cryptography

MDPI

Article

Image Encryption with Dual Watermark Based on Chaotic Map

Ran Chu *, Jun Mou and Yuanhui Cui

Information Science and Engineering College, Dalian Polytechnic University, Dalian 116034, China; moujun@dlpu.edu.cn (J.M.); cuiyh@dlpu.edu.cn (Y.C.)
* Correspondence: churan@dlpu.edu.cn

Abstract

A dual watermark and DNA image encryption based on a chaotic map is proposed. Firstly, a new discrete chaotic map is proposed, and the dynamic characteristics are analyzed. Then, the hash value changes initial conditions, and the pseudo-random sequence is generated. The encrypted copyright image is fused with the feature value of the original image and then encrypted again to form zero-watermarking, which is registered with the copyright certification authority. The zero-watermarking is taken as a robust watermark and embedded into the original image based on a chaotic sequence to ensure its invisibility. Finally, a cross-mutation DNA encryption is proposed. The experimental results verify the performance of encryption and dual watermark copyright authentication, and the ability to resist attacks.

Keywords: dual watermark; zero-watermarking; chaotic map; DNA; image encryption

1. Introduction

With the arrival of big data, many images are stored, copied and disseminated, which requires watermarking and encryption technology to authenticate and protect image copyright and information security.

Most traditional watermarking techniques embed watermarks in the image frequency domain, but it is difficult to ensure invisibility and robustness at the same time. Embedding information in a low frequency will distort the image and embedding it in a high frequency will affect the anti-attack performance [1–3]. Wen et al. [4] proposed a zero-watermarking technology and registered it with the Copyright Protection Center. Since copyright information is not embedded in the main image, zero-watermarking can ensure the integrity and solve copyright disputes. Kang et al. [5] proposed zero-watermarking to construct distinguishable color images by encrypting copyright identifiers and feature sequences by chaotic map, which improves the equilibrium, but the security needs to be improved. Xiong et al. [6] proposed zero-watermarking generated directly from the relation between the mean value of pixels and the mean value of blocks in the spatial domain. However, the robustness of the feature constructed from the spatial relation is insufficient under rotation attack. Jiang et al. [7] proposed zero-watermarking based on tensor mode expansion to generate feature images through singular value decomposition and discrete cosine transform. However, the singular values of images fluctuate greatly under geometric attacks, and the instability of singular values will lead to false alarms in copyright judgment. Chen et al. [8] proposed zero-watermarking with stability and uniqueness to avoid false alarms. However, its correction factor is a fixed constant, which will affect the security.

Due to the advantages and disadvantages of both traditional watermarking and zero-watermarking algorithms, multi-watermarking technology has been widely concerned,

Academic Editor: Krzysztof Szczypiorski

Received: 13 May 2025
Revised: 6 June 2025
Accepted: 26 June 2025
Published: 1 July 2025

Citation: Chu, R.; Mou, J.; Cui, Y. Image Encryption with Dual Watermark Based on Chaotic Map. *Cryptography* **2025**, *9*, 49. https://doi.org/10.3390/cryptography9030049

which increases the number of watermarking and combines the two algorithms to improve security. Xi et al. [9] proposed dual zero-watermarking, which improves the watermark capacity and has a better overall robustness than a single scheme. Shi et al. [10] proposed a dual watermarking protection, which protects the copyright and privacy of medical images based on zero-watermarking and robust watermarking. Wang et al. [11] proposed a tamper-detection dual watermarking for medical images, which divides images according to the subblock entropy of the security area. However, the above schemes are for medical images, which limits the application field, and the watermarking algorithm only protects the copyright and cannot protect the privacy information in the image.

Chaotic systems have remarkable characteristics and can be combined with image encryption and watermarking algorithms to enhance security [12–15]. Hua et al. [16] proposed a chaotic system by combining the outputs of two existing chaotic maps and performing sine transformations. Compared with a continuous chaotic system, discrete chaotic maps have a simple structure, low computation cost, fast iteration speed and easy implementation, which makes them widely used in watermarking and image encryption. High-dimensional chaotic systems are more prone to generating hyperchaotic phenomena, while low-dimensional chaotic systems generate pseudo-random sequences at a faster rate. Xu et al. [17] proposed a 3D image encryption based on a discrete chaotic system, which improved the randomness of existing discrete chaotic systems. Since pseudo-random sequences are required in three stages of Robust watermark, zero watermarking and Ciphertext generation, the three-dimensional chaotic system can quickly generate sufficient data at one time and is suitable for this algorithm.

An image encryption with dual watermark based on chaotic map is designed. The main contributions are the following:

1. A dual watermark protection mechanism based on robust watermark and zero-watermarking algorithms is proposed.
2. A three-dimensional discrete chaotic map based on STBCS and trigonometric function is proposed.
3. The watermark algorithm and image encryption algorithm are combined to improve the security level.

This paper is structured as follows. In Section 2, the chaotic system and its dynamic characteristics are introduced. In Section 3, the basic theory is introduced. In Section 4, the workflow of encryption algorithm and decryption algorithm is introduced. In Section 5, the simulation results and security performance are shown. In Section 6, important conclusions are drawn.

2. Chaotic System

2.1. STBCS Chaotic Map

Sinusoidal transformation based on a chaotic system (STBCS) generates a new chaotic map by transforming the linear weighted combination of the existing chaotic map, which can improve the shortcomings of classical Sine, Logistic and Tent maps, such as the low-complexity and small chaotic behavior region [16].

$$x_{i+1} = \sin(\pi(F(a, x_i) + G(b, x_i)) + \beta), \tag{1}$$

where $F(a,x_i)$ and $G(b,x_i)$ are subsystems with control parameters a and b, and β is shift constant.

The coupling structure is selected, the control parameter a is set to r, b is set to $1 - r$, r is the coupling parameter and variable β is set to move constant. STBCS is extended to a three-dimensional chaotic map to improve robustness and complexity.

$$\begin{cases} x_{i+1} = \sin(\pi(r \times F(x_i)) + (1-r)G(x_i)) + \beta) \\ y_{i+1} = \sin(\pi(r \times F(y_i)) + (1-r)G(y_i)) + \beta) \\ z_{i+1} = \sin(\pi(r \times F(z_i)) + (1-r)G(z_i)) + \beta) \end{cases}. \tag{2}$$

All one-dimensional chaotic maps can be selected for seed maps. Set r = 6, and the subsystems $F(x_i)$ and $G(x_i)$ adopt a modulation-coupled controlled discrete chaotic map [18].

$$\begin{cases} x_{n+1} = af(x_n)(1 - r \times g(x_n)) \\ y_{n+1} = bf(x_{n+1})(1 - r \times g(y_n)) \end{cases}, \tag{3}$$

where a, b and r are coupling parameters, and $f(\cdot)$ and $g(\cdot)$ are subfunctions of trigonometric form.

$F(x_i)$ is set as a 3D modulated chaotic map (3D-M-CS), $f(x) = \cos(x)$ and $g(x) = \sin(x)$.

$$\begin{cases} x_{n+1} = a_1 \cos(x_n)(1 - r_1 \times \sin(x_n)) \\ y_{n+1} = b_1 \cos(x_{n+1})(1 - r_1 \times \sin(y_n)) \\ z_{n+1} = c_1 \cos(y_{n+1})(1 - r_1 \times \sin(z_n)) \end{cases}. \tag{4}$$

When a_1 = 5, b_1 = 4, c_1 = 4, r_1 = 2, the initial value (x_0, y_0, z_0) = (1, 1, 1) and the Lyapunov exponents (LE_1, LE_2, LE_3) = (1.8129, 2.6377, −1.8898). When $r_1 \in [1, 5]$, the system is periodic in the regions $r_1 \in [1.44, 1.46]$ and [3.48, 3.50]. In addition, the system is in a chaotic state, and the 3D-M-CS is in a hyperchaotic state except $r_1 \in [1.49, 1.51]$.

$G(x_i)$ is set as a 3D modulated chaotic map (3D-M-SC), where $f(x) = \sin(x)$, $g(x) = \cos(x)$ and the modulated coupled system is extended to three dimensions.

$$\begin{cases} x_{n+1} = a_2 \sin(x_n)(1 - r_2 \times \cos(x_n)) \\ y_{n+1} = b_2 \sin(x_{n+1})(1 - r_2 \times \cos(y_n)) \\ z_{n+1} = c_2 \sin(y_{n+1})(1 - r_2 \times \cos(z_n)) \end{cases}. \tag{5}$$

When a_2 = 5, b_2 = 4, c_2 = 4, r_2 = 2, the initial value (x_0, y_0, z_0) = (1, 1, 1) and the Lyapunov exponents (LE_1, LE_2, LE_3) = (1.1346, 1.6311, 3.1682). The system changes from periodic to chaotic and then to a hyperchaotic state with the increase in parameter r_2. When $r_2 \in [1.87, 5]$, except for the periodic state in the region [3.57, 3.61], the rest of the system is the hyperchaotic state of chaotic state.

The STBCS system is composed of $F(x_i)$ and $G(x_i)$. When β = 5, control parameter range $r \in [-20, 20]$; the dynamic characteristics are shown in Figure 1. Except for the chaotic state in the $r \in [-0.4, -0.2]$ and [0.9, 1.1] regions, the system is in a hyperchaotic state.

The two seed maps in Figure 1a,b have positive LE only in a few parameter settings, while the new chaotic map generated by STBCS has positive LE in a larger parameter range. The chaotic maps generated by STBCS in Figure 1c have a greater LE than those generated by their corresponding seed maps, and the chaotic maps can achieve chaotic behavior throughout the parameter range, demonstrating their good chaos and robustness. The maximum LE of the system is significantly higher than that in References [19,20], and the proportion of hyperchaotic behavior occurring throughout the interval is close to 100%, which is higher than that in Reference [21].

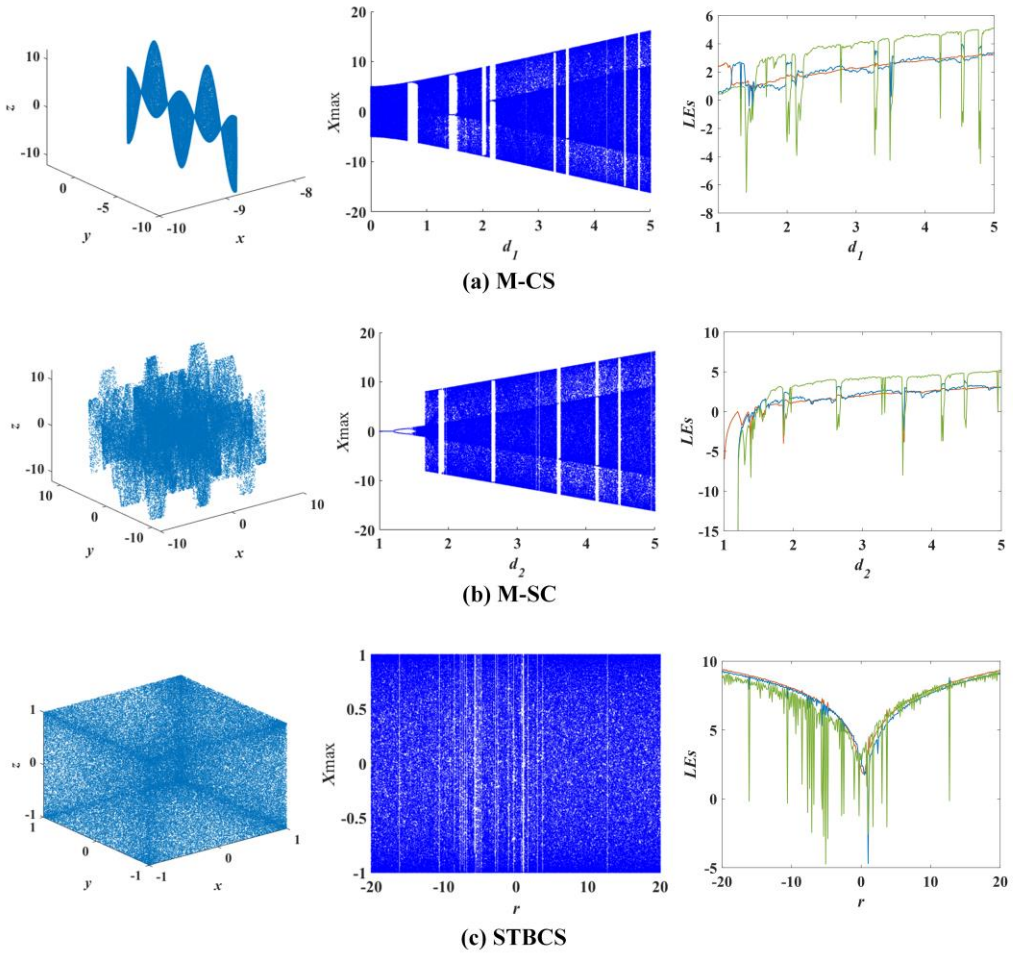

Figure 1. Phase diagrams, bifurcation diagrams and Lyapunov exponents.

2.2. Random Analysis

The National Institute of Standards and Technology (NIST) verifies the quality of random number generators. The random test results for the worst set are shown in Table 1. Even if the worst test sample is selected for random performance test, it can still pass all the NIST sub-tests.

Table 1. NIST test result.

Test		*p*-Value	Pass Rate	Result
Frequency		0.304126	1	Pass
Block Frequency		0.911413	0.96	Pass
Cumulative Sums	Forward	0.883171	1	Pass
	Reverse	0.816537	0.99	Pass
Runs		0.145326	0.97	Pass
Longest Run		0.834308	0.99	Pass
Binary Matrix Rank		0.739918	0.99	Pass
FFT		0.616305	0.99	Pass
Non-Overlapping Template Matching		0.699313	0.98	Pass
Overlapping Template Matching		0.350485	0.98	Pass
Maurer's "Universal Statistical"		0.978072	0.98	Pass
Approximate Entropy		0.616305	0.97	Pass

Table 1. *Cont.*

Test		*p*-Value	Pass Rate	Result
The Random Excursions	x = −4	0.082177	0.97	Pass
	x = −3	0.637119	1	Pass
	x = −2	0.804337	1	Pass
	x = −1	0.134686	0.99	Pass
	x = 1	0.671779	1	Pass
	x = 2	0.602458	0.99	Pass
	x = 3	0.324180	1	Pass
	x = 4	0.862344	0.99	Pass
Random Excursions Variant	x = −9	0.090936	1	Pass
	x = −8	0.082177	0.99	Pass
	x = −7	0.568055	1	Pass
	x = −6	0.739918	1	Pass
	x = −5	0.066882	1	Pass
	x = −4	0.739918	0.99	Pass
	x = −3	0.888137	0.99	Pass
	x = −2	0.637119	0.98	Pass
	x = −1	0.350485	0.99	Pass
	x = 1	0.407091	0.98	Pass
	x = 2	0.568055	0.99	Pass
	x = 3	0.350485	1	Pass
	x = 4	0.500934	1	Pass
	x = 5	0.931952	1	Pass
	x = 6	0.568055	1	Pass
	x = 7	0.706149	1	Pass
	x = 8	0.324180	1	Pass
	x = 9	0.213309	1	Pass
Serial	p-value$_1$	0.319084	1	Pass
	p-value$_2$	0.699313	0.99	Pass
Linear Complexity		0.554420	0.97	Pass

3. Basic Theory

3.1. Dynamic Modified Singular Value Decomposition

Singular value decomposition (SVD) is an orthogonal matrix decomposition method, which separates singular values in the form of diagonal matrix and extracts the energy of the decomposed matrix by obtaining the characteristic information of the energy concentration coefficient.

$$I = U \times S \times V^T, \tag{6}$$

where I is digital image, U and V are two orthonormal matrices, V^T is the transpose of V and the singular value matrix $S = \begin{bmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_n \end{bmatrix}$ is a singular value diagonal matrix arranged in descending order, $\lambda_1 > \lambda_2 > \ldots > \lambda_n$.

The singular value matrix contains important image features and has a strong stability. There is no correspondence between images and singular values. If only singular values are used to construct the feature information, watermark information may be extracted from other irrelevant images, resulting in false alarms. By introducing correction factors into SVD, the values of elements on the diagonal can be equalized.

$$I = U \times (S)^{\beta} \times V^T \ (0 < \beta < 1), \tag{7}$$

where β is the correction factor.

The sensitivity under attack can be reduced by the power operation of the diagonal matrix. The traditional algorithm chooses a fixed correction value, but it still has the risk of false alarm. In this paper, the dynamic correction factor is related to the chaotic system, and each singular value is adjusted to different degrees, so that the obtained feature is not only related to the image features, but can also be based on the chaotic system, which can avoid false alarms and improve security.

3.2. Dynamic Hidden Watermark

The traditional watermark method ensures visual quality and security by hiding the watermark in the statistical feature. The lifting wavelet transform (LWT) can decompose the image into the low-frequency component containing the main overview and approximation information and the high-frequency component containing the edge and detail, and it is completely reversible, requiring less storage space. The low-low-frequency coefficient matrix LL after LWT decomposition maintains the content information, and the high-high-frequency coefficient matrix HH holds diagonal high-frequency information. The schematic diagram of three-level LWT decomposition of images is shown in Figure 2. In order not to change the main visual features, the watermark is embedded in the HH of level 3.

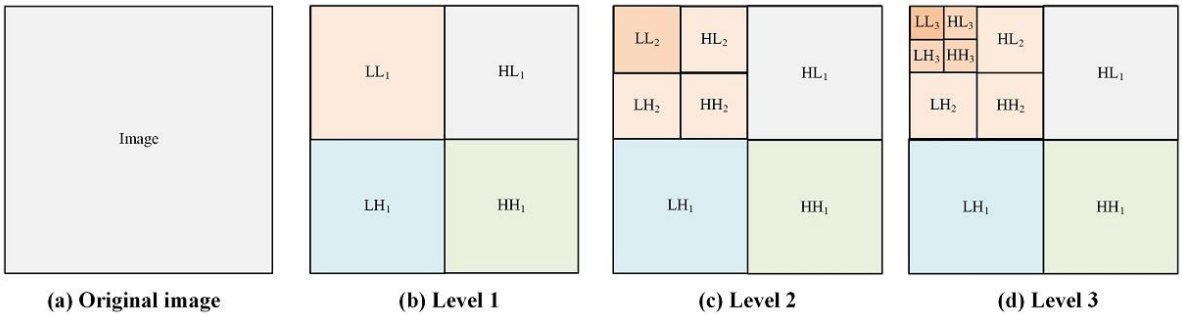

Figure 2. Three-level LWT decomposition diagram.

4. Proposed Scheme

Based on a chaotic sequence, a dynamic modified SVD algorithm to generate zero-watermarking and a dynamic hiding algorithm are designed, and a dynamic DNA cross-mutation image encryption algorithm is designed.

4.1. Design of Dual Watermark Encryption Algorithm

The dual watermark encryption process of color images includes the copyright authentication of zero-watermarking and robust watermark and image encryption algorithms. Firstly, encrypting copyright images based on a chaotic system, the SVD is corrected by a dynamic correction factor, and the generated feature matrix is fused with the encrypted copyright image and then encrypted again to generate zero-watermarking for registration. Then, the zero-watermarking is dynamically embedded in the high-high-frequency region for dual watermark copyright protection. Finally, the image protected by dual watermark is encrypted based on dynamic DNA algorithm to improve security. The flow chart of encryption is shown in Figure 3.

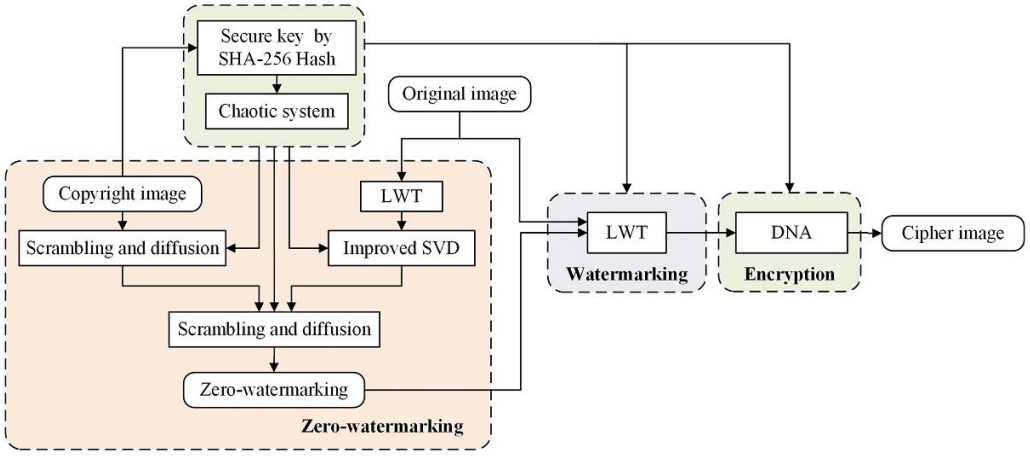

Figure 3. Flow chart of dual watermark encryption algorithm.

Step 1: The key is determined by parameters and initial conditions.

The initial value is affected by the hash value of copyright image, which is generated by SHA−256 algorithm and divided into 8 blocks, each with 8 digits.

$$k_i = 10^{-15} \times [(h_{i1} + h_{i2} + h_{i3} + h_{i4} + h_{i5} + + h_{i6} + h_{i7} + h_{i8}) \div 8] \tag{8}$$

where $i \in [1, 8]$, h is the hash value and k is the initial value.

Update initial conditions to improve sensitivity.

$$\begin{cases} x_0 = x_0' + k_1 + k_4 + k_7 \\ y_0 = y_0' + k_2 + k_5 + k_8 \\ z_0 = z_0' + k_3 + k_6 \end{cases}, \tag{9}$$

where x_0', y_0' and z_0' are given values, and x_0, y_0 and z_0 are the initial values after perturbation.

The chaotic system iterates under new initial conditions, generating a pseudo-random sequence (x, y, z), and a sequence of integers (X, Y, Z).

$$\begin{cases} X = \mathrm{mod}(\mathrm{floor}(|x| \times 10^{15}), 256) \\ Y = \mathrm{mod}(\mathrm{floor}(|y| \times 10^{15}), 256) \\ Z = \mathrm{mod}(\mathrm{floor}(|z| \times 10^{15}), 256) \end{cases}. \tag{10}$$

where mod represents modular operation and floor represents rounding down.

Step 2: Construct and register zero-watermarking.

First, the copyrighted image is encrypted so that they are randomly distributed. Sort the pseudo-random sequence in descending order and scramble the copyright images according to index. Diffusion image based on pseudo-random sequences.

Then, each channel of color image is decomposed by LWT, respectively. To improve the decomposition efficiency and ensure the accuracy of decomposition, the LL is divided into several 4×4 blocks before SVD operation, and the maximum singular value extracted is corrected by the correction factor generated by the pseudo-random sequence to construct the feature sequence. Since zero-watermarking is a binary image, the feature is converted to binary by the global threshold of the grayscale image.

$$T(i) = \begin{cases} 1 & T'(i) > T_{\mathrm{Thresh}} \\ 0 & T'(i) \le T_{\mathrm{Thresh}} \end{cases}, \tag{11}$$

where T_{Thresh} is the global threshold of the feature sequence, T' is the feature sequence of the image, T is the binary sequence and i is the position in the sequence.

The encrypted copyright information is combined with the binary feature sequence by XOR operation, and then scrambled, diffused, and converted to zero-watermarking, and registered with the time stamp and key in the intellectual property database.

Step 3: Hide watermark information.

Embed zero-watermarking into the high-high-frequency region of RGB channels by LWT based on a pseudo-random sequence to make the watermark invisible.

$$\mathrm{HH}' = x \times \mathrm{HH} + (1 - x) \times S. \tag{12}$$

where HH and HH′ are the high-high-frequency coefficient matrices of the original and watermark protected images, respectively, x is the chaotic sequence and S is zero-watermarking.

After the inverse LWT is carried out and RGB channels are combined, the dual watermark protection is achieved.

Step 4: Encrypts images protected by watermarks based on DNA algorithm.

DNA encryption includes encoding, diffusion and scrambling, mutation and decoding. The gene chain is composed of adenine (A), thymine (T), cytosine (C) and guanine (G). Encoding rules are shown in Table 2. Firstly, the watermark-protected image and pseudo-random sequence are converted into binary, and then transformed into a DNA sequence according to dynamic coding rules based on a pseudo-random sequence.

Table 2. DNA encode rules.

Rule	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
00	A	A	T	T	G	G	C	C
01	C	G	C	G	T	A	T	A
10	G	C	G	C	A	T	A	T
11	T	T	A	A	C	C	G	G

The DNA sequence is then encrypted through scrambling and diffusion operations. According to the descending index of chaotic sequence, DNA sequence is disordered after being scrambled. Diffusion sequence, chaotic system determines its calculation rules. The calculation rules are shown in Table 3.

Table 3. DNA addition and subtraction rules.

+	**A**	**C**	**G**	**T**	**−**	**A**	**C**	**G**	**T**
A	A	C	G	T	A	A	T	G	C
C	C	G	T	A	C	C	A	T	G
G	G	T	A	C	G	G	C	A	T
T	T	A	C	G	T	T	G	C	A

Finally, genes are mutated through crossover and mutational manipulation. Variation in image encryption can be achieved by exchanging pixel values, like the crossover of biological genes. Dividing the DNA sequence by equal lengths, converting pseudo-random sequence into a binary to determine intersection location, 1 exchanges codon, 0 does not exchange codons, and the crossing process diagram is shown in Figure 4. Combine the two sequences to complete the crossover operation.

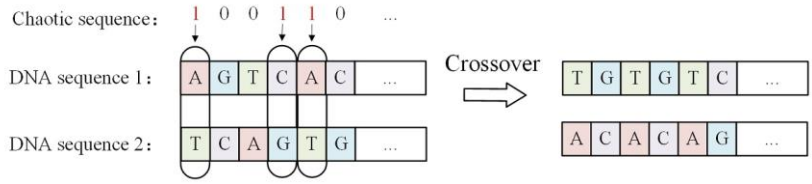

Figure 4. Schematic diagram of the crossing process.

Among structural variations, translocation mutations refer to the exchange of chromosome fragments. The length of mutation fragments is determined by the chaotic system to ensure flexibility, and the length of mutation fragments is set to 1 to 3 to ensure the effect and efficiency, so the mutation mode can be divided into three modes. The mutation length and two mutation units are based on a chaotic sequence that mutates a chromosome segment with the mutation unit structure. Mutation result will change due to the different length and unit of mutant fragment. The mutation process diagram is shown in Figure 5.

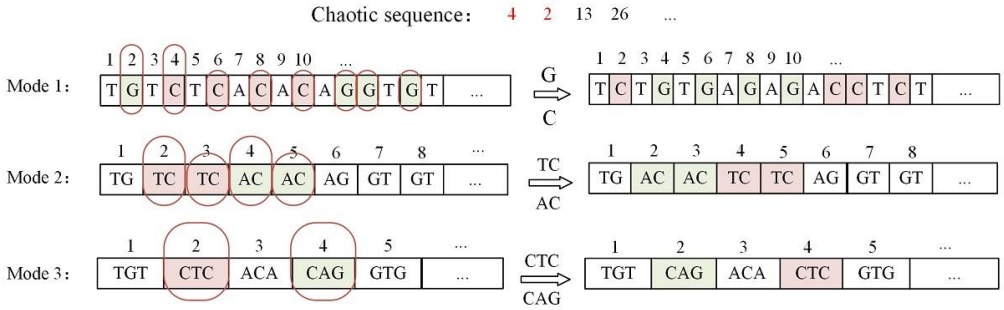

Figure 5. Schematic diagram of the mutation process.

The decoding rule is selected according to pseudo-random sequence, and the DNA sequence is decoded to binary and then converted to decimal to obtain the ciphertext.

4.2. Decryption and Dual Watermark Copyright Authentication

The authentication process is the restoration of copyright images. First, DNA algorithms are used to decrypt images. Then, the zero-watermarking is extracted, the copyright image is restored. The copyright image is meaningful, so the copyright image recovered from zero-watermarking can also be intuitively recognized by the eye. In addition, the copyright can be re-authenticated by the similarity between the authenticated image generated and registered zero-watermarking. The decryption and dual watermark copyright authentication process is shown in Figure 6.

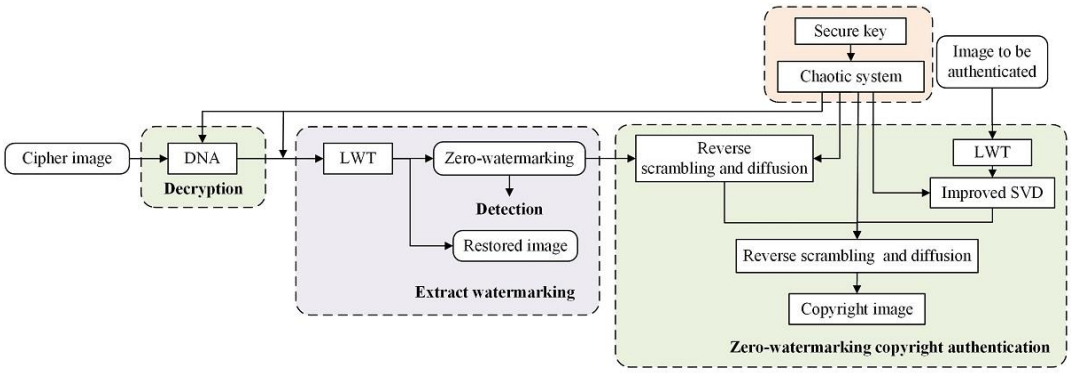

Figure 6. Flow chart of decryption and dual watermark copyright authentication.

Step 1: Decrypt ciphertext by DNA algorithms.

Based on the chaotic sequence decryption of ciphertext, the watermark protected image is obtained.

Step 2: Copyright authentication by robust watermark.

Firstly, LWT is applied to RGB channels of visual security images to extract the embedded zero-watermarking.

$$S = \left(\mathrm{HH}' - x \times \mathrm{HH}\right)/(1 - x). \tag{13}$$

where HH and HH′ are the high-high-frequency coefficient matrices of the original and watermark protected image, x is the chaotic sequence, and S is the extracted zero-watermarking.

Then, confirm the copyright. Not only can the copyright be determined by comparing the similarity between the extracted and registered zero-watermarking, but also the copyright image could be recovered by extracting zero-watermarking and directly recognized by the eye. Moreover, since copyright images are embedded in RGB channels, respectively, the copyright images extracted from each channel can be combined through the voting mechanism in the authentication stage to improve copyright authentication.

$$\mathrm{W}'_{one}(i,j) = \begin{cases} 1 & [\mathrm{W}'_1(i,j) + \mathrm{W}'_2(i,j) + \mathrm{W}'_3(i,j)] \geq 2 \\ 0 & [\mathrm{W}'_1(i,j) + \mathrm{W}'_2(i,j) + \mathrm{W}'_3(i,j)] \leq 1 \end{cases} \quad 1 \leq i \leq M \ , 1 \leq j \leq N, \tag{14}$$

where $W_1{}'$, $W_2{}'$ and $W_3{}'$ are the copyright images extracted from RGB channels, respectively, and $W_{\mathrm{one}}{}'$ is merged copyright image.

Step 3: Copyright authentication by zero-watermarking.

First, the image being attacked is corrected. Detect and correct rotation attacks on color images. Then, zero-watermarking is generated by the extracted feature of the attacked image, and registered zero-watermarking is extracted from IPR. Finally, the copyright is verified by their similarity.

5. Performance Analysis

5.1. Simulation Result

Simulation was performed on matlab2014 software of 64-bit Windows operating system. Select 9 images of size 256 × 256 × 3 as the original images. Select 3 watermark of size 32 × 32 × 3 (logo image, English letter, and Arabic numeral) as the copyright image. The experimental results are shown in Figure 7, indicating that dual watermark and encryption protection are feasible. In the protection stage, zero-watermarking generated by original and copyright image has no obvious visual features, and the zero-watermarking embedded in the original image has good invisibility. The image protected by watermark based on chaotic sequence encryption can successfully hide the original image information. In the receiving phase, the receiver can decrypt the ciphertext based on the chaotic sequence. In the verification stage, the watermark was extracted from the decrypted image. For meaningful copyright information, the copyright can be identified visually. Moreover, the zero-watermarking can be re-made from the image to be authenticated, and the copyright can be authenticated. There is no obvious change in the visual effect between the image protected by watermark and the original image, and the watermark is visually concealed.

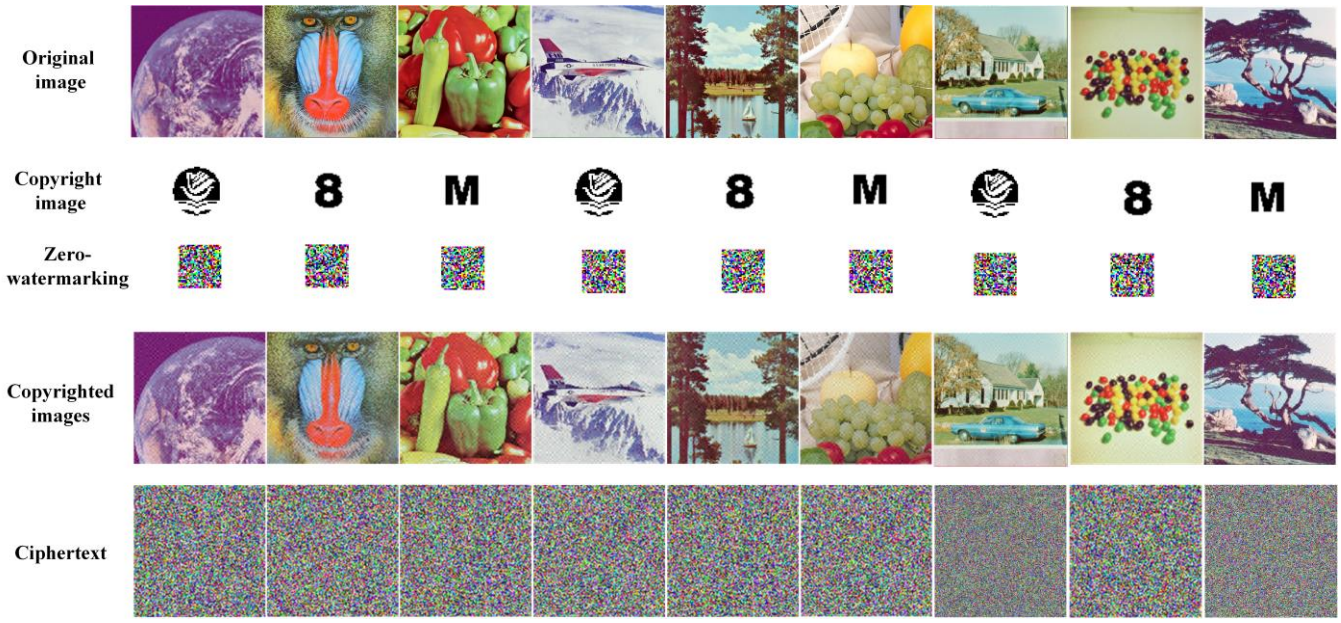

Figure 7. Simulation results of dual watermark and encryption protection.

Peak signal-to-noise ratio (PSNR) measures the similarity between images.

$$\mathrm{PSNR} = 10\lg \frac{M \times N \times 3 \times \max\limits_{i,j,k}\left[I(i,j,k)^2\right]}{\sum\limits_{i=1}^{M}\sum\limits_{j=1}^{N}\sum\limits_{k=1}^{3}\left[I(i,j,k) - I'(i,j,k)\right]^2}, \tag{15}$$

where max is the maximum value function, I and I' are the images and M and N are the length and width.

Embedding a watermark into the original image will change the image feature. The high similarity between the watermark-protected image and the original image means high security. Therefore, it is necessary to measure the invisibility of the watermark. When I and I' are the original image and watermark-protected image, respectively, the PSNR value measures the invisibility of the watermark. The image is vulnerable to attack during transmission. Attack resistance can be measured by PSNR. When I and I' are the original image and restored image, respectively, the PSNR value measures the recovery effect.

Embedding watermarks requires both invisibility and robustness. The less embedded the watermark, the smaller the impact on the original image, and the higher the invisibility of the watermark. However, the more embedded the watermark data, the better its robustness. Therefore, it is difficult to satisfy both invisibility and robustness when designing watermark algorithms. The visual security simulation results are compared using the PSNR of the images before and after embedding the watermark, as shown in Table 4. For different original images, embedding watermarks has different degrees of influence on their visual effects. However, the PSNR of this algorithm is all greater than 33, and different watermarks have little influence on invisibility, proving that its invisibility is high. The PSNR was all higher than that in Reference [19]. However, the PSNR values of individual images are lower than those in Reference [10]. This is because the algorithm adopts a voting mechanism in the copyright determination stage and needs to embed the watermark simultaneously in the RGB channel, improving the robustness by sacrificing the invisibility of the watermark.

Table 4. Comparison of visual security simulation results.

Algorithm	Proposed			Ref. [19]	Ref. [10]
	Earth	Baboon	Peppers	Mean	Mean
Number character	43.2671	37.0417	47.0893	32.0359	42.0000
English character	49.3960	37.0798	45.7277		
Logo design	43.2634	33.7379	47.3498		

5.2. Key Analysis

5.2.1. Key Space Analysis

The key is generated by the watermark, including the following: (1) system parameters β, r, a_1, b_1, c_1, r_1, a_2, b_2, c_2 and r_2; (2) system initial value (x_0', y_0' and z_0') and (3) hash values k_1, k_2, k_3, k_4, k_5, k_6, k_7 and k_8. When the calculation accuracy is 10^{-15}, the key space is close to 2^{1046}, exceeding the minimum requirement of 2^{100} [21]. Compared with the key space of other algorithms, as shown in Table 5, the key space is larger.

Table 5. Key space for different algorithms.

Algorithm	Proposed	Ref. [20]	Ref. [22]	Ref. [23]	Ref. [24]
Key space	2^{1046}	2^{233}	2^{250}	2^{280}	2^{294}

5.2.2. Key Sensitivity Analysis

During the detection process, each small change in the key results in the recovered copyright image being completely different from the original. Even if the difference with the correct key is only 10^{-15}, the copyright authentication and decryption of the ciphertext cannot be performed, as shown in Figure 8. No one without the correct key can get the plaintext information and steal the copyright.

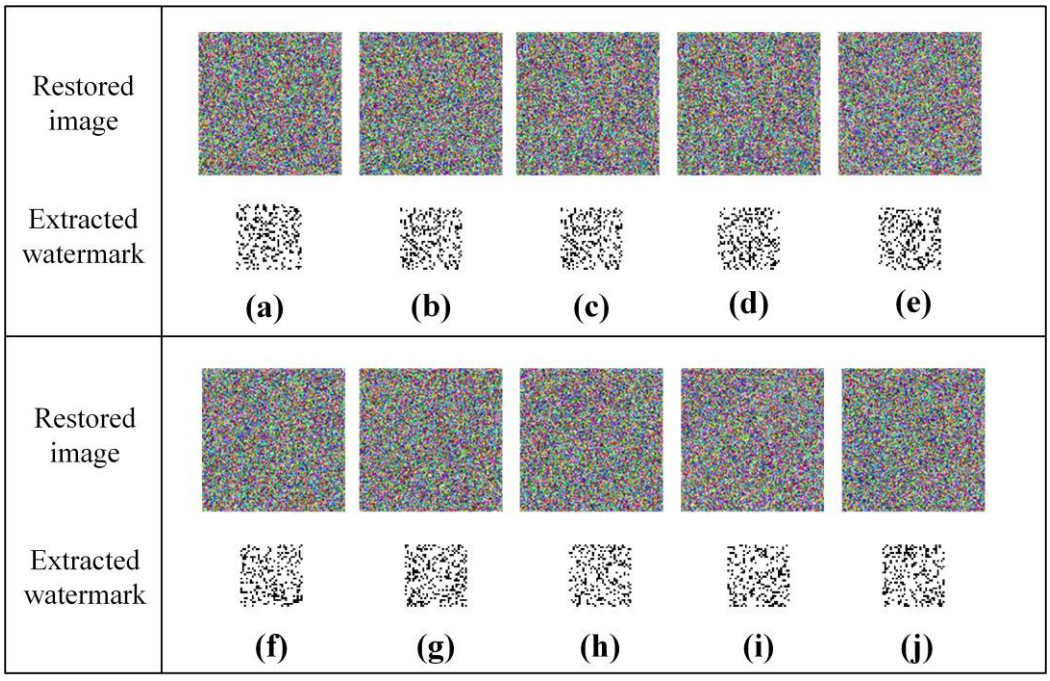

Figure 8. Key sensitivity analysis results: (**a**) $\beta + 10^{-15}$, (**b**) $r + 10^{-15}$, (**c**) $a_1 + 10^{-15}$, (**d**) $b_1 + 10^{-15}$, (**e**) $c_1 + 10^{-15}$, (**f**) $r_1 + 10^{-15}$, (**g**) $a_2 + 10^{-15}$, (**h**) $b_2 + 10^{-15}$, (**i**) $c_2 + 10^{-15}$ and (**j**) $r_2 + 10^{-15}$.

5.3. Statistical Analysis

5.3.1. Correlation Analysis

Low correlation between plaintext and ciphertext can make encryption undetectable to an attacker. For watermark encryption, the watermark before and after encryption should be significantly different; this difference can be characterized by the normalized correlation coefficient of the similarity parameter.

$$\mathrm{NC}(\mathrm{W},\mathrm{W}') = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\mathrm{W}(i,j)\times\mathrm{W}'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(\mathrm{W}(i,j))^2}\times\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(\mathrm{W}'(i,j))^2}}, \tag{16}$$

where W and W′ are two watermarks, and M and N are the length and width, NC∈[0, 1].

The optimal NC value of the watermark before and after encryption is 0.5, and an NC close to 0 or 1 means that the security becomes worse. Experimental results of correlation coefficients for different watermarks are shown in Table 6. The correlation of this algorithm is close to 0.5.

Table 6. Experimental results of watermark correlation coefficient.

Watermark	Proposed			
	Number Character	English Character	Logo Design	Mean
NC	0.5414	0.5044	0.5327	0.5262

Image encryptions reduce the correlation between adjacent data and hide the statistics in the plaintext. The correlation experiment results are shown in Figure 9. Plaintext has a strong correlation and dense distribution, while ciphertext has a low correlation and scattered distribution.

The normalized covariance can measure the correlation of two images.

$$\gamma_{\mathrm{xy}} = \frac{\frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)][y_i - E(y)]}{\sqrt{D(x)D(y)}}, \tag{17}$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $D(x) = \frac{1}{N}\sum_{i=1}^{N}[x_i - E(x)]^2$ are the expectation and variance of variable x.

The experimental results of the correlation are shown in Table 7. The absolute value of correlation coefficient is close to 1 in plaintext, and the correlation between adjacent pixels is high in all directions, while the correlation is low and close to 0 in ciphertext.

Table 7. Correlation coefficient analysis.

Image	Channel	Plain Image			Cipher Image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Earth	R	0.9374	0.9485	0.9024	−0.0017	−0.0043	−0.0012
	G	0.9386	0.9505	0.9061	0.0058	−0.0005	−0.0001
	B	0.9256	0.9381	0.8860	0.0018	0.0045	0.0021
Baboon	R	0.9474	0.9208	0.9014	0.0085	0.0017	0.0019
	G	0.8728	0.8380	0.7905	0.0002	0.0012	0.0084
	B	0.9216	0.9139	0.8767	−0.0009	−0.0007	−0.0000

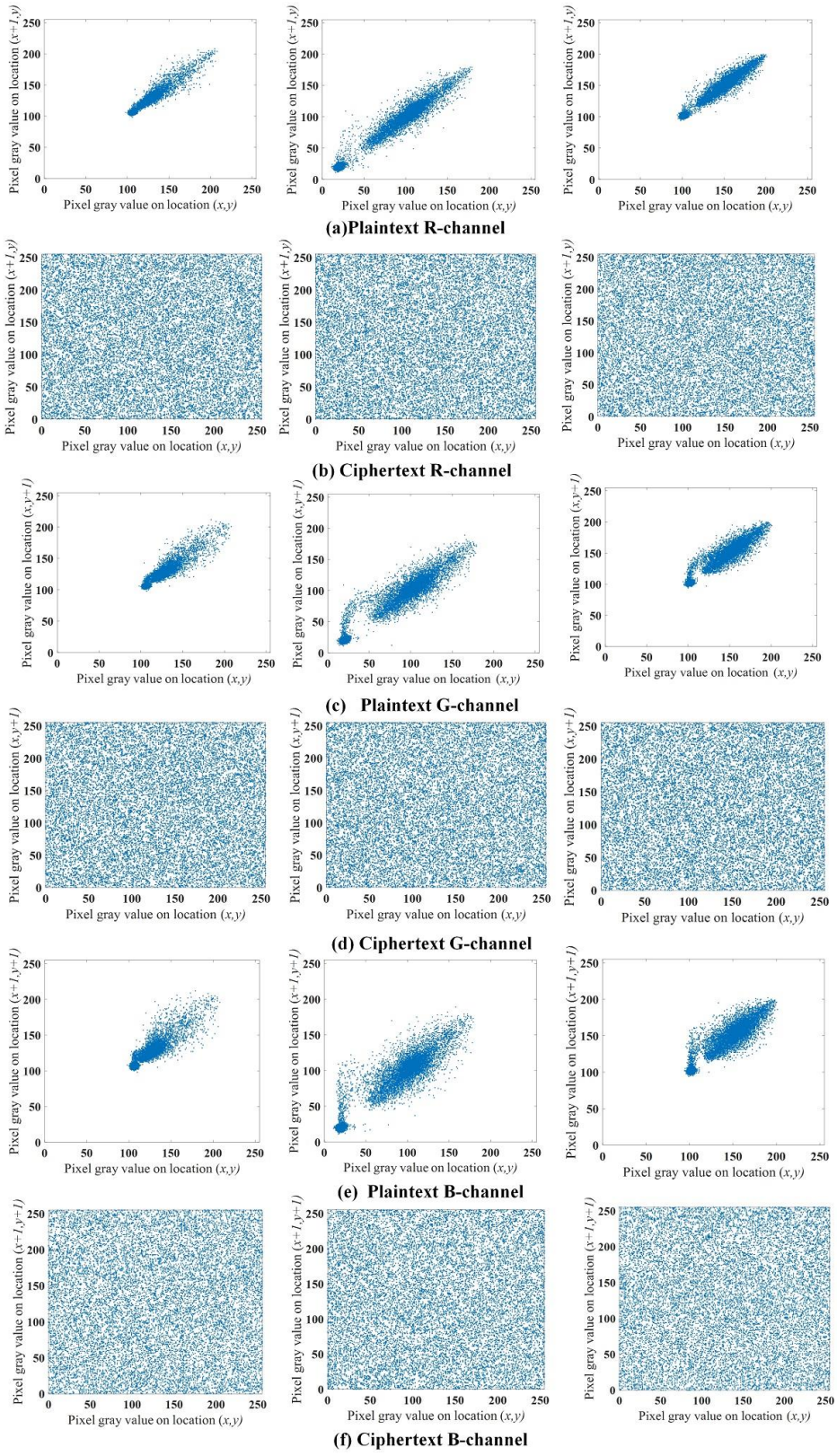

Figure 9. Correlation analysis result.

5.3.2. Histogram Analysis

The histogram analysis results in plaintext and ciphertext R, G and B channels are shown in Figure 10. The ability to measure anti-statistical attacks can be visually measured

directly from the histogram. The plaintext histograms have a clear coordinate aggregation interval, while the ciphertext histograms are flat and evenly distributed.

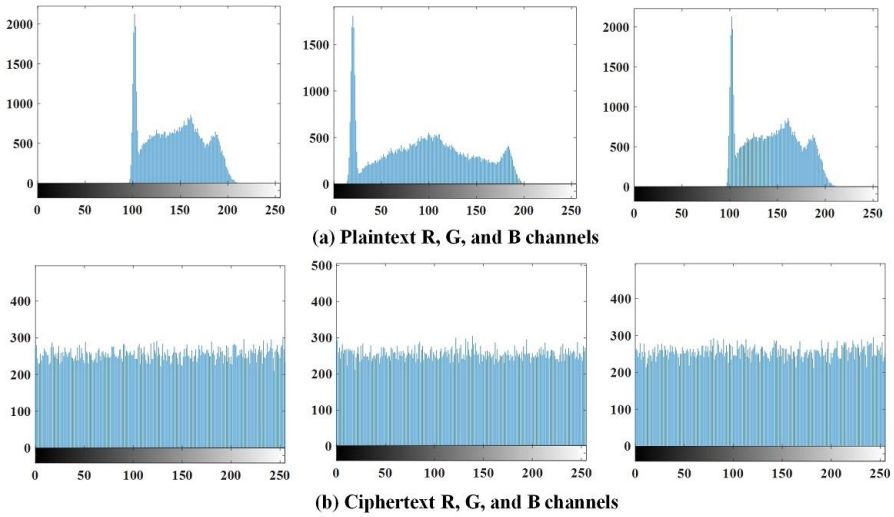

Figure 10. Histogram analysis results of 'Earth'.

5.3.3. Information Entropy Analysis

Image entropy describes the average information content of an image source.

$$H(m) = \sum_{i=0}^{n} p(m_i) \log_2 \frac{1}{p(m_i)}. \tag{18}$$

where n is the sample space, $p(m_i)$ represents the probability of symbol m_i.

The information entropy is shown in Table 8. The information entropy of ciphertext is higher than that of plaintext and close to the theoretical value 8. The ability of this algorithm to resist statistical attack is better than other comparison algorithms.

Table 8. Information entropy of different images.

Image	Proposed Scheme			Ref. [25]			Ref. [26]
	Earth	Baboon	Peppers	Lena	Baboon	Peppers	Mean
Plain image	7.2753	7.6785	7.7038	7.2544	7.6599	7.2118	6.8030
Cipher image	7.9990	7.9989	7.9991	7.9959	7.9959	7.9959	7.9980

5.3.4. Equilibrium Analysis

The zero-watermarking should be balanced for security and measured by E_N.

$$E_N = \frac{|N_0 - N_1|}{N_0 + N_1}, \tag{19}$$

where N_0 and N_1 are the number of '0' and '1'.

An E_N value close to zero means a high equilibrium. The equilibrium of zero-watermarking is shown in Table 9. The equilibrium of this algorithm is 0.0078, and the N_0 and N_1 of zero-watermarking are almost equal.

Table 9. The equalization test results of zero-watermarking.

Image	Proposed	Ref. [27]	Ref. [28]	Ref. [5]
Lena	0.0046	0.0137	0.0117	0.0107
Baboon	0.0098	0.0083	0.0156	0.0093
Peppers	0.0091	0.0142	0.0176	0.0098
Mean	0.0078	0.0122	0.0137	0.0085

5.4. Differential Attack Analysis

NPCR and UACI represent the number of changing pixels between two encrypted images and the average change intensity between two encrypted images, respectively.

$$\mathrm{NPCR} = \frac{1}{W \times H} \times \left\{ \sum_{j=1}^{H} \left[\sum_{i=1}^{W} D(i,j) \right] \right\} \times 100\%, \tag{20}$$

$$\mathrm{UACI} = \frac{1}{W \times H} \left\{ \sum_{j=1}^{H} \left[\sum_{i=1}^{W} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \right\} \times 100\%, \tag{21}$$

where $D(i,j) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j) \\ 0, \text{otherwise} \end{cases}$, C_1 and C_2 represent two ciphertext data and W and H are the length and width.

When the confidence level of gray image is 0.05, the expected values of NPCR and UACI are 99.5693% and (33.2824%, 33.6447%). The NPCR and UACI results are shown in Table 10. NPCR are greater than the expected value and close to 1, and a small change in the plaintext leads to great differences in the ciphertext. The UACI values are within the theoretical interval. The algorithm has a strong anti-differential attack capability.

Table 10. NPCR and UACI test results.

Image	Earth	Baboon	Peppers	Airplane	Sailboat	Fruit
NPCR	99.6104	99.6147	99.6181	99.6251	99.6150	99.6282
UACI	33.4423	33.4632	33.4214	33.4945	33.4964	33.4288

5.5. Attack Analysis

Image transmission will encounter a variety of attacks. It is necessary to recover the image under various attacks and extract clear copyright information.

5.5.1. Anti-Attack Analysis of Ciphertext

Gaussian noise with variance of 0.0001, 0.0003 and 0.0005 and pepper and salt noise with density of 0.01, 0.05 and 0.1 are added to ciphertext, respectively, to test the anti-attack capability. Experimental results are shown in Figure 11. The visual effect of restored images decreases with noise enhancement, but the restored images remain sharp.

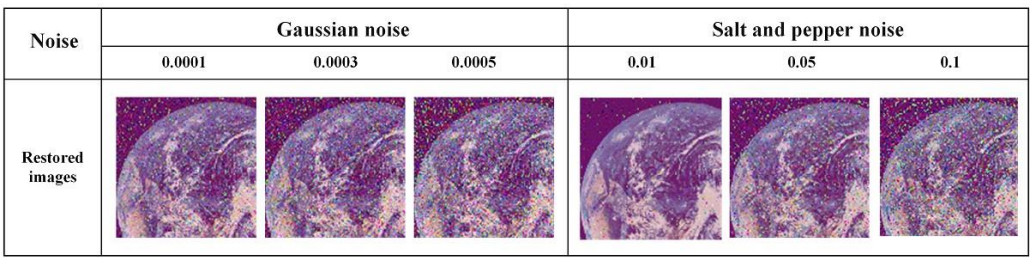

Figure 11. Experimental results of encryption under noise attack.

The experimental results of the anti-noise attack are shown in Table 11. The PSNR value of the restored image decreases with noise enhancement, and the restoration effect becomes worse. The anti-noise capability of this algorithm is better than that of the comparison algorithm.

Table 11. Comparison of experimental results under ciphertext noise attack.

Attack	Gaussian Noise			Salt and Pepper Noise		
	0.0001	**0.0003**	**0.0005**	**0.01**	**0.05**	**0.1**
Proposed	31.0475	29.7909	29.2037	40.1298	33.8694	31.4819
Ref. [12]	11.8431	11.0575	8.6600	-	21.4684	18.4260
Ref. [29]	-	-	-	28.4866	-	18.5106
Ref. [30]	-	-	-	20.28	13.84	11.61

Add six kinds of data loss in ciphertext to test the anti-cropping capability, with loss rates of 10%, 25% and 50%, respectively. Experimental results of the cropping attack are shown in Figure 12. The plaintext can still be recovered after cutting ciphertext in different degrees and ways, which proves its ability to resist cropping attacks.

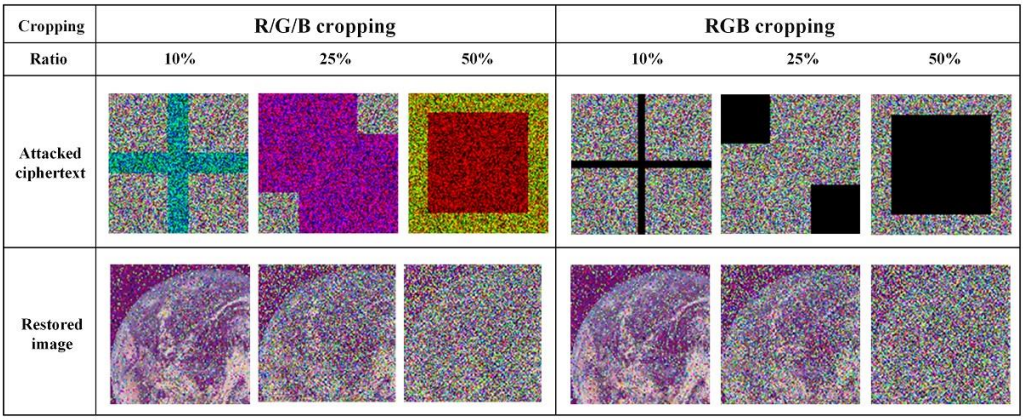

Figure 12. Experimental results of encryption under cropping attack.

Experimental results of image restoration under cropping attack are shown in Table 12. The PSNR value decreases with the increase in cropping area, and the restoration effect deteriorates with the increase in data loss, but it still has better anti-cropping capability than the comparison algorithm.

Table 12. Comparison of experimental results under ciphertext cropping attack.

Cropping Area	Cropping Attack		
	10%	**25%**	**50%**
Proposed	31.6300	28.8645	27.7738
Ref. [29]	18.7021	14.572	11.5940
Ref. [30]	17.35	14.48	11.60
Ref. [23]	17.28	14.47	-

5.5.2. Anti-Attack Analysis of Robust Watermark

Experimental results of the Median filtering attack are shown in Figure 13. The quality of the extracted watermark decreases with the expansion of the filter attack template, but it is still clearly visible.

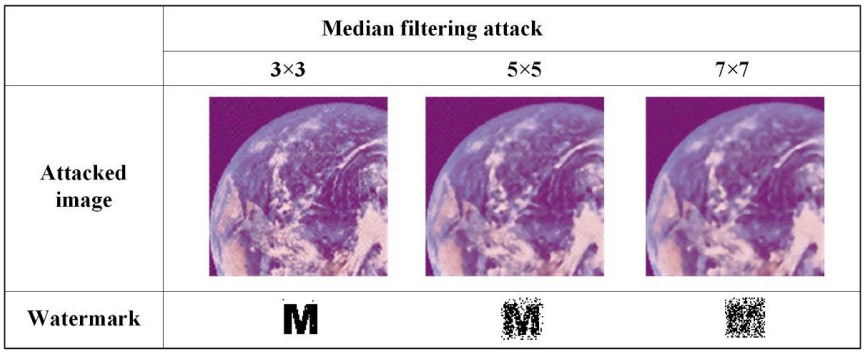

Figure 13. Experimental results of watermark under Median filter attack.

NC can measure the robustness of the watermark. The NC value can indicate the similarity between watermarks; when NC is 1, the two watermarks are completely consistent, and when NC is 0, the two watermarks are not correlated.

The NC values of watermark extraction under Median filter attacks are shown in Table 13. The NC value decreases with the increase in filtering template. Because watermarks are hidden in high frequency of three channels, this algorithm is very sensitive to the modification of the high-frequency components, and Median filters have a great impact on the extracted watermarks. Compared with other algorithms, the quality of watermark extraction for the small filter attack template is better than other algorithms. The quality of the watermark decreases with the filter attack template increase, which is worse than other algorithms.

Table 13. Comparison of experimental results under Median filter attack.

Attack	Factor	Proposed	Ref. [10]	Ref. [11]	Ref. [31]	Ref. [32]
Median filtering	3 × 3	0.9955	0.9873	0.9930	0.9746	0.93
	5 × 5	0.8410	0.9539	-	0.7266	-
	7 × 7	0.7959	0.9120	0.9755	-	0.87

Add Gaussian noise with variances of 0.001, 0.002 and 0.005 and pepper and salt noise with densities of 0.005, 0.01 and 0.02; the test results are shown in Figure 14. The resolution of extracted watermark gradually decreases with noise enhancement, but the visual effect is still good.

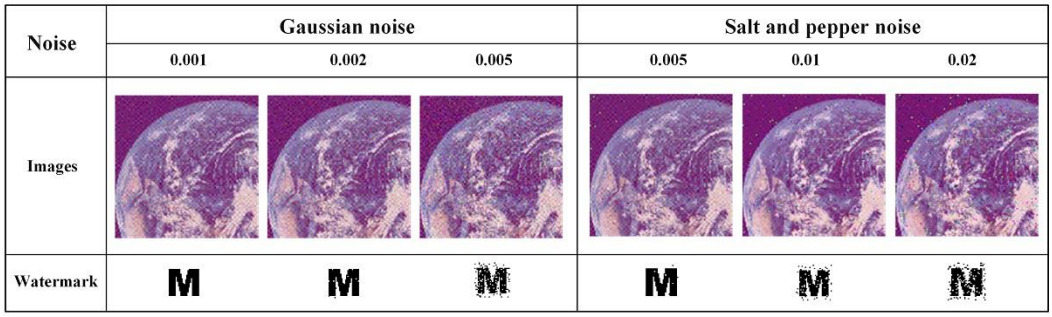

Figure 14. Experimental results of watermark under noise attack.

Experimental results of anti-noise attack are shown in Table 14. NC value decreases continuously with noise enhancement, but it can still meet the requirements of copyright authentication.

Table 14. Comparison of experimental results under noise attack of rubust watermark.

Algorithm		Proposed	Ref. [10]	Ref. [33]	Ref. [34]
Gaussian noise	0.001	1.0000	0.9869	0.9466	0.8984
	0.002	0.9910	0.9816	0.8748	-
	0.005	0.9114	0.9299	-	0.7283
Salt and pepper noise	0.005	0.9928	0.9381	0.9886	0.8823
	0.01	0.9410	-	0.9286	0.8077
	0.02	0.8873	-	0.8673	0.7028

Six different degrees, 8%, 10%, 15%, 19%, 32% and 35%, of data loss are applied to the image. Experimental results of the cropping attack are shown in Figure 15. The extracted watermark is blurred as the cropping area increases. However, even with a cut ratio of 35%, the extracted watermark is still clear.

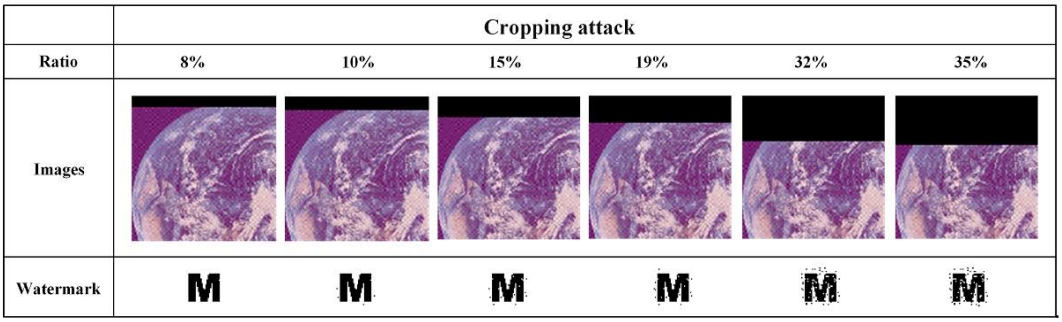

Figure 15. Experimental results of watermark under cropping attack.

The NC values under cropping attack are shown in Table 15. NC value decreases with the increase of cropping area, but it can still resist strong cropping attack.

Table 15. Comparison of experimental results under cropping attack of rubust watermark.

Cropping Area	8%	10%	15%	19%	32%	35%
Proposed	0.9991	0.9955	0.9846	0.9810	0.9429	0.9382
Ref. [32]	0.81	0.80	0.74	0.75	0.59	0.63
Ref. [31]	0.9863	0.9824	-	0.8789	-	-
Ref. [31]	0.984	0.957	-	0.849	-	-
Ref. [11]	-	0.8608	-	0. 8201	-	-

5.5.3. Zero-Watermarking Anti-Attack Analysis

The stronger the robustness of the algorithm, the stronger the ability to resist attacks. The experiments are carried out, and the extracted watermarks are shown in Figure 16. Although the image quality is reduced with filter template expansion and compression quality reduction, it is only slightly affected, and the extracted watermarks are still clear.

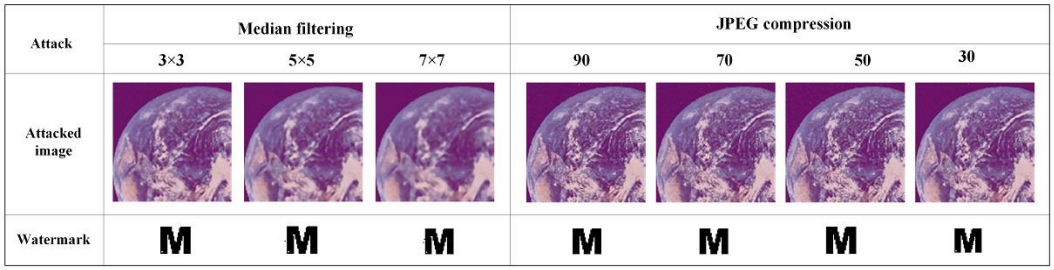

Figure 16. Experimental results of zero-watermarking under Median filter and JEPG compression attack.

The NC values under Median filtering and JEPG compression attacks are shown in Table 16. Under Median filter attack, the NC value decreases with filter template increase, but can still reach 0.9964. The NC value under compression attack can reach 0.9991. The proposed algorithm has better resistance to Median filtering and compression attacks than the comparison algorithm.

Table 16. Comparison of experimental results under Median filter and JEPG compression attack.

Attack	Factor	Proposed	Ref. [27]	Ref. [35]	Ref. [7]	Ref. [36]	Ref. [37]
Median filtering	3 × 3	0.9991	0.9954	0.9961	0.9987	1	0.95
	5 × 5	0.9973	0.9911	0.9883	-	0.999	0.86
	7 × 7	0.9964	0.9874	0.9844	-	0.998	0.80
JPEG compression	90%	1.0000	0.9964	0.9922	1	-	1
	70%	1.0000	0.9911	0.9805	1	-	1
	50%	1.0000	0.9899	0.9727	0.9994	0.9997	0.99
	30%	0.9991	0.9872	0.9570	0.9993	0.999	0.90

The image is rotated 1, 3, 5, 10, 20 and 30 angles in the rotation attack test. The watermark is clear, as shown in Figure 17. Due to rotation correction, the watermark quality is basically unaffected.

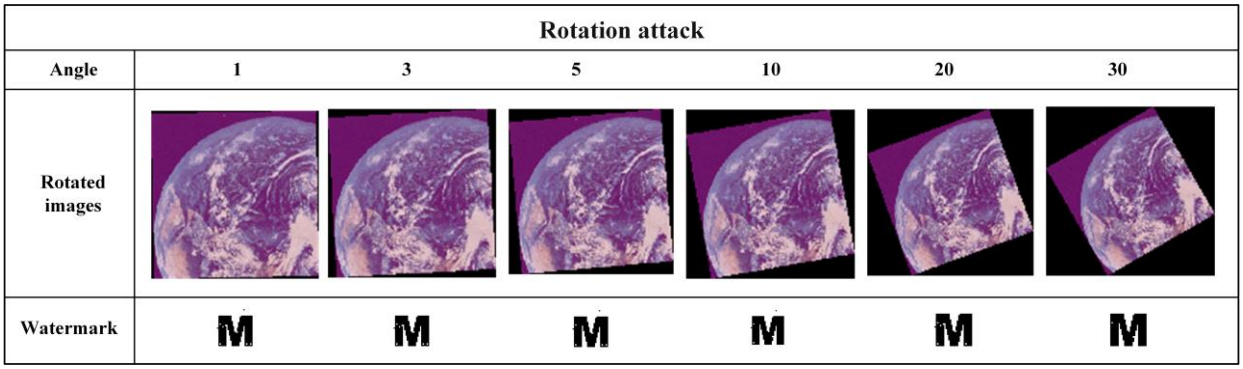

Figure 17. Experimental results of zero-watermarking under rotation attack.

The NC values under rotation attack are shown in Table 17. Correction greatly improves the resist rotation attacks ability, copyright authentication accuracy and robustness.

Table 17. Comparison of experimental results under rotation attack.

Angle	Proposed	Ref. [38]	Ref. [6]	Ref. [39]	Ref. [27]
1°	0.9919	0.980	0.9211	0.9971	0.9536
3°	0.9928	0.936	0.8203	0.9902	0.8691
5°	0.9937	-	0.7569	0.9863	0.8123
10°	0.9955	0.823	0.6636	0.9775	0.7152
20°	0.9937	0.773	-	-	-
30°	0.9982	-	0.5579	-	-

Gaussian noise with a variance of 0.001, 0.02 and 0.025 and pepper and salt noise with a density of 0.01, 0.02 and 0.025 are added, and the results are shown in Figure 18. The watermark clarity gradually decreases with noise enhancement, but it is still very clear.

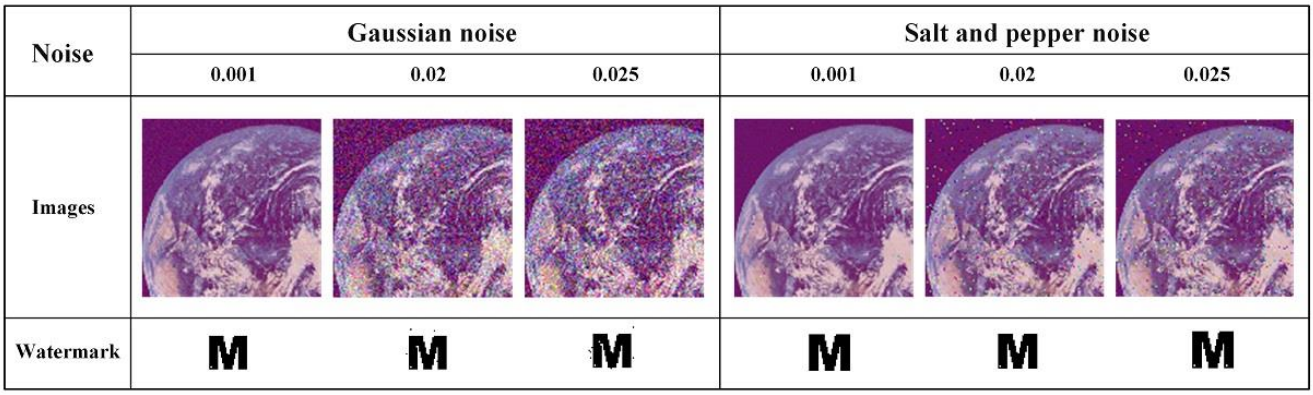

Figure 18. Experimental results of zero-watermarking under noise attack.

The experimental results under noise attack are shown in Table 18. NC value of this algorithm is above 0.99, which can better resist the noise attack compared with other algorithms.

Table 18. Comparison of experimental results under zero-watermarking noise attack.

Algorithm		Proposed	Ref. [40]	Ref. [41]	Ref. [42]	Ref. [43]
Gaussian noise	0.001	0.9991	1	0.9981	0.8508	1
	0.02	0.9946	1	0.9974	0.7645	0.9688
	0.025	0.9909	0.840	-	-	0.9063
Salt and pepper noise	0.001	1.0000	1	0.9885	0.9461	0.9688
	0.02	0.9991	0.949	0.9846	0.9157	0.9375
	0.025	0.9973	0.919	0.9559	0.8952	-

Different ways of data loss are added to the image; cut the selected parts of one channel or all channels, respectively, and select different cropping degrees. Experimental results of the anti-cropping attack are shown in Figure 19. As the cropping area increases, the watermark becomes less clear. But even with a cut ratio of 1/4, the watermark is still clear.

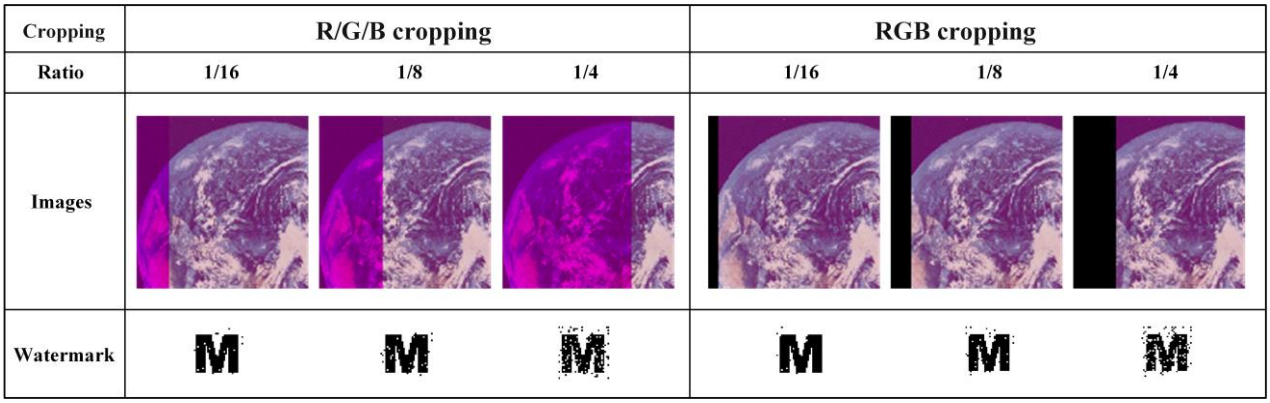

Figure 19. Experimental results of zero-watermarking under cropping attack.

NC values under cropping attack are shown in Table 19. The NC value decreases as the cropping area increases. Even if 1/4 of the original image is cropped, the NC value is still higher than 0.93.

Table 19. Comparison of experimental results under zero-watermarking cropping attack.

Cropping Area	Proposed		Ref. [43]	Ref. [38]	Ref. [31]
	R/G/B	RGB			
1/4	0.9602	0.9337	0.9063	0.892	0.9004
1/8	0.9874	0.9730	0.9063	0.949	0.9824
1/16	0.9937	0.9873	0.9688	0.969	0.9863

Combinatorial attacks have a strong influence on robustness. Five combinatorial attacks are selected for the experiments. The results under the combined attack are shown in Figure 20. The combination attack affects the plaintext greatly, but the watermark changes only slightly.

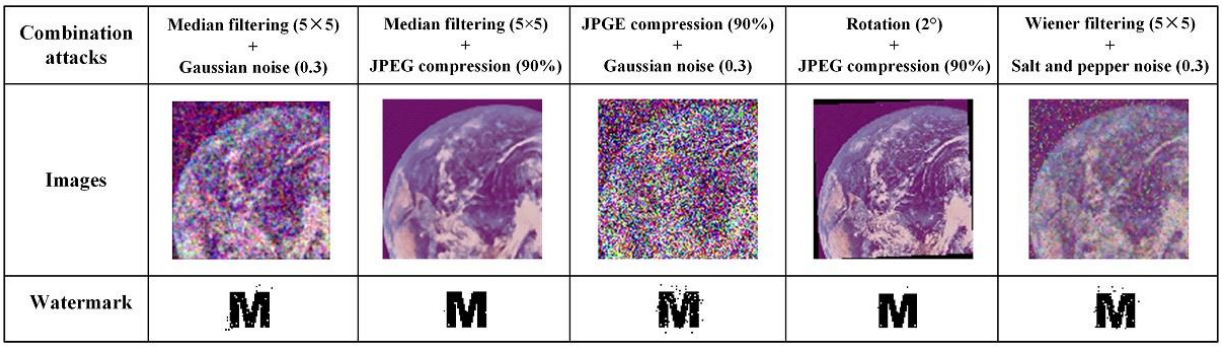

Figure 20. Experimental results of zero-watermarking under combination attack.

NC values under combination attacks are shown in Table 20. Because the image will lose pixels during the cropping process, the integrity of the extracted watermark is affected, but the NC value is still above 0.95. Even in the case of the simultaneous combination interference of multiple attacks, the normalized correlation value for proving their similarity is close to the ideal value of 1 and is higher than that of the comparison algorithm, proving that this algorithm can still guarantee the authentication of copyright under strong attacks.

Table 20. Comparison of experimental results under combination attack.

Combination Attack	Proposed	Ref. [27]	Ref. [6]
Median filtering (5 × 5) + Gaussian noise (0.3)	0.9723	0.9504	0.8901
Median filtering (5 × 5) + JPEG compression (90%)	0.9964	0.9835	0.9762
JPGE compression (90%) + Gaussian noise (0.3)	0.9558	0.9379	0.9551
Rotation (2°) + JPEG compression (90%)	0.9955	0.8989	0.8628
Wiener filtering (5 × 5) + salt and pepper noise (0.3)	0.9720	0.9215	0.8926

5.6. Time Analysis

The encryption process includes the generation of zero-watermarking, robust watermark and image encryption. The running time of the generation of zero-watermarking is 0.706042 s, the embedding time of robust watermark is 0.149570 s and the image encryption time is 8.567327 s. The decryption process includes decrypting ciphertext, robust watermark authentication copyright and zero-watermarking authentication copyright. The running time of decrypting ciphertext is 5.702601, the time of robust watermark authentication copyright is 0.097688 s and the time of zero-watermarking authentication copyright is 0.105223 s. The algorithm authenticates copyright through dual watermarking, protects image information through encryption and increases the running time, so the security is improved by increasing the complexity.

6. Conclusions

A dual watermark algorithm based on chaotic map and DNA image encryption is proposed. The STBCS chaotic system was designed, which can generate chaotic sequences related to plaintext. The DNA mutation algorithm was designed to encrypt the copyright image information, and the encrypted watermark embedding algorithm was designed to ensure the security and invisibility of the watermark. A zero-watermark for secondary protection was designed, which is significantly different from the robust watermark, has balance and can resist statistical analysis attacks. Image encryption, robust watermarking and zero watermarking provide multiple protections for image security. The experimental results show that the algorithm can resist exhaustive attacks, and is sensitive to key, and is robust under compression and Median filtering, noise, cropping and rotation attacks.

This algorithm verifies copyright through double watermarking, which improves security while prolonging the running time. In the future, we will attempt to optimize the watermarking algorithm to shorten the running time while ensuring robustness.

Author Contributions: R.C. provided the idea of algorithms, carried out the simulations, arranged the architecture and drafted the manuscript. J.M. and Y.C. revised the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the Basic Scientific Research Operation Fund of Liaoning Provincial Universities in 2024 (LJ212410152016).

Data Availability Statement: The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest: We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

1. Gao, S.; Zhang, Z.; Iu, H.H.-C.; Ding, S.; Mou, J.; Erkan, U.; Toktas, A.; Li, Q.; Wang, C.; Cao, Y. A Parallel Color Image Encryption Algorithm Based on a 2-D Logistic-Rulkov Neuron Map. *IEEE Internet Things J.* **2025**, *12*, 18115–18124. [CrossRef]
2. Zhou, S.; Wei, Y.; Zhang, Y.; Iu, H.H.-C.; Zhang, H. Image encryption algorithm based on the dynamic RNA computing and a new chaotic map. *Integration* **2025**, *101*, 102336. [CrossRef]
3. Zhou, S.; Yin, Y.; Erkan, U.; Toktas, A.; Zhang, Y. Novel hyperchaotic system: Implementation to audio encryption. *Chaos Solitons Fractals* **2025**, *193*, 116088. [CrossRef]
4. Wen, Q.; Sun, T.; Wang, S. Based zero-watermark digital watermarking technology. In Proceedings of the 3rd National Conference in Information Hiding; Xidian University Press: Xian, China, 2001; Volume 109, pp. 102–109. [CrossRef]
5. Kang, X.; Zhao, F.; Chen, Y.; Lin, G.; Jing, C. Combining polar harmonic transforms and 2D compound chaotic map for distinguishable and robust color image zero-watermarking algorithm. *J. Vis. Commun. Image Represent.* **2020**, *70*, 102804. [CrossRef]
6. Xiong, X.G. A Zero Watermarking Scheme with Strong Robustness in Spatial Domain. *Acta Autom. Sin.* **2018**, *44*, 160–175. [CrossRef]
7. Jiang, F.; Gao, T.; Li, D. A robust zero-watermarking algorithm for color image based on tensor mode expansion. *Multimed. Tools Appl.* **2020**, *79*, 7599–7614. [CrossRef]
8. Chen, J.; Sun, Y.; Yang, M. Zero-Watermarking Algorithm Based on Modified Singular Value and Chaos Scrambling. In *International Conference on Intelligent Automation and Soft Computing*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1091–1098. [CrossRef]
9. Xi, X.; Zhang, X.; Liang, W.; Xin, Q.; Zhang, P. Dual Zero-Watermarking Scheme for Two-Dimensional Vector Map Based on Delaunay Triangle Mesh and Singular Value Decomposition. *Appl. Sci.* **2019**, *9*, 642. [CrossRef]
10. Shi, H.; Weng, K.; Song, T.; Feng, Z. Dual-watermarking scheme for copyright and privacy protection in medical image. *Joummal Liaoning Norm. Univ.* **2023**, *46*, 43–55.
11. Miao, W.; Deyang, W.; Hu, S.; Jiayan, W.; Yan, W.; Haibo, J.; Wave, S.L. Double Watermarking Algorithm for Tamper Detection of Medical Images. *Laser Optoelectron. Prog.* **2023**, *60*, 0617001. [CrossRef]
12. Sha, Y.; Bo, S.; Yang, C.; Mou, J.; Jahanshahi, H. A chaotic image encryption scheme based on genetic central dogma and kmp method. *Int. J. Bifurc. Chaos* **2022**, *32*, 2250186. [CrossRef]

13. Zhou, S.; Zhang, H.; Zhang, Y.; Iu, H.H.-C.; Zhang, H. Constructing a novel n-dimensional chaotic map with application to image encryption. *Int. J. Mod. Phys. C* **2025**, *36*, 1–28. [CrossRef]
14. Zhou, S.; Liu, H.; Iu, H.H.-C.; Erkan, U.; Toktas, A. Novel n-Dimensional Nondegenerate Discrete Hyperchaotic Map with Any Desired Lyapunov Exponents. *IEEE Internet Things J.* **2025**, *12*, 9082–9090. [CrossRef]
15. Gao, S.; Iu, H.H.-C.; Erkan, U.; Simsek, C.; Toktas, A.; Cao, Y.; Wu, R.; Mou, J.; Li, Q.; Wang, C. A 3D Memristive Cubic Map with Dual Discrete Memristors: Design, Implementation, and Application in Image Encryption. In *IEEE Transactions on Circuits and Systems for Video Technology*; IEEE: Piscataway, NJ, USA, 2025; p. 1. [CrossRef]
16. Hua, Z.; Zhou, B.; Zhou, Y. Sine-Transform-Based Chaotic System with FPGA Implementation. *IEEE Trans. Ind. Electron.* **2018**, *65*, 2557–2566. [CrossRef]
17. Xu, J.; Mou, J.; Xiong, L.; Li, P.; Hao, J. A flexible image encryption algorithm based on 3D CTBCS and DNA computing. *Multimed. Tools Appl.* **2021**, *80*, 25711–25740. [CrossRef]
18. Han, X.; Mou, J.; Jahanshahi, H.; Cao, Y.; Bu, F. A new set of hyperchaotic maps based on modulation and coupling. *Eur. Phys. J. Plus* **2022**, *137*, 1–13. [CrossRef]
19. Sinhal, R.; Ansari, I.A. A multipurpose image watermarking scheme for digital image protection. *Int. J. Syst. Assur. Eng. Manag.* **2019**, *11*, 274–286. [CrossRef]
20. Wei, X.; Guo, L.; Zhang, Q.; Zhang, J.; Lian, S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *J. Syst. Softw.* **2012**, *85*, 290–299. [CrossRef]
21. Gao, X.; Yu, J.; Banerjee, S.; Yan, H.; Mou, J. A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion. *Sci. Rep.* **2021**, *11*, 15737. [CrossRef]
22. Joo, J.; Zhu, K.; Cheng, J. Color image encryption via compressive sensing and chaotic systems. *MATEC Web Conf.* **2020**, *309*, 03017. [CrossRef]
23. Chai, X.; Fu, X.; Gan, Z.; Lu, Y.; Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* **2019**, *155*, 44–62. [CrossRef]
24. Gan, Z.; Bi, J.; Ding, W.; Chai, X. Exploiting 2D compressed sensing and information entropy for secure color image compression and encryption. *Neural Comput. Appl.* **2021**, *33*, 12845–12867. [CrossRef]
25. Joshi, A.B.; Kumar, D.; Gaffar, A.; Mishra, D.C. Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform. *Opt. Lasers Eng.* **2020**, *133*, 106139. [CrossRef]
26. Wang, X.; Xu, M.; Li, Y. Fast encryption scheme for 3D models based on chaos system. *Multimed. Tools Appl.* **2019**, *78*, 33865–33884. [CrossRef]
27. Kang, X.; Lin, G.; Chen, Y.; Zhao, F.; Zhang, E.; Jing, C. Robust and secure zero-watermarking algorithm for color images based on majority voting pattern and hyper-chaotic encryption. *Multimed. Tools Appl.* **2019**, *79*, 1169–1202. [CrossRef]
28. Hosny, K.M.; Darwish, M.M.; Fouda, M.M. New Color Image Zero-Watermarking Using Orthogonal Multi-Channel Fractional-Order Legendre-Fourier Moments. *IEEE Access* **2021**, *9*, 91209–91219. [CrossRef]
29. Nazir, L.P.; Deep, S.; Hussain, M.U. Image encryption using DNA coding and three-dimensional chaotic systems. *Multimed. Tools Appl.* **2022**, *81*, 5669–5693.
30. Zhang, D.; Chen, L.; Li, T. Hyper-Chaotic Color Image Encryption Based on Transformed Zigzag Diffusion and RNA Operation. *Entropy* **2021**, *23*, 361. [CrossRef]
31. Kazemi, M.F.; Mazinan, A.H. Neural network based CT-Canny edge detector considering watermarking framework. *Evol. Syst.* **2021**, *13*, 145–157. [CrossRef]
32. Zhang, W.; Li, J.; Bhatti, U.A.; Liu, J.; Zheng, J.; Chen, Y.-W. Robust Multi-Watermarking Algorithm for Medical Images Based on GoogLeNet and Henon Map. *Comput. Mater. Contin.* **2023**, *75*, 565–586. [CrossRef]
33. Zear, A.; Singh, A.K.; Kumar, P. A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. *Multimed. Tools Appl.* **2016**, *77*, 4863–4882. [CrossRef]
34. Singh, A.K. Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. *Multimed. Tools Appl.* **2019**, *78*, 30523–30533. [CrossRef]
35. Liu, F.; Ma, L.H.; Liu, C.; Lu, Z.M. Zero watermarking scheme based on U and V matrices of quaternion singular value decomposition for color images. *J. Inf. Hiding Multimed. Signal Process.* **2018**, *9*, 629–640.
36. Zheng, Q.; Liu, N.; Cao, B.; Wang, F.; Yang, Y. Zero-watermarking algorithm in transform domain based on RGB channel and voting strategy. *J. Inf. Process. Syst.* **2020**, *16*, 1391–1406. [CrossRef]
37. Wang, Y.-R.; Lin, W.-H.; Yang, L. An intelligent watermarking method based on particle swarm optimization. *Expert Syst. Appl.* **2011**, *38*, 8024–8029. [CrossRef]
38. Jiang, Z.T.; Chen, W. Zero-watermarking algorithm for color image based on DWT-DCT-SVD. *Microelectron. Comput.* **2016**, *33*, 107–111. [CrossRef]
39. Song, W.; Hou, J.J.; Li, Z.H.; Huang, L. A novel zero-bit watermarking algorithm based on Logistic chaotic system and singular value decomposition. *Acta Phys. Sin.* **2009**, *58*, 4449–4456. [CrossRef]

40. Chen, Q.; Weng, X. Novel blind image watermarking based on pseudo Zernike moments. *Appl. Res. Comput.* **2016**, *33*, 2810–2813. [CrossRef]
41. Liu, W.; Sun, S.; Haicheng, Q.U.; Software, C.O.; University, L.T. Fast Zero-Watermarking Algorithm Based on Schur Decomposition. *J. Front. Comput. Sci. Technol.* **2019**, *13*, 494. [CrossRef]
42. Zhang, H.; Zhang, S.; University, L.T. Research on zero watermarking algorithm for hyper-chaos-based image. *Appl. Res. Comput.* **2019**, *36*, 3387–3391. [CrossRef]
43. Pan, H.; Chen, G.; Yong, D. A zero-watermark algorithm of color image based on DWT and SVD. *J. Guilin Univ. Electron. Technol.* **2011**, *31*, 399–402. [CrossRef]