Hindawi
Advances in Mathematical Physics
Volume 2021, Article ID 7511245, 12 pages
https://doi.org/10.1155/2021/7511245

Research Article

Image Processing Method Based on Chaotic Encryption and Wavelet Transform for Planar Design

Yiying Liu[1] **and Young Chun Ko**[2]

[1]*College of Art, Hunan City University, Yiyang, Hunan 413000, China*
[2]*Department of Teaching Profession, Sehan University, Chonnam 58447, Republic of Korea*

Correspondence should be addressed to Young Chun Ko; ycko@sehan.ac.kr

Received 24 September 2021; Revised 15 October 2021; Accepted 16 October 2021; Published 31 October 2021

Academic Editor: Miaochao Chen

This paper provides an in-depth study and analysis of image processing for graphic design through chaotic encryption combined with a wavelet transform algorithm. Firstly, the traditional Mallat algorithm is optimized; since the mean value of the transform coefficients generated after the wavelet transform of the image is used as the initial value of the chaotic system to iterate, when the image is modified, then the mean value of the wavelet coefficients will also change, and the final iteration comes out as two different sequences using the property that the chaotic system is extremely sensitive to the initial conditions, so the algorithm has a certain sensitivity to tampering and localization effect. The image of the encrypted graphic design is decrypted by the chaos decryption system, and the final image information of the graphic design is obtained. In terms of the security of the graphic design image itself, the complex dynamical properties of chaos are fully utilized to encrypt it, and the algorithm has a good encryption effect after statistical characteristic analysis, attack complexity, difference analysis, adjacent pixel correlation analysis, and key sensitivity analysis. The plaintext image is decomposed in odd-even sequence using the boosting algorithm to get the sequence with an even index and the sequence with an odd index; then, the diffusion algorithm is applied to the two sequences by the prediction and update algorithm, and this process is repeated many times to get the two ciphertext sequences after scrambling, merging these two sequences, and matrixing them to get the ciphertext image. Finally, the testing of the embedded planar designed image revolves around four aspects, namely, image processing, tamper sensitivity, robustness, and imperceptibility, to examine the designed planar designed image system. In the diffusion manipulation, the key matrix for diffusion is obtained using the threshold processing method of the Local Binary Pattern (LBP) algorithm for the matrices generated by the Logistic Chaos system, which improves the randomness of the algorithm. The experimental results verify the effectiveness and security of the algorithm.

1. Introduction

In the development of the information society in recent years, the rapid development of network and cloud computing technologies has provided a convenient means for people to access and share multimedia data, such as documents, images, and videos, via the Internet. Digital images have evolved into the most common and critical information carriers in the digital information system and modern communications because of their ability to represent information visually and graphically. For example, life photos taken by people with digital devices, electronic medical images for medical treatment of diseases, images of the earth taken by satellites, and electronic photos used in criminal investigations are all related to images [1]. However, the inherent contradiction between the limitation of network bandwidth and storage space and the huge amount of image data, as well as the contradiction between the open environment of the network and the privacy protection of image information, presents a challenge for us [2]. To meet the efficient and secure transmission and storage of images on the Internet, preventing image information leakage to protect private data and compressing image data to save network bandwidth have become urgent issues to be solved. A practical

solution to prevent the leakage of digital image information for secure transmission and storage is to encrypt the image information.

At this stage, the imaging technology of digital graphic design can effectively protect the intellectual copyright of digital products; standing in the technical analysis, the imaging technology of digital graphic design is an information hiding measure, which involves the knowledge of cryptography [3]. In the field of cryptography, some researchers are actively analyzing the plaintext encryption technique; by using this technique, the original information is protected. Encryption techniques can provide some protection during the storage and transmission of data, but they cannot protect multimedia digital products during processing; in other words, when a user is using a multimedia product, it is required that the product is in a decrypted state, but if the product is already decrypted, it is difficult to provide effective protection [4]. Information hiding studies how to hide secret information in public information, and it can be subdivided into steganography and image techniques for digital graphic design. Steganography focuses on hiding the existence of information [5]. The compression of the digital video signal is based on the above two conditions, which makes the amount of video data to be greatly compressed, which is beneficial for transmission and storage. General digital video compression coding methods are hybrid coding, i.e., a combination of transform coding, motion estimation and motion compensation, and entropy coding for compression coding. Typically, transform coding is used to remove intraframe redundancy, motion estimation, and motion compensation to remove interframe redundancy, and entropy coding to further improve the efficiency of compression. Cryptography does not hide the existence of information; the attacker knows the existence of secret information, which is an essential difference between cryptography and steganography. The imaging technology of digital graphic design allows some hidden information to be written into the digital product, but of course, for added security, private information is usually encrypted as well, thus achieving copyright protection. A chaotic system is a nonlinear system with characteristics such as ergodicity and initial parameter sensitivity, which makes a natural connection between a chaotic system and cryptography. Therefore, the application of chaotic systems to encryption algorithms will improve the encryption performance. In addition, with the advent of the era of big data, the volume of image data is increasing, and both compression and encryption are needed during image transmission and storage; otherwise, it will increase the pressure of data transmission and storage. Compressive sensing (CS), as a new sampling theory, can achieve simultaneous compression and encryption for signals, so combining compressive sensing with image encryption is also a hot spot in information security research and has good application prospects.

Many image encryption algorithms have been designed by some scholars using chaotic systems and compression perception, which can secure images to some extent, but these encryption schemes have a common drawback that the resulting noise-like or texture-like ciphertext images can easily attract the attention of hackers during transmission or storage and then be focused on. If we make the ciphertext image visually secure, i.e., the ciphertext image acquires a meaningful appearance, then the ciphertext image will be more secure. The password text box is similar in appearance to the single-line text box, and both have the same properties (value, size, maxlength, etc.). However, they are fundamentally different: the characters entered in the single-line text box are visible, while the characters entered in the password text box are not seen. Therefore, it is important to design visually secure image encryption algorithms for image data security and appearance security. Compared to traditional textual information, digital images contain a larger amount of data and there is more redundant information in image information, such as spatial redundancy due to correlation between adjacent pixels of an image and temporal redundancy due to correlation between different frames in an image sequence. The purpose of image compression is to minimize the number of bits required to represent the image data by removing this redundant information, and the receiver can effectively recover the original image. With the rapid development of visual communication, multimedia communication, and other services, the image data that needs to be processed has grown tremendously, and the huge amount of data has a very high demand on storage resources and network bandwidth, so it is necessary to compress the image data effectively. Two common operations of image encryption are obfuscation and diffusion. Obfuscation means disrupting the original position of pixel values in a two-dimensional matrix, while diffusion means that a small change of one-pixel value in the original image can lead to a huge change of pixel values in the whole image. Commonly used obfuscation methods are sorting, circular shift, Arnold transform, phantom square transform, etc., by using different principles to achieve the purpose of changing the pixel positions.

2. Current Status of Research

Digital images have been widely used in various application areas such as military, financial, legal, and medical, where the requirements for image security are getting higher and higher [6]. This section analyzes and compares the current state of research on digital image encryption techniques, focusing on the advantages and shortcomings of digital image encryption algorithms based on chaotic systems, and finally discusses the application of chaotic image encryption techniques in medical image encryption. Preprocessing is required in encrypting images, converting the two-dimensional image pixel matrix into a one-dimensional stream of plaintext data, and then applying the corresponding algorithm to encrypt under the control of the key and restore it to the original image when decrypting [7]. The advantage of this type of cryptographic algorithm is that the algorithm is open, and the disadvantage is that it is inefficient, so it is often used in combination with other encryption techniques [8]. Shankar et al. proposed a satellite image encryption algorithm based on chaos and AES techniques [9]. The algorithm first uses Arnold cat mapping to permute

the image pixels and then uses Henon chaos mapping for generating a random sequence for the AES algorithm. Finally, the image is encrypted using the AES algorithm [8]. The algorithm improves the key sensitivity and has a large key space and uniform pixel distribution, and the encryption speed is within the acceptable range to ensure high security. Image scrambling has a limited number of transformations of the matrix of the image, which is periodic and reverts to the original image after several transformations [10]. The mathematical description corresponding to chaotic systems has no analytic solution, which means that the end position cannot be calculated directly by inputting initial values and time but can only be approximated continuously by iteration, but the approximation is never exact. Chaotic systems have the characteristic of significantly amplifying errors. Therefore, the results obtained when the input data are not precise can vary widely. If an attacker obtains the ciphertext and performs the same operation on the ciphertext a limited number of times, the original image can be easily cracked. In addition, the histogram of the ciphertext does not change after image scrambling encryption, and the attacker can get a lot of useful information by statistically analyzing the histogram of the ciphertext. Encryption by image pixel disruption alone is simple and fast, but not very secure, so it needs to be used in combination with other methods [11].

The algorithm states that if some non-bandwidth-limited signal contains only a finite number of pulses, then the entire Fourier transform of that signal can be reconstructed with high fidelity by its partial Fourier transform slice. Malik's algorithm essentially works by seeking the minimum norm of these finite Fourier measurements, which is analogous to the underdetermined recovery algorithm in CS theory [12]. The gradual emergence of reconciliation analysis and function approximation theory in the following decades also provided strong theoretical support for CS. The goal of this direction is to approximate or reconcile more complex objective functions by various combinatorial, linear transformations using several structurally simple basis (meta) functions while keeping some measurement errors as small as possible [13], for example, from the first well-known Fourier series and analysis with sine and cosine functions as basic functions to various wavelet basis functions as metafunctions to approximate function spaces of various shapes and sizes to the later proposed types of super wavelets with more scales and directions (e.g., ridge let, contourlet, and surface) to approximate functions containing function spaces with higher-order "singular" properties [14].

The obtained ciphertext image is visually secure, and a meaningful ciphertext image is not easily found by attackers when transmitted and stored over the Internet compared to current noise-like or texture-like ciphertext image; gaining security in image appearance and using compression perception technique, the size of the obtained ciphertext is equal to the size of the plaintext image and no additional storage space and transmission bandwidth is required. Finally, a visually secure ciphertext image of the same size as the plaintext image is obtained to achieve image appearance security and data security, and the use of two-dimensional compression perception reduces the amount of data in the encrypted image so that the size of the ciphertext obtained is smaller, which reduces the running time of the algorithm to a large extent and saves transmission bandwidth and storage space significantly. In this paper, we choose to embed the parameters associated with the plaintext into the carrier image, and the key parameters are transmitted directly to the receiver along with the visually secure ciphertext image, which avoids the waste of resources caused by additional transmission when large batches of images are encrypted simultaneously, greatly saves transmission bandwidth and storage space, and improves the security of this algorithm to a large extent.

3. Image Processing Analysis of Chaotic Encryption and Wavelet Transform Planar Design

3.1. Chaotic Encryption and Wavelet Transform Image Algorithm Design. With the rapid development of digital technology, more multimedia information is being generated and proliferated among the network. Among them, digital images carry private information that can be decrypted in some unauthorized ways, so the private information in them needs to be protected or encrypted. Among many features of discrete-time chaotic systems, the two features of positive Lie exponents and orbit global boundedness are a widely used chaos criterion nowadays [15]. Chaos is a deterministic, stochastic-like process that occurs in nonlinear dynamical systems and has a very sensitive dependence on the initial value. In the time domain, chaotic systems obtain sequences that resemble random sequences with a relatively weak correlation. Therefore, generating chaotic systems, i.e., chaotic inverse control or classification, for the field of cryptography is a very important topic. Selecting chaotic systems that satisfy the cryptographic properties is also the primary key issue in securing chaotic encryption. Force encryption of documents is edited by a specified program. Users accessing encrypted documents need to be connected to the server (online, not offline) and have the appropriate access rights. This encryption process is completely transparent and does not affect existing applications or user habits. Additional access control can be implemented through share, offline, and outbound management.

Hyperchaotic systems are a special class of chaotic systems with corresponding two or more positive Lyapunov exponents, which generate chaotic sequences controlled by more parameters and initial values than ordinary chaotic systems and therefore have better stochasticity and unpredictable dynamic behavior. From the point of view of attack resistance, there are significant advantages of hyperchaos over low-dimensional as well as three-dimensional chaos. Sequential cryptography is a text encryption method in which an encryption key is applied to individual binary digits of a data stream along with an algorithm that processes one bit at a time. This method is less commonly used in modern cryptography, and its main alternative is packet cipher, in which the key and algorithm are applied to blocks of data in the data stream instead of individual bits. It is

difficult to rely on deciphering to obtain the plaintext before encryption using more applied schemes such as spectral analysis, autocorrelation analysis, and regression mapping. Due to the multidimensional space, hyperchaotic systems can generate a larger number of sequences for encryption at the same time, thus increasing the efficiency of the operation. It is because hyperchaos has these advantages that its research has received increasing attention in recent years. In this chapter, we study and analyze the theory, construction, and dynamical behavior of hyperchaos and construct a new five-dimensional hyperchaotic system based on the specific need of generating chaotic mappings that satisfy cryptographic properties to be applied to the field of cryptography. Compared to some classical hyperchaotic systems, the generated new five-dimensional hyperchaotic system has a relatively higher Lyapunov exponent, so the chaotic behavior is more obvious:

$$\begin{cases} \dot{x} = hy + ax - yz, \\ \dot{y} = hx + by + xz, \\ \dot{z} = dz - xy. \end{cases} \tag{1}$$

For the above avalanche scenarios, there are many countermeasures, but there is no one-size-fits-all model that can cope with all scenarios. There are different solutions for different scenarios, respectively. Resource isolation usually means using different thread pools for different service calls. Fast failure of unavailable service calls is generally achieved through timeout mechanisms, fusers, and postfuse downgrade methods. The diffusion operation is to change the pixel values of the plaintext image to make the relationship between the plaintext and the ciphertext more complex. Usually, also the sequence of the output of the chaotic system and the plaintext image is used to perform the dissimilarity operation for diffusion purposes. Due to the high correlation between image pixels, it is less secure to perform only one of the two operations, dislocation or diffusion, on the image. Currently, it is most common to use chaotic systems to take dislocation and diffusion operations on images and even achieve multiple dislocation and diffusion to improve the security level of the algorithm, as shown in Figure 1.

Because the chaos-aware operator can be controlled and reproduced by a deterministic chaotic system, and its elements have similar randomness as random variables, achieving the unity of determinism and randomness, the chaos-aware operator has the following advantages [16]. First, because the chaotic sequence is pseudorandom, the chaos-aware operator is uncorrelated with most sparse domains, so the chaos-aware matrix and the random operator are both "universal." Second, the chaos-aware operator can be easily generated and controlled by deterministic systems, so it is very hardware-friendly. Furthermore, the elements of the chaos matrix are deterministic and reproducible, so in many applications, these elements can be computed dynamically without any storage, and the complexity of the algorithm is low. Finally, the chaos-aware matrix can also be considered a cryptographic operator, and thus, it is particularly popular in applications requiring high privacy and high security. The ciphertext feedback overcomes the drawback that the encryption algorithm is only related to the chaotic system and the key independent of the plaintext, overcoming the problem pointed out and making the encryption security further improved. The insertion only allows the diffusion of changes in each pixel of the plaintext image to affect as many ciphertext pixels as possible, giving the algorithm good diffusion and chaos characteristics and enhancing the resistance to various attack methods:

$$\Delta(x)_p = \sup\{\|x + F(A(x))\|\}. \tag{2}$$

It is well known that the analog world and the digital space are freely transformed by sampling operations. It is the sampling transformation that enables humans to use a wide range of digital devices to solve problems and to perceive and understand the world:

$$N(j) = <x, \varphi_j> - \varepsilon_j, \tag{3}$$

$$x(x) = \lim_{M \longrightarrow \infty} \sum_{j}^{M} N(j) \cos\left(\frac{ct}{T} + j\right). \tag{4}$$

The DWT transformation of discrete wavelets in an image I seems to be able to implement multiresolution processing on it; in the study, the author implements wavelet decomposition on me with the transform of two-dimensional discrete wavelets to obtain subbands of images with different frequencies and spaces. The low-frequency subbands can be further decomposed into a new layer of low-frequency signals and high-frequency signals:

$$I' = \left\{\left\{I^{ll2}, I^{lh2}, I^{hl2}, I^{hh2}\right\}, I^{ll2}, I^{lh2}, I^{hl2}, I^{hh2}\right\}. \tag{5}$$

Among these encryption algorithm classifications, the stream encryption algorithm technique is less secure than the group encryption technique, so group encryption is more widely used. Symmetric encryption has an advantage in terms of efficiency, but the security of asymmetric encryption techniques is higher than that of symmetric encryption techniques, and asymmetric encryption is rarely used to encrypt large amounts of data due to its high computational effort and slow speed:

$$I_{m,d}(i,j) = \begin{cases} I_{m,d}(i,j) - a_{m,d}(T_{m,d}(i,j) - w_v(i,j), \\ I_{m,d}(i,j), \end{cases} \tag{6}$$

$$a_{m,d} = \begin{cases} \sqrt{3}, \\ 2. \end{cases} \tag{7}$$

Design and implement an image encryption algorithm security evaluation system and a medical image encryption algorithm security analysis platform, including two parts:

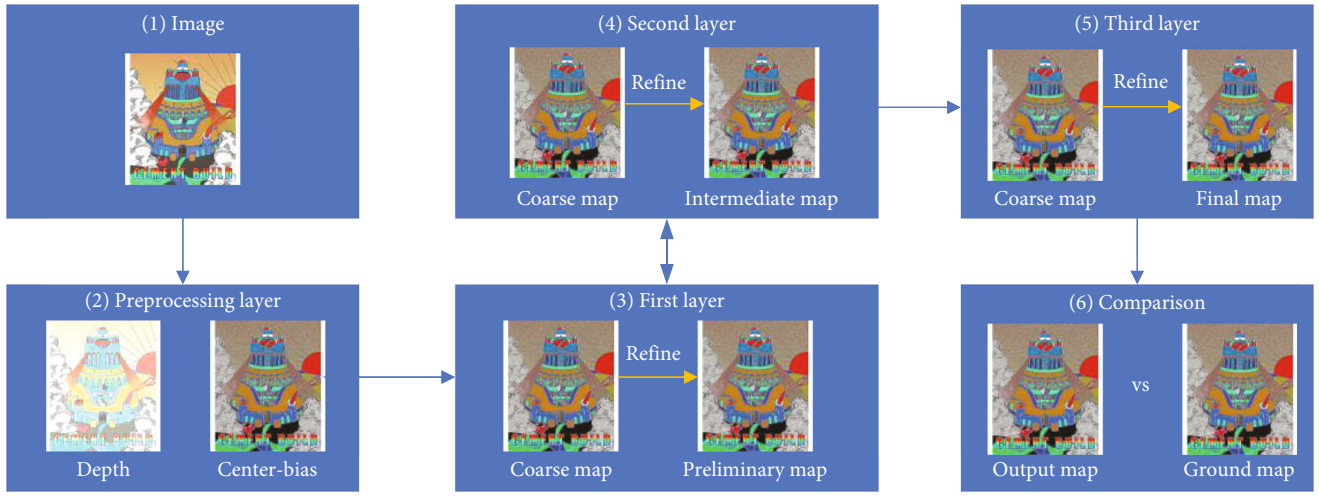

Figure 1: Framework of chaotic encryption and wavelet transform image algorithm.

an encryption algorithm implementation platform and an encryption algorithm comparison and evaluation platform [17]. The developed system can compare several metrics of image encryption algorithms: such as histogram, key space, key sensitivity, correlation of pixel points, differential attack, information entropy attack, and encryption and decryption time, horizontally and vertically with other different image encryption algorithms, to form a comprehensive and objective evaluation. The developed system allows both the calculation of various performance metrics and a preview of the effect of individual image encryption algorithms, as well as a comprehensive comparison and security evaluation of different image encryption algorithms.

As can be seen from the schematic diagram of chaotic encryption, chaotic synchronization is the key to the ability to accurately recover the transmitted plaintext signal. The chaotic sequence generated by the sender is determined by the equations, parameters, and initial conditions of the nonlinear system; therefore, the same chaotic system as the sender can be constructed at the receiver by setting the same system parameters and initial conditions, thus achieving synchronization, as shown in Figure 2.

Chaotic encryption methods conform to the requirements of modern cryptography and belong to the symmetric encryption regime. The security of this encryption regime depends on the degree of approximation of the keystream generated by the chaos generator to the random numbers, the better the randomness of the keystream the higher the security, and vice versa, the lower the security. The research based on chaotic encryption methods focuses on how to improve the randomness of chaotic keystreams and the reliability of chaotic synchronization:

$$x_{n+1} = \mu x_n (1 + x_n). \tag{8}$$

Within the chaotic attraction domain of a chaotic system, the chaotic motion is all-state ergodic, and the trajectory of the system traverses all state points within the chaotic attraction domain at each time:

$$\lambda = \lim_{n \longrightarrow \infty} \frac{1}{n} \sum_{i=0}^{n} \lg \left| f'_{x_i} \right|. \tag{9}$$

The next discretization is carried out for continuous chaotic systems and hyperchaotic Lorenz systems, using the classical fourth-order Loner-Kutta method:

$$y' = f(x, y). \tag{10}$$

However, in areas such as channel analysis, distributed radar imaging, and multichannel medical imaging, one often must solve multisignal joint and distributed information sensing tasks [18]. One can solve these multisignal vector sampling problems by solving the problem defined in a solver style multiple time. However, there is always a desire to achieve the multimeasurement vector CS problem at a lower cost by exploiting the correlation properties between the interiors of these multiple signals. For this situation, the joint sparse model (JSM), also known as the multimeasurement vector model, has been proposed:

$$\sum_{s} x = \left\{ X : \lim_{n \longrightarrow \infty} \frac{1}{n} \sum_{i=0}^{n} \lg \left| f'_{x_i} \right| \right\}. \tag{11}$$

The Lyapunov index quantifies the average rate of convergence and divergence of the chaotic sequence in the state space. The Kolmogorov entropy characterizes the rate of information loss of the system along the chaotic attractor. In addition, the dimensionality characterizes the geometric structure of the chaotic attractor. It is known that the trajectory of a deterministic dynamical system is unique, i.e., given an initial

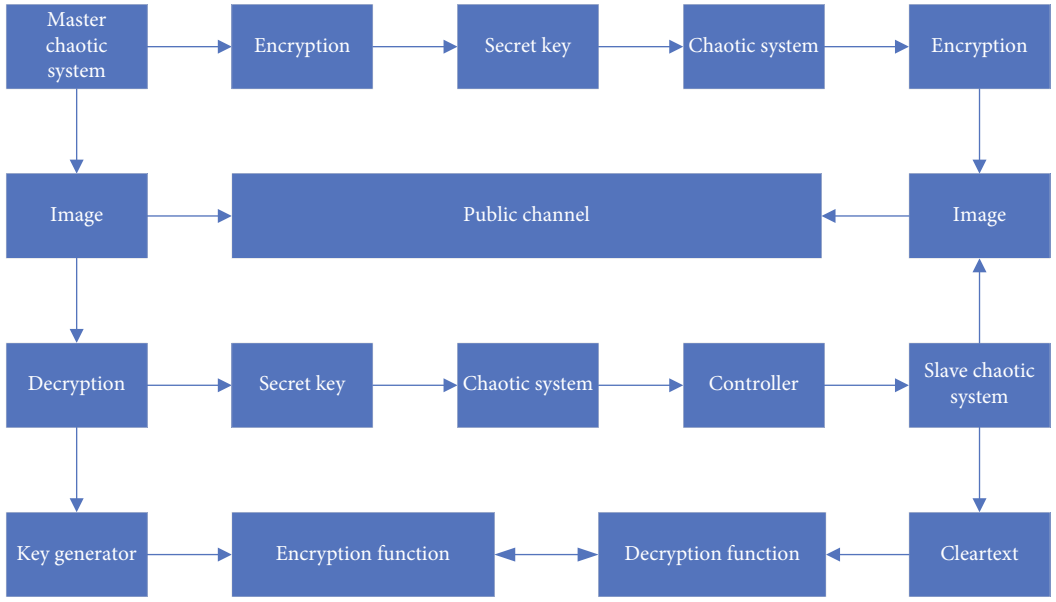

Figure 2: Chaotic encryption and decryption schematic.

state, its "next" state is determined accordingly. Therefore, if the same initial state is input to a deterministic system, then its output must follow the same trajectory into the state space. It is with this feature that one can achieve a preestimate of the system state if one has the initial value. The main purpose of image preprocessing is to eliminate irrelevant information from images, recover useful and true information, enhance detectability of relevant information, and maximize data simplification, thus improving the reliability of feature extraction, image segmentation, matching, and recognition.

3.2. Graphic Design Graphic Processing Design. Various chaos-based image encryption schemes have been proposed, as digital image encryption techniques have become a hot issue in the field of information security. The cryptographic flow for encryption is mainly generated by chaotic systems, and the encryption structure used in cryptosystems is mainly the "dislocation-diffusion" structure. The advantage of this structure is that, on the one hand, the correlation between adjacent pixels in the original image is reduced by the scrambling operation; on the other hand, the information of all pixels is mixed by the diffusion operation, so that the image information can be well hidden. However, the "scrambling-diffusion" structure also has disadvantages, one of which is that the simple scrambling operation has little security; second, when the number of cycles of scrambling-diffusion is small, it is vulnerable to selective or known-plaintext attacks, while when the number of cycles is high, the speed of encryption is significantly reduced. Many classical chaotic image encryption systems rely only on key encryption and the encryption process is independent of the plaintext image, which indicates to some extent that the key factor of encryption depends on the key and the encryption algorithm [19]. Cryptosystems relying only on key encryption may be subject to selection and known-plaintext attacks, so systems based on chaotic image cryptosystems associated with plaintext have emerged one after another. In such systems, the cipher not only depends on the key but also is associated with the plaintext image, i.e., for different images, using the same key, different ciphertext sequences are also generated. To effectively solve the above problem, this chapter designs a novel image encryption structure based on plaintext-associative image cryptosystems.

However, as such structures are somehow flawed, when the number of loops is small, the image encryption process is vulnerable to selective plaintext attacks; when the number of loops is large, the time required for the image encryption process will increase significantly, as shown in Figure 3.

An avalanche effect is a common form of cryptanalysis that studies how differences in input information affect the output result and can be used to analyze encryption algorithms by comparing the change in the encrypted image before and after a specific information change. Some pixels change rate (NPCR) and uniform average intensity change (UACI) are two common metrics that can be used to evaluate the performance of image encryption algorithms in avalanche effect analysis:

$$\mathrm{NPCR} = \sum_{i,j} \frac{D(i,j)}{M \cdot N} \times 100\%, \tag{12}$$

$$\mathrm{UACI} = \sum_{i,j} \frac{|D(i,j) - D_2(i,j)|}{255 \times M \cdot N} \times 100\%. \tag{13}$$

When a low probability event occurs, that event carries more information than when a high probability event occurs. The amount of information conveyed by each event

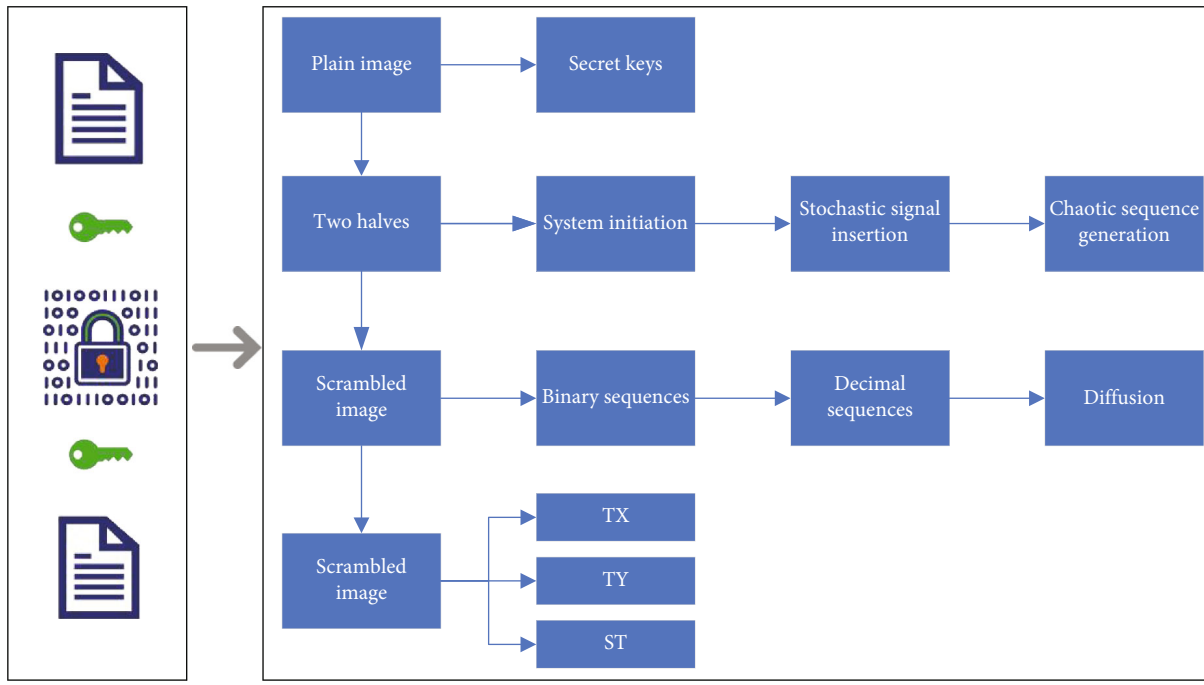

Figure 3: Image encryption system with plaintext correlation.

defined in this way becomes a random variable whose expectation is called the information entropy. The greatest uncertainty arises when the probability of an event occurring is uniformly distributed, in which case the information entropy is greatest:

$$H(x) = \lim_{N \longrightarrow \infty} \sum_{i=1}^{N} p(x_i) \lg p(x_i). \tag{14}$$

The weakness of Shannon entropy can be overcome by calculating the average value of Shannon entropy of multiple nonoverlapping image blocks randomly selected from the encrypted images. Thirty nonoverlapping image blocks were randomly selected from each encrypted image, and their Shannon entropy and local Shannon entropy were calculated [20]. The Shannon entropy and local Shannon entropy of the test images and their encrypted images are listed in Figure 4. From the results in Figure 4, the Shannon entropy of the test images is much smaller than the ideal value, while the Shannon entropy and local Shannon entropy of the encrypted images are close to the ideal value and meet the critical values at 5%, 1%, and 0.1% significance levels. Therefore, the encrypted images of the image compression and encryption algorithm proposed in this chapter are highly randomized. The hyperchaotic system generates the initial value parameters of the Lorenz hyperchaotic system and iteratively generates the keystream. To change the position and gray value size of the original image pixel points, the image is additive modulo diffusion to achieve the first hiding of image information. In order to realize the information of the plaintext pixel points to be diffused into the whole ciphertext image, the add-and-take mode diffusion algorithm needs to be looped twice. Finally, the final ciphertext image can be obtained. The experimental results prove that the image encryption scheme proposed in this study is effective and has strong resistance to attacks as well as key sensitivity.

Select plaintext attack is a common cryptanalysis attack mode in which an attacker can arbitrarily select plaintext and obtain the corresponding ciphertext. Based on the plaintext ciphertext pair, the attacker can try to obtain the key used in encryption. For a linear encryption system, the attacker can select the unit matrix as the plaintext input; then, the obtained ciphertext contains the whole encryption process of the encryption algorithm, and the attacker can potentially decrypt other ciphertexts and obtain the corresponding plaintext information based on this ciphertext. In the algorithm proposed in this chapter, a chaotic system is used to control the heterogeneous operation, which is a nonlinear process that can effectively scramble the information in the plaintext image. Also, the key used in the algorithm is related to the plaintext information, and it is almost impossible that the keys corresponding to different plaintext images are the same. In the selective plaintext attack, the attacker obtained a matrix that is garbled and related only to the plaintext input by the attacker, from which the key used in the algorithm in this chapter or a matrix equivalent to the encryption process cannot be deduced. Therefore, the image compression encryption algorithm proposed in this chapter is effective in resisting the selective plaintext attack.

During image transmission, encrypted images almost inevitably suffer from various noises and even loss of part of the image. The noise resistance of the encryption algorithm is measured by analyzing the quality of the decrypted image by artificially adding some noise to the encrypted

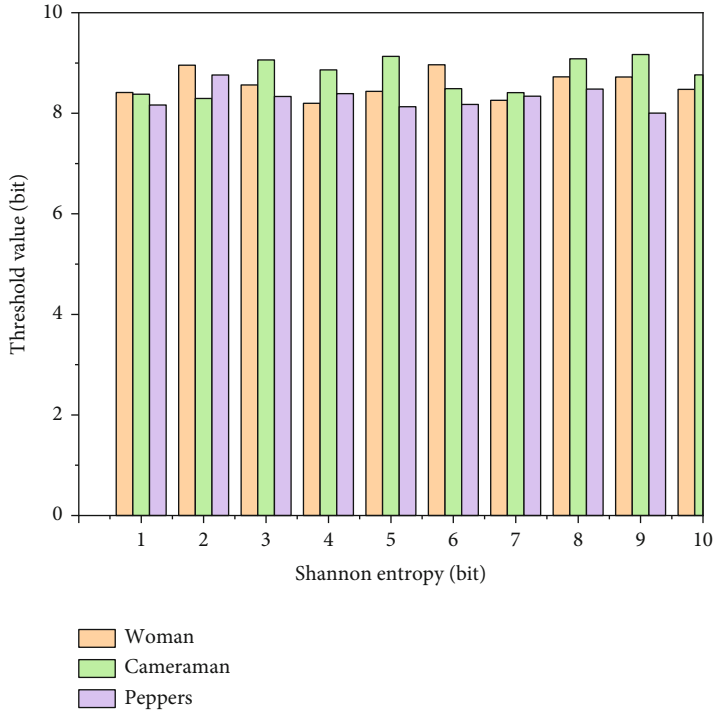

Figure 4: Shannon entropy and local Shannon entropy results.

image and acquiring the corresponding decrypted image using the exact correct key:

$$C' = C - gC. \tag{15}$$

In the past, the measurement matrix must be sent to the receiver for decryption, but we use the information of the plaintext image to design some key parameters to generate the measurement matrix, the sender only needs to send these key parameters to the receiver, and the receiver can get the same measurement matrix to recover the original image, which can save a lot of transmission bandwidth and storage space, and with different system parameters and initial values, different measurement matrix. And the chaotic system has the characteristics of being sensitive to parameters and initial values and good randomness, and the three-dimensional cat-mapped chaotic system is used to generate the measurement matrix, which can improve the security level of the encryption algorithm:

$$Q = \text{floor}\left(\left(I + I^2\right) \bmod 255\right) - 1. \tag{16}$$

Embedding 1 bit of information of the planar design image in each subband, considering the characteristics of HVS, the imperceptibility becomes worse if a larger amount of information is embedded. In the generation stage of the planar design image, the mean value of the wavelet transform coefficients of the four subbands of the chunk is used as the initial value of the chaotic system, and after the iteration of the chaotic system, the quantized generated 4-bit planar design image information must change if tampered, the mean value of the tampered wavelet transform coefficients, so the algorithm has a tamper detection mechanism. However, the existing means of understanding and decoding the chaos-aware matrix are still in a rudimentary stage and not very mature [21]. There are two main categories of mainstream encryption and decryption techniques: one is symmetric and the other is asymmetric. In simple terms, symmetric means that both parties exchanging messages use the same key, such as a fixed number of bits in a string. On the contrary, asymmetric has been exchanging messages between two parties using different keys, which is what we commonly see in asymmetric encryption and decryption algorithms where there are public and private keys. Most researchers are still at the stage of seeking new chaos-aware operators and their applications, rather than systematically analyzing and discussing strategies for designing and optimizing dense chaos-aware operators. For this reason, there is always a desire to find strategies to optimize dense chaos-aware operators more efficiently to further improve the theoretical study of chaos-aware operators. In addition, one of the current directions in this field is how to make existing chaos-aware matrices simpler and easier to map onto hardware imaging devices, especially in the era of "big data" where higher resolution and shorter imaging times are required.

4. Analysis of Results

4.1. Chaotic Encryption and Wavelet Transform Image Algorithm Results. For chaotic systems, on the one hand, the dissipative action of the dissipative dynamical system causes the kinematic trajectories to converge stably and form

attractors, which is a stabilizing action from a global point of view; at the same time, the actual problem of local instability in turn gives rise to the phenomenon of separation of the kinematic trajectories. As a result, the kinematic trajectories of the system fold and elongate infinitely, which gives rise to strange attractors. An attractor is said to be a strange attractor if its streamline depends sensitively on the initial value, as shown in Figure 5.

A pseudorandom sequence generator is constructed for subsequent cryptographic operations. When implementing a chaotic system on a finite precision computer, the chaotic mapping has a finite number of periodic orbits. At the same time, generating pseudorandom sequences using chaotic systems requires the sequences to be processed in a discretized manner. That discretization processing will also cause the period degradation problem of the sequence due to the limitation of computer accuracy. Therefore, the period degeneracy problem of chaos needs to be dealt with when designing a pseudorandom sequence generator. To solve this problem and improve the cryptographic properties of chaotic sequences, the LFSR and the hyperchaotic system are combined to generate pseudorandom sequences by perturbing the generation of hyperchaotic sequences with the LFSR with the help of the feature that the LFSR can generate sequences with sufficiently long periods. Within this scheme, the perturbation of the LFSR can guarantee the long period of the sequence and the hyperchaotic system can guarantee features such as attack resistance and randomness.

The algorithm implements encryption and user identity verification for common compressed image formats. First, the image file is loaded while the user identity verification file is generated based on the hyperchaotic system. To encrypt the image data, the image file needs to be preprocessed, i.e., decoded according to the specific image file format. Then, the decoded image data is encrypted using the dislocation diffusion method. To effectively balance security and efficiency, the encryption algorithm uses bidirectional diffusion. To increase the key space and improve the security, the algorithm uses a dynamic chunking dislocation method for the 3D baker based on the hyperchaotic system.

We calculate the information entropy of the ciphertext to evaluate the performance of the algorithm against statistical attacks, and the test results are shown in Figure 6. For JPEG, the plaintext data is stored assigned words and the individual values usually take values in the range -128-127. To improve security, we encrypt the lower 7 bits of each byte in the plaintext, so the ideal value of the estimated entropy of JPEG ciphertext is 7.

From the test results in Figure 6, for JPEG images, the information entropy is close to the ideal value 7, and for PNG images, the information entropy is close to the ideal value 8, which has a better encryption effect. For GIF images, since the total number of colors used in the image is limited, the information entropy of each of the red, green, and blue colors is a certain distance away from the ideal value 8, but the information entropy of the index sequence is close to the ideal value 8. Meanwhile, compared with the encryption of the Logistic equation, the classical encryption algorithm AES, the designed method is slightly better in terms of information entropy value. The test results show that the correlation coefficient of each component decreases significantly after encryption, and the correlation coefficient of the ciphertext is 10% or even less than that of the plaintext. The algorithm effectively reduces the correlation between adjacent pixels. From the results, our designed method is better than the method of Logistic equation and the classical symmetric cipher algorithm.

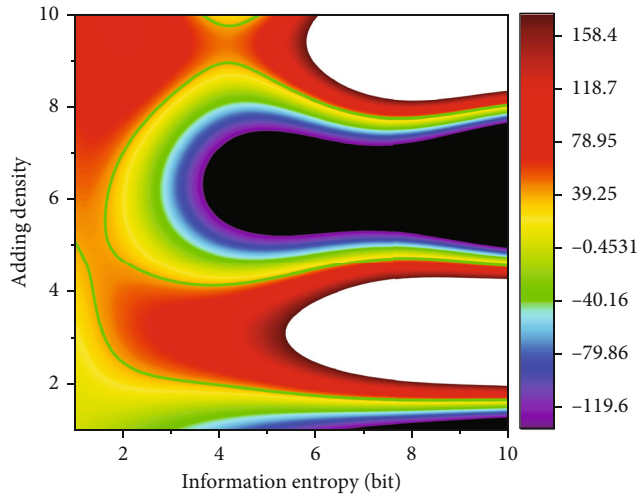

Figure 5: Phase point trajectory diagram for the hyperchaotic system.

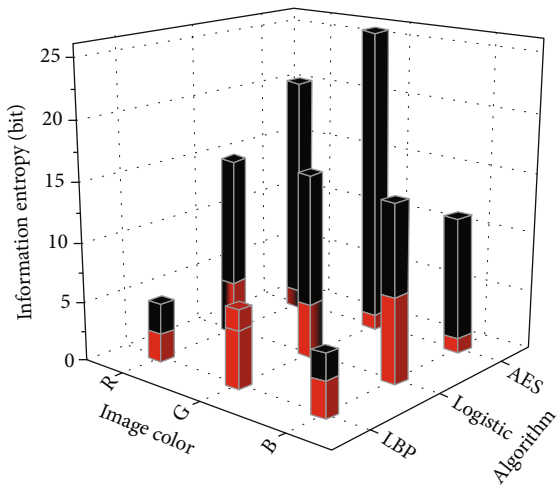

Figure 6: Comparison of information entropy.

The limitation of computer accuracy has made low-dimensional chaotic systems prone to performance degradation problems, which affects the security of encryption. Compared with low-dimensional chaotic and three-dimensional chaotic systems, hyperchaotic systems have obvious advantages in terms of resistance to attacks. Meanwhile, the property of hyperchaotic systems to generate multiple sequences in one iteration can effectively improve the generation efficiency of pseudorandom sequences. Based on these, this chapter generates a new five-dimensional hyperchaotic system based on the Rabinovich system by adding two-state feedback controllers to the Rabinovich system and correlates its Lyapunov exponent,

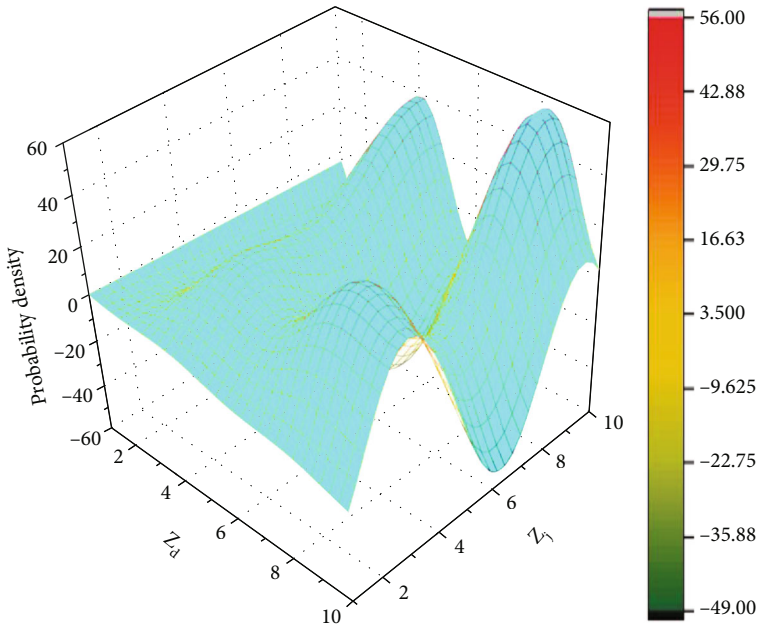

Figure 7: Lyapunov exponent and joint probability density function.

dissipative, and other related dynamical behaviors. Compared with some classical hyperchaotic systems, the new five-dimensional hyperchaotic system has a higher maximum Lyapunov exponent and has a more desirable use in cryptography.

4.2. Experimental Results of Graphic Design Graphic Processing. To address the problem that traditional binary perception matrices have the limitation of the number of rows or columns while real-valued chaotic perception matrices still have densities, this chapter proposes to construct binary chaotic perception operators using bipolar chaotic sequences generated by chaotic systems and use them in image compression sampling and design an image compression sampling algorithm based on bipolar chaotic perception matrices. Specifically, we first introduce the asymmetric threshold function method that allows multiple one-dimensional chaotic systems to generate bipolar chaotic sequences. Subsequently, these generated bipolar sequences are used to efficiently construct information-aware operators of arbitrary dimensionality. In particular, the constructed bipolar chaos-aware operators are not limited by the dimensionality of rows and columns and satisfy near-optimal sampling efficiency in terms of both bounded equidistantness and autocorrelation. In addition, the specificity of the elements makes the bipolar chaos-aware operator uniquely advantageous in terms of memory overhead, computational complexity, and hardware implementation. Therefore, the ICS algorithm based on the bipolar chaos perception operator can efficiently ensure its information perception capability, effectively overcome the shortcomings of similar image compression sampling algorithms, and bring the numerous advantages of the bipolar chaos perception operator, as shown in Figure 7.

In the encryption process, the compressed encryption of plaintext images of different sizes takes almost the same amount of time and takes very little time, about 20-40% of the total encryption time. However, the time used for the LSB embedding process is more, about 60-80% of the total encryption time. This indicates that as the image size increases, increased time is used for LSB data embedding and the relative proportion of time used for compressed encryption decreases; this is because as the image size gets larger, the amount of data to be embedded becomes larger. In the decryption process, the time used to extract plaintext images of different sizes is almost the same, accounting for about 20-25% of the total decryption time, and the time used for the reconstruction process accounts for about 75-80% of the total decryption time. However, the extraction time for ciphertext images of size 1024×1024 is about 6% of the total decryption time; the reconstruction process is about 94% of the total decryption time. This means that the larger the image size, the more time is spent on reconstruction, and the relative time spent on ciphertext extraction decreases. Thus, our proposed encryption scheme is suitable for small- and medium-size images, and the time complexity is very high when the image size is large. So, in the following work, we will plan to use 2-D compressed sensing (2-D CS) instead of compressed sensing (CS) to reduce the computational complexity and shorten the encryption and decryption time, as shown in Figure 8.

For the four chaotic systems, as the compression rate CR increases, the corresponding PSNR values also increase. At the same compression rate, the PSNR values of the chaotic system using Logistic-Sine (LSS) are higher than the other three chaotic systems when the measurement matrix is not optimized. When the measurement matrix is optimized with the optimization algorithm in this paper, the PSNR values of both the decrypted image and the original image are much higher than the unoptimized PSNR values, and the PSNR values are very similar for the four chaotic systems after optimization at the same compression rate, which indicates that the

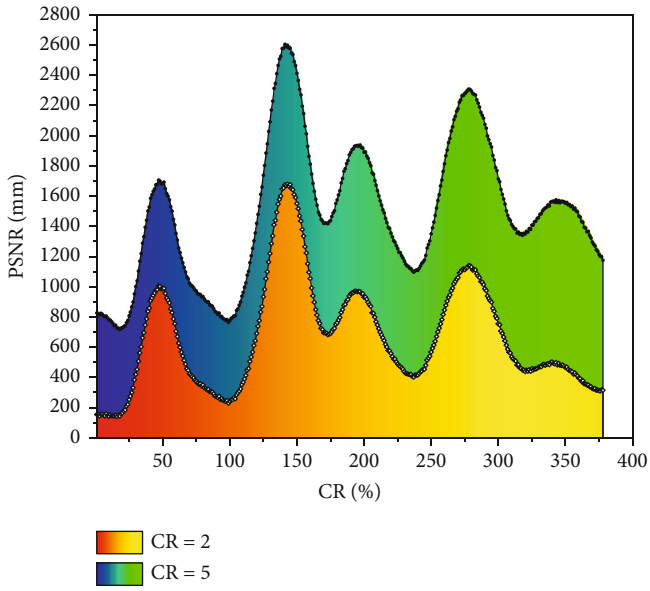

Figure 8: PSNR values for different chaotic systems.

requirements for chaotic systems are reduced and the selectivity is greatly increased after using our optimization algorithm.

In the experiment, Walsh-Hadamard transformation is used to simulate the measurement process of a single-pixel camera. In the encryption process, the plaintext image is first processed using Walsh-Hadamard transformation to make it compressible and then measured with the help of a measurement matrix to get the measurement value. Then, the pixel dislocation method controlled by the chaotic system is used to dislocate the image and reduce the correlation between pixels. To make the pixels uniformly distributed, a DNA sequence operation is chosen to change the gray value of the pixels. Moreover, the key used in the algorithm is related to the original image and can also be controlled with the help of initial input values, which enhances the security of the algorithm. The designed image compression and encryption algorithm are tested in various aspects, and the results confirm that the algorithm is effective and highly secure and has good resistance to common types of attacks.

5. Conclusion

The imaging technology of digital graphic design is of great concern to the community, and there are still big research scenarios in the field of copyright protection and content authentication; the combination of images of robust graphic design and images of fragile graphic design is a research direction, because, with the continuous development of digital products, there are more and more occasions where the balance between images of robust graphic design and images of fragile graphic design is urgently needed. In this paper, the main research object is digital images, mainly taking the measure of chaotic encryption, and the application value of encrypted planar-designed images, as well as the robustness and vulnerability situation, is studied in depth, and two types of image algorithms based on wavelet transform and chaotic encryption for a kind of digital image planar design are proposed. Then, an image algorithm for robust planar design is designed, the carrier image belongs to a kind of grayscale image, and the image of digital planar design applied in the research and analysis process of this paper is a kind of grayscale image or binary image, which already includes the copyright information, and the encryption operation is performed by the chaotic system, and then, the imaging system of digital planar design is embedded into the wavelet domain of the original image. Finally, an image algorithm for fragile planar design is designed, which improves the traditional algorithm and speeds up the computation of the algorithm, and proposes a method to set the initial value of the chaotic system as the coefficients of the wavelet transform of the image, using the characteristics of the chaotic system sensitive to the initial value as the sensitivity of the image of the fragile planar design to detect tampering. Finally, it can be learned through simulation that the proposed two types of image planar design of the image exist visual imperceptibility and are better for common noise interference and signal processing.

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 known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H. R. Shakir, "An image encryption method based on selective AES coding of wavelet transform and chaotic pixel shuffling," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26073–26087, 2019.

[2] R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Medical & Biological Engineering & Computing*, vol. 58, no. 7, pp. 1445–1458, 2020.

[3] Y. Shen, C. Tang, L. Zhou, and Z. Lei, "Optical single-channel cryptosystem based on the discrete wavelet transform and the chaotic standard map for multi-image," *Applied Optics*, vol. 59, no. 30, pp. 9558–9567, 2020.

[4] E. A. Umoh, O. N. Iloanusi, and U. A. Nnolim, "Image multi-encryption architecture based on hybrid keystream sequence interspersed with Haar discrete wavelet transform," *IET Image Processing*, vol. 14, no. 10, pp. 2081–2091, 2020.

[5] R. Sundararaman, H. N. Upadhyay, A. Sridevi et al., "Cellular automata with synthetic image a secure image communication with transform domain," *Defence Science Journal*, vol. 69, no. 3, pp. 259–265, 2019.

[6] A. Gupta, D. Singh, and M. Kaur, "An efficient image encryption using non-dominated sorting genetic algorithm-III based 4-D chaotic maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 3, pp. 1309–1324, 2020.

[7] S. Aashiq Banu and R. Amirtharajan, "Bio-inspired cryptosystem on the reciprocal domain: DNA strands mutate to secure health data," *Frontiers of Information Technology & Electronic Engineering*, vol. 22, no. 7, pp. 940–956, 2021.

[8] X. Z. Li, W. W. Chen, and Y. Q. Wang, "Quantum image compression-encryption scheme based on quantum discrete cosine transform," *International Journal of Theoretical Physics*, vol. 57, no. 9, pp. 2904–2919, 2018.

[9] K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu, and X. Yuan, "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 5, pp. 1821–1833, 2020.

[10] S. Jeevitha and N. A. Prabha, "Novel medical image encryption using DWT block-based scrambling and edge maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3373–3388, 2021.

[11] Y. Zhou, C. Li, W. Li, H. Li, W. Feng, and K. Qian, "Image encryption algorithm with circle index table scrambling and partition diffusion," *Nonlinear Dynamics*, vol. 103, no. 2, pp. 2043–2061, 2021.

[12] A. Malik, S. Dhall, and S. Gupta, "An improved bit plane image encryption technique using RC4 and quantum chaotic demeanour," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7911–7937, 2021.

[13] M. Kumar, R. A. Lahcen, R. N. Mohapatra, C. Alwala, and S. V. Kurella, "Review of image encryption techniques," *Journal of Computing and Information Science in Engineering*, vol. 14, no. 1, pp. 31–37, 2020.

[14] H. Singh, "Watermarking image encryption using deterministic phase mask and singular value decomposition in fractional Mellin transform domain," *IET Image Processing*, vol. 12, no. 11, pp. 1994–2001, 2018.

[15] K. Hannoun, H. Hamiche, M. Lahdir, M. Laghrouche, and S. Kassim, "A novel DWT domain watermarking scheme based on a discrete-time chaotic system," *IFAC-PapersOnLine*, vol. 51, no. 33, pp. 50–55, 2018.

[16] X. J. Tong, P. Chen, and M. Zhang, "A joint image lossless compression and encryption method based on chaotic map," *Multimedia Tools and Applications*, vol. 76, no. 12, pp. 13995–14020, 2017.

[17] S. Arumugham, S. Rajagopalan, J. B. B. Rayappan, and R. Amirtharajan, "Tamper-resistant secure medical image carrier: an IWT–SVD–chaos–FPGA combination," *Arabian Journal for Science and Engineering*, vol. 44, no. 11, pp. 9561–9580, 2019.

[18] S. Farwa, N. Bibi, and N. Muhammad, "An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling," *Multimedia Tools and Applications*, vol. 79, no. 37-38, pp. 28225–28238, 2020.

[19] W. Wei, M. Woźniak, R. Damaševičius, X. Fan, and Y. Li, "Algorithm research of known-plaintext attack on double random phase mask based on WSNs," *Journal of Internet Technology*, vol. 20, no. 1, pp. 39–48, 2019.

[20] V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," *Multiscale and Multidisciplinary Modeling, Experiments and Design*, vol. 2, no. 4, pp. 233–248, 2019.

[21] Y. Luo, R. Zhou, J. Liu, S. Qiu, and Y. Cao, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26191–26217, 2018.