECG signal is used as the initial condition for the chaotic map to handle the fixed key problem. Next, the hash values are extracted from a plain-image by the SHA-3 function and are employed to update the initial keys, which can avoid key-dependence problem. Similar to the entire algorithm, more than one cycle of the permutation-diffusion operation is considered before obtaining the final cipher-image. Moreover, compared with some recent references, the proposed method has numerous advantages. For example, in reference [3], an image encryption algorithm based on a two-dimensional (2D) chaotic map is presented. However, the keystream used in the encryption process is not related to the plain-image. Thus, secret keys x and y are fixed without considering the different plain-images. A hyperchaotic Rössler map was employed in [31] to design a confusion-permutation-based image encryption algorithm, in which $x_1(0)$, $x_2(0)$, and $x_3(0)$ are the keys. However, keystreams S_{ren}, S_{col} (for permutation), and M_{cc} (for diffusion) are the same for any plain-image of the same size. A new encryption method with a confusion-diffusion structure for the confidentiality and privacy of clinical information has been proposed by [32]. A 1D logistic map was used to generate the chaotic sequence. However, it suffers from numerous shortcomings, for example, small secret key space, nonuniform chaotic data distribution, and discontinuous chaotic ranges. Furthermore, sequences P and D used in [32] are also fixed for different ECG signals (original message) of the same length. In [33], a 3D chaotic system was adopted to generate random numbers. However, x and z for the S-box generation algorithm and y for the bit exclusive OR (XOR) are obtained only from the fixed keys. A plain-image-based keystream generation was proposed in [34], in which pixel summation $AK_{R,G,B}$ for the pixels were computed to affect the secret keys. However, if we modify two pixels with same summation for the plain-image, then the keystream will also be the same. Thus, this scheme suffers from summation invariance. To solve the problems of fixed keys and summation invariance, a new image encryption algorithm is designed in this study.

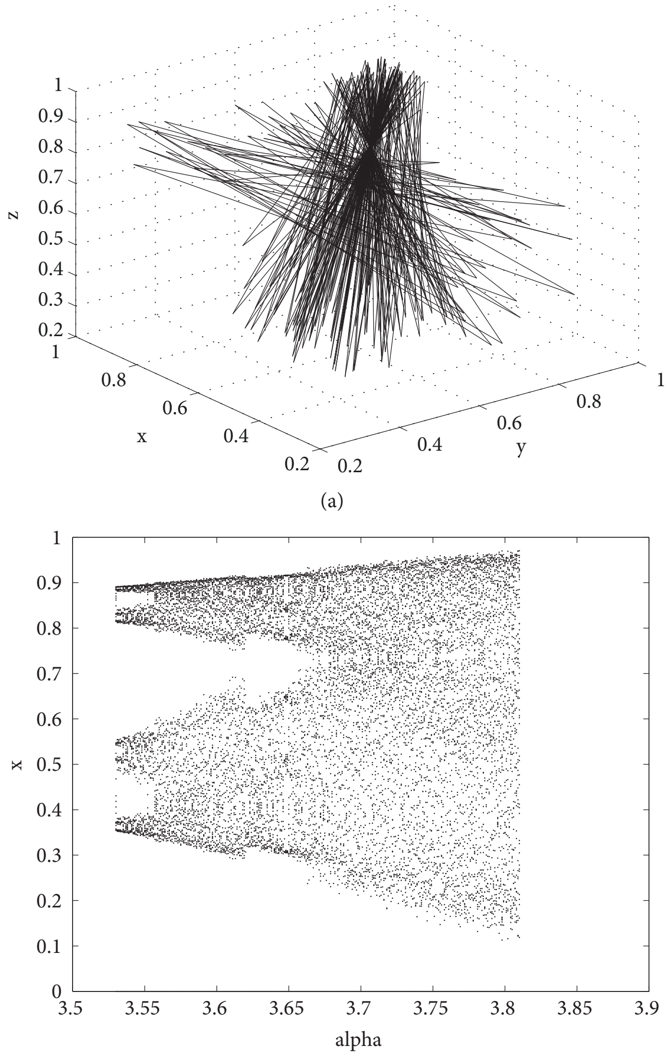
The remainder of this paper is organized as follows. Section 2 describes in detail the proposed image encryption algorithm. The simulation results are presented in Section 3 together with the security analysis. Finally, some conclusions are drawn in Section 4.

2. Proposed Image Encryption Algorithm

2.1. 3D Logistic Map and SHA-3. Recently, a 3D logistic map [35] with a better chaotic property than a 1D logistic map was studied. It can be defined by the following equation (1):

$$\begin{aligned} x_{i+1} &= \alpha x_i\left(1 - x_i\right) + \beta y_i^2 x_i + \gamma z_i^3 \\ y_{i+1} &= \alpha y_i\left(1 - y_i\right) + \beta z_i^2 y_i + \gamma x_i^3 \\ z_{i+1} &= \alpha z_i\left(1 - z_i\right) + \beta x_i^2 z_i + \gamma y_i^3 \end{aligned} \tag{1}$$

When $0.35 < \alpha < 3.81$, $0 < \beta < 0.022$, and $0 < \gamma < 0.015$ are set, the 3D logistic map (1) exhibits a chaotic behavior if



(a)

(b)

Figure 1: Chaos test: (a) chaotic behavior; (b) bifurcation diagram for x.

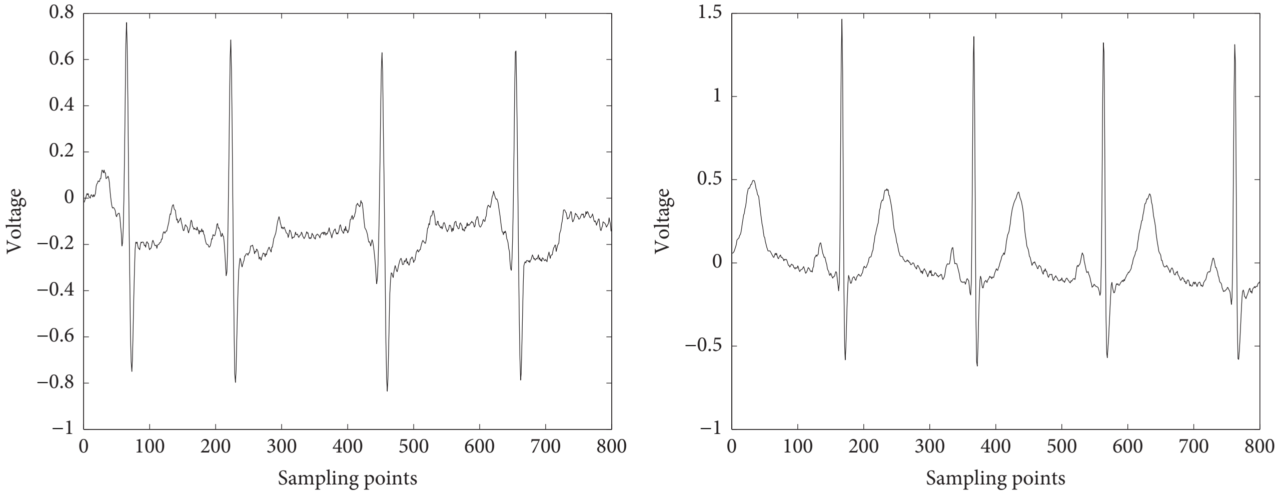
$x_i, y_i, z_i \in (0, 1)$. Figure 1(a) shows the chaos phenomena of the 3D logistic map (initial 20 iterated values are discarded) using the initial conditions: $\alpha = 3.6324$, $\beta = 0.0193$, $\gamma = 0.0146$, $x_0 = 0.4212$, $y_0 = 0.1436$, and $z_0 = 0.7108$. Figure 1(b) displays the bifurcation diagram for x. Moreover, the Kolmogorov entropy is used to prove the chaos, for example, if α=3.6324, β=0.0193, and $0 < \gamma < 0.015$, then the Kolmogorov entropy is 0.4230, indicating the chaos behavior of the 3D logistic map.

SHA-3, designed by Bertoni, Daemen, Peeters, and Asschewest [36], is the newest hash function announced by the national institute of standards and technology (NIST), and it is highly sensitive to the input message and can perform quasi all symmetric cryptographic functions [36]. To solve the summation invariance in the plain-image and the problem of fixed keys, SHA-3 is used to compute the hash values of the plain-image. Here, the length of the output is set as 256 bits that are converted into 32 integer numbers (arranged into a vector h). Currently, the code package of SHA-3 algorithm has been made available to all the users.

2.2. Generation of Initial Conditions. To solve the shortcoming of fixed keys, the secret keys will not be assigned ahead by the sender and receiver in our algorithm. It is known that different persons have different ECG signals, and they can even be different for the same person at different times. For example, Figure 2 shows two different ECG signals (all the ECG signals used in this study are chosen from [37]). The complexity of the biology of the human body makes it difficult to simulate or produce an ECG signal for any subject. Here, the Wolf algorithm [38] is employed to extract the property of an ECG signal, noted as $\lambda \in [-1, 1]$. Subsequently, λ is decomposed into several decimal numbers treated as the control parameters and initial conditions for the 3D logistic map through the following equation:

$$\alpha = 3.6 + \frac{\lambda}{100}$$

$$\beta = \left| \frac{\lambda}{100} \times 2 \right|$$



(a)

(b)

Figure 2: ECG signals for (a) first person and (b) second person.

$$
\begin{aligned}
\gamma &= \left|\frac{\lambda}{100} + 0.004\right| \\
x_0 &= \frac{\lambda+1}{2} \times 10 - \left\lceil \frac{\lambda+1}{2} \times 10 \right\rceil \\
y_0 &= \frac{\lambda+1}{2} \times 100 - \left\lceil \frac{\lambda+1}{2} \times 100 \right\rceil \\
z_0 &= \frac{\lambda+1}{2} \times 1000 - \left\lceil \frac{\lambda+1}{2} \times 1000 \right\rceil
\end{aligned} \tag{2}
$$

where $|a|$ represents the absolute value of a, whereas $\lceil a \rceil$ rounds-off the element of a to the nearest integer toward negative infinity.

2.3. Encryption Process. One cycle of permutation-only, diffusion-only, or permutation-diffusion has been found to be insecure for image encryption. Therefore, to enhance the security with the proposed algorithm, three rounds of permutation-diffusion are employed in our new method. It is supposed that the plain-image is P with size $m \times n$, and the cipher-image is denoted as C.

2.3.1. Permutation Operation. There is a natural strong correlation between adjacent pixels in a relevant plain-image, and a good encryption scheme should have the ability to decrease this correlation and obscure the pixel positions. Given a ECG signal, we can extract its property λ and then generate the initial conditions $\alpha, \beta, \gamma, x_0, y_0$, and z_0 for the 3D logistic map. To relate the keystream to the plain-image, SHA-3 is firstly applied to the plain-image P and we obtain hash vector h that is divided into three factors by the following equation:

$$
\begin{aligned}
h_x &= \frac{\sum_{i=1}^{10} h_i}{10 \times 255} \\
h_y &= \frac{\sum_{i=11}^{20} h_i}{10 \times 255} \\
h_z &= \frac{\sum_{i=21}^{32} h_i}{12 \times 255}
\end{aligned} \tag{3}
$$

Subsequently, initial conditions x_0, y_0, and z_0 are updated by (4) and form new $\overline{x}_0$, $\overline{y}_0$, and $\overline{z}_0$. If the 3D logistic map is iterated a few times by the updated keys, chaotic sequences $\{\overline{x}_i\}$, $\{\overline{y}_i\}$, $\{\overline{z}_i\}$ can be obtained. To increase the randomness degree, the initial iterated values should be discarded. Suppose three vectors $\overline{X}, \overline{Y}$, and $\overline{Z}$ with length $\max\{m, n\}+200$ are produced (here, 200 is a random constant number considered as a control parameter). All the decimal numbers within $\overline{X}$, $\overline{Y}$, and $\overline{Z}$ are transferred using (5), and the summation is calculated for $\overline{Z}$ Factor $\tau = \sum \overline{Z} \bmod 200$ is obtained and is employed to select m numbers from $\overline{X}$ and n numbers from $\overline{Y}$. Assume that vectors $H = \{\overline{X}_{\tau+1}, \overline{X}_{\tau+2}, \ldots, \overline{X}_{\tau+m}\}$ and $L = \{\overline{Y}_{\tau+1}, \overline{Y}_{\tau+2}, \ldots, \overline{Y}_{\tau+n}\}$ are generated and then used to perform a circular permutation for the plain-image P along the row and column, respectively. After completing the permutation operation, permuted image A can be obtained.

$$
\begin{aligned}
\overline{x}_0 &= x_0 + h_x \mod 1 \\
\overline{y}_0 &= y_0 + h_y \mod 1 \\
\overline{z}_0 &= z_0 + h_z \mod 1
\end{aligned} \tag{4}
$$

$$
\begin{aligned}
\overline{X} &= \left\lceil \overline{X} \times 10^{14} \right\rceil \mod n \\
\overline{Y} &= \left\lceil \overline{Y} \times 10^{14} \right\rceil \mod m \\
\overline{Z} &= \left\lceil \overline{Z} \times 10^{14} \right\rceil \mod 256
\end{aligned} \tag{5}
$$

2.3.2. Diffusion Operation. We know that a permutation-only scheme is insecure for any image encryption algorithm owing to the invariance of the statistical property; it only shuffles the pixel positions. Therefore, to ensure the security, a diffusion operation for the above permuted image, A, is further considered in our method. By iterating the 3D Logistic map using the initial conditions x_0, y_0, and z_0, vector S is obtained containing all the elements x_i, y_i, and z_i. Subsequently, it is arranged into matrix D having the same size as the plain-image. Before being used in the diffusion

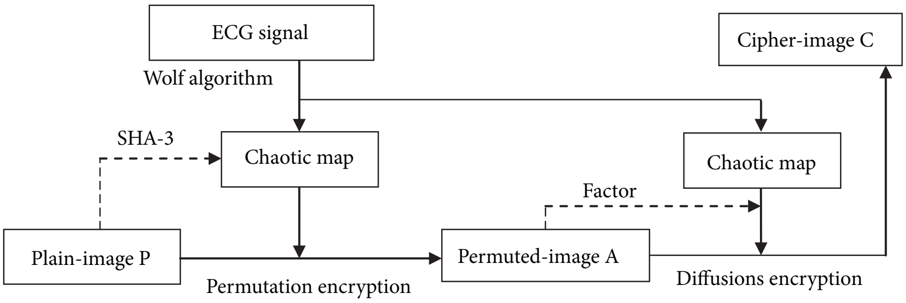


Figure 3: Flowchart of the proposed image encryption algorithm.

operation, all the elements in D should be transformed into integer numbers between 0 and 255 through (6) to satisfy the pixel interval.

$$D_{i,j} = \left\lceil D_{i,j} \times 10^{14} \right\rceil \bmod 256, \quad i = 1, 2, \ldots, m; \; j = 1, 2, \ldots, n. \tag{6}$$

For the keystream to be dependent on the permuted image, factor ρ is introduced in the function of the diffusion operation. Equation (7) applies the diffusion in the row direction. Here, a natural row is treated as a unit.

$$\begin{aligned} \rho &= \sum A_{i+1} \quad \bmod 256 \\ B_i &= A_i + \rho + D_i \quad \bmod 256, \; i = 1, 2, \ldots, m, \end{aligned} \tag{7}$$

where A_i represents the ith row of image A. A_{m+1} is a constant vector. Similarly, the diffusion operation along the column direction can be processed for image B. Finally, cipher-image C is obtained after both permutation and diffusion are completed.

2.3.3. Encryption Steps. For the entire permutation-diffusion structure (see the flowchart in Figure 3), our image encryption algorithm can be described by the following steps.

Step 1. Read the plain-image as matrix P and obtain its size $m \times n$.

Step 2. Use the Wolf algorithm to produce initial conditions x_0, y_0, and z_0 and the three control parameters for the 3D logistic map from the ECG signal.

Step 3. Calculate the hash values for the plain-image using SHA-3 and convert them into hash vector h.

Step 4. Generate factors h_x, h_y, and h_z and update initial conditions x_0, y_0, and z_0 to obtain new $\overline{x}_0$, $\overline{y}_0$, and $\overline{z}_0$.

Step 5. Iterate the 3D logistic map with new $\overline{x}_0$, $\overline{y}_0$, and $\overline{z}_0$ and obtain vectors H and L.

Step 6. Perform the circular permutation operation for plain-image P and obtain permuted image A.

Step 7. Iterate the 3D logistic map by x_0, y_0, and z_0 and obtain matrix D.

Step 8. Compute factor ρ for each row and column before the diffusion operation.

Step 9. Perform the diffusion operation for permuted image A using D along the row and column.

Step 10. Obtain cipher-image C.

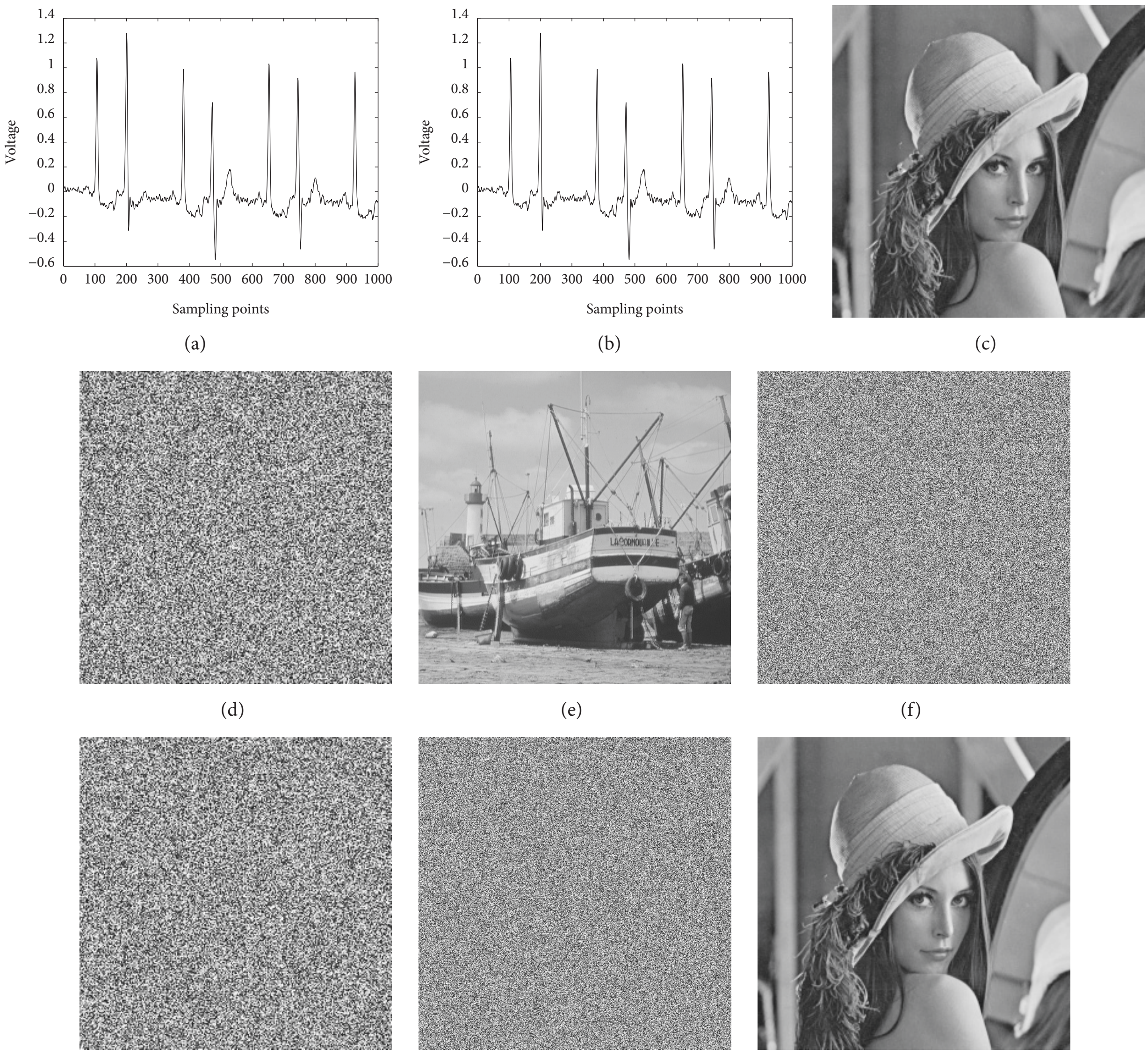
In view of the symmetric structure, the decryption steps for our encryption algorithm are the same but in an inverse order.

3. Simulations and Security Analysis

For the simulations discussed in this section, plain-images Lena and Boat are randomly chosen for the tests. Some common security analyses are also used to evaluate the security of the proposed algorithm.

3.1. Simulations. Using a computer equipped by a platform of Windows 7 with Intel(R) Core(TM) i3-2350, 2.30 GHz CPU, all the simulations are performed by the software Matlab R2011b. Figures 4(a) and 4(b) show the ECG signals of the same person but with one sample shifting. By considering the ECG signal in Figure 4(a) as the initial condition for the 3D Logistic map, Figure 4(d) shows the cipher-image generated corresponding to plain-image Lena in Figure 4(c), whereas the cipher-image for plain-image Boat in Figure 4(e) is displayed in Figure 4(f) after using our new method. The computational time cost for a plain-image of size 256×256 is 0.1227s on an average.

3.2. Key Space and Its Sensitivity. Normally the key space should be kept as large as 10^{30} to resist brute-force attack [39]. In our algorithm, the ECG signals from 1000 samples are taken to generate the initial conditions for the 3D logistic map by the Wolf algorithm. Therefore, the data is sufficiently large to avoid key analysis. Moreover, if there is one sample shifting in the ECG signal, then the correct plain-image cannot be obtained. For example, Figure 4(g) shows the wrong decrypted image for Figure 4(d), whereas Figure 4(h) displays the decryption result for Figure 4(f). Figure 4(i)



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 4: Simulation: (a) ECG signal, (b) ECG signal with one sample shifting, (c) plain-image of Lena, (d) cipher-image of Lena, (e) plain-image of Boat, (f) cipher-image of Boat, (g) wrong depiction of Lena, (h) wrong depiction of Boat, and (i) correct recovery for Lena.

displays the correct decryption for the Lena image under the condition of using the same ECG signal. Therefore, the proposed algorithm is highly sensitive to the keys.

3.3. Sensitivity of the Plain-Image. Any minor change in a plain-image should lead to a significant difference in the cipher-image to satisfy an ideal encryption algorithm. For the plain-image Lena, Figure 5(a) shows the cipher-image when there is a one-bit change in the plain-image, whereas Figure 5(b) depicts the difference before and after the one-bit change. Similarly, Figures 5(c) and 5(d) display the case for the Boat image. To numerically evaluate the sensitivity of the plain-image, the unified averaged changed intensity (*UACI*) and number of changing pixel rate (*NPCR*) [40, 41] defined by (8) and (9) are usually considered in a cipher design. Various plain-images are randomly chosen to measure the sensitivity and the results are presented in Table 1. It can be seen that the values are approximately 33.4% and 99.6% [42]; i.e., the proposed method has a high sensitivity for the plain-image.

$$UACI = \frac{1}{m \times n}\left[\sum_{i,j}\frac{\left|C_1(i,j) - C_2(i,j)\right|}{255}\right] \times 100\% \quad (8)$$

$$NPCR = \frac{\sum_{ij} D(i,j)}{m \times n} \times 100\% \quad (9)$$

3.4. Histogram Analysis. A statistical attack is a common analysis approach employed by cryptanalysts. If a designed encryption algorithm can generate a uniform distribution

Table 1: *UACI* and *NPCR* tests.

Images	Lena	Boat	Baboon	Peppers
UACI	33.3961	33.4685	33.5116	33.4245
NPCR	99.6277	99.6059	99.6315	99.5934

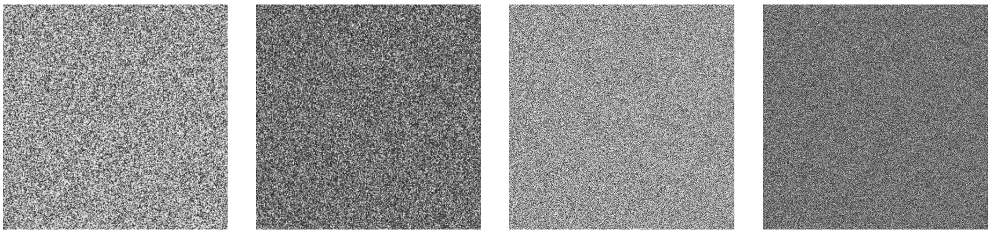
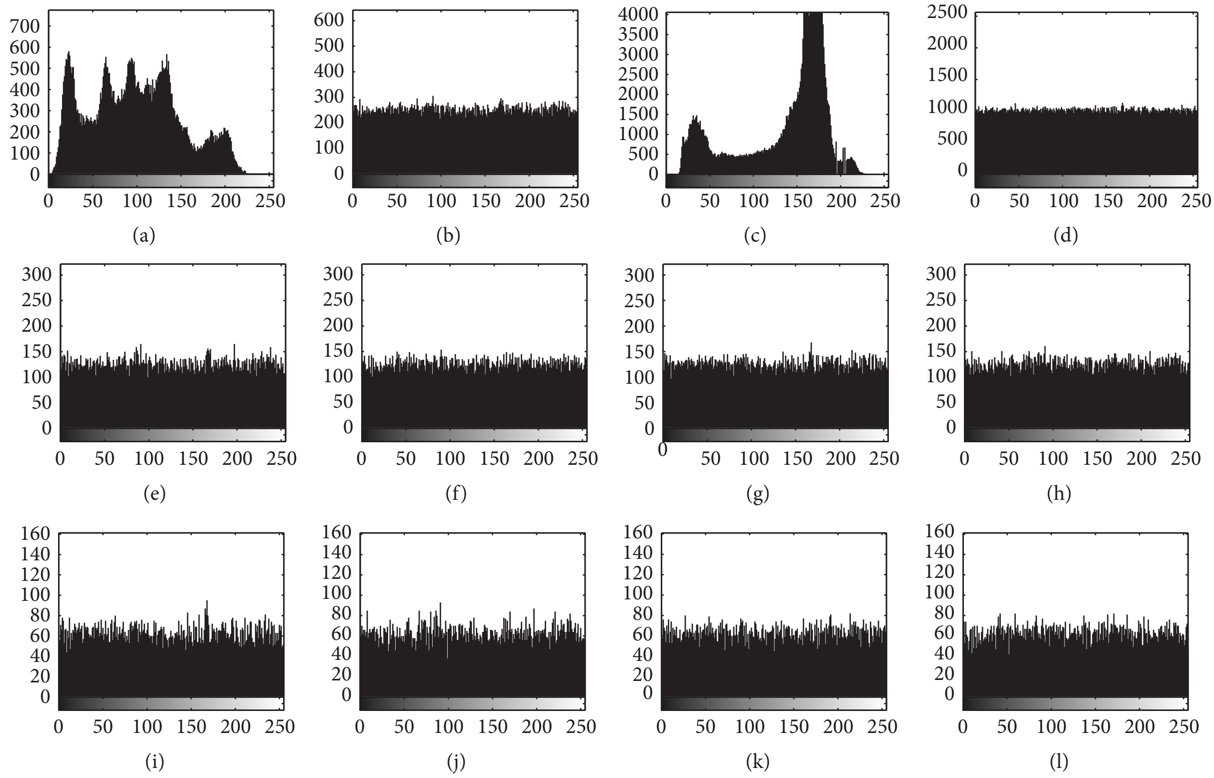

(a) (b) (c) (d)

Figure 5: Sensitivity tests: (a) cipher-image of Lena with one-bit change in the plain-image, (b) difference before and after one-bit change for Lena, (c) cipher-image of Boat with one-bit change in the plain-image, and (d) difference before and after one-bit change for Boat.

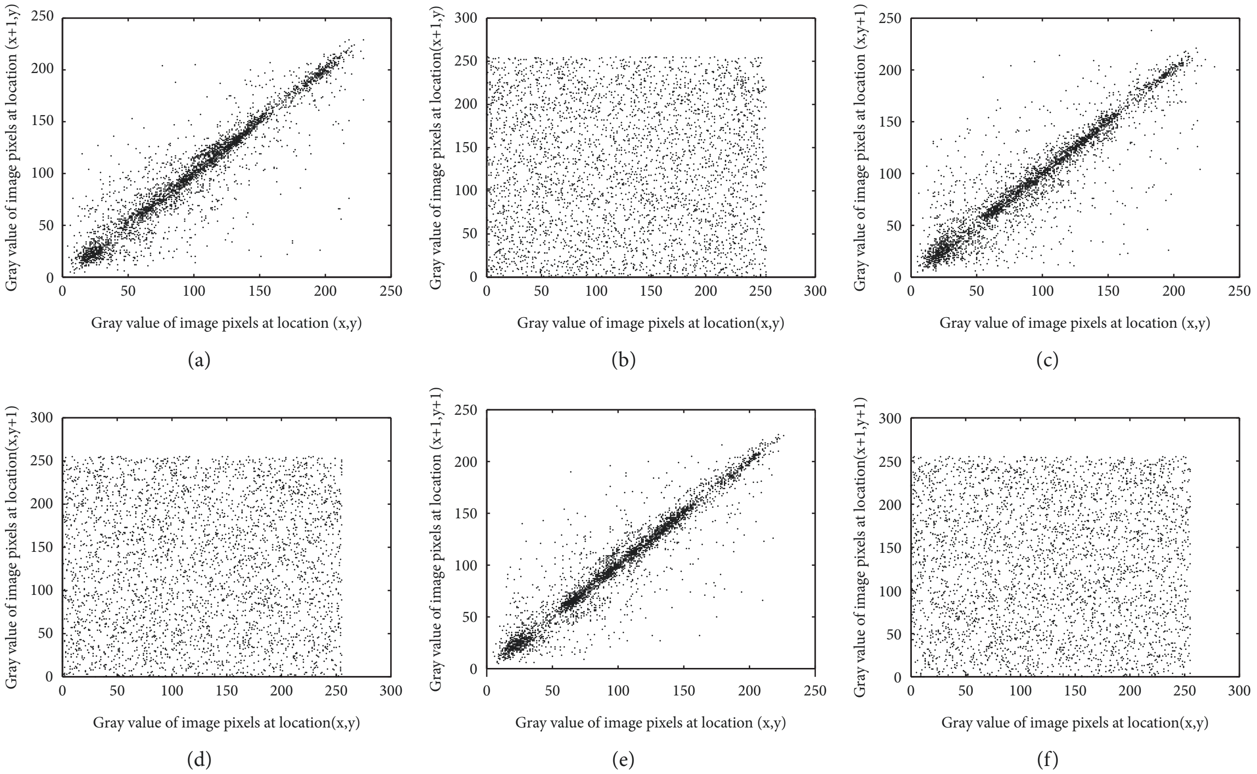


(a) (b) (c) (d)
(e) (f) (g) (h)
(i) (j) (k) (l)

Figure 6: Histogram tests: (a) histogram of plain-image Lena, (b) histogram of cipher-image for Lena, (c) histogram of plain-image Boat, (d) histogram of cipher-image for Boat; cipher-image of Lena: (e) top block, (f) bottom block, (g) left block, (h) right block, (i) top-left block, (j)top-right bock, (k) bottom-left block, and (l) bottom-right bock.

of the pixels in the cipher-image, then it can effectively resist the histogram attack [43–45]. Figure 6(a) shows the histogram of the plain-image Lena, whereas Figure 6(b) displays the histogram of its corresponding cipher-image obtained by using our method. Similarly, Figures 6(c) and 6(d) display the histograms for the Boat image before and after the encryption. Furthermore, the cipher-image of Lena is divided into two blocks vertically and horizontally and four blocks averagely. The results for the block histogram tests are displayed in Figures 6(e)–6(l). All confirm that the histogram of the cipher-image is different from that of the plain-image, and that an illegal statistical attack [46–48] will not affect our algorithm.

3.5. Correlation Coefficients Analysis. For an image in a natural case, a high correlation normally exists among most pairs of adjacent pixels because of pixel continuity. To test the ability of decreasing this correlation and then hiding



(a) (b) (c)

(d) (e) (f)

Figure 7: Correlation tests for Lena: (a) plain-image by horizontally, (b) cipher-image by horizontally, (c) plain-image by vertically, (d) cipher-image by vertically, (e) plain-image by diagonally, and (f) cipher-image by diagonally.

Table 2: Entropy comparison.

Images	Boat	Lena	Baboon	Barb
Plain-image	7.5715	7.5683	7.3579	7.4664
Cipher-image	7.9993	7.9974	7.9993	7.9993
Cipher-image in [40]	7.9915	7.9896	7.9915	7.9913
Cipher-image in [43]	7.9980	7.9974	7.9992	7.9990
Cipher-image in [46]	7.9912	7.9891	7.9912	7.9917
Cipher-image in [49]	7.9994	7.9972	7.9994	7.9993

the original information, the following function is usually employed to calculate the correlation coefficients:

$$r_c = \frac{E\left(\left(x - E\left(x\right)\right)\left(y - E\left(y\right)\right)\right)}{\sqrt{D\left(x\right)}\sqrt{D\left(y\right)}} \tag{10}$$

where N is the total number of the samples, x and y represent the gray values of two adjacent pixels in the image, and $E(x) = (1/N)\sum_{i=1}^{N} x_i$, $D(x) = (1/N)\sum_{i=1}^{N}(x_i - E(x))^2$. Figure 7 shows the visual test results for the Lena image after applying the proposed method. It can be clearly seen that the correlation coefficients can be significantly deduced in the cipher-image compared with that of the plain-image.

Table 3: *UACI* and *NPCR* comparison.

Images	Lena	Boat
OBC of *UACI* in [43]	33.3807	33.4903
OBC of *UACI* in ours	33.3281	33.4370
OBC of *NPCR* in [43]	99.6140	99.6166
OBC of *NPCR* in ours	99.5895	99.6201
TBS of *UACI* in [43]	1.1968×10^{-7}	2.9919×10^{-8}
TBS of *UACI* in ours	33.3461	33.4156
TBS of *NPCR* in [43]	3.0518×10^{-5}	7.6294×10^{-6}
TBS of *NPCR* in ours	99.6216	99.6128

3.6. Some Comparisons. In this subsection, to highlight the better performance of our method, we compare it with *UACI*, *NPCR*, and entropy. Table 2 lists the results of the entropy analysis using different images. Clearly, the values from this work are more in agreement with the theoretical value 8. Regarding *UACI* and *NPCR*, Table 3 shows the results of a one-bit change (OBC) at position (186,33) and two bits change at positions (186,33) and (105,110) but with the same

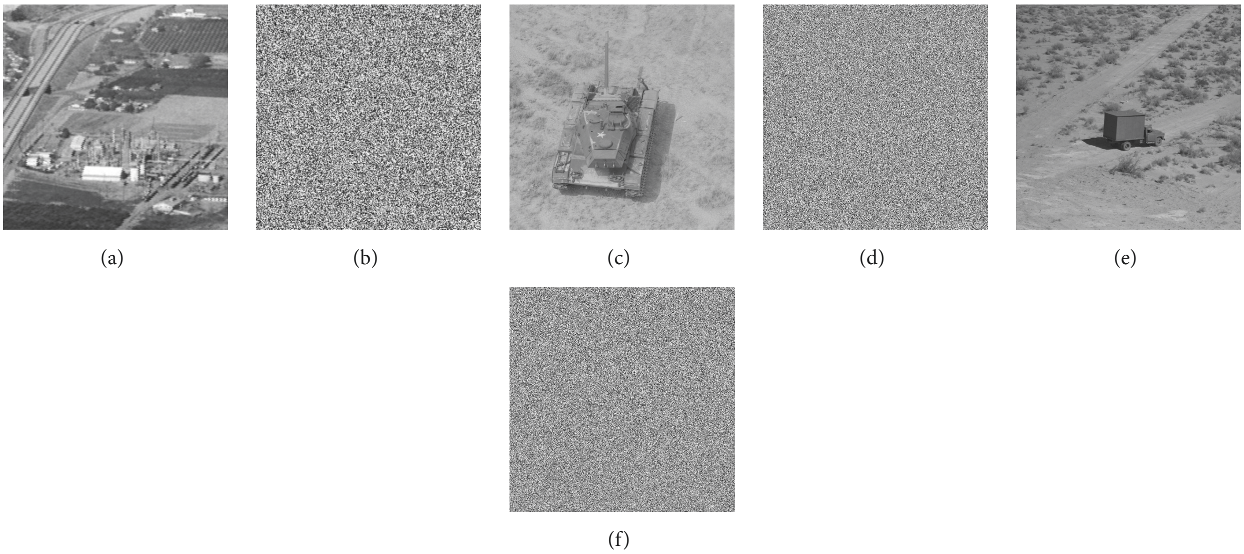


Figure 8: Tests for SIPI image database: (a) plain-image of chemical plant, (b) cipher-image of chemical plant, (c) plain-image of tank, (d) cipher-image of tank, (e) plain-image of truck, and (f) cipher-image of truck.

Table 4: Chosen/known plain-image attack.

Methods	[31]	[32]	[33]	[34]	[35]	Ours
Pass or not	No	No	No	Pass	No	Pass

Table 5: Entropy analysis for color images.

Cipher-images	Size	R	G	B	Averagely
Lena	256 × 256	7.9977	7.9971	7.9973	7.9974
Peppers	512 × 512	7.9993	7.9993	7.9993	7.9993

summation (TBS) for different plain-images. Therefore, the sensitivity to the plain-image is higher particularly when two bits are changed, but the same summation is kept in the plain-image. Regarding the chosen/known plain-image attack, we mainly consider the relationship between the plain-image and generation of the keystream. Table 4 displays the comparisons with some references that show the advantages of our method.

3.7. Extension to Other Images. Three more images are randomly taken from the SIPI image database as a test. Figure 8(a) shows the plain-image of a Chemical plant and Figure 8(b) displays its cipher-image for it. The corresponding images for a tank and truck are shown in Figures 8(c)–8(f).

3.8. Application to Color Image. As to the case of color image, it can be divided into three channels, R, G, and B. Then we treat each of them as a gray image correspondingly. Consequently, the encryption process for each channel is similar using our proposed encryption algorithm. After that, the cipher-image can be obtained by integrating again the encryption result of each channel into a color image. Table 5 lists the entropy results for color images Lena and Peppers by the proposed algorithm. All values are near to the ideal case.

4. Conclusions

To enhance the sensitivity of a plain-image and avoid the summation invariance in a plain-image associated with some algorithms, SHA-3 is employed in our proposed method to calculate the hash value. Then, an ECG signal generated by a human body is used to produce the initial conditions for the chaotic map including the control parameters. Consequently, the fixed key problem can be solved. Related analysis and experimental results have demonstrated that the proposed image encryption algorithm can be a secure model for image communication. There are two contributions, i.e., (1) avoiding the low sensitivity in case of summation invariance and (2) solving the fixed key and producing the effect of a dynamic key.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was fully supported by the National Natural Science Foundations of China (no. 61602124, no. 61702116), the Natural Science Foundation of Guangdong Province of China (no. 2016A030310333), the Science and Technology Planning Project of Guangdong Province of China (no. 2017A010101025), the Program for Scientific Research Start-up Funds of Guangdong Ocean University of China (no. R17037), the Special Funding Program for Excellent Young Scholars of Guangdong Ocean University of China (no. HDYQ2017006), and the Natural Science Foundation of Guangdong Ocean University of China (no. P15238).

References

[1] X. Q. Zhou, H. K. Huang, and S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Transactions on Medical Imaging*, vol. 20, no. 8, pp. 784–791, 2001.

[2] S. K. Rajput and N. K. Nishchal, "Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem," *Optics Communications*, vol. 309, pp. 231–235, 2013.

[3] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.

[4] Y. Wu, Y. Zhou, J. P. Noonan, and S. Agaian, "Design of image cipher using latin squares," *Information Sciences*, vol. 264, pp. 317–339, 2014.

[5] J.-X. Chen, Z.-L. Zhu, C. Fu, and H. Yu, "An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism," *Optics Express*, vol. 21, no. 23, pp. 27873–27890, 2013.

[6] G. Ye, X. Huang, L. Y. Zhang, and Z. Wang, "A self-cited pixel summation based image encryption algorithm," *Chinese Physics B*, vol. 26, no. 1, p. 010501, 2017.

[7] X. Huang and G. Ye, "An efficient self-adaptive model for chaotic image encryption algorithm," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 12, pp. 4094–4104, 2014.

[8] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.

[9] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," *Quantum Information Processing*, vol. 14, no. 4, pp. 1193–1213, 2015.

[10] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics & Laser Technology*, vol. 82, pp. 121–133, 2016.

[11] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[12] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[13] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Processing: Image Communication*, vol. 41, pp. 144–157, 2016.

[14] S. Mohammad Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," *Signal Processing*, vol. 92, no. 5, pp. 1202–1215, 2012.

[15] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 11, pp. 3075–3085, 2013.

[16] I. Hussain, T. Shah, and M. A. Gondal, "Application of S-box and chaotic map for image encryption," *Mathematical and Computer Modelling*, vol. 57, no. 9-10, pp. 2576–2579, 2013.

[17] S.-J. Xu, J.-Z. Wang, and S.-X. Yang, "An improved image encryption algorithm based on chaotic maps," *Chinese Physics B*, vol. 17, no. 11, pp. 4027–4032, 2008.

[18] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos," *Multimedia Tools and Applications*, vol. 74, no. 3, pp. 781–811, 2013.

[19] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics Lasers in Engineering*, vol. 88, pp. 197–213, 2017.

[20] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and Secure hash algorithm SHA-2," *Nonlinear Dynamics*, vol. 83, no. 3, pp. 1123–1136, 2016.

[21] Y. Liu, X. Tong, and J. Ma, "Image encryption algorithm based on hyper-chaotic system and dynamic S-box," *Multimedia Tools and Applications*, vol. 75, no. 13, pp. 7739–7759, 2016.

[22] Y. Zhang, "The image encryption algorithm with plaintext-related shuffling," *IETE Technical Review*, vol. 33, no. 3, pp. 310–322, 2015.

[23] C. Fu, B. Lin, Y. Miao, X. Liu, and J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Optics Communications*, vol. 284, no. 23, pp. 5415–5423, 2011.

[24] A. Jolfaei, X. Wu, and V. Muthukkumarasamy, "On the Security of Permutation-Only Image Encryption Schemes," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 235–246, 2016.

[25] H. Zhu, C. Zhao, X. Zhang, and L. Yang, "An image encryption scheme using generalized Arnold map and affine cipher," *Optik - International Journal for Light and Electron Optics*, vol. 125, no. 22, pp. 6672–6677, 2014.

[26] Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, and K.-W. Wong, "Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2241–2250, 2016.

[27] Y. Zhang, D. Xiao, W. Wen, and M. Li, "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Nonlinear Dynamics*, vol. 76, no. 3, pp. 1645–1650, 2014.

[28] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Processing*, vol. 118, pp. 203–210, 2016.

[29] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 38, pp. 5973–5978, 2008.

[30] B. Nini and C. Lemmouchi, "Security analysis of a three-dimensional rotation-based image encryption," *IET Image Processing*, vol. 9, no. 8, pp. 680–689, 2015.

[31] F. Abundiz-Pérez, C. Cruz-Hernández, M. A. Murillo-Escobar, R. M. López-Gutiérrez, and A. Arellano-Delgado, "A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rössler

Map," *Mathematical Problems in Engineering*, vol. 2016, Article ID 2670494, 15 pages, 2016.

[32] M. A. Murillo-Escobar, L. Cardoza-Avendaño, R. M. López-Gutiérrez, and C. Cruz-Hernández, "A Double Chaotic Layer Encryption Algorithm for Clinical Signals in Telemedicine," *Journal of Medical Systems*, vol. 41, p. 59, 2017.

[33] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons & Fractals*, vol. 95, pp. 92–101, 2017.

[34] M. Mollaeefar, A. Sharif, and M. Nazari, "A novel encryption scheme for colored image based on high level chaotic maps," *Multimedia Tools and Applications*, vol. 76, no. 1, pp. 607–629, 2017.

[35] Y. Li, X. Li, X. Jin et al., "An Image Encryption Algorithm Based on Zigzag Transformation and 3-Dimension Chaotic Logistic Map," in *Applications and Techniques in Information Security*, vol. 557 of *Communications in Computer and Information Science*, pp. 3–13, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[36] G. Bertoni, J. Daemen, M. Peeters, and G. van Assche, "The Keccak sponge function family," http://keccak.noekeon.org/index.html.

[37] A. L. Goldberger, L. A. Amaral, L. Glass et al., "PhysioBank, PhysioToolkit, and PhysioNet: components of a new research resource for complex physiologic signals.," *Circulation*, vol. 101, no. 23, pp. E215–E220, 2000.

[38] C.-K. Chen, C.-L. Lin, C.-T. Chiang, and S.-L. Lin, "Personalized information encryption using ECG signals with chaotic functions," *Information Sciences*, vol. 193, pp. 125–140, 2012.

[39] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[40] G. Ye, H. Zhao, and H. Chai, "Chaotic image encryption algorithm using wave-line permutation and block diffusion," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2067–2077, 2016.

[41] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography," *Signal Processing*, vol. 125, pp. 187–202, 2016.

[42] D. Xiao, Q. Fu, T. Xiang, and Y. Zhang, "Chaotic Image Encryption of Regions of Interest," *International Journal of Bifurcation and Chaos*, vol. 26, no. 11, p. 1650193, 2016.

[43] J. S. A. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 3, pp. 578–588, 2014.

[44] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Optics and Lasers in Engineering*, vol. 77, pp. 118–125, 2016.

[45] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "A Novel Image Encryption Scheme Using the Composite Discrete Chaotic System," *Entropy*, vol. 18, no. 8, p. 276, 2016.

[46] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[47] X. Huang and G. Ye, "An image encryption algorithm based on hyper-chaos and DNA sequence," *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 57–70, 2014.

[48] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Information Sciences*, vol. 396, pp. 97–113, 2017.

[49] Z. Eslami and A. Bakhshandeh, "An improvement over an image encryption method based on total shuffling," *Optics Communications*, vol. 286, no. 1, pp. 51–55, 2013.