Research Article

Self-Adaptive Image Encryption Algorithm Based on Quantum Logistic Map

Youxia Dong, Xiaoling Huang, Qixiang Mei, and Yuanju Gan

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

Correspondence should be addressed to Xiaoling Huang; xyxhuang@hotmail.com

Received 9 December 2020; Revised 28 December 2020; Accepted 31 December 2020; Published 15 January 2021

Academic Editor: Nanrun Zhou

Copyright © 2021 Youxia Dong et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This study proposes a self-adaptive image encryption algorithm based on the quantum logistic map. First, the initial values are substituted into the quantum logistic map based on an iteration process to generate three random sequences. After preprocessing, three new random sequences with better randomicity were obtained from the generated random sequences. In particular, the correlation coefficients for random sequences before and after preprocessing are compared to determine the best model to make the correlation coefficients closer to zero. Second, one random sequence in the scrambling stage is selected with respect to the plain image. The selected random sequence is then used to perform row-column perturbation on the plain image. Finally, the remaining two random sequences are used to perform forward and reverse diffusion to obtain the final cipher image. Because of the dependence on the plain image, the algorithm can frustrate the chosen-plaintext and known-plaintext attacks. Experimental results show that the proposed encryption algorithm can achieve secure communications.

1. Introduction

With the rapid development of network technology and multimedia, the forms of information expression on the network are also diversified. This digital information is transmitted through the network to all corners of the world to facilitate the daily needs of people. As the most universal and key information carrier in the field of digital information systems and modern communication, digital images may contain abundant private information. If an unauthorized person accesses this information, there could be serious consequences. Therefore, the protection of image information from being leaked and stolen has become the focus of the field of information security [1].

The randomness, ergodicity, and unpredictability of chaotic systems can satisfy the requirements of image encryption. In [2], a chaotic system is used for image encryption, in which the iterative state value of the chaotic system is directly used to scramble image pixel points proposed. This study introduces the performance of an image cryptosystem, including key space, known-plain attacks, ciphertext-only attacks, and chaotic map pseudorandom sequence generators. Then, this type of image encryption method based on the chaotic system is extensively used in image encryption systems. A new chaotic system was presented in [3] based on two existing one-dimensional chaotic maps that can be used to implement a sorting-based scrambling algorithm. The new chaotic system has good chaotic behavior, and the distribution of chaotic sequences is uniform. Image encryption was also realized by combining the Arnold map and the Rivest–Shamir–Adleman (RSA) algorithm [4]. First, the initial value of the Arnold map is generated by the RSA algorithm followed by the XOR diffusion operation. After the scrambling operation of the rows and columns, the additive mode diffusion operation is performed. This achieves a three-layer image hiding effect. Because the security of the encryption scheme depends on the RSA algorithm, the security is at a high level. In [5], an image encryption scheme based on the RSA and Arnold transform was proposed that is better than the traditional ones that are based on the Arnold transform and row-column chaos. First, two sets of parameters are generated by the RSA algorithm. Subsequently, during the scrambling operation, two sets of parameters are applied to
the Arnold transform. A set of parameters is used in block scrambling, and another set is used in global scrambling. In turn, in [6], an improved image encryption and decryption algorithm was proposed that combined Tent and Arnold maps. The plain image was first transformed by the Hadamard transformation and then scrambled using the Arnold map, finally XOR diffusion using the Tent map. Reference [7] suggested image encryption with two different sets of chaotic maps. First, the Tent-Sine map was used to generate the measurement matrix and the random numbers needed for embedding. The plain image was then scrambled using the Logistic-Tent map. The experiments proved that the system has enhanced security and improved robustness characteristics. A chaos-based asymmetric color image encryption scheme was proposed in [8], in which different keys were distributed to different receivers by a key conversion mechanism. Using the hash value of the plain image as two initial values of the Henon map, the random sequence needed for encryption was generated. However, owing to the short cryptosystem period and low precision in the low-dimensional chaotic system, the security of image encryption was difficult to promise. With the development of cryptographic security analysis, these low-dimensional chaotic systems are no longer secure considering key space. Thus, a method that combines high-dimensional chaotic systems to design the image encryption algorithm needs our attention. Reference [9] proposed an image cryptosystem based on a lifting scheme and a chaotic system. In the lifting scheme, the plain image data were split into even- and odd-indexed sequences. Based on these two sequences, one low-frequency and three high-frequency components of the image were obtained by computing wavelet transforms. The pseudorandom sequences generated by the chaotic system with the secret key were used to disturb the detailed components’ high frequency and were then used to disturb the approximation components’ low frequency of the image. The two disturbed components are inverted separately to execute the prediction and update operations once more to achieve the cipher image. A new digital image encryption scheme was proposed combining with Lorenz chaotic system in [10]. In the process of generating a random keystream, the hash value of the plain image was embedded into the encryption system, and the initial key was changed dynamically to improve the security level. However, the chaotic sequences obtained by the Lorenz system have some problems such as weak wideband characteristics, imperfect sequence correlation, and local monotonicity. Therefore, an improved version of the Lorenz system was proposed in [11]. By replacing the nonlinear term in the Lorenz system with the sum of the exponential and the quadratic terms of a single variable, more complex chaotic attractors with larger positive Lyapunov exponents can be generated. Reference [12] combined chaotic systems with compression sensing technology to design a visually meaningful encryption scheme. In the process of preencryption, compressed perceptual technology and Zigzag obfuscation were used to obtain the middle encrypted image. The random sequence generated by 3D-cat map and the middle encrypted image are embedded with the least significant bit to obtain the final cipher image. Reference [13] proposed a new image encryption algorithm that included a quantum chaotic map, Lorenz chaotic map, and deoxyribonucleic acid (DNA) coding. It used four DNA base pairs to dynamically select DNA coding rules, DNA additions, and XOR rules. Dynamic selection of DNA coding and decoding rules was achieved by the dynamic changes in pixel DNA encoding that effectively improved the security of the encryption algorithm. Reference [14] proposed a color image encryption based on DNA and a 4D memristive hyperchaos. The main feature was to use the dynamic DNA mechanism based on hyperchaos in the processes of encoding, confusion, and diffusion. In [15], an efficient bit-level quantum color image encryption scheme based on quantum cross-exchange operation and 5D hyperchaotic system was proposed, which shows high security and enough capacity of resisting noise attack.

Image encryption is usually pursued in the frequency and spatial domains. Reference [16] used frequency domain encryption, wherein the plain image was first transformed with the discrete wavelet transform and then compressed. The carrier image was then processed by lifting the wavelet transform and discrete cosine transform together with a Schur decomposition. Finally, an embedding operation was performed to achieve visually meaningful image encryption. Although frequency domain encryption greatly improves encryption efficiency, the implementation of frequency domain transformation leads to data loss. A secure and efficient image encryption algorithm based on adaptive permutation diffusion and DNA random coding was proposed in [17]. Plain images were first transformed into DNA sequences using random coding rules to disperse the distribution of the plain image. The adaptive permutation-diffusion process was then introduced to encrypt. In [18], the perturbation operation was designed as a self-adaptive method to replace the traditional confusion method. In addition, it provided a feedback-based diffusion mechanism that could act on internal blocks so that minor changes can affect the value of the current and another block. A new multi-image encryption scheme based on QDFrHT and an improved pixel adaptive diffusion was proposed in [19], which can achieve large-capacity image compression and encryption. Moreover, it is more convenient for key storage and transmission. Zhou et al. [20] proposed a quantum image encryption and decryption scheme, which was based on iterative generalized Arnold transforms and quantum image cycle shift operations. Different parameters and different iteration times were suggested for high security. In [21], a DQWT and 3D hyperchaotic Henon map based image compression and encryption algorithm was presented. For a high security, the quantum image is scrambled by the iterative generalized Arnold transforms to eliminate the block effect. Ye et al. [22] proposed an image encryption scheme by employing DCT, quantum logistic map, and substitution-permutation structure which has a high sensitivity to plain text and keys. Reference [23] proposed an efficient pixel-level chaotic image encryption algorithm based on the two-dimensional sine logistic modulation map. To be different from the traditional encryption architecture, the method
enhances the connection between pixel shuffling and value changing. In [24], a three-dimensional chaotic map was employed for fast image encryption. The scheme, especially, uses the latest generated numbers to permute the next block. There are some other encryption methods, for example, public-key cryptosystem based [25] and random numbers insertion based [7].

Because the low-dimensional chaotic system has certain security problems and the frequency domain encryption will cause data loss, therefore, this study uses the quantum logistic map to conduct the encryption algorithm in the spatial domain. The range of the parameters is wider, and the random sequence generated can be preprocessed to produce a more random sequence which improves the encryption effect. This article is organized as follows: the proposed encryption algorithm is given in Section 2 with detailed image encryption and decryption processes. Section 3 executes the simulation and obtains the experimental result. Security analysis is performed in Section 4. Section 5 presents some conclusions of the proposed method.

2. Proposed Encryption Algorithm

2.1. Quantum Logistic Map. A quantum chaotic map was presented in [26], which is defined as

\[
\begin{align*}
    x_{n+1} &= r(x_n - |x_n|^2) - r^2, \\
    y_{n+1} &= -y_n e^{-2\beta} + e^{-\beta} r [2 - x_n - 2x_n y_n - x_n z_n], \\
    z_{n+1} &= -z_n e^{-2\beta} + e^{-\beta} r [2 - 1 - x_n] z_n - 2x_n y_n - x_n]
\end{align*}
\]

where the control parameter \( r \in 3.74, 4.00 \), the parameter \( \beta \geq 3.5 \), and \( x_n \) and \( z_n \) are the complex conjugations of \( x_n \) and \( z_n \), respectively. The above quantum logistic map has the advantages of natural parallelism, simple structure, and large capacity. Moreover, the generated chaotic sequences are more pseudorandom. When \( r = 3.99 \) and \( \beta \geq 6 \), the quantum chaotic map can exhibit better chaotic behavior. In this study, \( r = 3.99 \), \( \beta = 7 \), and the initial conditions \( x_0 = 0.067 \), \( y_0 = 0.247 \), and \( z_0 = 0.863 \), are randomly selected and substituted 2500 times; then, three random sequences are obtained, and the first 500 are discarded to eliminate the transient effect.

The autocorrelation and cross-correlation diagrams of the sequences \( x, y, z \) are shown in Figure 1. Because the ideal pseudorandom sequence needs to be uniformly distributed, the autocorrelation function should satisfy the shape of a delta function, and the cross-correlation function is close to zero. As can be observed from Figure 1, the autocorrelation and cross-correlation functions of the sequences \( x, y, z \) are not very close to the ideal case. Thus, a preprocess is designed for these sequences as follows with test results listed in Table 1:

\[
\begin{align*}
    x' &= x \times 10^8 - \text{round}(x \times 10^8), \\
    y' &= y \times 10^8 - \text{round}(y \times 10^8), \\
    z' &= z \times 10^8 - \text{round}(z \times 10^8)
\end{align*}
\]

When we set \( \alpha = 6 \), the autocorrelation and cross-correlation of the new sequences \( x', y', z' \) are shown in Figure 2. It can be observed that the treated sequence autocorrelation function is closer to the delta function and the cross-correlation function is closer to zero. Compared with the random sequence before processing, the random sequence after processing is closer to the ideal random sequence, and the randomness is improved. To prove that the randomness of the processed sequences is better, the histograms of the sequence before and after processing are shown in Figure 3. Obviously, the new sequences are more random. It is noted that \( \alpha = 6 \) is chosen due to the smallest mean value of the cross-correlation coefficient as seen in Table 1.

2.2. Image Encryption Process. The flowchart of our image encryption algorithm is shown in Figure 4. The encryption steps are as follows:

Step 1: read the size of the plain image \( P \) as \( m \times n \), and compute sum \( s = \sum_{i=1}^{M} \sum_{j=1}^{N} P(i,j) \). Then, sequences \( x = \{x_1, x_2, \ldots, x_{s_1+m00}\}, y = \{y_1, y_2, \ldots, y_{s_1+m00}\}, \) and \( z = \{z_1, z_2, \ldots, z_{s_1+m00}\} \) with lengths \( s_1 \times m \times n \) are generated with keys \( x_0, y_0, z_0 \), where \( s_1 \) is \((\text{smod200}) + 300\).

Step 2: preprocess the sequences \( x, y, z \) with \( \alpha = 6 \), and then new sequences \( x' = \{x'_1, x'_2, \ldots, x'_{s_1+m00}\}, \) \( y' = \{y'_1, y'_2, \ldots, y'_{s_1+m00}\}, \) and \( z' = \{z'_1, z'_2, \ldots, z'_{s_1+m00}\} \) are obtained. \( m \) numbers are taken from \( s_1 + m + 1 \) to form a sequence \( L = \{x'_{s_1+1}, \ldots, x'_{s_1+m+2}, \ldots, x'_{s_1+m00}\} \) which is used to scramble the plain image, and \( n \) numbers are taken from \( s_1 + m + 1 \) to form sequence \( T = \{x'_{s_1+1}, x'_{s_1+2}, \ldots, x'_{s_1+m00}\} \), which is also used to scramble the plain image. \( m \times n \) numbers from location 301 are taken to form the sequences \( Y = \{y'_{301}, y'_{302}, \ldots, y'_{300+m00}\} \) and \( Z = \{z'_{301}, z'_{302}, \ldots, z'_{300+m00}\} \), respectively.

Step 3: map all values in the random sequence \( L \) into the range of \([1, m]\) and the random sequence \( T \) into the range of \([1, n]\) according to

\[
\begin{align*}
    L &= \left(\text{floor}\left((L - \text{floor}(L)) \times 10^{14}\right) \mod m\right) + 1, \\
    T &= \left(\text{floor}\left((T - \text{floor}(T)) \times 10^{14}\right) \mod n\right) + 1.
\end{align*}
\]

Step 4: perform the scrambling operation on the plain image \( P \) to obtain \( M \) using updated sequence Land sequence \( T \)

\[
\begin{align*}
    P'(i,\cdot) &= P(L(i,\cdot)), \\
    M(\cdot, j) &= P'(\cdot, T(j)),
\end{align*}
\]

where \( i = 1, 2, \ldots, m \) and \( j = 1, 2, \ldots, n \).
Figure 1: Autocorrelation and cross-correlation: (a) autocorrelation of $x$, (b) autocorrelation of $y$, (c) autocorrelation of $z$, (d) cross-correlation of $x, y$, (e) cross-correlation of $x, z$, and (f) cross-correlation of $y, z$.

Table 1: Cross-correlation coefficients.

| Sequence | Cross-correlation coefficient before preprocessing | Cross-correlation coefficients of different $\alpha$-values after preprocessing |
|----------|--------------------------------------------------|--------------------------------------------------------------------------------|
| $x - y$  | 0.0392                                           | $\alpha = 4$                                                               |
| $x - z$  | $-0.1211$                                        | $\alpha = 5$                                                               |
| $y - z$  | 0.0343                                           | $\alpha = 6$                                                               |
| Mean     | 0.0649                                           | $\alpha = 7$                                                               |
|          |                                                  | $\alpha = 8$                                                               |

Step 5: the random sequences $Y, Z$ are mapped into the range of $[0–255]$ by

$$
\begin{align*}
Y &= \text{floor}[ (Y – \text{floor}(Y)) \times 10^{14} ] \mod 256, \\
Z &= \text{floor}[ (Z – \text{floor}(Z)) \times 10^{14} ] \mod 256.
\end{align*}
$$

(5)

Step 6: arrange the image $M$ into a one-dimensional matrix $M'$, and do the XOR operation for it by sequence $Y$ as follows:

$$
\begin{align*}
A_i &= Y_i \oplus M'_i, \\
A_i &= A_{i-1} \oplus Y_i \oplus M'_i,
\end{align*}
$$

(6)

where $i = 2, \ldots, m \times n$.

Step 7: perform a reverse diffusion operation again to achieve a better diffusion effect as follows:

$$
\begin{align*}
B_{\text{new}} &= Z_{\text{new}} \oplus A_{\text{new}}, \\
B_j &= B_{j+1} \oplus Z_j \oplus A_j,
\end{align*}
$$

(7)

where $j = m \times n - 1, \ldots, 1$.

Step 8: convert sequence $B$ into matrix $C$ with size $m \times n$ to obtain the final image $C$.

2.3. Image Decryption Process.

Step 1: the receiver puts the correct initial values into the quantum logistic map and produces three sequences $x, y, z$. Then, $\alpha = 6$ is used to generate three new sequences $x', y', z'$ by a preprocessing. Sequences $L, T, Y, Z$ can be obtained by the same operations.

Step 2: the cipher image $C$ is arranged into a one-dimensional vector $B$, and the sequence $Z$ is used to do the XOR diffusion to obtain $A$ as follows:

$$
\begin{align*}
A_{\text{new}} &= B_{\text{new}} \oplus Z_{\text{new}}, \\
A_j &= B_j \oplus B_{j+1} \oplus Z_j,
\end{align*}
$$

(8)

where $j = mn - 1, mn - 2, \ldots, 1$.

Step 3: XOR diffusion is performed again on $A$ to obtain $M$ by sequence $Y$ as follows:
Figure 2: Autocorrelation and cross-correlation. (a) Autocorrelation of $x'$, (b) autocorrelation of $y'$, (c) autocorrelation of $z'$, (d) cross-correlation of $x', y'$, (e) cross-correlation of $x', z'$, and (f) cross-correlation of $y', z'$.

Figure 3: Frequency distribution histogram: sequences of (a) $x$, (b) $y$, (c) $z$, (d) $x'$, (e) $y'$, and (f) $z'$. 
\[
\begin{align*}
M_i &= A_i \oplus Y_i, \\
M_i &= A_i \oplus A_{i-1} \oplus Y_i,
\end{align*}
\]  
(9)

where \( i = 1, 2, \ldots, m \).

Step 4: inverse scrambling operation is performed on the matrix \( M \) to obtain the plain image using sequences \( L \) and \( T \) as follows:

\[
\begin{align*}
E(:, T(j)) &= M(:, j), \\
P(L(i,:), :) &= E(i,:),)
\end{align*}
\]  
(10)

where \( i = 1, 2, \ldots, m \) and \( j = 1, 2, \ldots, n \).

### 3. Experimental Results

The encryption algorithm presented in this study was implemented with MATLAB (version R2019a) on the Windows 10 platform with a 1.90GHz processor. In the experiment, two gray-scale images and two-color images were selected randomly as the plain images to do the tests. Initial values \( x_0 = 0.067 \), \( y_0 = 0.247 \), and \( z_0 = 0.863 \) and parameters \( r = 3.99 \), \( \beta = 7 \), \( \alpha = 6 \) are set. As can be observed from Figure 5, no effective information about the plain image can be seen in the cipher image. Table 2 shows the value \( s_1 \) used in different rounds of perturbation for different images. Because different images have different pixels, the values of \( s_1 \) are also different. As a result, the random sequence used in the scrambling stage is different, and the final encryption effect is different, which reflects the adaptive encryption method very well.

### 4. Performance Analysis

#### 4.1. Key Space

The key space is a set of all keys in the algorithm. An encryption system with a large key space can resist violent attacks effectively and has enhanced security. In this algorithm, the initial values \( x_0, y_0, z_0 \) are used in the chaotic map. When the computational accuracy is set as \( 10^{-14} \), the key space can reach \( 10^{14} \times 10^{14} \times 10^{14} = 10^{42} \approx 2^{139.5} > 2^{100} \). Therefore, the proposed algorithm has a large key space that can effectively resist violent attacks.

#### 4.2. Key Sensitivity Analysis

This part mainly tests the key sensitivity of the proposed algorithm. If an encryption algorithm has high-key sensitivity, the cryptosystem can effectively resist violent attacks and ensure the security of the images. Consider a bridge image with a size of \( 512 \times 512 \) as an example used for testing purposes. Figure 6 shows the corresponding decryption image when the key is changed only with \( 10^{-14} \) during the decryption process. Because the scrambling phase is determined by the sum value \( s \) of the plain image, the correct image cannot be decrypted when a small change occurs. It can be observed that when the decryption key changes slightly, the cipher image cannot be restored to the original plain image. So, the proposed encryption algorithm is sensitive to the key.

#### 4.3. Histogram Analysis

The histogram is used to show the distribution of each pixel in an image; we use the histogram to show the encryption effect of the proposed encryption scheme. Usually, the histogram of a plain image has obvious statistical characteristics, while the histogram of the encrypted image is evenly distributed. It can be observed from Figure 7 that the histogram of the cipher image is evenly distributed and can resist statistical attacks. So, if the attacker obtains a cipher image, he or she cannot obtain any information about the plain image.

#### 4.4. Correlation Coefficient

Commonly, each pixel in a meaningful image has a strong correlation with its neighbors in the horizontal, vertical, and diagonal directions; an encryption algorithm is supposed to destroy the correlation between pixels to protect the secret information more
The lower the correlation of adjacent pixels in the secret image is, the better the performance of the algorithm is, and the better the antistatistical attack is. Figure 8 analyzes the correlation between adjacent pixels in the plain and cipher images from three directions: horizontal, vertical, and diagonal. The correlation coefficient is calculated as follows:

\[ R_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)D(y)}} \]  \hspace{1cm} (11) \]

\[ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{x})(y_i - \bar{y}) \]  \hspace{1cm} (12)
where $R_{xy}$ is the correlation coefficient, $x$ and $y$ are the gray values of the two adjacent pixels, and $N$ is the number of adjacent pixels selected from the image. It can be seen from Figure 8 that the correlation of the cipher images is much weaker than that of the original images. Table 3 lists the correlation values in the three directions of the test image. It can be observed that the correlation coefficient of the plain image is close to one, and that of the cipher image is closer to zero. This shows that the proposed encryption algorithm can eliminate the correlation between pixels. This makes the pixel arrangement of the cipher image more random.

4.5. Information Entropy. As we know, the bigger the information entropy is, the more uniform the distribution of the gray value is, and the more random the image is. Table 4 shows the results of gray and color images. As observed from the table, the information entropy value of the plain image is smaller than that of the cipher image, and the information entropy value of the cipher image is closer to the theoretical value of eight. This shows that the cipher image has better randomness and higher security. Compared with [20, 21, 24], the test results by our method are nearer to the theory value:
Figure 7: Histograms of (a) plain image of baboon, (b) cipher image of baboon, (c) plain image of peppers, and (d) cipher image of peppers.

Figure 8: Continued.
4.6. Differential Attack Analysis. For an ideal encryption algorithm, the more sensitive the encryption algorithm is to plain images, the more robust the algorithm is to differential attacks. The sensitivity of encryption algorithms to plain images can be measured by the number of pixels change rate (NPCR) and by the unified average changing intensity (UACI), which are defined by

\[ H = - \sum P(X(i, j)) \log_2 P(X(i, j)), \]  

\[ \text{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \]  

\[ \text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| C_1(i, j) - C_2(i, j) \right| \frac{255}{255} \times 100\%. \]

When there is only one-pixel difference between two plain images, let the pixel value of point \((i, j)\) in their cipher images be \(C_1(i, j)\) and \(C_2(i, j)\). If \(C_1(i, j) = C_2(i, j)\), then \(D(i, j) = 0\); if \(C_1(i, j) \neq C_2(i, j)\), then \(D(i, j) = 1\). Table 5 lists the test results of NPCR and UACI. It can be observed...
from the table that the proposed image encryption algorithm has the ability to resist differential attacks since the values of NPCR and UACI are close to their theoretical values.

5. Conclusions

In this study, a self-adaptive image encryption algorithm was proposed based on the quantum logistic map. Because the random sequence used in image encryption needs strong randomness and the random sequence generated directly by the quantum logistic map does not yield a good performance, we suggested a preprocessing for these random sequences. The test analysis showed that if our preprocessed model was applied, the randomness of the random sequence displayed better behavior. In the process of image encryption, each round of encryption selects a random sequence according to the preencrypted image of the previous rounds of encryption. In other words, the random sequence required in the first round was determined by the plain image, while the second round was determined by the cipher image obtained from the first round, and so on. As a result, the encryption algorithm in our method was dependent both on the keys and on the plain image. Therefore, the encryption effect can yield good performance for security communications.

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 no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (no. 61972103), the Natural Science Foundation of Guangdong Province of China (no. 2019A1515011361), the Guangdong Postgraduate Education Innovation Project of China (no. 2020JGXM059), and the Key Scientific Research Project of Education Department of Guangdong Province of China (no. 2020ZDZX3064).

References

[1] E. Zhang, F. Li, B. Niu, and Y. Wang, “Server-aided private set intersection based on reputation,” Information Sciences, vol. 387, pp. 180–194, 2017.
[2] J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps,” International Journal of Bifurcation and Chaos, vol. 08, no. 6, pp. 1259–1284, 1998.
[3] C. Pak and L. Huang, “A new color image encryption using combination of the 1d chaotic map,” Signal Processing, vol. 138, pp. 129–137, 2017.
[4] K. Jiao, G. Ye, Y. Dong, X. Huang, and J. He, “Image encryption scheme based on a generalized arnold map and rsa algorithm,” Security and Communication Networks, vol. 2020, Article ID 9721675.
[5] X.-L. Huang, Y.-X. Dong, K.-X. Jiao, and G.-D. Ye, “Asymmetric pixel confusion algorithm for images based on rsa and arnold transform,” Frontiers of Information Technology & Electronic Engineering, vol. 21, no. 12, pp. 1783–1794, 2020.
[6] P. S. Sneha, S. Sankar, and A. S. Kumar, “A chaotic colour image encryption scheme combining Walsh-hadamard transform and Arnold-Tent maps,” Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 3, pp. 1289–1308, 2020.
[7] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, “Image encryption and hiding algorithm based on compressive sensing and random numbers insertion,” Signal Processing, vol. 172, Article ID 107563.
[8] H. Liu and A. Kadir, “Asymmetric color image encryption scheme using 2D discrete-time map,” Signal Processing, vol. 113, pp. 104–112, 2015.
[9] J. Zhang, “The fast image encryption algorithm based on lifting scheme and chaos,” Information Sciences, vol. 520, pp. 177–194, 2020.
[10] O. M. Al-Hazimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, “Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys,” Neural Computing and Applications, vol. 31, no. 7, pp. 2395–2405, 2019.
[11] L. Tu, Y. Wang, and C. Zhang, “A new image encryption algorithm based on optimized Lorenz chaotic system,” Concurrency and Computation Practice and Experience, vol. 43, 2020.
[12] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, “An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding,” Optics and Lasers in Engineering, vol. 124, Article ID 105837.
[13] J. Zhang and D. Huo, “Image encryption algorithm based on quantum chaotic map and DNA coding,” Multimedia Tools and Applications, vol. 78, no. 11, pp. 15605–15621, 2019.
[14] Z. Liu, C. Wu, J. Wang, and Y. Hu, “A color image encryption using dynamic DNA and 4-D memristive hyper-chaos,” IEEE Access, vol. 7, pp. 78367–78378, 2019.
[15] N. Zhou, W. Chen, X. Yan, and Y. Wang, “Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system,” Quantum Information Processing, vol. 17, no. 6, p. 137, 2018.
[16] G. Ye, C. Pan, Y. Dong, K. Jiao, and X. Huang, “A novel multi-image visually meaningful encryption algorithm based on compressive sensing and schur decomposition,” Transactions on Emerging Telecommunications Technologies, vol. 32, 2020.
[17] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, “Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption,” Signal Processing, vol. 142, pp. 340–353, 2018.
[18] D.-D. Liu, W. Zhang, H. Yu, and Z.-L. Zhu, “An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion,” Signal Processing, vol. 151, pp. 130–143, 2018.
[19] H.-S. Ye, N.-R. Zhou, and L.-H. Gong, “Multi-image compression-encryption scheme based on quaternion discrete number sequence,” Multimed Tools Appl, vol. 80, no. 25, pp. 13849–13864, 2021.
fractional Hartley transform and improved pixel adaptive diffusion,” *Signal Processing*, vol. 175, Article ID 107652, 2020.

[20] N. Zhou, Y. Hu, L. Gong, and G. Li, “Quantum image encryption scheme with iterative generalized Arnold transform and quantum image cycle shift operations,” *Quantum Information Processing*, vol. 16, no. 6, p. 164, 2017.

[21] N.-R. Zhou, L.-X. Huang, L.-H. Gong, and Q.-W. Zeng, “Novel quantum image compression and encryption algorithm based on DQWT and 3D hyper-chaotic Henon map,” *Quantum Information Processing*, vol. 19, p. 284, 2020.

[22] G. Ye, K. Jiao, X. Huang, G.-B. Min, and W.-S. Yap, “An image encryption scheme based on public key cryptosystem and quantum logistic map,” *Scientific Reports*, vol. 10, Article ID 21044, 2020.

[23] G. Ye, C. Pan, X. Huang, and Q. Mei, “An efficient pixel-level chaotic image encryption algorithm,” *Nonlinear Dynamics*, vol. 94, no. 1, pp. 745–756, 2018.

[24] M. Y. Valandar, M. J. Barani, and P. Ayubi, “A fast color image encryption technique based on three dimensional chaotic map,” *Optik*, vol. 193, Article ID 162921, 2019.

[25] G. Ye, K. Jiao, H. Wu, C. Pan, and X. Huang, “An asymmetric image encryption algorithm based on a fractional-order chaotic system and the RSA public-key cryptosystem,” *International Journal of Bifurcation and Chaos*, vol. 30, no. 12, Article ID 2050233, 2020.

[26] M. E. Goggin, B. Sundaram, and P. W. Milonni, “Quantum logistic map,” *Physical Review A*, vol. 41, no. 10, pp. 5705–5708, 1990.