Hindawi
Security and Communication Networks
Volume 2021, Article ID 6677325, 16 pages
https://doi.org/10.1155/2021/6677325

Research Article

Visually Meaningful Image Encryption Scheme Based on DWT and Schur Decomposition

Youxia Dong, Xiaoling Huang, and Guodong Ye

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

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

Received 9 November 2020; Revised 26 December 2020; Accepted 27 January 2021; Published 20 February 2021

Academic Editor: Zhiyuan Tan

A visually meaningful image encryption scheme with an asymmetric structure based on the discrete wavelet transform (DWT) and Schur decomposition is proposed in this study. First, the RSA algorithm is used to generate the initial values for the chaotic system to produce the random sequence. Then, both scrambling and diffusion operations are performed on the plain image to obtain the preencrypted image. Moreover, the Schur decomposition is applied on the preencrypted plain image to obtain the upper triangular and orthogonal matrices. Second, the cover image is scrambled followed by a DWT operation. Four subbands are then formed, namely, LL, HL, LH, and HH. Finally, the former upper triangular matrix and orthogonal matrix are embedded into subbands LH and HH produced by the cover image. After the application of the inverse DWT and inverse scrambling operation, the final visually meaningful cover image embedded with a secret plain image can be obtained. No one can identify any useful information about the plain image from the final embedded cover image, nor can anybody know that there is any hidden secret image. Experimental simulations show that the normalized correlation values between the original cover image and the final visually meaningful cover image are approximately 0.9997. Therefore, the proposed encryption scheme is imperceptible for secret image communications.

1. Introduction

In the era of high-speed information operations manifested by the rapid development and wide applicability of network and multimedia technologies, an increased amount of information is spread conveniently and quickly on the network. This introduces inconvenience to the vast number of network users. With the rapid development of network information, there are specific hidden dangers associated with the data transmitted on the network. The issue of privacy leakage has also surfaced in recent years. Information security has affected all areas of human social life and has spanned aspects of personal work and life, social economic development, and even strategic policy on national security. Therefore, research on information security has become increasingly important. Furthermore, the protection of information security has also become a hot topic in international research. For a long time, data security technologies have mainly included data encoding, message authentication, and data hiding [1–3]. Data encoding involves the use of a key in a specific encryption algorithm to encrypt plaintext data into a disorderly distribution similar to garbled ciphertext information. This ensures that illegal users cannot obtain any useful plaintext information from the ciphertext information. Message authentication is used to realize the legal identity and data integrity of the sender and receiver through the use of related passwords or digital signature technology. Data encryption hiding is a method used to hide plaintext information, digital signatures, and digital certificates into publicly transmitted information subject to the premise of safe transmission of information. In this method, even if an attacker intercepts the information transmitted on the network, he cannot identify or extract effective information from it.

For a deterministic system, its characteristics are convergence, divergence, and periodicity. The characteristics of chaotic systems are nonconvergence, nondivergence, and nonperiodicity. Because chaotic systems are highly sensitive

to initial conditions and parameter values, this satisfies the sensitivity to the keys required in image encryption. The chaotic system obtains exponentially separated orbits after multiple iterations that are in line with the requirement of multiple rounds of scrambling and diffusion to disrupt the plaintext in image encryption. The topological transfer and chaotic characteristics of the chaotic system can satisfy the diffusion and confusion characteristics of image encryption. Based on the above analysis, it can be observed that the chaotic system meets our requirements for image encryption, so the chaotic system is extensively used in image encryption algorithms [4–9]. Nezhad et al. [4] proposed a new fingerprint image encryption method based on deoxyribonucleic acid (DNA) encoding and tent maps. First, the plaintext and chaotic maps were encrypted using DNA sequences. The encrypted plaintext image and the chaotic map then executed XOR operations to obtain the final encrypted image. The experimental results show that the proposed encryption algorithm has a good encryption effect.

However, owing to the short cipher cycle and low accuracy of the low-dimensional chaotic system, this causes difficulties in the security of image encryption, and it is easy to decompose. Therefore, a method for combining high-dimensional chaotic systems and image encryption was proposed. Wang et al. [5] introduced an image encryption method based on a time-delayed chaotic system. First, a time-delayed chaotic system was introduced that has complex dynamic behavior characteristics. Based on this new system, a new image encryption algorithm was implemented. The final experiment showed that the algorithm had good security characteristics. In turn, Firdous et al. [6] proposed a new chaotic system based on new power-exponential structures of chaotic maps (PESCM) to perform confusion and XOR operations on the rows and columns of the three channels (R, G, and B) extracted from the color image. The color image encryption algorithm proposed by Tong et al. [7] through a hyperchaotic system can compress and encrypt the image according to the requirements of the reconstructed image quality. It has certain flexibility and a large key space and can resist brute force attacks. Zhou and Wang [8] proposed an encryption scheme based on a hyperchaotic system which was used to change the value in each pixel block and achieve closed-loop diffusion. Cheng et al. [9] used a hyperchaotic mapping system and scrambling-diffusion algorithm to encrypt and transform color images. The chaotic system used in this study is a new high-dimensional chaotic system that hides the chaotic attractor for image scrambling-diffusion encryption operations.

There are many encryption algorithms such as one-time key based, bit-level permutation based, DNA rule based, and applied mathematical model based ones [10] that have shown good performance. The encryption system can be symmetric [11, 12] or asymmetric [13–20]. For a symmetric encryption system, the encryption and decryption processes use the same key that requires the transmission channel to be as safe as possible during the key transmission process. However, it is more difficult to achieve this. The encryption and the decryption keys in the asymmetric cryptosystem are different and can solve the problems caused by the symmetric key system. Wu et al. [15] proposed a scalable asymmetric image compression and encryption method using the discrete wavelet decomposition (DWT) and nonlinear operations in the cylindrical diffraction domain. The DWT reduces the amount of data and is more conducive to data transmission. Kumari et al. [19] proposed a new asymmetric color image encryption method that uses a discrete cosine transform in the Fresnel domain to encrypt and compress color images. First, the color image was divided into the three color channels R, G, and B. Each channel image was then converted into a phase image, combined with an amplitude mask, and was then subjected to Fresnel transformation. Phase reservation (PR) and phase truncation (PT) were then applied on the generated image with the phase-preserved part as the private key followed by the application of the Fresnel and DCT transforms. Finally, each channel was combined to form the final secret map. The final experimental simulation proved that the asymmetric encryption algorithm can resist various existing attacks and that security characteristics have improved. To propose a scheme with a larger key space compared with the traditional cryptosystems in the fields of Fourier transform (FT) and fractional FT (FRFT), Ren et al. [20] proposed an asymmetric image encryption scheme in conjunction with a phase-truncated discrete, multiparameter FRFT. The authors performed the pixel scrambling operation and random phase masking on the image and then used phase truncation to obtain asymmetric ciphertext with stable white noise.

Because traditional image encryption uses various encryption technologies, the original plaintext image was encrypted into meaningless noise-like images or texture-like images. These surface features attract the attention of the attacker. This renders the encrypted image more vulnerable to attacks. Bao and Zhou [21] first proposed a new encryption scheme: encrypting the original image into a visually meaningful ciphertext image. After the DWT was applied on the cover image, the preencrypted plaintext image was embedded in the intermediate frequency and high-frequency subbands of the cover image to form a meaningful ciphertext image. Compared with traditional image encryption algorithms, this visually meaningful image encryption method effectively hid the existence of plaintext images making it impossible for an attacker to see whether there are plaintext images in all visual images, thus achieving the hiding effect. To a certain extent, the security of plaintext images was improved. Based on this encryption framework, many visually meaningful image encryption algorithms have been proposed [22–30]. Pan et al. [28] proposed a new, visually meaningful image encryption method based on compressed sensing. First, the plaintext image was divided into blocks followed by a DWT transformation, and a zigzag operation was used for scrambling. A logistic map was used to generate the compressed sensing matrix, and the Logistic–Tent map was then used for scrambling and diffusion operations. Finally, the encrypted plaintext image was embedded into the carrier image. The experimental results showed that the algorithm had good imperceptibility and good reconstruction quality. Chai et al. [29] combined

compressed sensing with the least significant bit to propose a visually meaningful image compression sensing encryption scheme. In the preencryption process, compressed sensing technology and zigzag scrambling were used to obtain the encrypted plaintext. The image, the random sequence generated by the three-dimensional (3D) mapping, and the encrypted plaintext image are then embedded with the least significant bits to obtain the final, visually meaningful encrypted image.

In this paper, a new visually meaningful image encryption algorithm is proposed by combining the 3D chaotic system, public-key cryptography algorithm, DWT, and Schur decomposition. By using the 3D chaotic system and the public-key cryptography algorithm, the initial value of the chaotic system is encrypted. Then, the plain image is scrambled and diffused, and then, Schur decomposition is performed. Then, the embedding operation is performed after performing scrambling and DWT on the carrier image. Finally, IDWT and inverse scrambling transform are performed to get the encrypted image with a meaningful visual.

Our contributions are as follows: (1) by using the embedding method, the secret plain image can be hidden in a cover image with imperceptible effect; (2) by employing the asymmetric RSA to generate the initial value of the chaotic system, it can solve the distribution of the key between the receiver and sender. The organizational structure of the rest of the article is as follows. Section 2 introduces a 3D chaotic system and the RSA algorithm. The image encryption and decryption process of the proposed method is described in Section 3. Section 4 presents the simulation experiments. Then, security analysis is given in Section 5. Finally, Section 6 presents the conclusions of the whole paper.

2. Fundamental Techniques

2.1. 3D Chaotic System. A new chaotic system with a hidden attractor is designed in reference [31]. The experiment proves that the chaotic system has strong chaotic behavior. A detailed description can be found in Reference [31]. The chaotic system consisted of two second-order nonlinear equations. The specific equations used to describe the system are as follows:

$$\begin{cases} \dot{x}_1 = x_2, \\ \dot{x}_2 = -x_1 - x_2 - \alpha x_2 x_3, \\ \dot{x}_3 = \beta x_2^2 - \gamma x_1 - \theta. \end{cases} \tag{1}$$

In the above equation, x_2x_3 and x_2^2 are quadratic nonlinear terms and α, β, γ, and θ are the system parameters. When $\alpha = 0.1, \beta = 0.05, \gamma = 0.1$, and $\theta = 1$, the Lyapunov exponent of the system [31] are $L_1 = 0.02207, L_2 = 0$, and $L_3 = -0.02432$. Therefore, it shows chaotic behavior. This study uses this system to generate random sequences. According to the Runge–Kutta method, the iterative results of equation (1) are the two-dimensional projections on (x, y), (x, z), and (y, z), and the sequence diagrams of the three chaotic sequences x, y, and z generated are shown in Figure 1. Compared with the other low-dimensional chaotic system, the above 3D chaotic system is used with a large key space. Table 1 shows the NIST test for the random sequence produced from the 3D chaotic system.

2.2. RSA Encryption Algorithm. The RSA public-key algorithm was proposed by Rivest, Shamir, and Adleman, which is a universal public-key algorithm that is extensively accepted and implemented and has now become an international standard for public-key cryptography. The mathematical foundation of the algorithm is Euler's theorem in elementary number theory, and its security is based on the difficulty of factoring large integers. The specific description of the RSA public-key cryptosystem is as follows:

Step 1: generate the secret key

(1) Randomly and secretly choose two large prime numbers p and q, and compute $n = p \times q$ and $\varphi(n) = (p-1)(q-1)$
(2) Randomly select e in the range of $1 < e < \varphi(n)$, set $\gcd(e, \varphi(n)) = 1$, and calculate the decryption key d, where $d = e^{-1} \bmod (\varphi(n))$
(3) The public key is (e, n), and the private key is d

Step 2: encryption

For plaintext $m < n$, the corresponding ciphertext is $c = m^e \bmod n$

Step 3: decryption

For ciphertext c, the corresponding plaintext is $m = c^d \bmod n$

3. Proposed Encryption Scheme

3.1. Image Encryption Process. The framework of the proposed image encryption scheme is shown in Figure 2. The specific encryption steps are as follows:

Step 1: the receiver selects large prime numbers p and q and calculates the public key $e$and$n$ and the private key d. Make public keys e and n public, and keep the private key d for yourself.

Step 2: the sender randomly selects three numbers that are not less than zero and denotes them as a_1, a_2, and a_3. Calculate the pixel sum $S = \sum_{i=1}^{M} \sum_{j=1}^{N} P(i, j)$ of P from the plain image P of size $M \times N$, and use the public keys e and n of the receiver to encrypt a_1, a_2, a_3, and S with the RSA encryption algorithm to obtain the public parameters b_1, b_2, b_3, and R.

Step 3: use a_1, a_2, and a_3 to generate the initial value x_0, y_0, and z_0 required by the chaotic sequence; the specific operations are as follows:

$$\begin{cases} x_0 = \left|\sin\left(a_1 \left|\sin\left(a_1\right)\right|\right)\right|, \\ y_0 = \left|\sin\left(a_2 \left|\sin\left(a_2\right)\right|\right)\right|, \\ z_0 = \left|\sin\left(a_3 \left|\sin\left(a_3\right)\right|\right)\right|. \end{cases} \tag{2}$$

Proof: because a_1 is an integer greater than zero and the value range of the sine function is between $[-1, -1]$, after taking the absolute value, the value range is

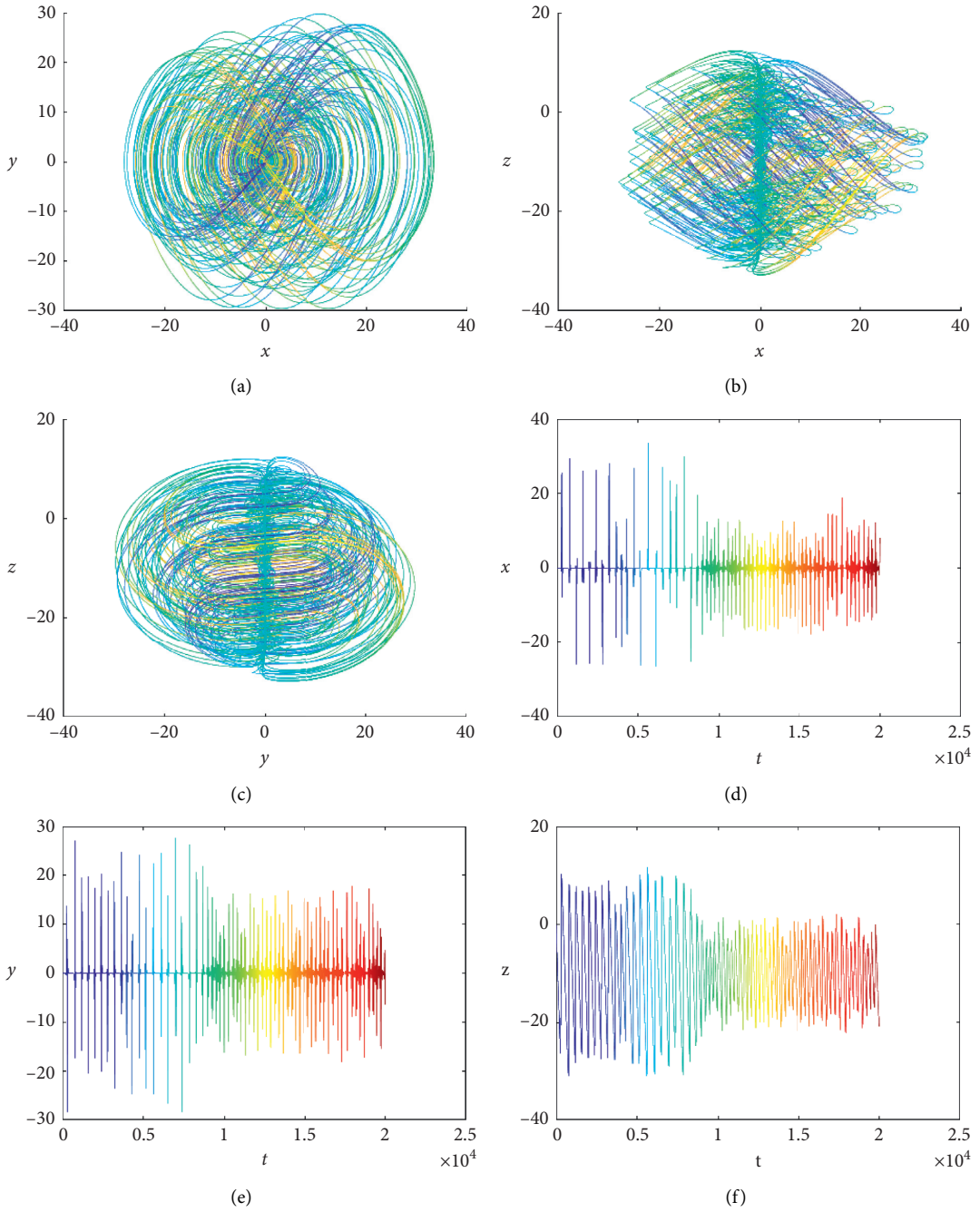


Figure 1: Iteration results of chaotic systems. (a) $x-y$ plane. (b) $x-z$ plane. (c) $y-z$ plane. (d) Sequence of x. (e) Sequence of y. (f) Sequence of z.

between $[0,-1]$; thus, $0<a_1|\sin(a_1)|<a_1$. So, the final value range of x_0 is between $[0,1]$ and can take any value. In the same way, it can be inferred that y_0, z_0 satisfies $[0,1]$ and can take any value.

Step 4: regard $x_0, y_0,$ and z_0 as the initial values of the chaotic system into equation (1) for $2M\times 2N+(\text{Smod}200)+300$ iterations, discard the first $(S \bmod 200)+300$ number to eliminate transient effects, and obtain the random sequence, $y=\{y_1,y_2,\cdots,y_{2M\times 2N}\}$ and $z=\{z_1,z_2,\ldots,z_{2M\times 2N}\}$.

Step 5: the random sequence $x, y,$ and z are mapped into the range of $[0,255]$ by the following equation:

$$\begin{cases} X=(x-x)\times 10^{14}\bmod 256, \\ Y=(y-y)\times 10^{14}\bmod 256, \\ Z=(z-z)\times 10^{14}\bmod 256, \end{cases} \tag{3}$$

where the symbol $\lfloor\rfloor$ denotes the rounding-down operator.

Table 1: The NIST test for the random sequence produced from the 3D chaotic system.

Statistical test	P value			Result
	X	Y	Z	
The frequency (monobit) test	0.2864	0.9156	0.0350	Pass
Frequency test within a block	0.0273	0.6979	0.2706	Pass
The runs' test	0.4539	0.6818	0.9892	Pass
Tests for the longest run of ones in a block	0.1243	0.7489	0.0201	Pass
The discrete Fourier transform (spectral) test	0.6424	0.6845	0.9076	Pass
The nonoverlapping template matching test	0.1243	0.7489	0.0201	Pass
The overlapping template matching test	0.1500	0.2807	0.0509	Pass
Maurer's "universal statistical" test	0.1706	0.7420	0.6638	Pass
The linear complexity test	0.8101	0.9978	0.4485	Pass
The serial test	0.1222	0.5990	0.0229	Pass
Cusums-forward	0.9313	0.3476	1.0000	Pass
Cusums-reverse	0.9925	0.2148	1.0000	Pass
The random excursions' test	0.4862	0.7142	0.1338	Pass
The random excursions' variant test	0.2863	0.9430	0.6506	Pass

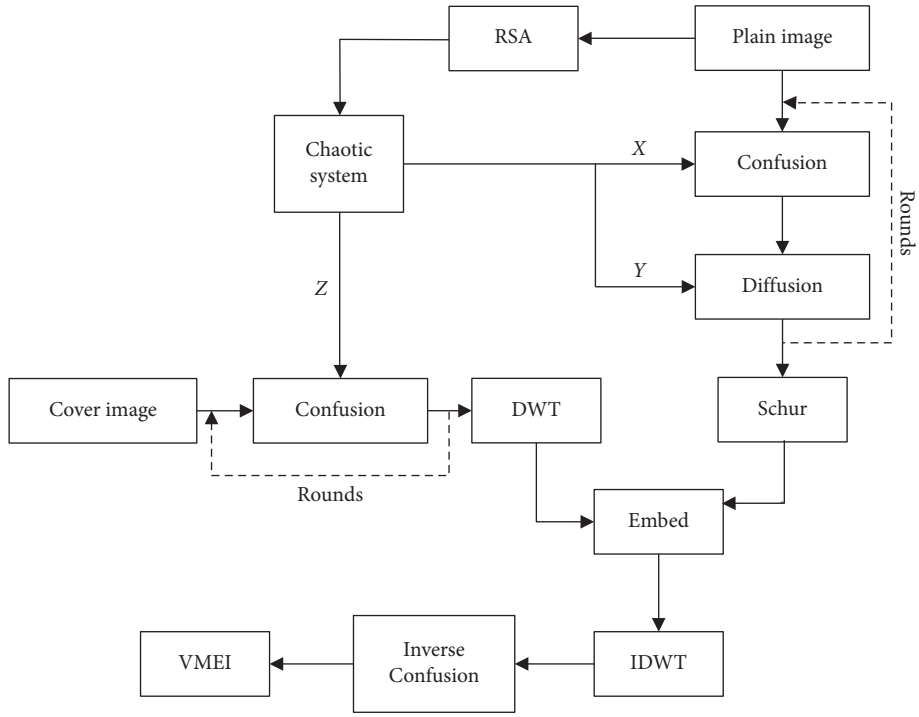


Figure 2: The flow of the proposed image encryption algorithm.

Step 6: perform a scramble operation on the plaintext image P. First, $M + N$ numbers are taken from the random sequence $X$to form a sequence $X = \{x_1, x_2, \ldots, x_{M+N}\}$. Perform row scrambling on P to obtain P', and then, perform column scrambling on P' to obtain P''. The specific operations are expressed as follows:

$$\begin{cases} P'(i,:) = P(X(i),:), \\ P''(:, j - M) = P'(:, X(j)), \end{cases} \tag{4}$$

where $i = 1{:}\ M$ and $j = M + 1{:}\ M + N$.

Step 7: $M \times N$ numbers are taken from 1 to form a sequence$Y = \{y_1, y_2, \ldots, y_{M\times N}\}$, and convert it into a matrix E with size $M \times N$. The modulo-diffusion operation on $P\prime$' to obtain A by matrix E is as follows:

$$\begin{cases} A'(i,:) = \mathrm{mod}\left(P''(i,:) + E(i,:), 256\right), \\ A(:, j) = \mathrm{mod}\left(A'(:, j) + E(:, j), 256\right). \end{cases} \tag{5}$$

where $i = 1{:}\ M$ and $j = 1{:}\ N$.

Step 8: perform Schur decomposition on A to obtain $p_U$andp_T.

Step 9: read the cover image Q with the size of $2M \times 2N$. First, $2M \times 2N$ numbers are taken from the random sequence Z to form a sequence $Z = \{z_1, z_2, \ldots, z_{2M+2N}\}$. Perform the row scrambling

operation on Q to obtain Q', and then, perform the column scrambling operation on Q' to obtain Q'' as follows:

$$\begin{aligned} Q'(i,:) &= Q(X''(i),:), \\ Q''(:, j-2M) &= Q'(:, X''(j)), \end{aligned} \tag{6}$$

where $i = 1{:}\ 2M$ and $j = 2M + 1{:}\ 2M + 2N$.

Step 10: perform DWT transformation on Q'' to obtain an approximate matrix q_LL and three detail matrices q_HL, q_LH, and q_HH.

Step 11: embed p_U into q_LH and embed p_T into q_HH, respectively, whereby the specific operations are as follows:

$$\begin{cases} q\_LH' = q\_LH + k \times p\_U, \\ q\_HH' = q\_HH + k \times p\_T, \end{cases} \tag{7}$$

where $k = (x_0 + y_0 + z_0)/3$.

Step 12: perform the IDWT transformation of q_LL, q_HL, q_LH', *and* q_HH' to obtain B, and then, perform an inverse scrambling operation on B according to equation (8) to obtain the visual image C:

$$\begin{aligned} B'(:, X''(j)) &= B(:, j), \\ C(X''(i),:) &= B'(:, i). \end{aligned} \tag{8}$$

3.2. Image Decryption Process

Step 1: the receiver first uses the private keys d, p, and q to decrypt the public parameters b_1, b_2, b_3, and R to obtain a_1, a_2, a_3, and S. Then, calculate the initial values $x_0, y_0,$ and z_0 of the chaotic system according to equation (2). According to the public parameters α, β, γ, and θ, three random sequences, namely, $x = \{x_1, x_2, \ldots, x_{2M\times 2N}\}$, $y = \{y_1, y_2, \ldots, y_{2M\times 2N}\}$, and $z = \{z_1, z_2, \ldots, z_{2M\times 2N}\}$, are obtained with equation (1).

Step 2: according to equation (3), the random sequence $x, y,$ and z is processed and mapped into the range of $[0, 255]$ to obtain $X = \{x_1, x_2, \ldots, x_{2M\times 2N}\}$, $Y = \{y_1, y_2, \ldots, y_{2M\times 2N}\}$, and $Z = \{z_1, z_2, \ldots, z_{2M\times 2N}\}$. These are used in subsequent scrambling and diffusion operations.

Step 3: perform a scrambling operation on the visual image C, and then, perform a DWT transformation to obtain an approximate matrix dq_LL and three detailed matrices dq_HL, dq_LH, and dq_HH. Extract p_U and p_T from dq_LH and dq_HH according to the following equation:

$$\begin{cases} p\_U = \dfrac{(dq\_LH\_q\_LH)}{k}, \\ p\_T = \dfrac{(dq\_HH\_q\_HH)}{K}, \end{cases} \tag{9}$$

where $k = (x_0 + y_0 + z_0)/3$.

Step 4: perform the inverse Schur transform $F = p\_U \times p\_T \times p\_U'$ to obtain F.

Step 5: inverse diffusion operation is performed on F to obtain I, and then, inverse scrambling operation is performed on I to obtain the decryption image D as follows:

$$\begin{cases} F'(:, j) = \mathrm{mod}(F(:, j) - E(:, j), 256), \\ I(i,:) = \mathrm{mod}(F'(i,:) - E(i,:), 256). \end{cases} \tag{10}$$

4. Experimental Results

The encryption algorithm presented in this study was implemented in MATLAB (version R2019a) on the Windows 10 platform with a 3.20 GHz processor. In this algorithm, the private keys are p, q, d, a_1, a_2, a_3, and S, and the public keys are α, β, γ, θ, e, n, b_1, b_2, b_3, and R. The values of the parameters used in this test are listed in Table 2. Among them, S and R are related to the plaintext, and these values are not uniformly assigned. In the experiment, grayscale images and color images were selected for the simulation. Figure 3 shows the grayscale image encryption test results, and Figure 4 shows the color image encryption test results. As one can observe from the figure, it is impossible to know from the visual image that other images are hidden in the meaningful image, and the decryption restores the plain image more effectively. Table 3 gives the NIST test for an encrypted image.

5. Security Analysis

5.1. Key Space. The key space is a collection of all algorithmic keys. An encryption algorithm with a large key space can resist brute violent attacks effectively and has enhanced security. In this algorithm, the initial values a_1, a_2, a_3, and $S$are used in the chaotic system. Because a_1, a_2, and a_3 are arbitrary positive integers, the combination can be greater than 2^{100}. For directly to the keys $x_0, y_0,$ and z_0, if the computational accuracy is set as 10^{-14}, the key space can reach $10^{14} \times 10^{14} \times 10^{14} = 10^{44} \approx 2^{146.1} > 2^{100}$. Therefore, the proposed algorithm has a large key space that can effectively resist violent attacks.

5.2. Key Sensitivity Analysis. This part mainly tests the key sensitivity of the proposed algorithm. When the decryption key changes slightly, the original plaintext image cannot be decrypted so the decryption key of the algorithm is more sensitive. A good image encryption algorithm requires a strong key sensitivity to effectively resist violent attacks. As shown in Figure 5, we choose the Lena image as the plaintext image and the Male image as the cover image for the test. First, a set of secret keys was used to encrypt and embed the plain image to obtain a visually meaningful encrypted image. Then, encrypt and embed the plain image to obtain another visually meaningful encrypted image. It can be observed

Table 2: Values of various parameters used in the experiment.

Parameter	Value
q	1,193
p	1,453
d	627,001
a_1	161
a_2	383
a_3	31
b_1	231,776
b_2	981,256
b_3	147,439
α	0.1
β	0.05
γ	0.1
θ	1
e	256
n	1,733,429

from Figure 5(e) that when the secret key changes slightly, it has a minor effect on the visual image. However, it can be observed from Figures 5(f) and 5(g) that although the visual images are not much different, the plain image cannot be decrypted even if the secret key is slightly changed for decryption. This shows that the algorithm has high key sensitivity and can resist brute force attacks.

5.3. Statistical Analysis. The histogram is used to show the distribution of each pixel value in an image, and the hidden effect of the encryption scheme that we propose is also displayed in the form of a histogram. We chose to hide the plain image (grayscale image Cameraman and color image Boat with a size of 256×256) in a different cover image, and the test result is shown in Figure 6. For the grayscale image, Figures 6(a) and 6(e) are the cover images with a size of 512×512, and the corresponding histograms are shown in Figures 6(b) and 6(f). The final encrypted image is shown in Figures 6(c) and 6(g), and the corresponding histograms are shown in Figures 6(d) and 6(h). For the color image, Figure 6(i) is the cover image with a size of 512×512, and the histograms of R, G, and B are shown in Figures 6(j), 6(k), and 6(l); the final encrypted image is shown in Figure 6(m), and the corresponding histograms of R, G, and B are shown in Figures 6(n), 6(o), and 6(p). It can be observed from Figure 6 that the final visual image and the histogram of the cover image are very similar, thus indicating that the hiding effect is very good.

By using variance of the histogram, we can evaluate uniformity of a cipher image easily. Lower value of variance indicates the higher uniformity of the cipher image. The variance of the histogram is presented as follows:

$$\mathrm{Var}(Z) = \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} \frac{1}{2} \left(z_i - z_j\right)^2, \tag{11}$$

where Z is the vector of the histogram value with $Z = \{z_1, z_2, \ldots, z_{256}\}$ and z_i and z_j are the numbers of pixels equalling to i and j, respectively. As seen from Table 4, the variance value of the visual image is very close to that of the carrier image. So, our algorithm has a good hiding effect. Table 5 gives the comparisons of different methods. It is easy to see that the values are smaller in the encrypted images.

Chi-squared analysis is employed to test the plain image and cipher image, which is defined as follows:

$$\chi^2_{\text{test}} = \sum_{i=0}^{255} \frac{\left(\text{obs}_i - \exp_i\right)^2}{\exp_i}, \tag{12}$$

where $\exp_i = (M \times N/256)$, $M \times N$ is the image size, and $\exp_i$ and obs_i are the expected and observed frequencies, respectively. Table 6 shows the results of Chi-square with all values pass.

5.4. Quality Analysis. In this study, the plaintext image is hidden in the cover image by asymmetric encryption. Thus, the imperceptibility of the algorithm is particularly important. The following compares and analyzes the normalized correlation coefficient (NC) and information entropy (H) between the cover and the visual images. Generally, the larger the NC value is, the higher the similarity of the two images is, that is, the better the hiding effect. Additionally, the values of H of the cover and the visual images are close, thus indicating that the two images are also approximately similar. The definitions of NC and H are as follows:

$$\begin{cases} \text{NC} = \dfrac{\sum X(i,j) Y(i,j)}{\sqrt{\sum (X(i,j))^2} \sqrt{\sum (Y(i,j))^2}}, \\ \\ H = -\sum P(X(i,j)) \log_2 P(X(i,j)). \end{cases} \tag{13}$$

Among them, X and Y are two different images, $P(X(i,j))$ is the number of times $X(i,j)$ appears, and the size of the image is $M \times N$. Table 7 shows the NC and H values between different cover images and visual images of grayscale images, and Table 8 lists the NC and H values between different cover images and visual images of color images. It can be observed from Tables 7 and 8 that irrespective of whether it is a color image or a grayscale image, the NC value between the cover image and the corresponding visual image is approximately 0.9997, which is very close to the theoretical NC value of one. Moreover, the information entropy between the cover and the visual images are also very close, thus indicating that our encryption scheme has a good hiding effect.

5.5. Classical Attacks. There are four classical types of attacks which are as follows: (1) ciphertext-only attack; (2) known-plaintext attack; (3) chosen-plaintext attack; (4) chosen-ciphertext attack. Chosen-plaintext attack CPA and known-plaintext attack KPA are two most important types of attacks that attackers use to make an illegal attack. In our encryption process, the generated random sequence is related to the plaintext, and the chaotic system is sensitive to the initial value. Therefore, any attacker cannot extract

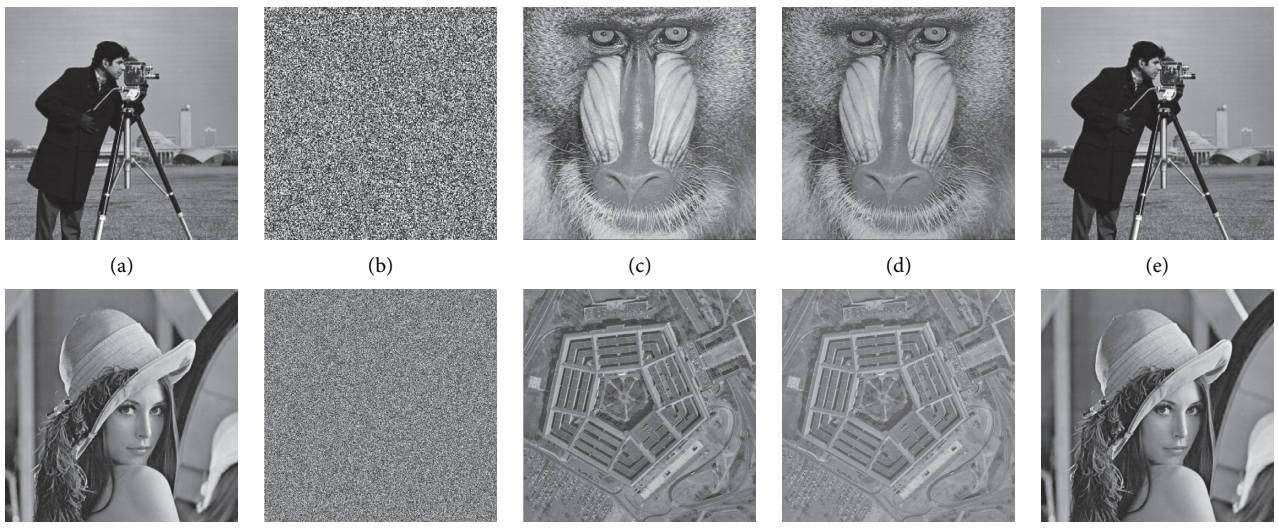


Figure 3: Grayscale image test results. (a) Plain image of Cameraman (256 × 256). (b) Encrypted image of (a). (c) Host image of Baboon. (d) Visual image. (e) Decrypted image. (f) Plain image of Lena (512 × 512). (g) Encrypted image of (f). (h) Host image of Pentagon. (i) Visual image. (j) Decrypted image.

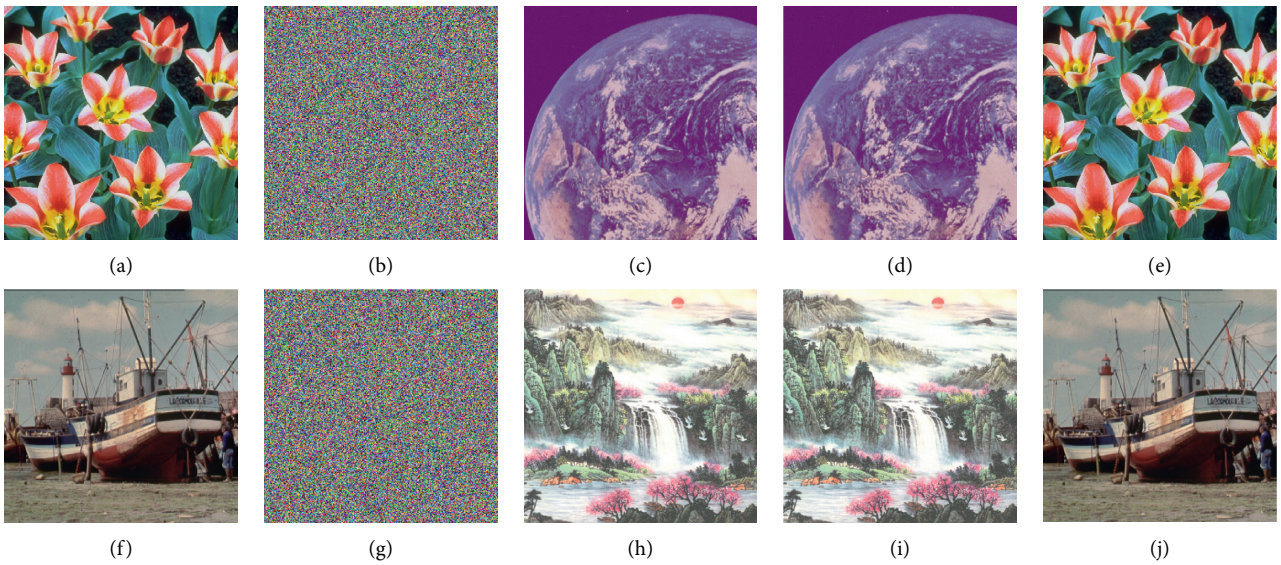


Figure 4: Color image test results. (a) Plain image of Tulips (256 × 256). (b) Encrypted image of (a). (c) Host image of Earth. (d) Visual image. (e) Decrypted image. (f) Plain image of Boat (256 × 256). (g) Encrypted image of (f). (h) Host image of Sun. (i) Visual image. (j) Decrypted image.

useful information by encrypting certain selected images because the encrypted output is only relevant to the selected image. Therefore, the proposed algorithm can resist CPA and KPA.

As to the black image and white image, Figure 7 shows the simulation results for them with different size, i.e., 256× 256, 256 × 512, and 512 × 512. By observing the encrypted images, we can find that it is impossible to extract any information from the encrypted images.

5.6. Computational Complexity and Time Complexity Analysis. For a plain image of size $M \times N$ and a cover image of size $2M \times 2N$, the computational complexity to generate randomly based on the 3D chaotic system is $O(5 \times 4MN) = O(20MN)$. In the encryption stage, the computational complexity is $O(2MN)$. So, the overall computational complexity to perform encryption operation is $O(20MN + 2MN) = O(22MN)$. That is to say, for a message with length $n = MN$, the computational complexity

Table 3: The NIST test for the encrypted image with size 1024×2014.

Statistical test	P value	Results
The frequency (monobit) test	0.1977	Pass
Frequency test within a block	0.8234	Pass
The runs test	0.6573	Pass
Tests for the longest run of ones in a block	0.4794	Pass
The discrete Fourier transform (spectral) test	0.6218	Pass
The nonoverlapping template matching test	0.6954	Pass
The overlapping template matching test	0.4796	Pass
Maurer's "universal statistical" test	0.8838	Pass
The linear complexity test	0.5744	Pass
The serial test	1.0000	Pass
Cusums-forward	0.8580	Pass
Cusums-reverse	1.0000	Pass
The random excursions' test	0.9651	Pass
The random excursions' variant test	0.3932	Pass

is $O(n)$ besides of DWT and Schur decomposition. Moreover, Table 9 lists the time cost for both grayscale and color images.

5.7. Mean Square Error and Peak Signal-to-Noise Ratio Analysis. Mean square error (MSE) measures the difference between two images. The bigger value of MSE shows the larger difference. MSE is defined by the following equation:

$$\begin{cases} \mathrm{MSE}_{\mathrm{PE}} = \dfrac{1}{M \times N} \displaystyle\sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{ij} - E_{ij}\right)^2, \\ \mathrm{MSE}_{\mathrm{PD}} = \dfrac{1}{M \times N} \displaystyle\sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{ij} - D_{ij}\right)^2, \\ \mathrm{MSE}_{\mathrm{CV}} = \dfrac{1}{M \times N} \displaystyle\sum_{i=1}^{M} \sum_{j=1}^{N} \left(C_{ij} - V_{ij}\right)^2, \end{cases} \tag{14}$$

where P, E, D, C, and V represent the plain image, encrypted image, decrypted image, cover image, and visual image, respectively, and $\mathrm{MSE}_{\mathrm{PE}}$, $\mathrm{MSE}_{\mathrm{PD}}$, and $\mathrm{MSE}_{\mathrm{CV}}$ are the MSE between plain image and encrypted image (PE), plain image and decrypted images (PD), and cover image and visual images (CV), respectively. PSNR measures the fidelity of an image. The low value of PSNR shows the large difference of the encrypted and plain image. The peak signal-to-noise ratio (PSNR) between two images is as follows:

$$\begin{cases} \mathrm{PSNR}_{\mathrm{PE}} = 10\log_{10}\left(\dfrac{\left(2^n - 1\right)^2}{\mathrm{MSE}_{\mathrm{PE}}}\right), \\ \mathrm{PSNR}_{\mathrm{PD}} = 10\log_{10}\left(\dfrac{\left(2^n - 1\right)^2}{\mathrm{MSE}_{\mathrm{PD}}}\right), \\ \mathrm{PSNR}_{\mathrm{CV}} = 10\log_{10}\left(\dfrac{\left(2^n - 1\right)^2}{\mathrm{MSE}_{\mathrm{CV}}}\right), \end{cases} \tag{15}$$

where n is the number of bits, which is equal to 8 for a gray image and $\mathrm{PSNR}_{\mathrm{PE}}$, $\mathrm{PSNR}_{\mathrm{PD}}$, and $\mathrm{PSNR}_{\mathrm{CV}}$ are the PSNR between plain image and encrypted image (PE), plain image and decrypted image (PD), and cover image and visual image (CV), respectively. Table 10 and 11 show the test resutls for MSE and PSNR.

From Table 10, we can see that the $\mathrm{MSE}_{\mathrm{PE}}$ is very large, and the $\mathrm{PSNR}_{\mathrm{PE}}$ is very small. This shows that the encrypted image is very different from the plain image. The $\mathrm{MSE}_{\mathrm{PD}}$ is zero, and the $\mathrm{PSNR}_{\mathrm{PD}}$ is infinite. This shows that the decrypted image and the plain image are the same. The $\mathrm{MSE}_{\mathrm{CV}}$ is small, and the $\mathrm{PSNR}_{\mathrm{CV}}$ is around 44. This shows that the visual image and cover image are very similar. Moreover, compared with Reference [32] and Reference [33], the encryption effect of our scheme shows better performance.

From Table 11, the PSNR values between the cover image and the visual image (CV) are bigger by using our method. Figure 8 is a bar chart showing the data in Table 11. So, the visual hiding effect of the proposed encryption scheme is in better performance.

5.8. Differential Attack Analysis. Two common measurements to evaluate the effect of differential attack, i.e., NPCR (number of pixels change rate) and UACI (unified average changing intensity), can be computed as follows:

$$\begin{aligned} \mathrm{NPCR} &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \\ \mathrm{UACI} &= \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\left|C_1(i, j) - C_2(i, j)\right|}{255} \times 100\%, \end{aligned} \tag{16}$$

where M and N represent the width and height of the image and C_1 and C_2 are the ciphered images before and after one pixel of the plain image being changed, respectively. For the pixel at position (i, j), if $C_1(i, j) \neq C_2(i, j)$, let $D(i, j) = 1$; else, let $D(i, j) = 0$. NPCR and UACI tests of our algorithm are listed in Table 12.

Table 13 shows some comparisons of NPCR and UACI. Therefore, there is strong plaintext sensitivity in our encryption scheme to resist differential attack.

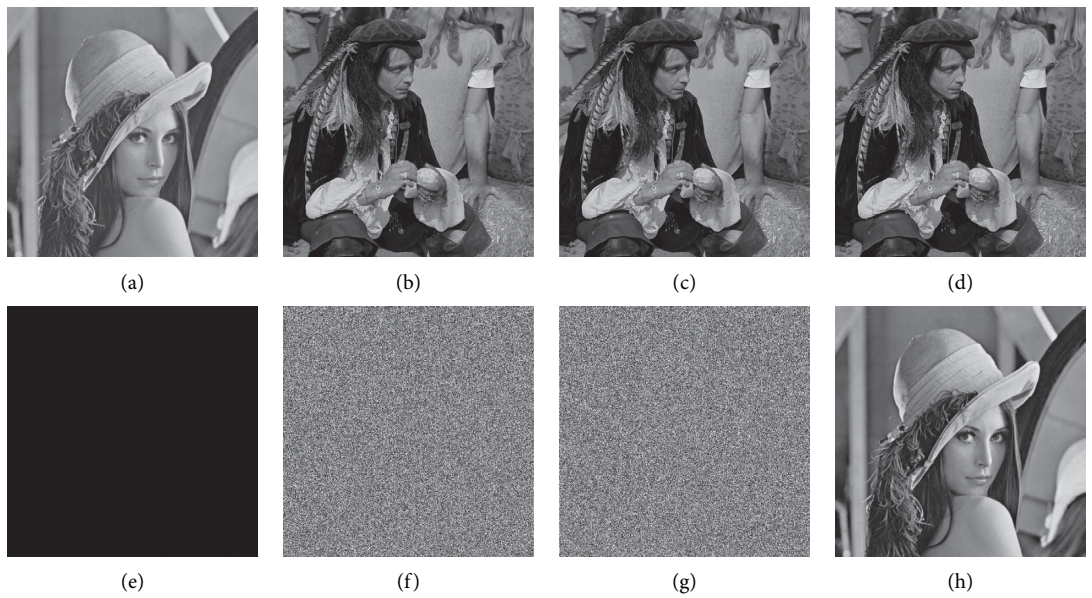


Figure 5: The key sensitivity test. (a) Plain image (512 × 512). (b) Host image. (c) Visual image. (d) Visual image with the change key. (e) Difference image estimated as the difference of images in (d)-(c). (f) Decrypted image (c) use of the keys of (d). (g) Decrypted image (d) using the keys of (c). (h) Decrypted image with the correct key.

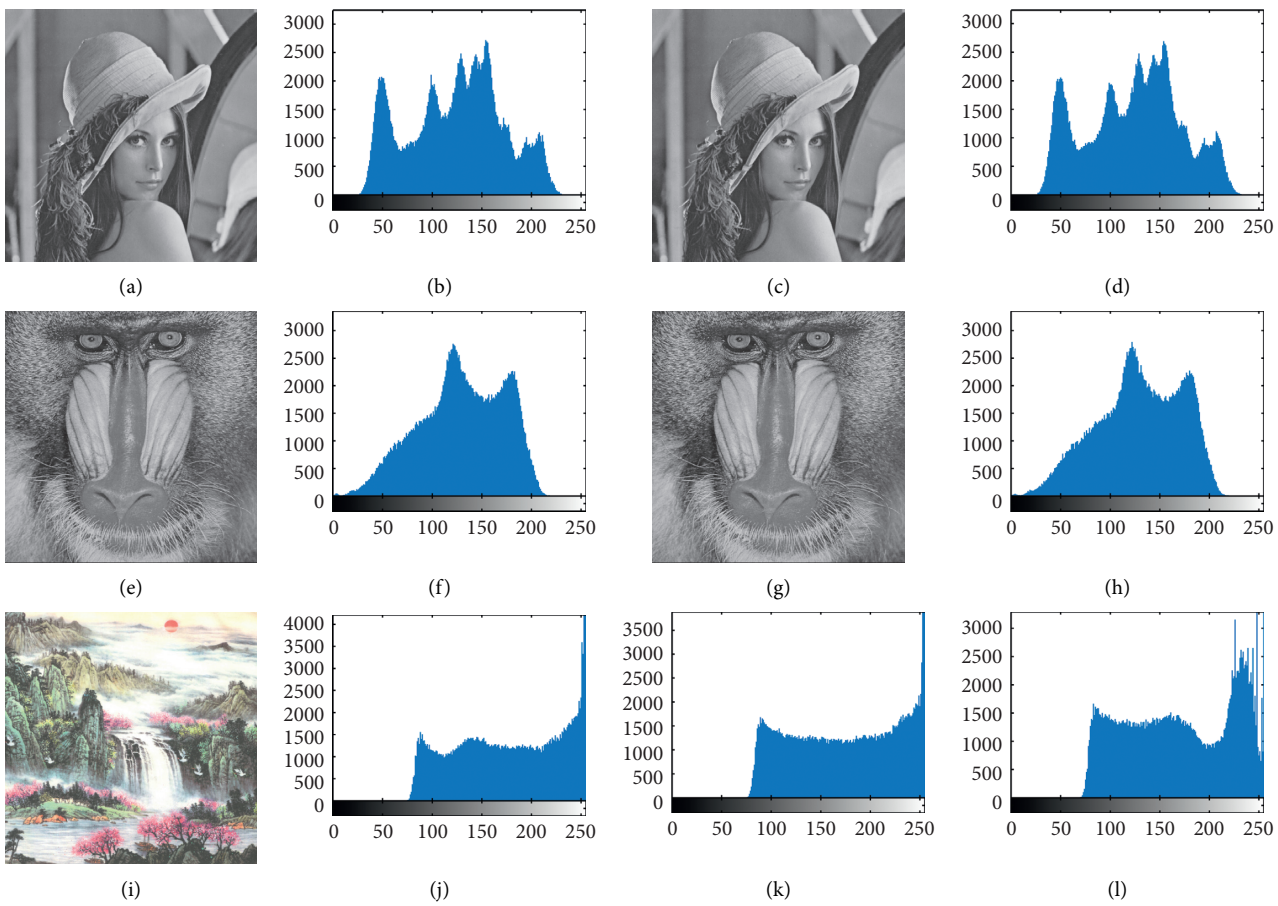
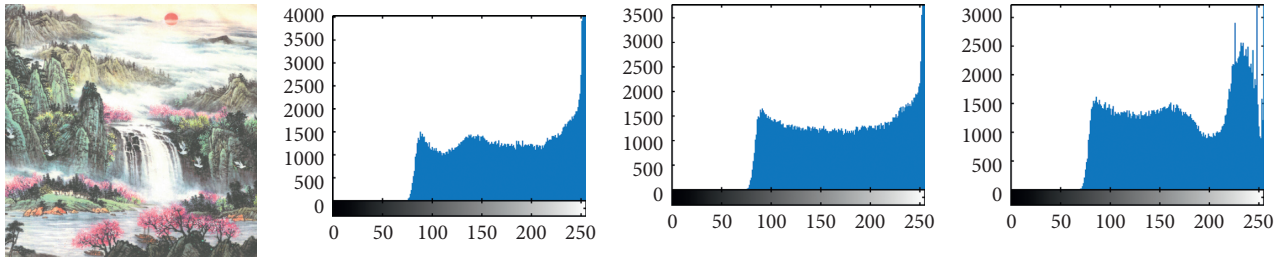


Figure 6: Continued.



(m) (n) (o) (p)

Figure 6: The histogram test. (a) Host image of Lena. (b) Histogram of Lena. (c) Visual image of Lena. (d) Histogram of the visual image of Lena. (e) Host image of Baboon. (f) Histogram of Baboon. (g) Visual image of Baboon. (h) Histogram of the visual image of Baboon. (i) Host image of Sun. (j) Histogram of *R* component. (k) Histogram of *G* component. (l) Histogram of *B* component. (m) Visual image of Sun. (n) Histogram of the visual image of *(R)*. (o) Histogram of the visual image of *(G)*. (p) Histogram of the visual image of B.

Table 4: The variance value of test images.

Plain image		Host image	Variance value		
			Host image	Cipher image	Visual image
Cameraman (256 × 256)		Lena	6.3210×10^5	228.5859	6.2543×10^5
		Baboon	7.5040×10^5	228.5859	7.4792×10^5
		Peppers	4.8066×10^5	228.5859	4.7388×10^5
Boat (256 × 256)	Sun	R	1.7877×10^6	249.8594	1.5441×10^6
		G	1.3600×10^6	263.8203	1.2139×10^6
		B	6.8248×10^5	254.0781	6.0780×10^5
	Earth	R	2.4461×10^6	249.8594	2.4139×10^6
		G	6.0912×10^5	263.8203	5.9477×10^5
		B	1.5403×10^6	254.0781	1.5240×10^6

Table 5: Comparisons of the variance value.

Algorithms	Images	Sizes	Plain images	Encrypted image
Ours	Tree	256 × 256	66009.679	248.8125
	Cameraman	256 × 256	110973.304	228.5859
	Boat	512 × 512	1583351.602	1016.523
	Lena	512 × 512	632097.477	915.6719
	Couple	512 × 512	1387095.813	1028.398
Reference [32]	Tree	256 × 256	66010	259.9297
	Cameraman	256 × 256	110970	250.4141
	Lena	512 × 512	633400	1077.3
Reference [33]	Boat	512 × 512	1535900	1044.9
	Lena	512 × 512	633400	982.5703
	Couple	512 × 512	1195500	967.3047
Reference [34]	Boat	512 × 512	1535878.750	1035.125
	Couple	512 × 512	1195460.976	1104.265

Table 6: Chi-squared test results.

Algorithm	Plain images	Sizes	Chi-square	Results
Ours	Lena	512×512	228.9180	Pass
	Couple	512×512	257.0996	Pass
	Boat	512×512	254.1309	Pass
	Baboon	512×512	250.3789	Pass
Reference [33]	Lena	512×512	245.6426	Pass
	Couple	512×512	241.8262	Pass
	Boat	512×512	261.2148	Pass
	Baboon	512×512	272.1797	Pass

Table 7: Grayscale images: the similarity test between different visual images and corresponding cover images.

Plain image	Host image	NC	H	
			Host image	Visual image
Cameraman (256 × 256)	Lena	0.9997	7.4456	7.4512
	Baboon	0.9997	7.3579	7.3604
	Peppers	0.9997	7.5937	7.5993
Boat (256 × 256)	Baboon	0.9997	7.3579	7.3603
	Bridge	0.9997	5.7056	7.2360
	Peppers	0.9997	7.5937	7.5997
Lena (512 × 512)	Pentagon	0.9998	6.7327	6.7489
	Landscape	0.9999	7.4402	7.4476
	Male	0.9996	7.5237	7.5344
Bridge (512 × 512)	Pentagon	0.9998	6.7327	6.7489
	Landscape	0.9999	7.4402	7.4474
	Male	0.9996	7.5237	7.5347

Table 8: Colour images: the similarity test between different visual images and corresponding cover images.

Plain image	Host image	Colour component	NC	H	
				Host image	Visual image
Boat (256 × 256)	Earth	R	0.9998	6.5724	6.5899
		G	0.9996	7.4512	7.4617
		B	0.9998	6.7626	6.7726
		Mean	0.9997	6.9287	6.9414
	Sun	R	0.9999	7.2018	7.2371
		G	0.9999	7.2732	7.2917
		B	0.9999	7.4110	7.4344
		Mean	0.9999	7.2983	7.3211
Tulips (256 × 256)	Earth	R	0.9998	6.5724	6.5889
		G	0.9996	7.4512	7.4619
		B	0.9998	6.7626	6.7736
		Mean	0.9997	6.9287	6.9415
	Sun	R	0.9999	7.2018	7.2384
		G	0.9999	7.2732	7.2927
		B	0.9999	7.4110	7.4344
		Mean	0.9999	7.2983	7.3218

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

Figure 7: Continued.

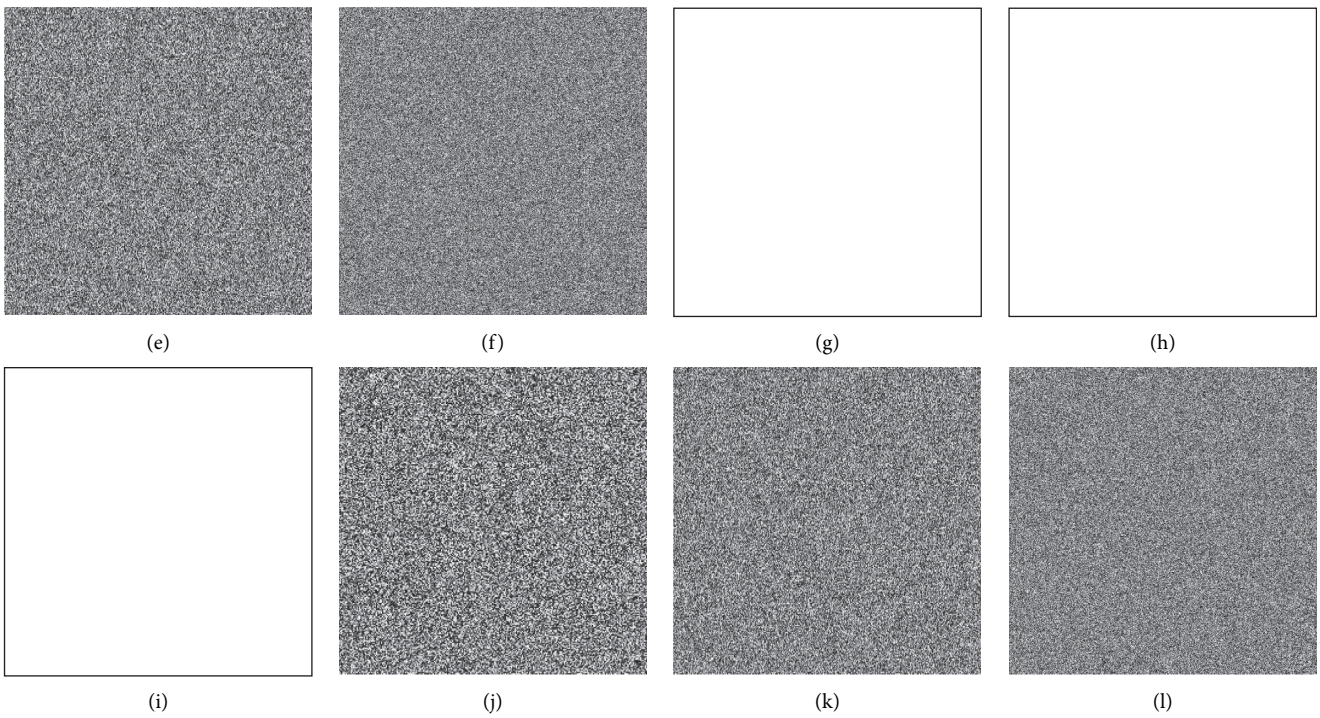


Figure 7: Tests for the black image and white image. (a) 256 × 256 black image. (b) 256 × 512 black image. (c) 512 × 512 black image. (d) Encryped image of (a). (e) Encryped image of (b). (f) Encryped image of (c). (g) 256 × 256 white image. (h) 256 × × 512 white image. (i) 512 × 512 white image. (j) Encryped image of (g). (k) Encryped image of (h). (l) Encryped image of (i).

Table 9: Time cost (average).

Algorithm	Sizes	Encryption time	Decryption time
Ours	256 × 256 (gray)	0.419665	0.266402
	512 × 512 (gray)	1.810313	1.079050
	256 × 256 (color)	1.138108	0.726431
	512 × 512 (color)	5.159817	3.102788
Reference [35]	256 × 256 (color)	1.85	—
	512 × 512 (color)	3.76	—
Reference [22]	256 × 256 (gray)	0.4049	1.4724
	512 × 512 (gray)	0.9279	10.5830

Table 10: MSE and PSNR test results.

Algorithms	Plain images	Size	Cover images	MSE			PSNR		
				PE	PD	CV	PE	PD	CV
Ours	Cameraman	256 × 256	Couple	9423.4	0	2.6300	8.3887	Inf	43.9319
			Bridge	9423.4	0	2.5808	8.3887	Inf	44.0132
	Boat	256 × 256	Couple	8075.7	0	2.7629	9.0590	Inf	43.7172
			Bridge	8075.7	0	2.6677	9.0590	Inf	43.8694
	Tree	256 × 256	Couple	10104.1	0	2.5703	8.0858	Inf	44.0310
			Bridge	10104.1	0	2.5900	8.0858	Inf	43.9978
	Lena	512 × 512	Pentagon	7757.4	0	2.4449	9.2336	Inf	44.2481
			Landscape	7757.4	0	2.4092	9.2336	Inf	44.3121
	Boat	512 × 512	Pentagon	8289.8	0	2.4328	8.9454	Inf	44.2697
			Landscape	8289.8	0	2.3953	8.9454	Inf	44.3372
	Pepper	512 × 512	Pentagon	8413.8	0	2.4649	8.8809	Inf	44.2128
			Landscape	8413.8	0	2.3828	8.8809	Inf	44.3599
Reference [32]	Cameraman	256 × 256	—	9453.2	0	—	8.2203	Inf	—
	Tree	256 × 256	—	9690.2	0	—	8.7405	Inf	—
	Pepper	512 × 512	—	8981.6	0	—	8.1099	Inf	—
Reference [33]	Lena	512 × 512	—	7762.6	0	—	9.2307	Inf	—
	Boat	512 × 512	—	7640.5	0	—	9.2996	Inf	—

Table 11: PSNR of CV test results.

Images	Ours	Reference [21]	Reference [36]	Reference [37]	Reference [38]
Lena	44.0293	28.684	36.142	40.365	41.912
Baboon	43.8180	27.946	36.617	40.547	41.923
Earth	43.8986	28.933	36.479	40.566	41.913
Couple	43.9313	27.920	35.598	39.547	40.987
Bridge	44.0132	26.553	36.132	39.828	41.116
Boat	43.8859	27.251	36.549	40.437	41.921
Pepper	44.0491	28.845	36.055	40.104	41.704
Mean	43.9465	28.019	36.225	40.199	41.639

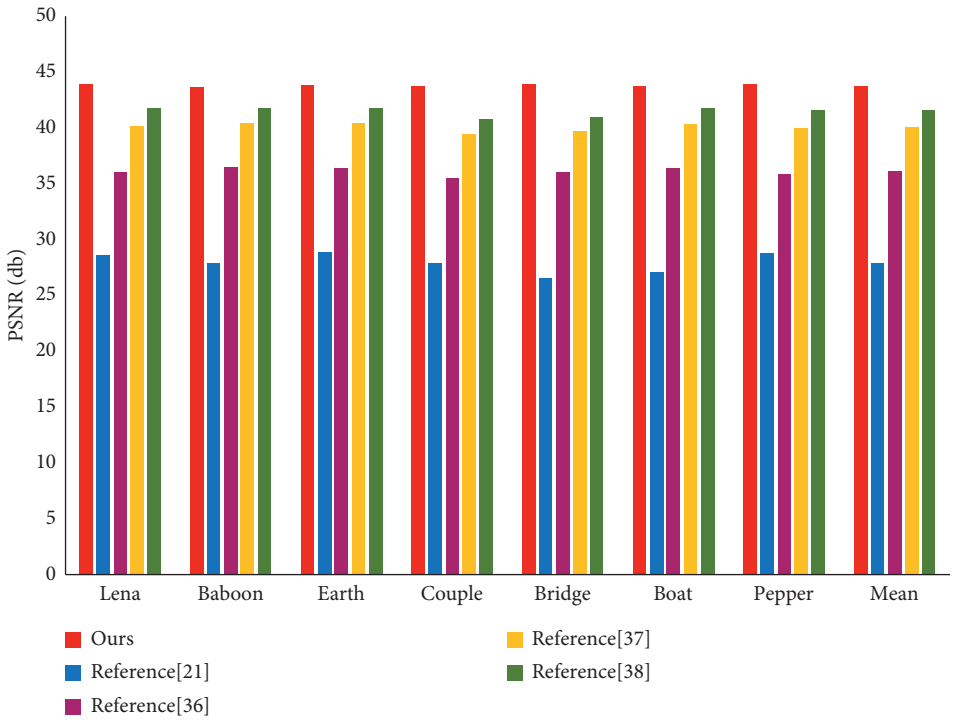


Figure 8: The bar chart of the PSNR.

Table 12: NPCR and UACI tests (average).

Image	Size	NPCR			UACI		
		Max	Min	Mean	Max	Min	Mean
Cameraman	256×256	99.6323	99.5804	99.6046	33.6808	33.2814	33.4338
Tree	256×256	99.6811	99.5514	99.6181	33.5978	33.3407	33.4933
Boat	256×256	99.6582	99.5682	99.6159	33.6314	33.4374	33.5430
Lena	512×512	99.6235	99.5991	99.6091	33.5194	33.4315	33.4732
Bridge	512×512	99.6204	99.5861	99.6073	33.5254	33.4237	33.4702
Couple	512×512	99.6315	99.5983	99.6150	33.5519	33.4054	33.4657
Boat	512×512	99.6300	99.6078	99.6175	33.5882	33.3520	33.4643

Table 13: Comparisons of NPCR and UACI.

Algorithms	NPCR	UACI
Ours	99.6125	33.4776
Reference [11]	99.60	33.48
Reference [17]	99.6395	33.3992

6. Conclusions

By using DWT and Schur decomposition, an asymmetric, visually meaningful image encryption scheme was described in this study. A secret image was embedded into another cover image to effectively hide the secret image and fully realize visually meaningful image encryption. In our method, the asymmetric encryption algorithm RSA was chosen to solve the key management and distribution problems caused by the symmetric encryption structure. Moreover, the plain image feature was extracted from our encryption scheme and used in the image encryption process to select the random sequence. This can effectively resist the chosen plaintext and known plaintext attacks. Schur decomposition was employed on the preencrypted image to embed the secret image into a cover image within its DWT domain that made the final visual cover image more imperceptible with an increased NC value.

In the future work, due to the large redundancy of the image, compressive sensing technology is suggested and applied into the image encryption algorithm. As a result, we do not need to process every pixel in the process of encryption. By using compressive sensing technology to compress and encrypt the image, it can improve the speed and effect of encryption effectively. However, it will also lead to much time cost to reconstruct the image. So, there are still a lot of works that should be considered in the future.

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

References

[1] J. Yang, M. Fan, and G. Wang, "Encryption scheme with mixed homomorphic signature based on message authentication for digital image," *The Journal of Supercomputing*, vol. 76, no. 2, pp. 1201–1211, 2020.

[2] S. Khan, L. Han, Y. Qian, H. Lu, and S. M. Jiao, "Security of multimedia communication with game trick based fast, efficient, and robust color-/gray-scale image encryption algorithm," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, Article ID e4034, 2021.

[3] A. A. Mohammad, A. Al-Haj, and M. Farfoura, "An improved capacity data hiding technique based on image interpolation," *Multimedia Tools and Applications*, vol. 78, no. 6, pp. 7181–7205, 2019.

[4] S. Y. D. Nezhad, N. Safdarian, and S. A. H. Zadeh, "New method for figureprint images encryption using DNA sequence and chaotic tent map," *Optik*, vol. 224, Article ID 165661, 2020.

[5] B. Wang, B. F. Zhang, and X. W. Liu, "An image encryption approach on the basis of a time delay chaotic system," *Optik*, vol. 225, Article ID 165737, 2021.

[6] A. Firdous, A. ur Rehman, and M. M. Saad Missen, "A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2," *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 24809–24835, 2019.

[7] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyperchaotic system," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2333–2356, 2016.

[8] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, Article ID 107484, 2020.

[9] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *International Journal of Bifurcation and Chaos*, vol. 29, no. 9, Article ID 1950115, 2019.

[10] K. A. K. Patro and B. Acharya, "A novel multi-dimensional multiple image encryption technique," *Multimedia Tools and Applications*, vol. 79, no. 19-20, pp. 12959–12994, 2020.

[11] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.

[12] R. Ponuma and R. Amutha, "Encryption of image data using compressive sensing and chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11857–11881, 2019.

[13] C. Wu, Y. Wang, Y. Chen, J. Wang, and Q.-H. Wang, "Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain," *Optics Communications*, vol. 431, pp. 203–209, 2019.

[14] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated fourier Transforms," *Optics Letters*, vol. 35, no. 2, pp. 118–120, 2010.

[15] C. Wu, K.-Y. Hu, Y. Wang, J. Wang, and Q.-H. Wang, "Scalable asymmetric image encryption based on phase-truncation in cylindrical diffraction domain," *Optics Communications*, vol. 448, pp. 26–32, 2019.

[16] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017.

[17] 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, 2020.

[18] S. K. Rajput and N. K. Nishchal, "Image encryption based on interference that uses fractional Fourier domain asymmetric keys," *Applied Optics*, vol. 51, no. 10, pp. 1446–1452, 2012.

[19] E. Kumari, S. Mukherjee, P. Singh, and R. Kumar, "Asymmetric color image encryption and compression based on discrete cosine transform in Fresnel domain," *Results in Optics*, vol. 1, Article ID 100005, 2020.

[20] G. Ren, J. Han, J. Fu, and M. Shan, "Asymmetric image encryption using phase-truncated discrete multiple-parameter fractional Fourier transform," *Optical Review*, vol. 25, no. 6, pp. 701–707, 2018.

[21] L. Bao and Y. Zhou, "Image encryption: generating visually meaningful encrypted images," *Information Sciences*, vol. 324, pp. 197–207, 2015.

[22] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Processing*, vol. 134, pp. 35–51, 2017.

[23] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Processing*, vol. 155, pp. 218–232, 2019.

[24] M. Yousefi Valandar, M. Jafari Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimedia Tools and Applications*, vol. 78, pp. 9971–9989, 2019.

[25] P. Ping, J. Fu, Y. Mao, F. Xu, and J. Gao, "Meaningful encryption: generating visually meaningful encrypted images by compressive sensing and reversible color transformation," *IEEE Access*, vol. 7, pp. 170168–170184, 2019.

[26] M. Fakhredanesh, M. Rahmati, and R. Safabakhsh, "Steganography in discrete wavelet transform based on human visual system and cover model," *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 18475–18502, 2019.

[27] R. Ponuma, R. Amutha, S. Aparna, and G. Gopal, "Visually meaningful image encryption using data hiding and chaotic compressive sensing," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 25707–25729, 2019.

[28] C. Pan, G. Ye, X. Huang, and J. Zhou, "Novel meaningful image encryption based on block compressive sensing," *Security and Communication Networks*, vol. 2019, Article ID 6572105, 2019.

[29] 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, 2020.

[30] L. D. Singh and K. M. Singh, "Visually meaningful multi-image encryption scheme," *Arabian Journal for Science and Engineering*, vol. 43, pp. 7397–7407, 2018.

[31] S. Vaidyanathan, A. Sambas, M. Mamat, and W. Mada Sanjaya, "A new three-dimensional chaotic system with a hidden attractor, circuit design and application in wireless mobile robot," *Archives of Control Sciences*, vol. 27, no. 4, pp. 541–554, 2017.

[32] K. A. K. Patro, B. Acharya, and V. Nath, "Secure multilevel permutation-diffusion based image encryption using chaotic and hyper-chaotic maps," *Microsystem Technologies*, vol. 25, no. 12, pp. 4593–4607, 2019.

[33] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *Journal of Information Security and Applications*, vol. 52, p. 102470, 2020.

[34] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Optics and Lasers in Engineering*, vol. 80, pp. 1–11, 2016.

[35] X. Wu, B. Zhou, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enchanced chaotic tent maps," *IEEE Access*, vol. 99, pp. 6429–6436, 2017.

[36] A. Kanso and M. Ghebleh, "An algorithm for encryption of secret images into meaningful images," *Optics and Lasers in Engineering*, vol. 90, pp. 196–208, 2017.

[37] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. Amin Sheikh, "Visual meaningful encryption scheme using intertwinning logistic map," in *Proceedings of the SAI 2018: Intelligent Computing*, pp. 764–773, London, UK, September 2018.

[38] J. O. Armijo-Correa, J. S. Murguía, M. Mejía-Carlos, V. E. Arce-Guevara, and J. A. Aboytes-González, "An improved visually meaningful encrypted image scheme," *Optics & Laser Technology*, vol. 127, Article ID 106165, 2020.