electronics

MDPI

Article

Optical Color Image Encryption Algorithm Based on Two-Dimensional Quantum Walking

Guohao Cui [1], Xiaoyi Zhou [1], Hao Wang [1], Wentao Hao [1], Anshun Zhou [2] and Jianqiang Ma [1,*]

[1] School of Cyberspace Security, Hainan University, Haikou 570228, China; 21210839000004@hainanu.edu.cn (G.C.); xy.zhou@hainanu.edu.cn (X.Z.); 20213007681@hainanu.edu.cn (H.W.); 21220854000051@hainanu.edu.cn (W.H.)

[2] China Unicom (Hainan) Innovation Research Institute, Haikou 570100, China; zhouanshun@chinaunicom.cn

* Correspondence: hdmjq@hainanu.edu.cn

Abstract: The double random phase encoding (DRPE) image encryption method has garnered significant attention in color image processing and optical encryption thanks to its R, G, and B parallel encryption. However, DRPE-based color image encryption faces two challenges. Firstly, it disregards the correlation of R, G, and B, compromising the encrypted image's robustness. Secondly, DRPE schemes relying on Discrete Fourier Transform (DFT) and Discrete Fractional Fourier Transform (DFRFT) are vulnerable to linear attacks, such as Known Plaintext Attack (KPA) and Chosen Plaintext Attack (CPA). Quantum walk is a powerful tool for modern cryptography, offering robust resistance to classical and quantum attacks. Therefore, this study presents an optical color image encryption algorithm that combines two-dimensional quantum walking (TDQW) with 24-bit plane permutation, dubbed OCT. This approach employs pseudo-random numbers generated by TDQW for phase modulation in DRPE and scrambles the encrypted image's real and imaginary parts using the generalized Arnold transform. The 24-bit plane permutation helps reduce the R, G, and B correlation, while the generalized Arnold transform bolsters DRPE's resistance to linear attacks. By incorporating TDQW, the key space is significantly expanded. The experimental results validate the effectiveness and security of the proposed method.

Keywords: optical color image encryption; image encryption; two-dimensional quantum walking; double random phase encoding

check for updates

Citation: Cui, G.; Zhou, X.; Wang, H.; Hao, W.; Zhou, A.; Ma, J. Optical Color Image Encryption Algorithm Based on Two-Dimensional Quantum Walking. *Electronics* **2024**, *13*, 2026. https://doi.org/10.3390/electronics13112026

Academic Editor: Andreas Mauthe

Received: 5 April 2024
Revised: 12 May 2024
Accepted: 17 May 2024
Published: 22 May 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

As network and information technologies advance, digital image security faces considerable risks during storage, transmission, and reception, prompting cryptography to emerge as an effective means of safeguarding images [1,2]. In comparison to grayscale images, color images offer richer information. Optical image encryption, with its benefits of parallelism and flexibility, enables concurrent encryption of the R, G, and B of color images, drawing growing interest from researchers [3,4].

In the realm of optical image encryption, various optical encryption techniques have been proposed, including full-phase encryption [5], amplitude-based encryption [6], and polarization-encoding encryption [7,8]. Among various techniques, the Fractional Fourier Transform (FrFT) is frequently used to manipulate polarization information in the time domain [9–11], whereas the Optical Fourier Transform (OFT) finds application in the encoding process [12,13]. OFT typically consists of two cascaded lenses, and cascaded phase structures are one of the most commonly used optical structures in light field modulation. This structure was first applied to the Double Random Phase Encoding (DRPE) system by Javidi et al. in 1996. DRPE modulates waves by introducing two random phase masks to scramble spatial and frequency domains, resulting in ciphertext without white noise [14,15]. DRPE has become one of the most commonly used and effective optical encryption schemes [16,17].

Thanks to the parallelism inherent in DRPE, the three components of R, G, and B can all be encrypted concurrently. Faragallah O's proposed algorithm involves encrypting a color image's R, G, and B three times independently [18]. Nonetheless, the color image remains susceptible to attacks because of the strong correlation between R, G, and B [19]. Wang Yonghui put forth an optical single-channel color image encryption approach rooted in chaotic fingerprint phase masks and diffraction imaging [20]. Independently encrypting the R, G, and B three times in color images does not provide adequate defense against attacks; as stated in the existing literature [15,18], color encryption systems based on DRPE have exposed the following two key issues.

Issue 1: Ignoring the correlation of R, G, and B will lead to decreased robustness of the encrypted image. It has been demonstrated that reducing the correlation values between R, G, and B can effectively lower the correlation of DRPE images, thereby enhancing the robustness of the encryption system [21,22].

Issue 2: The DRPE system itself is susceptible to linear analysis attacks. This linear transformation allows two random phase masks (RPMs) to be guessed through Known Plaintext Attack (KPA)/Chosen Plaintext Attack (CPA)/Ciphertext-Only Attack (COA), consuming significantly fewer resources compared to brute force attacks [21,22].

To tackle Issue 1, Yildirim M proposed a DRPE scheme based on chaotic system-based sub-block image swapping [23] and another DRPE scheme based on a chaotic system and DNA-encoding algorithm [24]. These schemes reduce the correlation of R, G, and B and have been experimentally demonstrated to possess good robustness. However, they overlook the issue of the weak linear analysis capability of DRPE, resulting in Issue 2. Further analysis [23,24] reveals that while these schemes significantly improve robustness by reducing the correlation of R, G, and B, they do not conduct in-depth analysis. Lowering the correlation of R, G, and B disrupts the {0, 1} bit sequence values of the pixel's three categorized R, G, and B. This paper hypothesizes that directly scrambling the bits of a color image would disrupt the {0, 1} sequence values and reduce the correlation at the bit level, potentially enhancing the image's robustness. The experiments conducted in this paper ultimately validate this hypothesis.

To tackle Issue 2, numerous scholars have explored nonlinear optical image encryption methods. Qin W and colleagues introduced a cutting-edge secure nonlinear cryptosystem in the Fourier transform domain, leveraging phase truncation techniques. It effectively addressed the linear vulnerabilities present in the DRPE system [25], but was later deciphered by Wang X et al. [26]. In addition, Li Ming put forth an attack scheme targeting a specific type of DRPE encryption system that relies on scrambling and diffusion. This scheme can efficiently breach DRPE encryption systems by employing scrambling and diffusion mechanisms [27]. Zhou Qingming and colleagues presented a novel optical image encryption method that relies on dual-channel detection and deep learning. While this scheme demonstrates good performance, it demands significant time [28]. Singh P and colleagues strengthened the DRPE system's resilience against statistical analysis attacks by incorporating nonlinear terms [29].

In some cases, chaotic systems may exhibit periodic orbits, which renders them partially predictable to attackers with computational capabilities [30,31]. Unlike chaotic systems, the essence of quantum walk lies in the unique properties of microscopic particles. These quantum particles exhibit wave–particle duality, meaning they can simultaneously exist in vastly different wave and particle states [18]. In quantum image encryption methods, the quantum principles, including the inherent unpredictability and quantum entanglement, are utilized to achieve theoretically absolute security during data transmission [31]. This field has garnered significant academic attention since Aharonov et al.'s groundbreaking research on quantum walks in 1993 [32]. In 2023, Rehman M U et al. proposed a color image encryption scheme that integrates multiple encryption techniques, including alternating quantum random walks, controlled Rubik's cube transformations, an integrated system of Elliptic Curve Cryptosystem and Hill Cipher (ECCHC), and DNA encoding [33]. Although this scheme theoretically has an infinitely large cube encryption capability, it may

be limited by computer precision in practical applications. For the encryption of large-scale images or a large number of images, the efficiency and practicality of this scheme remain to be verified.

Furthermore, the core of Rehman M U's scheme lies in DNA encoding. Schemes based on DNA encoding have insufficient defenses against chosen plaintext and noise attacks. Conversely, the virtual optical DRPE image encryption technology can employ various physical parameters (frequency, orbital angular momentum, phase, amplitude, polarization, etc.) as keys, providing higher security and key space. In terms of encryption speed and efficiency, DNA encryption involves complex biochemical reactions that affect its speed and efficiency. In contrast, DRPE encryption utilizes optical parallel processing capabilities to achieve fast image transmission and processing. In terms of technological maturity and practicality, DNA encryption is still in the research and experimental stages, and its practicality and maturity remain to be verified [33]. In contrast, DRPE encryption technology has been widely researched and applied domestically and internationally. In 2023, Hu M et al. introduced a quantum image encryption scheme that combines a novel cross-two-dimensional chaotic map based on a sine and logistic chaotic system proposed by the team [34]. The new system exhibits a hyperchaotic state compared to traditional sine and logistic chaotic systems. However, Miaoting Hu's core focus is on the chaotic system rather than the quantum image encryption scheme itself. When considering only the chaotic system, its key space is minimal. When focusing solely on the quantum image encryption scheme, it is still in the research and experimental stages, and its practicality and maturity need further verification. Converting images to a quantum state for encryption remains a debatable issue [34]. In 2022, Hu W et al. proposed a quantum color image encryption algorithm based on a three-dimensional chaotic system [21]. The encrypted quantum color image undergoes scrambling operations through the Arnold and three-dimensional chaotic systems. Like Miaoting Hu's scheme, Hu W's core viewpoint is that chaotic systems are not quantum encryption schemes. In 2023, Gao X et al. introduced a color image encryption algorithm based on a hyperchaotic map and DNA mutation [35]. The core component of this scheme remains DNA, and it faces similar issues to those encountered by Rehman M U. In 2024, Arslan Shafique presented an image encryption scheme rooted in Support Vector Machines (SVM) [36]. This approach eliminates redundant information and retains crucial data for encryption. However, it is a lossy encryption scheme, focusing on the problem of lossless encryption discussed in this paper. In conclusion, designing a reliable DRPE image encryption system grounded in quantum walks holds immense significance.

This paper draws inspiration from the theories of nonlinear chaotic systems and nonlinear AES [37], exploring the possibility of incorporating nonlinear correlation algorithms into DRPE to enhance its resistance against linear attacks. Consequently, the OCT (Optical Color Image Encryption) scheme was implemented, with an improved DRPE as the core encryption algorithm. A two-dimensional quantum walk was employed to optimize the optical encryption algorithm, further enhancing the encryption effectiveness and security. The experimental results indicate that the proposed scheme lowers the correlation among the R, G, and B components and reinforces the DRPE system's immunity to linear attacks, specifically CPA and KPA. The main contributions of this paper are as follows:

(I) The analysis reveals that the increased robustness of encrypted images after reducing the correlation of R, G, and B stems from the enhanced robustness achieved by lowering the correlation between the 24-bit plane layers. Therefore, the paper proposes a scheme utilizing 24-bit plane permutation to reduce the correlation of R, G, and B in color images.

(II) The paper introduces the generalized Arnold transformation to independently permute the real and imaginary parts of the complex matrix obtained after DRPE encryption. The experimental results demonstrate that this approach effectively enhances resistance against linear analysis attacks such as CPA and KPA.

(III) The incorporation of a two-dimensional quantum walk into the optical image encryption scheme is presented. It is noted that two-dimensional quantum walks exhibit better randomness compared to chaotic systems.

The subsequent sections of this paper are structured as follows: In Section 2, the author introduces two-dimensional quantum walk (TDQW) and double random phase encoding (DRPE) image encryption. Section 3 offers comprehensive details about the image encryption system's various components and experimental steps. Section 4 showcases simulation results, evaluates the security performance, and conducts a comparative analysis. Lastly, Section 5 summarizes the entire paper.

2. Preliminaries

2.1. Double Random Phase Encoding (DRPE)

In 1995, Javidi and Refregier proposed a DRPE system composed of four focal-length lenses (4-f), a brand-new image encryption technology [14,15]. In 2020, Abd-El-Atty B proposed a new encryption method based on quantum walks (QWs) and DRPE technology, introducing quantum walks into optical image encryption [19]. Image encryption and decryption are achieved through the Fourier transform utilizing lenses., as shown in Figure 1. This chapter will introduce the basic principle and computer simulation method of double random phase optical image encryption. The standard 4f system is realized in Figure 1; RM1 () represents mask 1, which represents the original image; and Lens1's front focal plane is RM1 () and is coherent. The collimated light of unit amplitude on the front focal plane P_{e_1} is the vertical illumination. Another random phase mask is RM2 () in the FT plane. After the IFT of Lens2, the Lens2 rear focal plane P_{e_3} stands for the encrypted image, as shown in Equation (1):

$$g(x,y) = FFT^{-1}\left\{FFT\left\{f(x,y)\cdot e^{j2\pi\varphi(x,y)}\right\}\cdot e^{j2\pi\psi(\mu,\nu)}\right\} \tag{1}$$

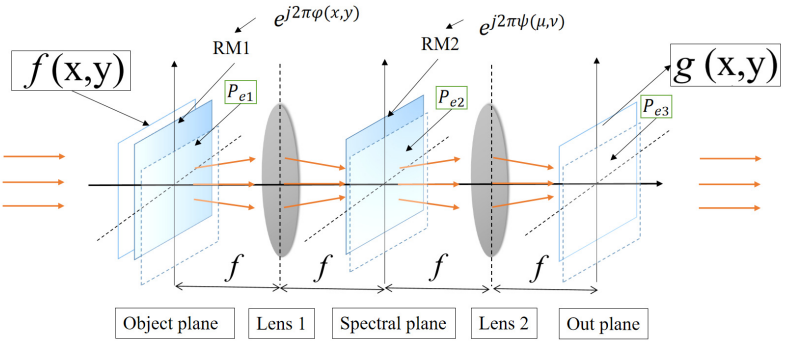


Figure 1. Double random phase encoding (DREP).

In Equation (1), $f(x,y)$ represents the original image, $g(x,y)$ represents the encrypted images, $FFT\{\cdot\}$ and $FFT^{-1}\{\cdot\}$ represent FT and IFT, and $e^{j2\pi\varphi(x,y)}$ and $e^{j2\pi\psi(\mu,\nu)}$ are two random phase plates. In the equation involving $\varphi(x,y)$ and $\psi(\mu,\nu)$, the selection of values (x,y) and (μ,ν) is determined by a random number generator, whose values are randomly distributed among $[0,1]$. Therefore, these are two independent random white noises. Similarly, the decryption formula is as follows in Equation (2):

$$f\prime(x,y) = FFT^{-1}\left\{FFT\left\{g(x,y)\cdot e^{-j2\pi\varphi(x,y)}\right\}\cdot e^{-j2\pi\psi(\mu,\nu)}\right\} \tag{2}$$

In Equation (2), $f\prime(x,y)$ is the decrypted image; the other elements are consistent with the encryption process described above; and it is evident that the decryption process is essentially the reverse of the encryption operation.

2.2. Improved DREP

The generalized Arnold transform algorithm is an extension and improvement of the Arnold algorithm, which was used in image encryption by Sun, Gege et al. in 2024 [30]. Discrete generalized Arnold mapping transformation and inverse transformation formulas

can be expressed as Equations (3) and (4), where a and b are real numbers: $x_n, y_n \in [0, 1)$. In Guodong Ye's scheme, generalized Arnold introduces a chaotic system to initialize a and b to be real numbers, which solves the periodicity problem of the Arnold algorithm. To improve the DRPE's ability to resist KPA and CPA, this paper uses a two-dimensional quantum walk to initialize the selection matrix of a and b in generalized Arnold and introduces it into the DRPE scheme. $g(x, y)$ is the image after Fourier transformation; the pixels of the encrypted image are complex, as shown in Equation (5).

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 1 & b \\ a & 1+ab \end{bmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} mod(N); \tag{3}$$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 1+ab & -b \\ -a & 1 \end{bmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} mod(N) \tag{4}$$

$$pixelZ = \gamma + \delta_i. \tag{5}$$

where $pixelZ$ is a complex pixel consisting of real and imaginary parts, satisfying the equation $|pixelZ| = \sqrt{\gamma^2 + \delta^2}$, γ represents the real part, and δ indicates the imaginary part. The optical encryption image $g(x, y)$ is decomposed into real matrix $\|\gamma\|$ and imaginary matrix $\|\delta\|$, and then generalized Arnold transformation is applied separately. The transformed real matrix and imaginary matrix are combined into a complex matrix $g\prime(x, y)$, which represents the Arnold encryption image. Therefore, from Equation (5), the improved DRPE equation can be derived as Equation (6):

$$g'(x, y) = IFT\{FT\{f(x, y) \cdot RM_1\} \cdot RM_2\} \cdot Arnold. \tag{6}$$

In Equation (6), FT represents FFT, IFT represents FFT^{-1}, RM_1 represents $e^{j2\pi\varphi(x,y)}$, and RM_2 represents $e^{j2\pi\psi(\mu,\nu)}$. The encryption algorithm is described by Algorithm 1, where the *img_fft* represents the encrypted image $g(x, y)$ and the *img_complex* represents the encrypted image $g\prime(x, y)$.

Algorithm 1: Improved DRPE algorithm

Input: img_fft,X(sequence generated by the TDQW);
Output: img_complex
Process:

```
//The function of Arnold complex matrix
function img_complex = deComplexIArnold(img_fft,X)
    A_re = real(img_fft);
    A_im = imag(img_fft);
    imgnE_re = makeIArnold(A_re,X);
    imgnE_im = makeIArnold(A_im,X);
    img_complex = complex(imgnEA_re, imgnE);
end
//The functionof Generalized Arnold
function A = makeArnold(P,X)
    [M,N] = size(P); A = P;
    a = reshape(X(1:M*N),M,N);
    for i = 1:M
        for j = 1:N
            k = mod ([1 a (i, j); b (i, j) a (i, j) * b (i, j) + 1] * [i; j], [M, N]) + [1; 1];
            t = A(i,j); A(i,j) = A(k(1),k(2)); A(k(1),k(2)) = t;
        end
    end
end
```

2.3. Two-Dimensional Quantum Walking (TDQW)

The one-dimensional quantum walk is a quantum extension of classical random walks, while the two-dimensional quantum walk further generalizes this concept. In classical random walks, each step of the walker is influenced by random step lengths and directions, resulting in a degree of uncertainty. However, two-dimensional discrete quantum walks differ in that they combine position space and coin space, collectively constructing the state space of quantum walkers. TDQW was utilized by Hao et al. in 2023 for image encryption [31] and extends the concept of a one-dimensional discrete quantum walk. The state space for quantum wandering encompasses both position space (S) and coin space (C). Typically, the entire system can be represented as $U = S \cdot (C \bigotimes I)$. A TDQW system comprises a walker U, two coin evolutions C, and an observation set. The coin space, represented by a two-dimensional Hilbert space $\mathcal{H}_c$, characterizes the coin's state on the x-axis, while $\mathcal{H}_{c_x}$ and $\mathcal{H}_{c_y}$ depict the coin's state on the y-axis. $\mathcal{H}_c = \mathcal{H}_{c_x} \otimes \mathcal{H}_{c_y}$ are included.

The evolution operator of quantum wandering consists of conditional transfer and coin operators: coin operator $\hat{C}$ by $\hat{C}_x$ and $\hat{C}_y$. In this paper, we take the coin operator as the Hadamard operator, as shown in Equations (7)–(9).

$$\hat{C}_x = \hat{H}_x = \frac{1}{\sqrt{2}}(|0\rangle_{cx}\langle 0| + |0\rangle_{cx}\langle 1| + |1\rangle_{cx}\langle 0| - |1\rangle_{cx}\langle 1|) \tag{7}$$

$$\hat{C}_y = \hat{H}_y = \frac{1}{\sqrt{2}}\Big(|0\rangle_{cy}\langle 0| + |0\rangle_{cy}\langle 1| + |1\rangle_{cy}\langle 0| - |1\rangle_{cy}\langle 1|\Big) \tag{8}$$

$$\forall x \in S, p \in P(f), nf|f^n(x)| - |f^n(y)| = 0 \tag{9}$$

Condition: The transfer operator is $\hat{S}$ by $\hat{S}_x$ and $\hat{S}_y$ composition, which determines the position of motion. The operator S, taking one step to the left, is shown in Formula (10), and that taking one step to the right is shown in Formula (11):

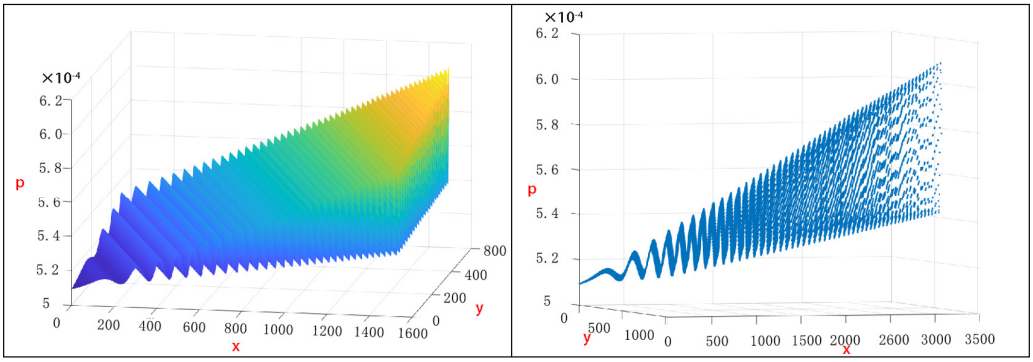
$$\hat{S}_x = |0\rangle_{cx}\langle 0| \otimes \sum_i |i+1\rangle_{px}\langle i| + |1\rangle_{cx}\langle 1| \otimes \sum_i |i-1\rangle_{px}\langle i| \tag{10}$$

$$\hat{S}_y = |0\rangle_{cy}\langle 0| \otimes \sum_j |j+1\rangle_{py}\langle j| + |1\rangle_{cy}\langle 1| \otimes \sum_j |j-1\rangle_{py}\langle j| \tag{11}$$

The probability amplitude of TDQW is described using Fourier integration's smooth-phase method, which involves converting the walker's time domain space to the frequency domain through Fourier transformation. After the t steps, a specific formula can determine the discrete quantum state (12). R or L means the walker goes to the right or left, and F or B means the walker goes forward or backward. $\mathrm{k} \in [-\pi, \pi], \mathrm{x} = \mathrm{y} = \{2, 4, 6 \cdots \mathrm{M} * \mathrm{N}\}, \mathrm{t} = 10^5, \mathrm{k} = \pi/6$ under these conditions. The probability of TDQW proposed by Hao et al. is shown in Figure 2. The TDQW algorithm is presented in Algorithm 2.

$$\mu_t = P(X_t = x, Y_t = y) = \sum_{i=R}^{L} \sum_{j=B}^{F} |\Psi_i(x,t)\Psi_j(y,t)|^2 \tag{12}$$

The randomness of the pseudo-random numbers (PRNs) generated was evaluated using the National Institute of Standards and Technology (NIST) SP800-22 test suite. This evaluation is essential, as the production and quality assessment of PRNs are pivotal in cryptographic applications. As summarized in Table 1, the NIST SP800-22 test suite assesses the randomness and quality of binary sequences, which are the backbone of PRNs. Successfully passing all 15 subtests within this suite verifies the robustness and efficacy of the PRN generation process. Our experimental results confirm that the TDQW implementation produces non-periodic outputs characterized by a significant level of randomness, thereby validating its appropriateness for image encryption tasks.



(a) (b)

Figure 2. Two-dimensional quantum walk. (**a**) Continuous probability distribution; (**b**) three-dimensional discrete probability distribution.

Algorithm 2: Random number generation algorithm for TDQW.

Input: imageSize n, k, t;
Output: X, Y
Process:
1. for x $= 2:2:2^{n+1}$ do
2. for y $= 2:2:2^{n+1}$ do
3. $a = \frac{x}{t}, b = \frac{y}{t}, c = (\frac{x+y}{t})^2, d = \sqrt{\frac{2c-1}{c-1}}$
4. $k_{ab} = \sin^{-1} d, w_0 = \frac{sink}{\sqrt{2}}, w = \sin^{-1} w_0$
5. $i_2 = (1-(-1)^t)^2 * (1-(-1)^{x+y})^2 * 10;$
6. $i_2 = (1-(-1)^t)^2 * (1-(-1)^{x+y})^2 * 10;$
7. $i_3 = \sqrt{1-2*(a+b)^2}, i_4 = \pi * t * (1-(a+b)^2)$
8. $i_5 = i_3 * i_4, i_6 = \frac{a+b+1}{(1-a-b)^2}$
9. $i_7 = 10*(a+b)^4 - 3*(a+b)^3 - 4*(a+b)^2 + (a+b)$
10. $i_8 = (1-a-b)^4, i_9 = \sin(2*(t*w - k_{ab}*x - k_{ab}*y))$
11. $i_{10} = 7*(a+b)^3 - 2*(a+b)^2 - (a+b)$
12. $i_{11} = \cos(2*(t*w - k_{ab}*x - k_{ab}*y))$
13. $p = \frac{i_1+i_2}{i_5} * (i_6 - \frac{i_7*i_9}{i_8}) - (\frac{i_{10}*i_{11}*i_3}{i_8})$
14. $X(\frac{x}{2}) = p * 10^{(floor(\log_{10} t))-1};$
15. $Y(y/2) = p * 10^{(floor(\log_{10} t))-1};$
16. end for
17. end for

Table 1. NIST SP800-22 test results of the pseudo-random numbers (PRNs).

Sub-Tests	Success Rate	Sub-Tests	Success Rate	Sub-Tests	Success Rate
Approximate Entropy	100% pass	Linear Complexity	100% pass	Random Excursions Variant	100% pass
Block Frequency	100% pass	Longest Run	100% pass	Rank	100% pass
Cumulative Sums	100% pass	Non-Overlapping Template	99.4% pass	Runs	100% pass
FFT	100% pass	Overlapping Template	100% pass	Serial	100% pass
Frequency	100% pass	Random Excursions	100% pass	Universal	100% pass

2.4. Bit Layer Scrambling

Optical color image encryption schemes were proposed by Yildirim M [23,24], Faragallah O [18], and Liu [13], with cross-layer permutation enhancing chaos. Faragallah O showed that reducing RGB component correlation can boost encryption robustness [18]. This paper delves into Faragallah O's algorithm, revealing that minimizing correlation among the color image's 24-bit plane layers is key to this robustness.

Initially, RGB 3-plane scrambling alters the histogram, but peaks and patterns may persist, leaving some image features detectable. However, 24-bit layer scrambling disrupts every pixel bit, erasing all original distribution patterns. The resulting histogram is uniform,

lacking discernible peaks or patterns and thwarting histogram-based attacks (Figure 3c). Compared to Yildirim M and Liu's methods (Figure 3b), this 24-bit scrambling offers superior resistance to analysis (Figure 3c).

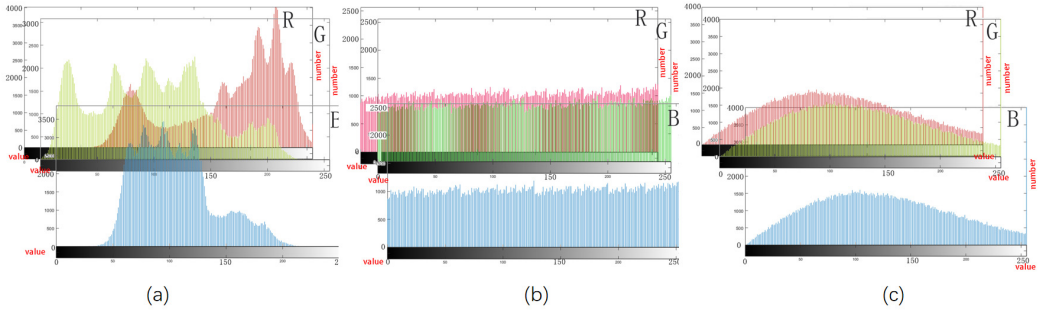
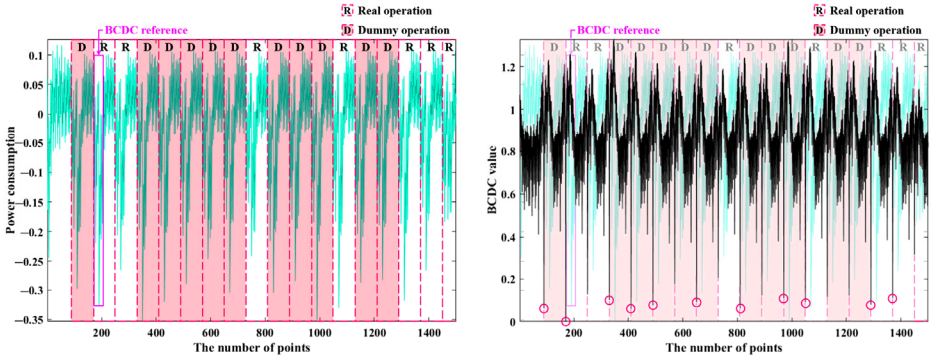


Figure 3. Histogram analysis. (**a**) "Lena" original RGB three-plane histogram analysis, (**b**) RGB three-plane scrambling histogram analysis, (**c**) 24-bit layer-scrambling three-plane histogram analysis.

2.5. AES with Dummy and Shuffling

Side-channel analysis (SCA) is an analytical method that exploits additional information, such as power consumption, electromagnetic radiation, and sound generated by devices, while executing cryptographic algorithms to extract confidential information. Due to the close correlation between side-channel information and intermediate computational values and their associated operations, there is a risk of confidential information leakage. When plaintext or ciphertext is known to attackers, they may infer these intermediate values by guessing secret information. To counteract SCA, the goal is to sever the connection between side-channel information and computable intermediate values. The central defensive strategies are divided into masking and hiding. Masking schemes introduce random values as masks to modify intermediate values, thereby increasing the difficulty for attackers of guessing the intermediate values. The hiding scheme aims to achieve defense by randomly adjusting the execution time of critical operations or changing the intensity of relevant side-channel signals.

JongHyeok Lee's study found that attackers could clearly distinguish between dummy and real operations in individual power consumption traces when combining the AES algorithm with randomly inserted dummy operations and a shuffling scheme [37]. This vulnerability was consistent across all masking schemes, regardless of the optimization level of the assembly code. Attackers could perform side-channel attacks (SCA), such as differential power analysis (DPA) or correlation power analysis (CPA), with an attack complexity lower than expected. JongHyeok Lee proposed an AES strategy that references random memory addresses. In traditional AES methods, values for real and virtual operations are stored sequentially in the CFA_IN array and executed according to the order stored in the ORD variable. To address the issue of different memory addresses, JongHyeok Lee first stored the values in temporary variables based on the order specified by the ORD variable and then performed Sbox operations sequentially. After the operation, to prevent the shuffling scheme from affecting other operations, the output values of the Sbox were restored to their original order and stored in the CFA_OUT variable. The experimental results showed that the new countermeasure made distinguishing between real and virtual Sbox operations in power consumption traces impossible. An analysis of one million traces confirmed that the success rate of distinguishing between virtual and real operations was only 49.98%, as shown in Figure 4, which is equivalent to being indistinguishable. This algorithm demonstrates strong resistance to side-channel analysis (SCA). This paper adopts the AES scheme provided by JongHyeok Lee.



(a) Power consumption trace (b) BCDC trace

Figure 4. AES with dummy and shuffling [37]. (**a**) Power consumption trace, (**b**) BCDC trace.

In the modern high-performance computing landscape, multi-core and multi-threading architecture has emerged as the de facto standard. The AES (Advanced Encryption Standard), a widely adopted symmetric encryption algorithm, comprises four essential steps: AddRoundKey (ARK), SubBytes (SB), ShiftRows (SR), and MixColumns (MC). These steps are chained together in a specific order and repeatedly applied to 128-bit input data blocks to accomplish the encryption or decryption process. Regarding the performance optimization of the AES algorithm in a multi-core and multi-threading environment, research conducted by Barhoush, Malek et al. has demonstrated that the introduction of pipelining technology can significantly enhance the execution efficiency of the AES algorithm, achieving a performance improvement of up to 1.7 times [38]. Pipelining technology achieves this by processing algorithm steps in parallel, reducing dependencies and latency between steps, thereby enhancing overall processing speed. This paper leverages the pipelining technique proposed by Barhoush, Malek et al. to optimize the AES algorithm, as mentioned above, aligning it with the modern multi-core and multi-threading computing architecture.

3. Encryption Algorithm and Decryption Algorithm

3.1. Encryption Algorithm

Due to its sensitivity to initial conditions and chaotic dynamical characteristics, quantum walks have become increasingly valuable for modern cryptographic systems [32]. Because of the excellent properties of two-dimensional quantum walks (TDQW) [31], this paper proposes a new optical image encryption method based on TDQW. TDQW generates permutation and diffusion images, thus realizing two random masks for the DRPE process. The overall encryption process in Figure 5 and the encryption algorithm are described in Algorithm 3. The specific steps are as follows:

Algorithm 3: Color image encryption algorithm

Input: imageI, sm-key, x, y, k1, t1, k2, t2, k3, t3;
Output: encryptionArnoldIm
Process:
//Stage 1.Get four Sequences X, X2, X3 form TDQW
1. [M,N] = size(imageI);countNum = 24*M*N;
2. X = Two-dimensionalQuantumWalk(sm-key,k1,t1,countNum);
3. X2 = Two-dimensionalQuantumWalk(sm-key,k2,t2,M,N);
3. X3 = Two-dimensionalQuantumWalk(sm-key,k3,t3,M,N);
4. RM2Im = exp(2*1i*pi*mat2gray(reshap(X2,M,N)));
5. RM2Im = exp(2*1i*pi*mat2gray(reshap(X3,M,N)));
//Stage 2.24-bit layers Scrambling
6. img_matrix = pic2mat(imageI);
7. for i = 1:floor(countNum/2)
8. t = img_matrix(X(i));
9. img_matrix(X(i)) = img_matrix(X(countNum-i + 1));
10. img_matrix(X(countNum-i + 1)) = t;

Algorithm 3: Color image encryption algorithm

11. end
12. imgEncoding24 = *AES*(mat2pic(img_matrix));
//Stage 3.Enhanced DREP
13. for i = 1:3
14. Img = im2double(uint8(imgEncoding24(:,:, i)));
15. encryptionIm (:,:, i) = ift2 (fft2 ((double (Img)). * RM1Im). * RM2Im);
16. encryptionArnoldIm (:,:, i) = deComplexIArnold (encryptionIm (:,:, i), X);
17. end

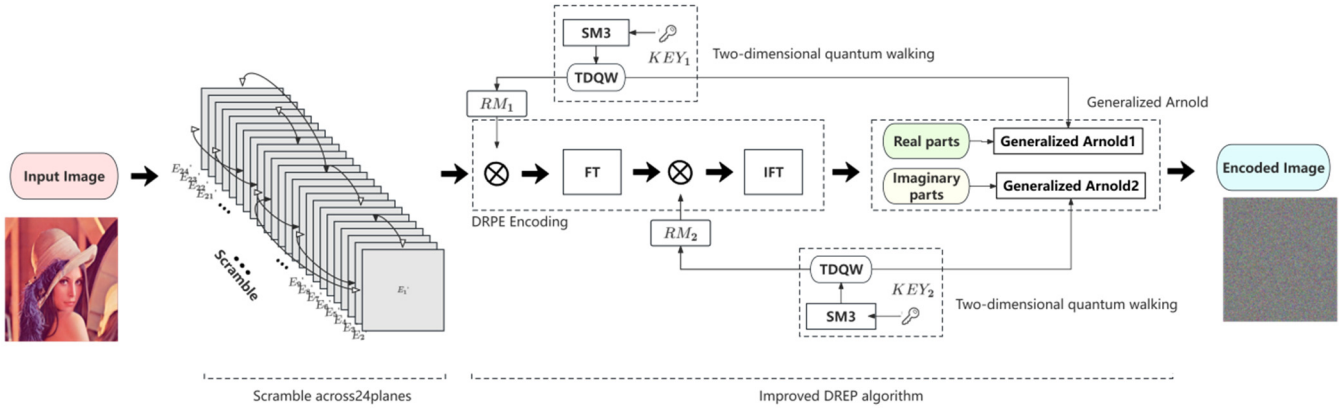


Figure 5. Overall encryption flow chart.

Step 1: The color picture is hashed using the SM3 national secret algorithm to derive a unique picture key, termed "sm-key". This key is subsequently employed to initialize the TDQW system to generate random numbers.

Step 2: The initial values x, y, k, and t are set for the TDQW system. Additionally, three conditions must be met, as illustrated by the Equation (13). "sm-key" is the TDQW initial value, and three random number sequences, X, X2, and X3, are generated.

$$\begin{cases} 1-2\left(\frac{x+y}{t}\right)^2 > 0 \\ t \text{ is odd and } x+y \text{ is odd} \\ t \text{ is even and } x+y \text{ is even} \end{cases} \tag{13}$$

Step 3: The RGB color image is converted to a 24-layer bit matrix "*img_matrix*" using X sorted index pairs. The "*img_matrix*" of the 24 layers is scrambled and then put into the *AES* to obtain the encrypted image "*img_encoding24*".

Step 4: First, TDQW is used to generate X2 and X3 to initialize the two phases, RM1 and RM2, for DRPE. Second, the image "*imgEncoding24*" is put into the DRPE system for the FT and ITF encryption process to obtain the image "*encryptionIm*".

Step 5: First, TDQW is used to generate X2 and X3 to initialize the parameter selection matrix of generalized Arnold. Second, the "*encryptionIm*" image is split into a real and an imaginary matrix. Third, generalized Arnold scrambling is used for two matrices, and finally, "*encryptionArnoldIm*" is obtained. The "*encryptionArnoldIm*" is the final encryption image. The whole process can be expressed as Equation (14).

$$g'(x,y) = IFT\{FT\{f(x,y)\cdot 24 \text{ bit}\cdot RM_1\}\cdot RM_2\}\cdot Arnold. \tag{14}$$

3.2. Decryption Algorithm

The decryption process is essentially the reverse of the encryption method depicted in Figure 6. The decryption formula is shown in Equation (15). The steps are as follows:

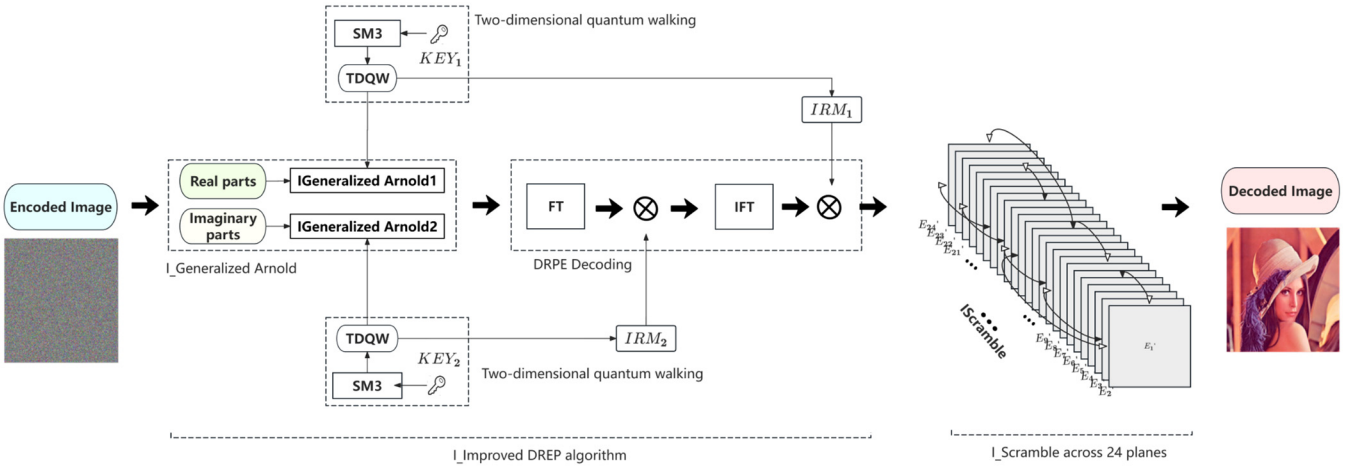


Figure 6. Overall decryption flow chart.

Step 1: The initial values and control parameters x, y, k, t, and "sm-key" are set as TDQW's initial value, which generates three random number sequences, X, X2, and X3.

Step 2: First, the TDQW is used to generate X2 and X3 and the parameter selection matrix of generalized Arnold is initialized. Second, the "*ArnoldIm*" is divided into a real matrix and an imaginary matrix, and inverse scrambling is performed using inverse Arnold transformation to obtain "*encryptionIm*". Third, the "*encryptionIm*" is used as the input for the next step.

Step 3: First, the TDQW is used to generate X2 and X3, and the two phases *IRM1* ($RM_1{}^{-1}$) and *IRM2* ($RM_2{}^{-1}$) are initialized. Second, the *encryptionIm* image is introduced into the DRPE decoding system, and the *FT* and *ITF* encryption processes are used to obtain the image "*imgEncoding24*".

Step 4: "*imgEncoding24*" is inserted into the *I_AES* to obtain "*imgEncoding24*". Second, X sorted index pairs are utilized to perform inverse scrambling on the 24-layer bit matrix of "*imgEncoding24*" to acquire "*img_matrix*", and then the bit matrix of "*img_matrix*" is integrated into an RGB color image, resulting in the decoded image $f(x,y)$.

$$f(x,y) = IFT\left\{FT\{g'(x,y)\cdot IArnold\}\cdot RM_2{}^{-1}\right\}\cdot RM_1{}^{-1}\cdot I24 \text{ bit.} \quad (15)$$

3.3. Observational Statistical Model Checking (OSM) Framework Integration

Observational statistical model checking (OSM) is an advanced framework designed to craft executable formal models directly from foundational system code, enabling the observation of dynamic behaviors in aspect-oriented applications [39]. The OSM framework marries the principles of model checking with aspect-oriented modularization, providing a robust tool for system verification. It is particularly suited for ensuring the safety, reliability, and adaptability of real-time embedded and safety-critical systems, especially in the ever-changing context of electronic health record systems. The OSM framework finds application in two key areas in optical color image encryption.

(1) Dynamic Behavior Monitoring: During the operation of the encryption system, the OSM framework can monitor the dynamic behavior of the encryption algorithm in real time, detecting potential security threats and anomalies. It is crucial for timely detection of and responses to attack behaviors.

(2) Key Management: The OSM framework can optimize the key generation, distribution, and management processes. Formal verification ensures the security of keys during transmission and storage, preventing key leakage and tampering.

Incorporating OSM, this paper establishes six AOP aspects to validate the correctness of the algorithm. Four internal aspects focus on verifying the accuracy of BIT24 and the improved DRPE encryption and decryption steps, guarding against potential errors from

third-party attacks during the encryption process. The remaining two external aspects validate the correctness of the key and ciphertext image, safeguarding against any tampering with the key or ciphertext, as shown in Figure 7.

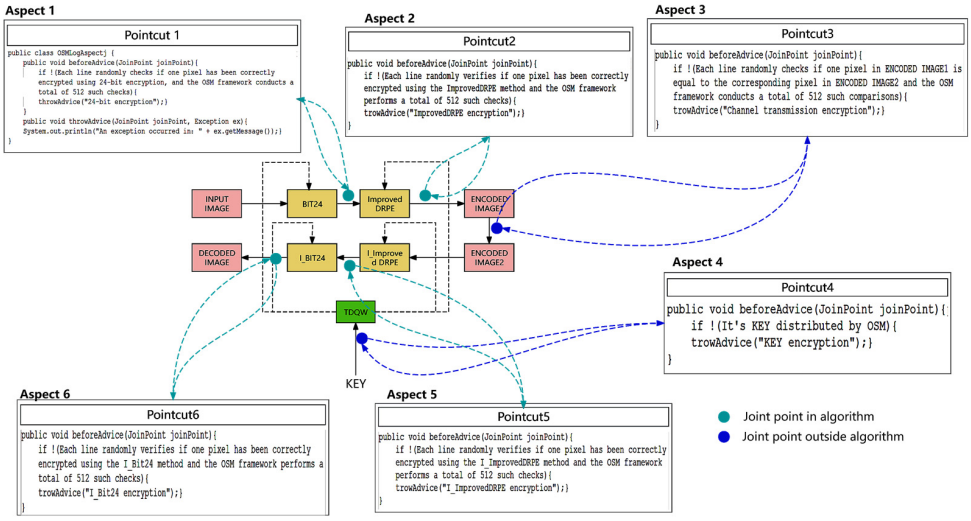


Figure 7. Observational statistical model checking (OSM) framework integration.

Integrating the OSM framework with the optical color image encryption algorithm based on TDQW provides a more robust and flexible tool for encryption systems. The OSM framework's capabilities in formal verification and dynamic behavior monitoring ensure the security and reliability of the encryption algorithm.

4. Numerical Simulation and Performance Analysis

The experimental conditions in this chapter are MATLAB R2021b, Win10, and i5-11260H@2.60GHz. The color images of 512 × 512 "Lena", "Mandril", and "Pepper" are tested. The encryption and decryption are shown in Figure 8.

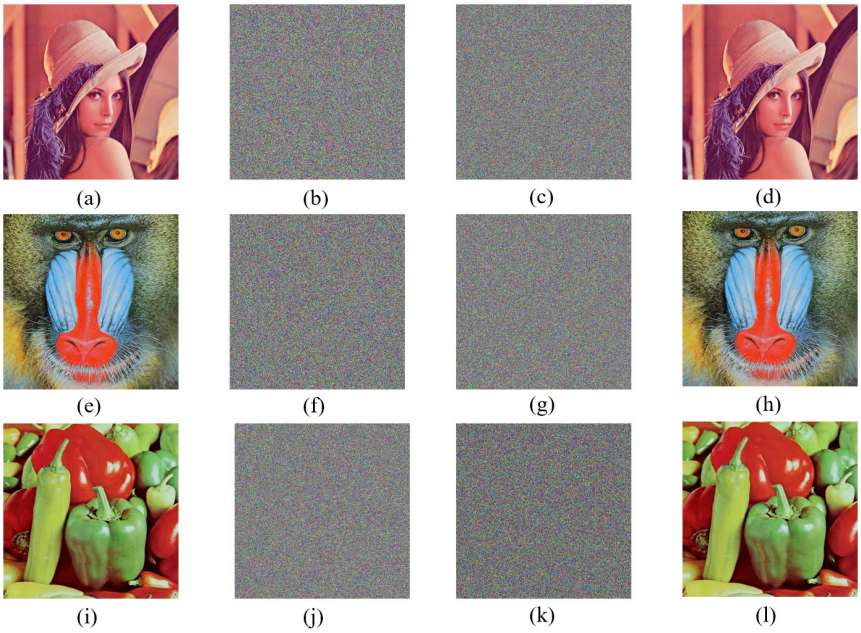


Figure 8. Schematic diagram of encrypted and decrypted images; (**a**,**e**,**i**) are plaintext images of "Lena", "Mandril", and "Pepper"; (**b**,**f**,**j**) are encrypted images after 24-bit plane permutation; (**c**,**g**,**k**) are encrypted images after OCT; (**d**,**h**,**l**) are decrypted images of "Lena", "Mandril", and "Pepper".

4.1. Correlation Analysis

Correlation analysis involves assessing the correlation coefficients of adjacent pixels in three directions: horizontal, vertical, and diagonal. From the pixel value matrix of the image, N pairs of neighboring pixels are chosen randomly and labeled as C_{AB}. The correlation coefficient is calculated as shown in Equation (16), where A_n and B_n represent pixel values of neighboring pixels and $\overline{A}$ and $\overline{B}$ represent N pairs of average pixels of pixels A_n and B_n.

$$C_{AB} = \frac{\sum_{n=1}^{N} (A_n - \overline{A})(B_n - \overline{B})}{\sqrt{\sum_{n=1}^{N} (A_n - \overline{A})^2 \sum_{n=1}^{N} (B_n - \overline{B})^2}}. \quad (16)$$

From three color images ("Lena", "Mandril", and "Pappe") of plain RGB pixels, as well as 24-bit plane scrambled and OCT-encrypted RGB pixels, we randomly calculated 2000 pairs of RGB pixels. This process was repeated 100 times, and the mean values are presented in Table 2. We also provide a correlation distribution map for direct visualization between the plaintext "Lena" and its ciphertext. Figure 9 illustrates horizontal, vertical, and diagonal correlations. A more dispersed distribution of adjacent pixels indicates better image encryption quality. Figure 9 displays this distribution. Our experiments reveal that the OCT algorithm effectively resists statistical analysis.

Table 2. Correlation analysis.

Figure	Correlation.R			Correlation.G			Correlation.B		
	H	V	D	H	V	D	H	V	D
Figure 8a	0.9811	0.9811	0.9677	0.9830	0.9703	0.9516	0.9592	0.9362	0.8999
Figure 8b	−0.0075	−0.0083	0.0036	−0.0050	0.0003	−0.0052	−0.0016	0.0020	−0.0140
Figure 8c	0.0006	−0.0023	−0.0016	−0.0004	−0.0017	−0.0019	−0.0003	0.0009	0.0020
Figure 8e	0.7707	0.8563	0.7524	0.7465	0.8443	0.7311	0.8567	0.9081	0.8369
Figure 8f	−0.0097	0.0236	−0.0036	0.0086	−0.0125	0.0015	0.0051	−0.0084	−0.0230
Figure 8g	0.0025	0.0074	0.0019	0.0026	−0.0014	0.0070	0.0275	0.0036	−0.0025
Figure 8i	0.9772	0.9738	0.9587	0.9920	0.9892	0.9800	0.9749	0.9691	0.9427
Figure 8j	0.0013	−0.0037	0.0045	0.0191	0.0066	−0.002	−0.0036	0.0200	−0.0058
Figure 8k	−0.0101	0.0055	−0.0030	−0.0320	0.0003	0.0040	−0.0059	0.0016	0.0248

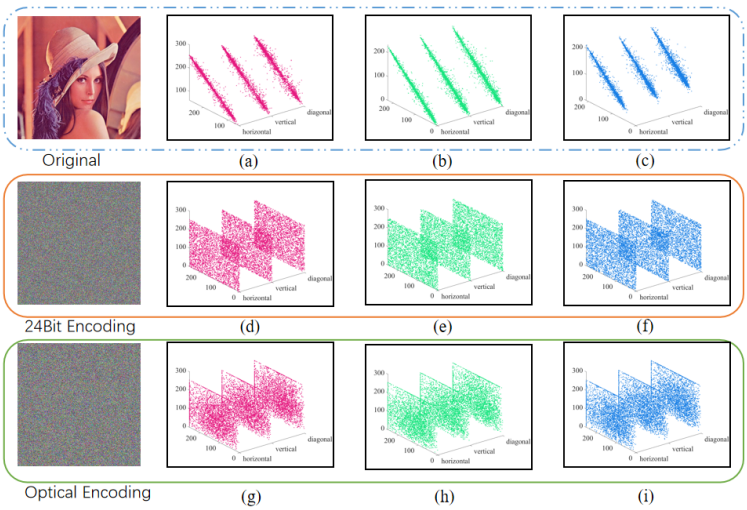


Figure 9. Correlation diagram. (**a**–**c**) are, respectively, correlation diagrams of R,G,B channels of "Lena"; (**d**–**f**) are, respectively, correlation diagrams of R,G,B channels of the encrypted image after 24-bit plane replacement; (**g**–**i**) are, respectively, correlation diagrams of R,G,B channels of the encrypted image after OCT.

4.2. Histogram

A histogram illustrates the gray distribution of an image by statistically evaluating the frequency of occurrence for each pixel's gray value. The histogram takes the pixel value as the horizontal axis and the corresponding pixel number as the vertical axis to form the histogram. Digital image pixels are discrete, and their value range is usually limited to 0 to 255. The more uniform histogram proves that the encryption is better. Figure 10 shows the color image "Lena", an encrypted image after 24-bit plane scrambling; the experimental results show that OCT can resist statistical analysis.

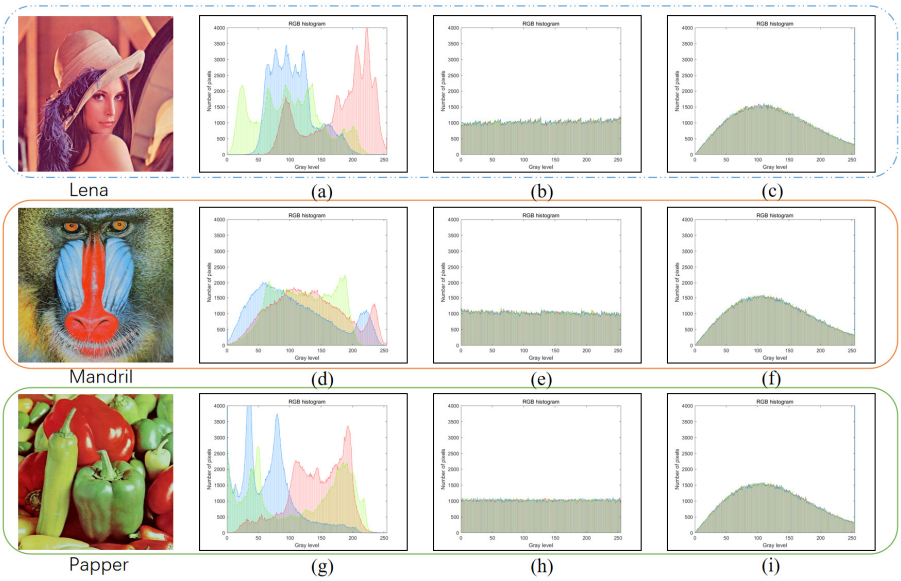


Figure 10. Histogram. (**a**,**d**,**g**) are, respectively, "Lena", "Mandril", and "Pepper"; RGB tri-plane histogram of image; (**b**,**e**,**h**) RGB tri-plane histogram of 24-bit plane permutation; (**c**,**f**,**i**) RGB tri-plane histogram after OCT encryption.

We performed statistical analysis on the generated histogram, including the calculation of histogram variance, maximum deviation, and irregular deviation, as shown in the table. Histogram variance (*Var*) indicates the dispersion of each bar's height (i.e., frequency or frequency count) in the histogram. The $\mathcal{F}_i$ denotes the frequency count of the ith bar, $\overline{\mathcal{F}}$ represents the average frequency count of all bars, and n denotes the number of bars; then, the variance (*Var*) can be calculated as shown in Equation (17). The histogram's maximum deviation (*MaxDev*) is evaluated based on the difference in pixel values between the plaintext image and the ciphertext image. A more significant deviation in pixel variation indicates more robust encryption technology in terms of security, as shown in Equation (18). M_i represents the difference in histogram counts between the plaintext image $\mathcal{F}_{i1}$ and the encrypted image $\mathcal{F}_{i2}$ at pixel index i. The irregular deviation (*IrregDev*) is also evaluated based on the difference in pixel values between the plaintext and ciphertext images. However, unlike *MaxDev*, in Equation (19), $H_{\mathcal{D}i}$ represents the count of pixels at index D_i, while H_c represents the average count of histogram values. A lower value of $IrregDev$ indicates better quality of the encrypted image.

$$Var = \frac{1}{n}\sum_{i=1}^{n}\left(\mathcal{F}_i - \overline{\mathcal{F}}\right)^2. \tag{17}$$

$$M_i = |\mathcal{F}_{i1} - \mathcal{F}_{i2}|, MaxDev = \frac{M_0 + M_{255}}{2} + \sum_{i=1}^{254} M_i. \tag{18}$$

$$H_{\mathcal{D}i} = \begin{cases} \frac{M*N}{256}, & 0 \le D_i \le 255 \\ 0, & elsewhere \end{cases}, IrregDev = \frac{\sum_{D_i=0}^{255} |H_{\mathcal{D}i} - H_c|}{M * N}. \quad (19)$$

Relevant experiments are conducted in this paper; the results are shown in Table 3. The results indicate that, using this algorithm, the histogram of the encrypted image can be maintained at a relatively small variance level. By taking images ("Lena", "Mandril", "Pappe") as measurement objects and comparing the average values of R, G, and B three-plane data with relevant literature, it can be found that the OCT scheme has better image data shown in Table 4, indirectly proving that reducing the correlation of three RGB planes can improve the robustness of image encryption.

Table 3. Histogram evaluation index.

	Var.R	Var.G	Var.B	MaxDev.R	MaxDev.G	MaxDev.B	IrregDev.R	IrregDev.G	IrregDev.B
Lena	254.62	258.64	257.62	256.53	271.33	240.39	47,310	45,001	44,390
Mandril	256.32	261.31	258.79	277.65	260.62	270.66	48,550	45,050	45,101
Pepper	258.65	260.11	249.39	270.65	270.36	272.92	45,703	45,180	45,100

Table 4. Comparisons of correlation histogram evaluation index.

	[34]	[40]	[41]	Proposed
Var	259.29	268.31	268.86	257.27
MaxDev	260.11	263.46	265.71	265.68
IrregDev	146,602.75	46,455.25	47,225	45,709

4.3. Information Entropy

Information entropy, a crucial statistical measure, reflects the average information content in an image $H(m)$ as Equation (20), representing the probability of random events (pixels). An entropy closer to 8 indicates better randomness and uniformity. Table 5 shows the average entropy of the original images ("Lena", "Pepper", and "Baboon") and the encrypted images using OCT.

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i) log_2 p(m_i). \quad (20)$$

Table 5. Average information entropy.

Image	Lena			Mandril			Pepper		
	Figure 8a	Figure 8b	Figure 8c	Figure 8e	Figure 8f	Figure 8g	Figure 8i	Figure 8j	Figure 8k
Entropy.R	7.3484	7.9994	7.7590	7.7593	7.9994	7.7249	7.3484	7.9994	7.7191
Entropy.G	7.5866	7.9994	7.7503	7.4594	7.9993	7.7222	7.5866	7.9994	7.7215
Entropy.B	7.0930	7.9992	7.7514	7.7556	7.9994	7.7213	7.093	7.9992	7.7209

4.4. Key Space and Key Sensitivity

In the field of cryptanalysis, there is a highly respected Kerckhoff hypothesis [42]. This hypothesis holds that the attacker has mastered all the details of the encryption algorithm except the key when cracking. In other words, the encryption algorithm is transparent and open to the attacker. Only when the key space is large enough can it effectively resist potential brute force attacks. Generally, it is considered that, when it is larger than 2^{100}, the key space is secure [3]. Owing to the boundaryless characteristic of two-dimensional quantum walks, the theoretical key space is rendered infinite, such that the key space equals ∞, but is constrained by the computational accuracy of the computer, assuming that the accuracy is 10^{-16}. The system has 10^{128} space, considered sufficient for optical image cryptography [43].

An efficient cryptosystem should recognize the variations in key parameters. This paper evaluates the image responses to minor variations in key parameters (sm-key, x, y, k1, t1, k2, t2, k3, t3). The parameters k1, k2, and k3 changed 10^{-13} in this experiment; the parameters t1, t2, and t3 changed by 1 bit; and the parameter sm-key changed by 1 bit, as shown in Figure 11. As can be observed from Figure 11, although the key underwent minimal changes, the outcome of image decryption varied significantly. This substantial disparity between the original image and the image obtained after altering the key underscores the remarkable sensitivity of the key.

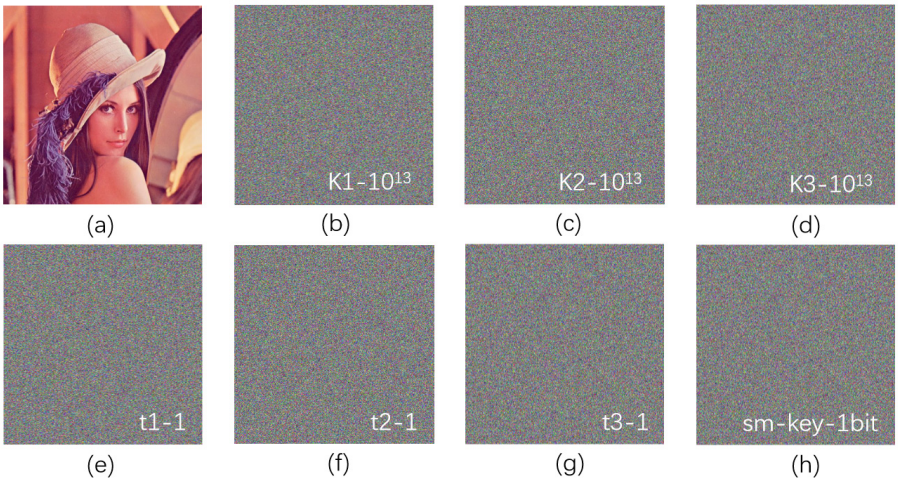


Figure 11. Effects of decryption of images with different keys ("Lena"). (**a**) is the correct key decryption diagram, and (**b**–**h**) are the images decrypted with the wrong keys.

The original image, the encrypted image of the 24-bit plane permutation, and the optically encrypted image after OCT encryption in terms of correlation, entropy, and key space can be compared with other schemes, as shown in Table 6. It can be observed that encrypted images using the OCT algorithm can achieve a more negligible correlation, a higher entropy value, and a larger key space, indirectly proving that reducing the correlation of three RGB planes can improve the robustness of image encryption. The results show that OCT has a better effect than other theories on correlation, entropy, and key space.

Table 6. Comparisons of correlation coefficients.

Ref.#	Cor.R	Cor.G	Cor.B	Entropy.R	Entropy.G	Entropy.B	Key Space
Original	0.9794	0.9909	0.9745	7.3484	7.5866	7.0930	-
[18]	−0.00006	0.0367	0.0247	7.7771	7.7190	7.7150	-
[23]	−0.0016	−0.0077	−0.0002	7.9968 (Modulo and XOR)			
[24]	−0.0014	0.0023	0.0015	7.9988 (DNA)			-
[22]	−0.0053	−0.0012	0.005		7.9973		2^{372}
[13]	−0.0119	−0.0087	−0.0045	7.7317	7.7864	7.6481	$(10^{15})^{16}$
[33]	−0.0018	−0.0018	−0.0017	7.9991	7.9990	7.9990	$(2^{45})^{10}$
[34]	0.0002	−0.0004	0.0073	7.9992	7.9993	7.9993	$(10^{16})^{3}$
[37]	−0.0013	0.0011	0.0031	7.9995	7.9972	7.9983	-
[21]	0.0014	−0.011	0.007	7.9899	7.9980	7.9892	10^{128}
Bit24	0.00133	0.00191	−0.0036	7.9994	7.9994	7.9993	∞
OCT	−0.00177	−0.00168	−0.000499	7.7590	7.7503	7.7514	∞
Theoretical value	0	0	0	8	8	8	∞

4.5. Computational Time Analysis

Two key factors must be balanced when designing image encryption technology: security strength and computational complexity. Security strength is evaluated using metrics

such as information entropy and correlation, while computational complexity assessment mainly includes time and space complexity. Due to modern computer storage technology advancements, many solutions prioritize time efficiency over space, often adopting a space-for-time approach. Additionally, multi-core processors enable multithreaded processing, making time complexity the most crucial factor to consider. The analysis of time complexity involves two aspects: evaluating the specific processing time of the algorithm and theoretically deriving the magnitude of time complexity, which refers to calculating the order of magnitude, denoted as O. Table 7 compares the computation time and theoretical complexity from relevant literature in this article. The experimental results demonstrate that the OCT scheme can be processed efficiently with lower computational complexity.

Table 7. Computational time analysis (sec).

	[36]	[38]	[40]	**Proposed**
Time	7.1365	4.3365	3.8479	3.8206
Complexity	$O(10^{16} * n * 2^{2n})$	$O(n^2)$	O(n)	O(n)

4.6. Known Plaintext Attack (KPA Attack)

The proposed scheme is evaluated for a known plaintext attack (KPA) [44]. In this attack, the attacker knows the input plaintext $f(x,y)$ and ciphertext $g(x,y)$ in advance. In the standard DREP algorithm, *RM2* can be derived from Equation (22) provided that *RM1* is known, as specified in Equation (21).

$$g(x,y) = IFT\{FT\{f(x,y)\cdot RM1\}\cdot RM2\} \tag{21}$$

$$RM2 = \frac{FT\{g(x,y)\}}{FT\{f(x,y)\cdot RM1\}}. \tag{22}$$

$$RM2' = \frac{FT\{g(x,y)\}}{FT\{f(x,y)\cdot 24\text{ bit}\cdot RM1'\}Arnold}. \tag{23}$$

When applying the same algorithm to assess the OCT scheme, it becomes apparent that Equation (14) cannot produce Equation (23), and it is impossible to obtain $RM2'$. The simulation outcomes for the OCT scheme under the KPA test are exhibited in Figure 12. Specifically, Figure 12a depicts an image encrypted using the conventional DRPE scheme, while Figure 12b illustrates the decryption of the DRPE-encrypted image employing the KPA algorithm. Figure 12c showcases an image encrypted via the OCT scheme, and Figure 12d presents the decrypted image of the OCT scheme using the KPA algorithm. Notably, the decrypted image in Figure 12d appears noisy and does not divulge any discernible information about the original image. Based on these findings, it is evident that the OCT scheme demonstrates resistance against the KPA.

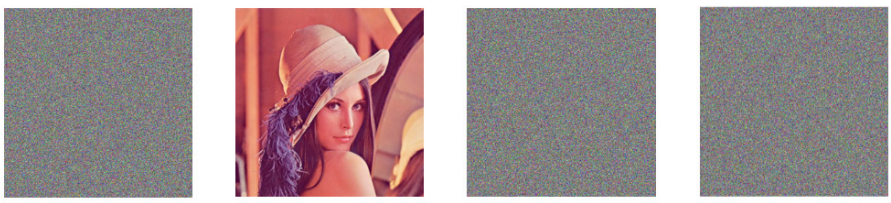


Figure 12. Known plaintext attack (KPA analysis): (**a**) images encrypted using DRPE scheme; (**b**) image decrypted using KPA algorithm; (**c**) image encrypted using OCT scheme; (**d**) image decrypted using KPA algorithm OCT.

4.7. Chosen Plaintext Attack (CPA Attack)

In DRPE, the Dirac function is chosen as the plaintext, as shown in Equation (21). DRPE is vulnerable to CPA attacks [3]. The 512 × 512 Dirac function is shown in Figure 13a, and its three-dimensional representation is shown in Figure 13b. When the Dirac function is used instead of the input image, the encryption process of DRPE scheme follows Equations (24) and (25).

$$\delta = \begin{cases} 1, x = 0, y = 0. \\ 0, otherwise. \end{cases} \tag{24}$$

$$\delta_{g(x,y)}\Big|_{CPA} = IFT\{FT\{\delta(x,y)\cdot RM_1\}\cdot RM_2\} \tag{25}$$

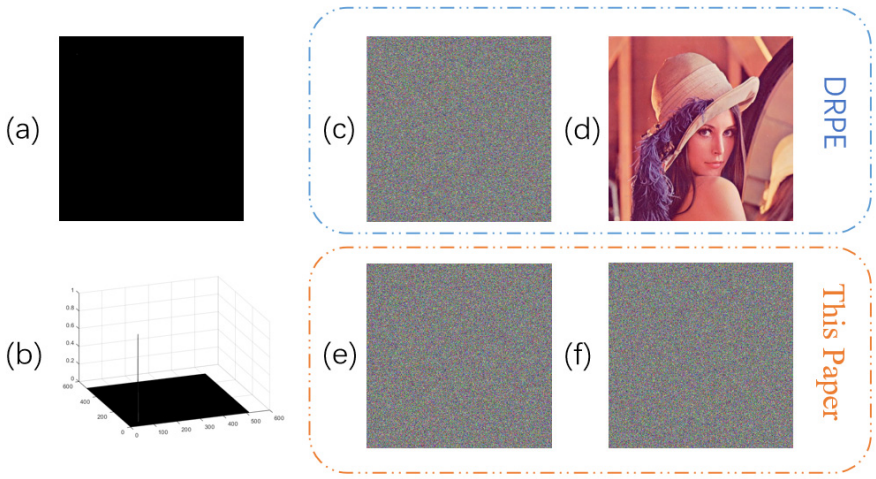


Figure 13. Chosen plaintext attack (CPA attack). (**a**) Dirac delta function; (**b**) Dirac delta function of three-dimensional map; (**c**) encrypting DREP image with CPA; (**d**) decrypting DREP image with CPA; (**e**) encrypting OCT image with CPA algorithm; (**f**) decrypting OCT image with CPA method.

The Dirac encryption $\delta_{g(x,y)}\Big|_{CPA}$, Dirac images $\delta(x,y)$, and plaintext encrypted image $g(x,y)$ are known, based on the fact that $f(x,y)\cdot RM_1$, which can be derived from Equation (26).

$$f(x,y)\cdot RM_1 = IFT\left(\frac{FT(g(x,y))}{FT\left(\delta_{g(x,y)}\Big|_{CPA}\right)}\right). \tag{26}$$

Therefore, in the DRPE scheme, the Dirac function is used as the selected plaintext image, and any input image can be deciphered. Now, this exact mechanism is applied to the proposed OCT scheme. In the OCT scheme, when the Dirac delta function replaces the input image during encryption, the equation is rewritten as Equation (27):

$$\delta_{g(x,y)}\Big|_{CPA} = IFT\{FT\{\delta(x,y)\cdot 24\text{ bit}\cdot RM_1\}\cdot RM_2\}\cdot Arnold. \tag{27}$$

From Equation (24), note that we do not know the information of 24 bit and *Arnold*. Therefore, the key information is also encrypted in this case, and the plaintext selected based on the Dirac delta function cannot crack the key information. Therefore, compared with the traditional DRPE scheme, the proposed scheme has higher security. The simulation results of the OCT scheme tested by CPA are shown in Figure 13.

Two key indicators, NPCR (number of pixels changed rate) and UACI (unified average changing intensity), can be adopted to demonstrate the system's ability to resist CPA. NPCR and UACI describe the differences between the encrypted image AttackE after

being attacked and the encrypted image E of the plaintext image without attack. They are calculated as shown in Formulas (28) and (29), respectively.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{2^{2n}} \times 100\%, \; where \; D(i,j) = \begin{cases} 0, \; e_1(i,j) = e_2(i,j) \\ 1, \; e_1(i,j) \neq e_2(i,j) \end{cases} \tag{28}$$

$$UACI = \frac{1}{2^{2n}} \left[\sum_{i,j} \frac{|e_1(i,j) - e_2(i,j)|}{255} \right] \times 100\% \tag{29}$$

Comparing the AttackE with CPA and E' without CPA for the three images of "Lena", "Mandril", and "Pepper", the result can be obtained as shown in Table 8. The theoretical expected values in a 256-level grayscale image are 99.6094% and 33.4635%, respectively. The data in Table 8 demonstrate that the results obtained from various test images closely approximate these theoretical values, providing strong evidence of the excellent plaintext sensitivity exhibited by the encryption algorithm.

Table 8. The values of NPCR and UACI.

Numble	Lena			Mandril			Pepper		
	R	**G**	**B**	**R**	**G**	**B**	**R**	**G**	**B**
UACI	99.6217	99.6016	99.5987	99.6033	99.5867	99.5865	99.5986	99.5879	99.5942
NPCR	33.6643	33.3611	33.3695	33.5258	33.3890	33.3780	33.4928	33.3977	33.4915

4.8. Noise and Shear Attack Test

Noise exists in most data channels and can easily cause damage or loss. Therefore, a well-designed cryptosystem should be capable of effectively preventing these attacks. Gaussian Noise (GN) and Salt and Pepper Noise (SPN) were introduced to OCT to verify the impact of noise attacks. The results are presented in Figure 14. When the algorithm was subjected to 0.5 intensity of SPN and 0.5 intensity of GN, the decrypted Lena portrait remained visible. This test indicates that the scheme possesses strong resistance to noise attacks.



Figure 14. Noise attack; (**a**) GN = 0.01; (**b**) GN = 0.1; (**c**) GN = 0.2; (**d**) GN = 0.5; (**e**) SPN= 0.01; (**f**) SPN = 0.1; (**g**) SPN = 0.2; (**h**) SPN = 0.5.

To assess the effect of cropping attacks on image decryption, encrypted and decrypted color images were derived by subjecting the cipher images of R, G, and B to varying intensities. Figure 15a–c exhibit the encrypted and decrypted color images after the loss of 50% of the data in the R, G, and B planes, correspondingly. Figure 15d–f display the

outcomes when 100% of the data are lost in the R, G, and B planes, respectively. Figure 15g–i illustrate situations where one plane loses all its data while another loses 50% of its data. Figure 15j–l illustrate situations where two planes each lose 100% of their data. Lastly, Figure 15m–o show cases where two planes lose 100% of their data and one plane loses 50% of its data. Despite losing two color planes (66.66% of the data), the decrypted Lena portrait remains visible in the decrypted image. This demonstrates that the proposed scheme exhibits excellent resistance to cropping attacks.

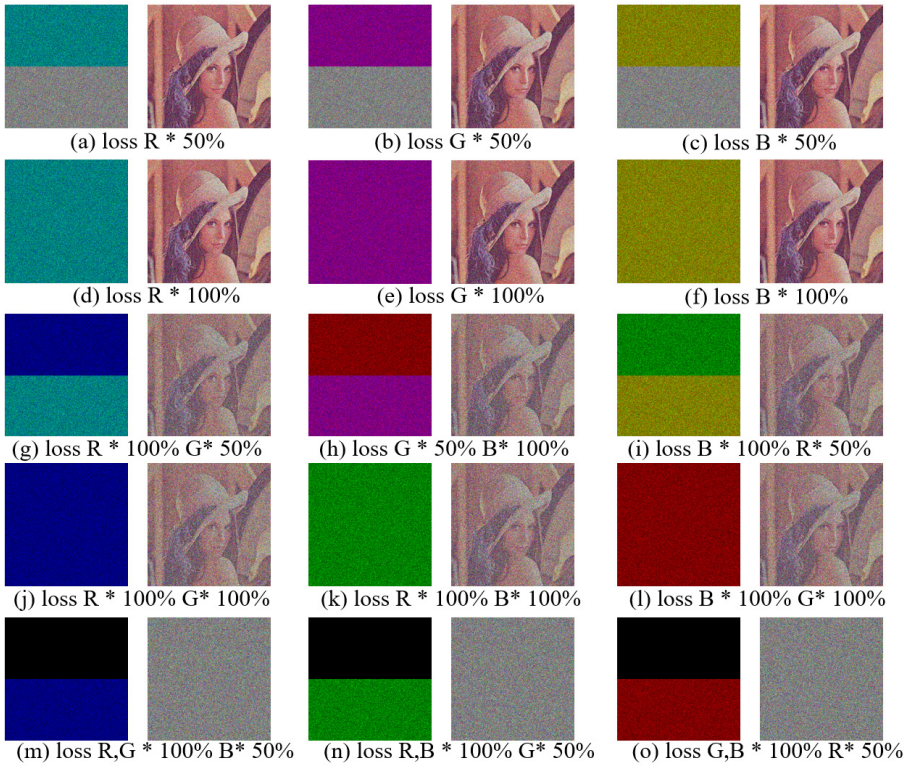


Figure 15. Shear attack.

5. Conclusions

This paper proposes a color double random phase encoding (DRPE) scheme based on 24-bit plane scrambling and two-dimensional quantum walking (TDQW), named OCT. The paper analyzes that the fundamental reason for enhancing image robustness lies in reducing RGB correlation, and the deeper reason is to reduce the correlation of the 24-bit planes. This paper analyzes and mathematically proves why the DRPE system cannot resist nonlinear problems. A scheme is proposed to increase the ability of the DRPE system to resist KPA and CPA analysis by introducing nonlinear terms to demonstrate OCT's resistance to linear attacks.

Specifically, first, this paper uses TDQW as a chaos system generator, not only to generate random numbers for 24-plane permutation, but also to generate two masks (RM1 and RM2) for the DRPE system, enhancing the Fourier domain scrambling of the DRPE system. The random numbers generated by the generator passed the NIST test. Then, the generated random number sequence cooperated with the 24-plane scrambling algorithm to convert the plaintext image into a ciphertext image. The ciphertext image was further encrypted using the AES algorithm, which can resist side-channel attacks. The resulting ciphertext image was the final encrypted image in the spatial domain. This step demonstrates that reducing the correlation of the three RGB planes can improve the robustness of image encryption. The spatial domain ciphertext image continued to be encrypted using the improved DRPE, where the random noise of TDQW generated RM1 and RM2 of the DRPE. Encrypting the spatial domain ciphertext image through DRPE

allowed us to obtain the Fourier domain ciphertext image. The Fourier domain ciphertext image consisted of natural and imaginary parts. The Fourier domain ciphertext image matrix was divided into a natural part matrix and an imaginary part matrix for encryption, allowing it to effectively resist KPA and CPA analysis.

Therefore, the introduction of TDQW greatly expands the key space. Through evaluations of correlation, entropy, histogram, shear attacks, and noise attacks, we further discovered that the fundamental reason for enhancing image robustness lies in reducing RGB correlation, and its essence is to reduce the correlation of 24-bit planes, proving that OCT has a special encryption effect. In addition, KPA and CPA analyses were also performed to confirm OCT's resistance to linear attacks. However, there are still some issues to be addressed in the algorithm presented in this paper, and improvements will be made in the following areas in the future:

(1) In terms of algorithmic efficiency, while the DRPE encryption algorithm is simple and fast, adding the AES 24-bit scrambling algorithm makes it seem cumbersome. In the future, computational complexity can be optimized.
(2) As quantum-based algorithms continue to iterate and develop, more efficient and secure quantum algorithms can be explored.
(3) With the development of hardware systems, consideration can be given to expanding the system to FPGAs or ASICs for distributed computing to improve efficiency.

Although the results obtained in this study are promising and provide some support for the conclusions, it is essential to acknowledge the potential limitations and vulnerabilities that may arise from applying quantum walks in encryption schemes.

Firstly, the complexity of implementing quantum walks in real-world encryption systems must be considered. While our experiments have demonstrated the effectiveness of TDQW in enhancing the security of optical image encryption, translating these findings into practical, large-scale encryption solutions remains challenging. The precise control required over quantum systems and the scalability issues associated with quantum computing may hinder the widespread adoption of quantum walk-based encryption. Secondly, the study has primarily focused on the encryption of static images. However, data are often dynamic in real-world applications and require real-time encryption. The performance of quantum walk-based encryption algorithms under such conditions has yet to be thoroughly investigated. There may be limitations in terms of speed and efficiency when applying these algorithms to encrypt streaming data or video. Thirdly, quantum walk-based encryption schemes are relatively new and may be vulnerable to novel, quantum-specific attacks. Attackers may develop more sophisticated methods to crack these encryption algorithms as quantum computing technology advances. The resilience of quantum walk-based encryption to such attacks needs further evaluation. Furthermore, the security of quantum walk-based encryption relies heavily on the confidentiality of the algorithm itself and the random number generators used. Any compromise in these areas could lead to significant vulnerabilities. Therefore, robust key management protocols and secure implementation methods are crucial for ensuring the overall security of such systems.

While the potential of quantum walk-based encryption is exciting, some vulnerabilities and limitations still need to be addressed before these algorithms can be safely and effectively deployed in real-world applications. Further research is necessary to mitigate these risks and enhance quantum walk-based encryption schemes' overall security and practicality. The OCT system can be further enhanced by addressing these limitations and implementing these suggestions to provide more compelling image encryption.

Author Contributions: Conceptualization, G.C. and X.Z.; methodology, G.C.; software, G.C. and W.H.; validation, G.C., J.M. and W.H.; formal analysis, J.M. and A.Z.; investigation, W.H. and A.Z.; resources, W.H. and W.H.; data curation, G.C.; writing—original draft preparation, G.C., W.H. and H.W.; writing—review and editing, G.C., X.Z. and H.W.; visualization, G.C., J.M. and X.Z.; supervision, J.M.; project administration, J.M., X.Z. and A.Z.; funding acquisition, X.Z. and J.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by [National Natural Science Foundation of China] grant number [No. 62362025] and [Hainan Province Key R&D plan project] grant number [No. ZDYF2022GXJS224].

Data Availability Statement: This paper does not generate any new data sets. The data that support the findings of this study are available in the Image Processing Standard Dataset at https://www.eecs.qmul.ac.uk/~phao/IP/Images/ (accessed on 22 May 2024).

Conflicts of Interest: The authors declare that this study received funding from Zhou, X. The funder had the following involvement with the study: National Natural Science Foundation of China (grant number 62362025) and the Hainan Province Key R&D Plan Project (grant number ZDYF2022GXJS224).

References

1. Zhang, Y.; Chen, A.; Tang, Y.; Dang, J.; Wang, G. Plain-text-related image encryption algorithm based on perceptron-like network. *Inf. Sci.* **2020**, *526*, 180–202. [CrossRef]
2. Hu, W.W.; Zhou, R.G.; Luo, J.; Jiang, S.X.; Luo, G.F. Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. *Quantum Inf. Process.* **2020**, *19*, 82. [CrossRef]
3. Farah, M.A.B.; Farah, A.; Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dyn.* **2020**, *99*, 3041–3064. [CrossRef]
4. Trujillo-Toledo, D.A.; López-Bonilla, O.R.; García-Guerrero, E.E.; Tlelo-Cuautle, E.; Lopez-Mancilla, D.; Guillen-Fernandez, O.; Inzunza-Gonzalez, E. Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. *Chaos Solitons Fractals* **2021**, *153*, 111506. [CrossRef]
5. Xiong, Y.; Wang, Y. Cryptoanalysis on the optical image encryption scheme based on full phase encoding and equal modulus decomposition. *Appl. Opt.* **2022**, *61*, 2743–2749. [CrossRef] [PubMed]
6. Inoue, K.; Cho, M. Amplitude based keyless optical encryption system using deep neural network. *J. Vis. Commun. Image Represent.* **2021**, *79*, 103251. [CrossRef]
7. Guo, X.; Zhong, J.; Li, B.; Qi, S.; Li, Y.; Li, P.; Wen, D.; Liu, S.; Wei, B.; Zhao, J. Full-color holographic display and encryption with full-polarization degree of freedom. *Adv. Mater.* **2022**, *34*, 2103192. [CrossRef]
8. Wang, H.L.; Ma, H.F.; Cui, T.J. A Polarization-Modulated Information Metasurface for Encryption Wireless Communications. *Adv. Sci.* **2022**, *9*, 2204333. [CrossRef]
9. Abuturab, M.R.; Alfalou, A. Multiple color image fusion, compression, and encryption using compressive sensing, chaotic-biometric keys, and optical fractional Fourier transform. *Opt. Laser Technol.* **2022**, *151*, 108071. [CrossRef]
10. Zhang, Y.; Zhang, L.; Zhong, Z.; Yu, L.; Shan, M.; Zhao, Y. Hyperchaotic image encryption using phase-truncated fractional Fourier transform and DNA-level operation. *Opt. Lasers Eng.* **2021**, *143*, 106626. [CrossRef]
11. Li, Y.M.; Wei, D.; Zhang, L. Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain. *Inf. Sci.* **2021**, *551*, 205–227. [CrossRef]
12. Peng, D.; Huang, Z.; Liu, Y.; Chen, Y.; Wang, F.; Ponomarenko, S.A.; Cai, Y. Optical coherence encryption with structured random light. *PhotoniX* **2021**, *2*, 6. [CrossRef] [PubMed]
13. Liu, Q.; Liu, L. Color image encryption algorithm based on DNA coding and double chaos system. *IEEE Access* **2020**, *8*, 83596–83610. [CrossRef]
14. Javidi, B.; Zhang, G.; Li, J. Experimental demonstration of the random phase encoding technique for image encryption and security verification. *Opt. Eng.* **1996**, *35*, 2506–2512. [CrossRef]
15. Javidi, B.; Sergent, A.; Zhang, G.; Guibert, L. Fault tolerance properties of a double phase encoding encryption technique. *Opt. Eng.* **1997**, *36*, 992–998. [CrossRef]
16. Jeong, O.; Moon, I. Adaptive transfer learning-based cryptanalysis on double random phase encoding. *Opt. Laser Technol.* **2024**, *168*, 109916. [CrossRef]
17. Zhang, R.; Xiao, D. Double image encryption scheme based on compressive sensing and double random phase encoding. *Mathematics* **2022**, *10*, 1242. [CrossRef]
18. Faragallah, O.S.; Afifi, A.; Elashry, I.F.; Naeem, E.A.; El-Hoseny, H.M.; El-Sayed, H.S.; Abbas, A.M. Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform. *Opt. Quantum Electron.* **2021**, *53*, 305. [CrossRef]
19. Abd-El-Atty, B.; Iliyasu, A.M.; Alanezi, A.; El-Latif, A.A.A. Optical image encryption based on Quantum walks. *Opt. Lasers Eng.* **2021**, *138*, 106403. [CrossRef]
20. Wang, Y.; Zhao, Q.; Zhang, H.; Li, T.; Xu, W.; Liu, S.; Su, Y. Optical single-channel color image encryption based on chaotic fingerprint phase mask and diffractive imaging. *Appl. Opt.* **2023**, *62*, 1009–1018. [CrossRef]
21. Hu, W.; Dong, Y. Quantum color image encryption based on a novel 3D chaotic system. *J. Appl. Phys.* **2022**, *131*, 114402. [CrossRef]
22. Tian, P.; Su, R. A Novel Virtual Optical Image Encryption Scheme Created by Combining Chaotic S-Box with Double Random Phase Encoding. *Sensors* **2022**, *22*, 5325. [CrossRef] [PubMed]
23. Yildirim, M. A color image encryption scheme reducing the correlations between R, G, B components. *Optik* **2021**, *237*, 166728. [CrossRef]
24. Yildirim, M. Optical color image encryption scheme with a novel DNA encoding algorithm based on a chaotic circuit. *Chaos Solitons Fractals* **2022**, *155*, 111631. [CrossRef]

25. Qin, W.; Peng, X. Asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Lett.* **2010**, *35*, 118–120. [CrossRef] [PubMed]
26. Wang, X.; Zhao, D. A special attack on the asymmetric cryptosystem based on phase-truncated Fourier transforms. *Opt. Commun.* **2012**, *285*, 1078–1081. [CrossRef]
27. Li, M.; Wang, M.; Fan, H.; Liu, Y.; Zhang, H.; Nan, H. On the security of image cryptosystems using DRPE based on scrambling and diffusion. *Opt. Quantum Electron.* **2023**, *56*, 241. [CrossRef]
28. Zhou, Q.; Wang, X.; Jin, M.; Zhang, L.; Xu, B. Optical image encryption based on two-channel detection and deep learning. *Opt. Lasers Eng.* **2023**, *162*, 107415. [CrossRef]
29. Singh, P.; Kumar, R.; Yadav, A.K.; Singh, K. Security analysis and modified attack algorithms for a nonlinear optical cryptosystem based on DRPE. *Opt. Lasers Eng.* **2021**, *139*, 106501. [CrossRef]
30. Sun, G.; Song, W.; Tian, M.; Tanougast, C.; Liu, Z.; Chen, H. A novel optical video cryptosystem based on improved 3D arnold transform in gyrator domains. *Opt. Laser Technol.* **2024**, *168*, 109891. [CrossRef]
31. Hao, W.; Zhang, T.; Chen, X.; Zhou, X. A hybrid NEQR image encryption cryptosystem using two-dimensional Quantum walks and Quantum coding. *Signal Process.* **2023**, *205*, 108890. [CrossRef]
32. Aharonov, D.; Ambainis, A.; Kempe, J.; Vazirani, U. Quantum walks on graphs. In Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing, Crete, Greece, 6–8 July 2001; pp. 50–59.
33. Rehman, M.U.; Shafique, A.; Usman, A.B. Securing medical information transmission between IoT devices: An innovative hybrid encryption scheme based on quantum walk, DNA encoding, and chaos. *Internet Things* **2023**, *24*, 100891. [CrossRef]
34. Hu, M.; Li, J.; Di, X. Quantum image encryption scheme based on 2d s ine 2-l ogistic chaotic map. *Nonlinear Dyn.* **2023**, *111*, 2815–2839. [CrossRef]
35. Gao, X.; Sun, B.; Cao, Y.; Banerjee, S.; Mou, J. A color image encryption algorithm based on hyperchaotic map and DNA mutation. *Chin. Phys. B* **2023**, *32*, 030501. [CrossRef]
36. Shafique, A.; Mehmood, A.; Alawida, M.; Elhadef, M.; Rehman, M.U. A fusion of machine learning and cryptography for fast data encryption through the encoding of high and moderate plaintext information blocks. *Multimed. Tools Appl.* **2024**, *1–27*, 1573–7721. [CrossRef]
37. Lee, J.H.; Han, D.G. Security analysis on dummy based side-channel countermeasures—Case study: AES with dummy and shuffling. *Appl. Soft Comput.* **2020**, *93*, 106352. [CrossRef]
38. Jaradat, A.; Barhoush, M.; Kofahi, N. Performance enhancement of the advanced encryption standard via pipelined implementation. *Comput. Sci.* **2019**, *97*, 15.
39. AlSobeh, A. OSM: Leveraging Model Checking for Observing Dynamic 1 Behaviors in Aspect-Oriented Applications. *arXiv* **2024**, arXiv:2403.01349. [CrossRef]
40. Kamal, S.T.; Hosny, K.M.; Elgindy, T.M.; Darwish, M.M.; Fouda, M.M. A new image encryption algorithm for grey and color medical images. *IEEE Access* **2021**, *9*, 37855–37865. [CrossRef]
41. El-Shafai, W.; Hemdan, E.E.D. Robust and efficient multi-level security framework for color medical images in telehealthcare services. *J. Ambient. Intell. Humaniz. Comput.* **2023**, *14*, 3675–3690. [CrossRef]
42. Simonson, S. Public Key Cryptography. *MAA Notes* **2005**, *68*, 109.
43. Zhang, Y. A unified image cryptography based on a perceptron-like network. *Vis. Comput.* **2022**, *39*, 4985–5000. [CrossRef]
44. Man, Z.; Li, J.; Di, X.; Sheng, Y.; Liu, Z. Double image encryption algorithm based on neural network and chaos. *Chaos Solitons Fractals* **2021**, *152*, 111318. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.