

Rotation Correction Algorithm Based on Polar Harmonic Fourier Moments and Optimization of Color Image Security Quantization Watermarking Scheme

Yuli Yang , Meiru Jiang, Xiufang Feng, Chenchen Lu, Yongle Chen , Shuang Zhou , and Hao Zhang 

Abstract—A continuous orthogonal moment is chosen as an image feature descriptor, and a rotation correction algorithm is proposed that can accommodate any order and repetition. In order to demonstrate the expanded application scope of the algorithm, a color image watermarking algorithm based on quantization concept is developed, which enhances the classical algorithm's resistance to rotation attacks. Taking into account the current research status of watermarking algorithms, a chaotic system is employed to bolster the security of the entire process. The experimental results indicate that the calibration algorithm exhibits strong universality and high accuracy. In comparison, the mean square error of the proposed rotation angle estimation model rose from 0.042 to 0.018, and the mean absolute error climbed from 0.065 to 0.032. With this enhancement, the robustness of color image watermarking algorithms against geometric attacks has taken a significant leap forward, the normalized correlation coefficient of quantization watermarking algorithm, which could not resist rotation attack, is now stable above 0.9. Furthermore, the modulated chaotic system heightens the security of the watermark algorithm, the key space up to 10^{15} , while also improving the quality of extracted watermarks.

Index Terms—Image continuous orthogonal moment, rotation correction, color image robust watermarking, chaotic system, safety watermarking.

I. INTRODUCTION

AS AN important digital image processing technology, anti-geometric distortion has always been the focus of researchers, including manual processing and deep learning solutions. It has a positive effect on medical images,

Manuscript received 5 March 2024; revised 17 July 2024; accepted 11 August 2024. Date of publication 14 August 2024; date of current version 23 August 2024. This work was supported in part by Key R&D Plan in Shanxi Province under Project 202102020101007, in part by the National Natural Science Foundation of China under Grant 61702356, and in part by the Natural Science Foundation of Shanxi Province under Grant 202303021221017 and Grant 20210302124050. (Corresponding author: Hao Zhang.)

Yuli Yang, Yongle Chen, and Hao Zhang are with the College of Computer Science and Technology, Taiyuan University of Technology, Taiyuan 030024, China (e-mail: yangyuliy1@126.com; chenyonle@tyut.edu.cn; zhangh545@126.com).

Meiru Jiang, Xiufang Feng, and Chenchen Lu are with the College of Software, Taiyuan University of Technology, Taiyuan 030024, China (e-mail: jamari0206@126.com; feng_tyut@126.com; luchenchen@163.com).

Shuang Zhou is with the School of Mathematical Sciences, Chongqing Normal University, Chongqing 401331, China (e-mail: zhoushuang@cqu.edu.cn). Digital Object Identifier 10.1109/JPHOT.2024.3443345

remote-sensing images and conventional image processing. The geometric correction is mostly achieved by manual processing with scale-invariant Feature transform (SIFT) and accelerated Robust feature (SURF) registration algorithms. Besides the above two algorithms, a feature-based registration method is proposed by comparing directional fast and rotating BRIEF (ORB), cross-correlation intensity-based and optical flow algorithms. The problem of Non-Uniform Rotational Distortion [1] is solved. In the field of image copyright protection, image registration schemes such as SURF are also often used to estimate geometric distortion parameters [2]. For fine large-scale remote sensing images, there are also corresponding geometric correction strategies based on frequency matching [3], gradient correlation and direction correlation [4], [5].

A deep learning-based registration method was used to correct nuclear magnetic resonance image (MRI) distortion. The synchronous correction algorithm used for conventional image protection has gradually formed a small branch to estimate a class of distribution features of the image through limited parameters [6]. A multivariate generalized Gaussian distribution is used to capture the significant features of color images, and a consistent near-end classifier is used to estimate the geometric distortion parameters [7]. A multi-layer perceptron is used to estimate the geometric distortion parameters by fitting the Cauchy distribution to the quaternion discrete cosine transform. Geometric and spectral distortion of remote sensing images is also a major obstacle to supervised classification and retrieval based on deep learning [8]. Artificial intelligence technology is used to generate models to perform the task of correcting satellite images and correcting errors [9]. A learnable joint spatial and spectral transformation model for remote sensing image retrieval is proposed to produce newly modified images with geometric and spectral corrections.

This paper proposes a rotation correction scheme based on geometric invariants for universal color images, which is realized by choosing a relatively new continuous orthogonal moment: polar harmonic Fourier moments [10]. As an excellent geometric invariant, image moment has strong geometric invariance and global feature description ability, and also has excellent performance in object recognition in recent years. Compared to the deep learning pathway, the computational complexity is

lower and the time and space consumption is less, which makes it more efficient in processing image problems.

With this kind of technical support, there will be more possibilities in the detailed field of image processing. Anti-geometric attacks are a major difficulty in digital image watermarking [11], [12], [13] and image information hiding technology [14], [15], [16]. Geometric attacks usually include rotation, scaling, cropping and shifting operations, which will seriously affect the synchronization of multimedia content. It makes many traditional watermarking algorithms ineffective. The key is how to ensure that the embedded information can be reliably detected and extracted after being subjected to various geometric transformations. So, this paper discusses the application of this scheme in the quantitative watermarking algorithm which cannot resist the rotation attack. In addition, the application of quaternion theory [17] to the overall processing of color images is more significant in research and application than the independent execution of multi-gray channels. Finally, in order to ensure the security of the complete algorithm, chaotic encryption technology [18], [19], which has been intensively studied in recent years, is adopted to enhance security and achieve the goal of image protection.

The major contributions and innovations of the proposed digital watermarking scheme can be summarized as follows:

(1) Based on the rotation characteristics of image moments, a rotation correction algorithm based on polar harmonic Fourier distance is designed; (2) The proposed rotation correction algorithm is applied to robust watermarking, and a new color image watermarking algorithm is designed to solve the problem that the original quantization watermarking scheme cannot resist rotation attack. Compared with the existing watermarking schemes of the same type and different types, it has better robustness to both conventional attacks and geometric attacks; (3) A novel one-way coupled mapping lattice system is coming up, which uses Sinusoidal mapping to dynamically affect the coupling coefficient to achieve chaotic enhancement; (4) The introduction of chaotic system not only enhances the security of the complete process, but also improves the original watermarking algorithm to resist the location correlation of cropping attacks, and optimizes the visual quality of watermark.

The following is the structure of this paper: in Section II, some preparatory work and basic theory are introduced. In Section III, the algorithm steps are detailed. Section IV discussed the experimental results and the conclusion in Section V.

II. PRELIMINARIES

A. Sinusoidal Dynamic Coupled Map Lattice

The coupled map lattice (CML) model was first proposed by K. Kaneko [20], and it was pointed out that the CML has chaotic characteristics in the space direction within a certain parameter range. The general model of the coupled map lattice is shown as:

$$x_{n+1}(i) = f(x_n(i)) + \sum_{j=1}^L \varepsilon_j g(x_n(j)). \quad (1)$$

Where, $x_n(i)$ represents the state value of the i -th lattice point at time n . n is the discrete time coordinate, i is the grid point

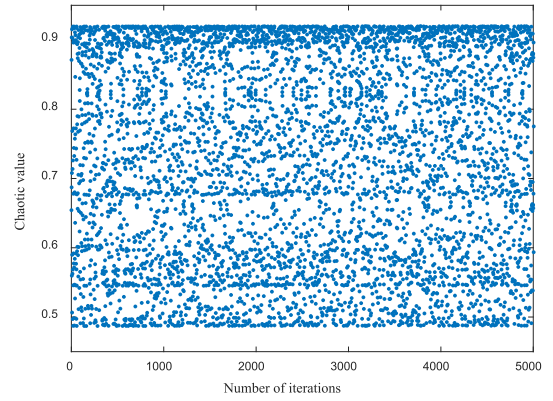


Fig. 1. The iterative state of the Sinusoidal mapping when $x_0 = 0.6543$, $a = 2.3$.

coordinate, and L is the number of grid points. ε indicates the coupling strength, $f(x)$ is the local nonlinear mapping function, usually using Logistic mapping, $g(x)$ is the coupling function, generally set $g(x) = f(x)$. According to the different values of ε , it is extended to one-way coupled map lattice (OCML), double-way coupled map lattice (DCML), and crossed coupled map lattice (CCML) several typical models. This paper is based on the OCML model, the expression is shown in (2):

$$x_{n+1}(i) = (1 - \varepsilon) f(x_n(i)) + \varepsilon f(x_n(i-1)). \quad (2)$$

Where $f(x) = \mu x(1-x)$ is the Logistic mapping with parameter $3.57 < \mu < 4$ and $0 < x < 1$. $0 < \varepsilon < 1$ is the coupling strength. That is to say, the chaotic performance of CML is determined by the parameters ε and μ . It has been proved that when $\varepsilon < 0.3$, the chaos of a large number of cells in CML will weaken or even disappear [21].

Meanwhile, a simple one-dimensional chaotic mapping of Sinusoidal as (3) has a chaotic value between 0.4870 and 0.9194, as shown in Fig. 1.

$$x_{k+1} = ax_k^2 \sin(\pi x_k). \quad (3)$$

This paper proposes a Sinusoidal dynamic coupled map lattice (SDCML) system, which introduces one-dimensional Sinusoidal mapping $h(x) = ax_k^2 \sin(\pi x_k)$ and dynamically controls the coupling coefficient ε to realize the chaotic enhancement of CML system.

In the proposed system SDCML, the meanings of i , n and f are the same as those of OCML, except that the coupling coefficient is ε in OCML and $h(\varepsilon) = a\varepsilon^2 \sin(\pi\varepsilon)$ in SDCML. In order to obtain the best dynamic coupling effect, μ is 3.99.

Fig. 2 shows the spatiotemporal chaotic diagrams of SDCML, with cell number $L = 50$ and control parameter $a = 2.3$. It can be seen that the proposed system has a complex space-time chaotic behavior, and the generated pseudo-random sequences are uniformly distributed throughout the space.

In order to evaluate the randomness of chaotic sequences rigorously, the random sequences generated by SDCML were tested using NIST SP800-22, a test standard published by the National Institute of Standards and Technology of the United States [22], including 15 test methods. If the P-value of the test

TABLE I
 NIST TEST RESULT FOR CHAOTIC SEQUENCES

Test name	P-value			Result
	S ₁	S ₂	S ₃	
The Monobit Frequency Test	0.0722	0.1957	0.1087	Pass
The Frequency within Block Test	0.7300	0.5102	0.7210	Pass
The Runs Test	0.3561	0.0528	0.0588	Pass
The Longest-Run-of-Ones in a Block Test	0.7104	0.8293	0.4966	Pass
The Binary Matrix Rank Test	0.0143	0.0251	0.0352	Pass
The Discrete Fourier Transform Test	0.3683	0.1726	0.5045	Pass
The Non-overlapping Template Matching Test	0.5398	0.7418	0.3017	Pass
The Overlapping Template Matching Test	0.7623	0.1437	0.4932	Pass
Maurer's "Universal Statistical" Test	0.3345	0.1299	0.9797	Pass
The Linear Complexity Test	0.6594	0.1823	0.6359	Pass
The Serial Test	0.3539	0.4550	0.0176	Pass
The Approximate Entropy Test	0.4391	0.6473	0.3423	Pass
The Cumulative Sums Test	0.9782	0.1002	0.9371	Pass
The Random Excursions Test	0.2743	0.5801	0.7545	Pass
The Random Excursions Variant Test	0.2425	0.5399	0.6358	Pass

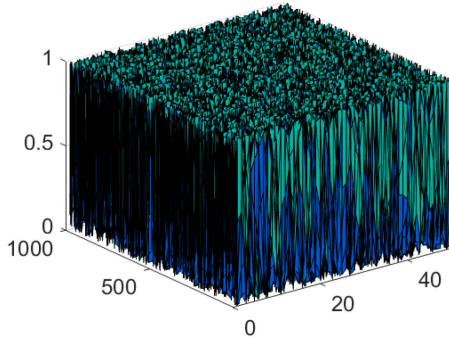


Fig. 2. The spatiotemporal chaotic diagrams of Sinusoidal dynamically coupled mapping.

result is larger than 0.01, it proves that the current sequence is random and passes the test.

The theoretical length of the test sequence is $10^3 \sim 10^7$, so the sequence of length 10^6 is used in the practical test. The results are shown in Table I, and the P-values of the test results are all greater than 0.01. The three chaotic sequences used in the experiment for security enhancement have passed the NIST test, which proves that the sequences have strict randomness and the watermarking system is safe and reliable.

B. Polar Harmonic Fourier Moments

As an excellent geometric invariant, image moment has strong geometric invariance and global feature description ability. According to whether the basis function is orthogonal, it can be divided into non-orthogonal moments and orthogonal moments. Non-orthogonal moments have a high degree of information redundancy and are difficult to reconstruct the original image. Limiting the development of image moments in more applications [23].

In contrast, orthogonal moments have great image reconstruction performance and are outstanding in various tasks of image processing. According to the discrete or continuous of the basis function, orthogonal moments can be divided into discrete

orthogonal moments and continuous orthogonal moments. The radial basis function is orthogonality in the unit circle, it can reconstruct the original image well, there is no information redundancy, and it has great geometric invariance.

In this paper, the polar harmonic Fourier moments (PHFMs) with low complexity and uniform zero distribution are selected to implement the rotation correction scheme, whose basis functions include radial basis function (RBF) and angular Fourier factor, as shown in (4):

$$\varphi_{mn} = \frac{2}{\pi} \int_0^{2\pi} \int_0^1 f(r, \theta) \overline{P_{mn}(r, \theta)} r dr d\theta. \quad (4)$$

Where $\overline{[\cdot]}$ denotes conjugation of complex numbers, $P_{mn}(r, \theta) = T_n(r) \exp(jm\theta)$, $T_n(r)$ represents the radial basis function and $\exp(jm\theta)$ stands for angular Fourier factors with imaginary unit j . The RBF of RHFMs and PHFMs are defined respectively as:

$$T_n(r) = \begin{cases} 1/\sqrt{2}, & n = 0; \\ \sin(n+1)\pi r^2, & n \text{ is odd}; \\ \cos(n)\pi r^2, & n \text{ is even}. \end{cases} \quad (5)$$

$T_n(r)$ is orthogonal for $0 \leq r \leq 1$. Compared with other continuous orthogonal moments, the RBF of the Fourier moments does not introduce complex factorial operations.

For an image containing $N \times N$ pixels, the double integral needs to be converted into two discrete summations. In the computation process, the image needs to be mapped to the unit circle, and there are two mapping methods: inscribed circle mapping and circumcircle mapping. Since the moment calculated by the circumcircle mapping algorithm is not rotation-invariant, it will affect the ability of the watermarking algorithm to resist the rotation attack. Therefore, the calculation method based on the inscribed circle is generally adopted. As shown in Fig. 3, the center of the image is mapped as the center of the unit circle, and (x_q, y_p) represents the center of the region $[x_q - \Delta x/2, x_q + \Delta x/2] \times [y_p - \Delta y/2, y_p + \Delta y/2]$, $\Delta x = \Delta y = 2/N$.

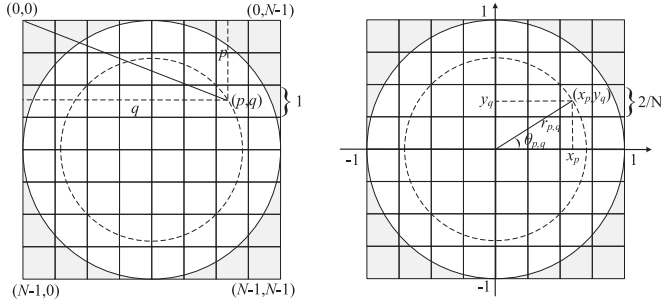


Fig. 3. Inscribed circle and unit circle mapping.

C. Rotation Angle Estimation Based on Moments

Assume that $f^\alpha(r, \theta) = f(r, \theta - \alpha)$ as the image $f(r, \theta)$ after rotation angle α , PHFM of $f^\alpha(r, \theta)$ and $f(r, \theta)$: $P_{mn}(f^\alpha)$ and $P_{mn}(f)$ meet the relations as: $P_{mn}(f^\alpha) = P_{mn}(f)\exp(-jm\alpha)$.

Define $\Phi = (P_{mn}(f^\alpha))/(P_{mn}(f)) = \exp(-jm\alpha) = \cos(m\alpha) - j\sin(m\alpha)$. The rotation angle α can be estimated by the $\text{Re}(\Phi) = \cos(m\alpha)$ or inverse function of $\text{Im}(\Phi) = -\sin(m\alpha)$. For any order of PHFM, the rotation angle can be estimated from this. [10] given the rotation angle estimation method using repetition $m = 1$ is processed: Firstly, the PHFMs of rotation image order n_{\max} is calculated, and then the moment of $m = 1$ is selected to use the above equation to estimate, so that n_{\max} estimated angles can be obtained, and then the mean of these n_{\max} angles is taken as the final estimated angle.

In this paper, it is considered that the rotation angle estimation based on the image moment amplitude of repetition $m = 1$ and order $n = n_{\max}$ alone cannot accurately explain the rotational invariance of the moment's argument. On this basis, an improved scheme is proposed to estimate the rotation angle of the PHFMs calculated by any order and any repetition, and it is combined with a quantization watermarking algorithm. The limitation that the watermarking algorithm cannot resist the rotation attack is eliminated. The details are described in Section III.

D. Quaternion Discrete Cosine Transform

The discrete cosine transform (DCT) is widely used in signal processing due to its strong energy concentration characteristics. In the DCT, the majority of the signal's energy is concentrated in the low-frequency part. Over the years, it has played a significant role in image, audio, noise processing, and signal modulation and demodulation. The DCT allows data to be transformed from the spatial domain to the frequency domain. For an $N \times N$ image $F(i, j)$, the DCT coefficient matrix $F(u, v)$ can be defined by (6), while the inverse discrete cosine transform (IDCT) formula is defined by (8).

$$\alpha(u) \alpha(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i, j) \cos \left[\frac{(2i+1)u\pi}{2N} \right] \times \cos \left[\frac{(2j+1)v\pi}{2N} \right], \quad (6)$$

$$\alpha(u) = \alpha(v) = \begin{cases} \sqrt{\frac{1}{N}}, & u/v = 0, \\ \sqrt{\frac{2}{N}}, & u/v \neq 0, \end{cases} \quad (7)$$

$$\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \alpha(u) \alpha(v) F(u, v) \cos \left[\frac{(2i+1)u\pi}{2N} \right] \times \cos \left[\frac{(2j+1)v\pi}{2N} \right]. \quad (8)$$

However, the traditional DCT only operates on two-dimensional information at most and supports single-channel gray information processing in images. To address this limitation, quaternion theory is introduced to simultaneously process three-channel components.

Quaternions are hypercomplex numbers that consist of one real part and three imaginary parts. They are represented by a combination of real numbers (a, b, c, d) and imaginary units (i, j, k). Pei et al. [24] proposed a quaternion model for color images while studying the properties of images in the quaternion discrete Fourier transform (QDFT) domain. In this model, the three imaginary parts of a quaternion correspond to the three channels in an RGB color image. Consequently, the color image can be represented as a set of pure quaternion forms.

The quaternion discrete cosine transform (QDCT) is an extension of the DCT to the quaternion domain, utilizing quaternion correlation theory. Since quaternion multiplication does not follow the commutative law, the QDCT has left and right forms as:

$$\begin{aligned} QDCT^L(p, s) &= \alpha(p) \alpha(s) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \mu \cdot f(x, y) N(p, s, x, y) \\ QDCT^R(p, s) &= \alpha(p) \alpha(s) \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) N(p, s, x, y) \cdot \mu. \end{aligned}$$

The parameter μ is a unit pure quaternion that satisfies the constraints $\mu^2 = -1$.

In this paper, the left form is used in the research, and the calculation method used in the experiment is introduced as follows.

The definition can either be directly employed when calculating the QDCT coefficients or transformed into the Cayley-Dickson form beforehand. Typically, the quaternion is considered in the latter computing paradigm, where it is expressed as the sum of its scalar and vector components as (9)–(10):

$$f(x, y) = A(x, y) + B(x, y)j. \quad (9)$$

$$F(x, y) = DCT(A(x, y)) + DCT(B(x, y))j. \quad (10)$$

Finally, the corresponding QDCT is obtained by left or right multiplication with the pure quaternion μ , as given by (11)–(12):

$$QDCT^L(f(x, y)) = \mu \cdot F(x, y), \quad (11)$$

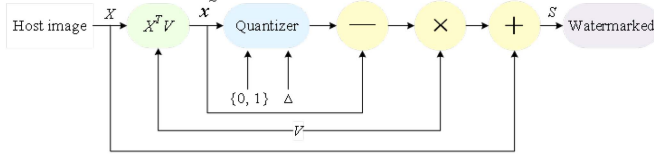


Fig. 4. Spread transform dither modulation based on projected vector.

$$QDCT^R(f(x, y)) = F(x, y) \cdot \mu. \quad (12)$$

E. Spread Transform Dither Modulation

Dither modulation (DM) coding, also known as quantization index modulation (QIM) coding, is a data hiding encoding method for watermark information indexing. Depending on the information to be embedded, QIM uses different quantizers to quantify the host image, and the quantized image is the image containing the watermark information. Suppose that the watermark signal $0 < m < 1$, each signal is represented by 1bit of information, x comes from the host signal, and $q(x)$ is a uniform scalar quantizer with step size Δ , which is the simplest QIM quantizer: $q(x) = \Delta \lfloor x/\Delta \rfloor$.

For the embedded information 0 and 1, $q(x)$ generates two new dither quantizers: $q_i(x) = q(x - d_i) + d_i$, and $d_0 = -\Delta/4$, $d_1 = \Delta/4$.

Spread-transform dither modulation (STDM) is a special coding modulation method based on QIM. The original host signal is not quantified directly, but the vector is extracted from the original signal for projection transformation, and then the projection results are dithered modulation.

As shown in Fig. 4, X is the vector obtained from the original signal and V is the selected projection vector. The vector S with watermark is obtained as $S = X + (q(\Delta, \{01\}) - X^T V) \times V$.

Dither modulation firstly dithered the carrier data, and then quantized it to realize the embedding of the watermark.

As an important factor in the performance of image STDM, the projection vector can be selected randomly in principle, as long as the projection vector itself is a unit vector. Therefore, it can also be combined with numerical decomposition methods, such as singular value decomposition (SVD).

The SVD of matrix A with size $N \times N$ is defined as:

$$A = USV^T = \begin{bmatrix} u_{1,1} & u_{1,2} & \cdots & u_{1,N} \\ u_{2,1} & u_{2,2} & \cdots & u_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ u_{N,1} & u_{N,2} & \cdots & u_{N,N} \end{bmatrix} \times \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \cdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_N \end{bmatrix} \times \begin{bmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,N} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ v_{N,1} & v_{N,2} & \cdots & v_{N,N} \end{bmatrix}. \quad (13)$$

Where U and V are $N \times N$ orthogonal matrices, S is a diagonal matrix, and the superscript T represents matrix transposition. The singular values of A , denoted by λ_i , are the diagonal

elements of S and satisfied $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$. These values play a significant role in matrix-related calculations. Additionally, the diagonal vectors and certain column vectors that exhibit stable properties within the matrix hold the potential to serve as projection vectors.

From the point of view of frequency, the coefficients in different frequency domains have different characteristics, and the projection vector makes the dither modulation affect only part of the coefficients, to obtain the expected performance.

III. THE PROPOSED WATERMARKING SCHEME

This section discusses the proposed secure watermarking system in detail, as shown in Fig. 5. The whole algorithm is divided into the following four steps: the adjustment and application of the one-way coupled map lattice system correspond to the contents of Part A, the embedding of robust watermarking corresponds to the contents of Part B, the calculation of correction information corresponds to the contents of Part C, and the last step is information encryption. In fact, the encryption operation appears in every link of the entire watermarking process. The detailed scheme is described at the end of Part A.

A. Pretreatment of Chaotic Mapping

As mentioned in Section II, when the one-way coupling map lattice generates chaotic sequences, Sinusoidal one-dimensional mapping is used to dynamically regulate the coupling coefficient to ensure that the system is in a chaotic state when generating sequences, thus generating chaotic random sequences (S_1 , S_2 , S_3). S_1 is used for logo pre-scrambling encryption to eliminate location correlation. S_2 is used to generate a chaotic matrix to resist position-invariant statistical attacks. When the copyright information is registered, the argument information of the watermarked is registered with it and used to resist the rotation attack. S_3 dynamic associative no repeat scrambling algorithm encrypts the argument information of the watermarked image before registration.

For pre-scrambling of logo, S_1 is employed to Arnold matrix a and b coefficients, as shown in:

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = T \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad (14)$$

$$T = \text{Arnold} = \begin{bmatrix} 1 & a \\ b & ab + 1 \end{bmatrix}. \quad (15)$$

Where M and N are the size of the logo to be scrambled, (x_0, y_0) are the pixels before the transformation, and (x_1, y_1) are the new pixels after the transformation. The goal is to avoid the periodicity of the simple Arnold transformation itself. Without disturbing the parameters, the Arnold transformation has a specific period. After a certain number of scrambles, the previous encryption is restored. Easy to crack problems are solved by correlating chaotic sequences with Arnold parameters.

However, if only dynamic scrambling does not change the watermark pixel value, the copyright information will still be at risk of statistical attacks. Therefore, S_2 is used to generate a chaotic matrix, and the chaotic matrix is binarized to change the pixel value within $\{01\}$ with the scrambled watermark

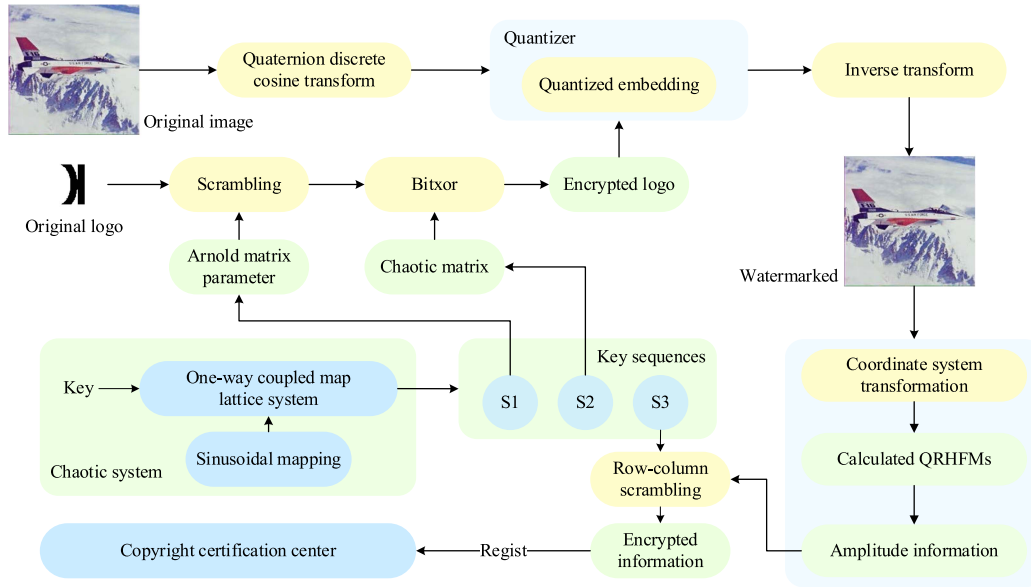


Fig. 5. Process of watermark embedding algorithm and security enhancement.

Algorithm 1: Dynamic no Repeat Scrambling.

Input: PHFMs argument information P , Chaotic sequence S_3 .

Output: Scrambled argument information S .

1. $[M, N] = \text{size}(P)$;
 2. $X = \text{mod}(\text{floor}(S_3 * 10^6), M * N) + 1$;
 3. $[\sim, \text{index}] = \text{unique}(X)$; $L = \text{length}(\text{index})$;
 4. $x = \text{zeros}(1, M)$; $x(1:L) = x(\text{sort}(\text{index}))$;
 $x(L+1:M * N) = \text{setdiff}(1:M * N, x)$; $X = x$;
 5. $S = P$;
 6. **for** $i = 1 : \text{floor}(M * N / 2)$
 7. $t = C(X(i))$;
 8. $C(X(i)) = C(X(M * N - i + 1))$;
 9. $C(X(M * N - i + 1)) = t$;
 10. **end**
 11. $S = \text{reshape}(S, [M, N])$;
-

information, taking the encrypted 64×64 size watermark as an example, the second chaotic sequence S_2 is processed as:

Chaotic sequence = $S_2(501:4596)$;
 Chaotic matrix = $\text{reshape}(\text{Chaotic sequence}, [64, 64])$;
 Chaotic matrix = $\text{mod}(\text{floor}(\text{Chaotic matrix} \times 10^6), 2)$.

The values of the first 500 iterations in sequence S_2 are discarded, and the values of the 501st iteration are taken from the beginning to ensure the high randomness of the sequence.

Then the one-dimensional vector is reconstructed into a two-dimensional matrix, and the floating-point moments are binarized by first enlarging and then taking the modulo operation, which is convenient for XOR with binary watermark.

S_3 is used to encrypt correct information. Based on the non-equal length information matrix, S_3 adopts the no repeat scrambling method, which is used as a random index to dynamically encrypt correct information as Algorithm 1.

B. Rotation Correction Algorithm Based on PHFMs

In order to optimize the ability of the quantization watermarking algorithm to resist the rotation attack, the proposed rotation angle estimation method is applied to the proposed color image watermarking algorithm to realize rotation correction. The calculation method in Section II is used to calculate the three-channel PHFMs of the watermark image, as shown in Fig. 6.

Firstly, the coordinate system transformation and unit circle mapping are processed. In order to facilitate the correction processing of the host image before the copyright verification and reduce the data storage, the calculated PHFMs need to be further processed. $\text{angle}(\cdot)$ indicates the calculation of the argument angle of the PHFMs currently existing in the plural form. Since the calculated result is the information of the radian angle, it is further converted into the angle value to facilitate the direct estimation of the rotation angle. Fig. 7 illustrates the size of the PHFMs information matrix with order n and repetition m . In fact, the parts of $m > 0$ and $m < 0$ are symmetric, and only one side of the data can be applied. The value of the $m = 0$ part is unstable and needs to be removed.

The PHFMs of each channel are carried out on the above operation, and registered with the copyright information after splicing.

The correction method does not limit the order and repetition, and can calculate the PHFMs of watermarked images according to any determined n and m . The further processing flow of the moment coefficient is shown in Fig. 8. After calculating the subtractive matrix according to the argument information of the watermarked and the current image, it can be summarized into three steps:

Step 1 is mainly to unify the rotation direction (clockwise or counterclockwise) that the image may suffer, and represent the argument data in the Subtractive matrix A in a unified direction.

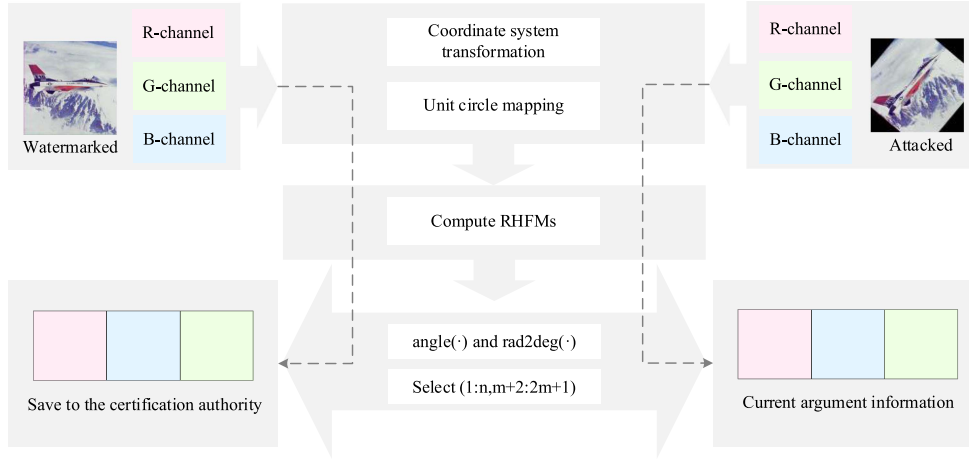


Fig. 6. Argument information preprocessing.

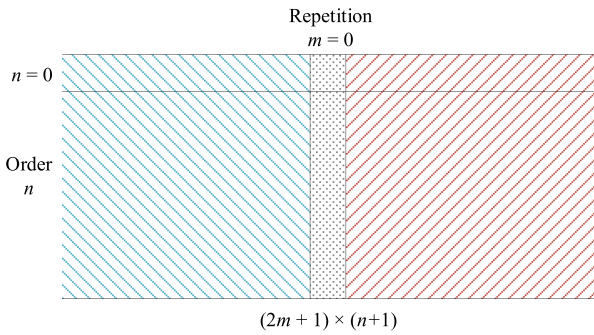


Fig. 7. Moment matrix calculated according to order n and repetition m .

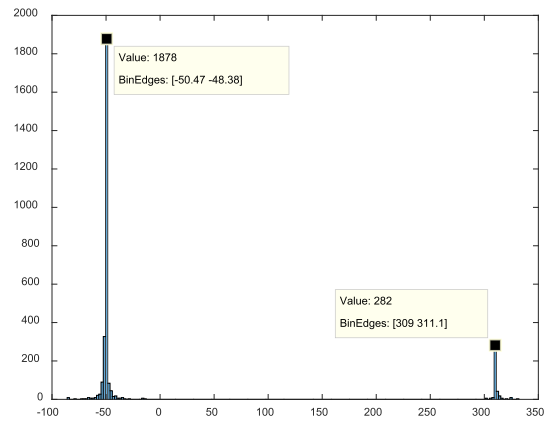


Fig. 9. Histogram representation with equivalent states.

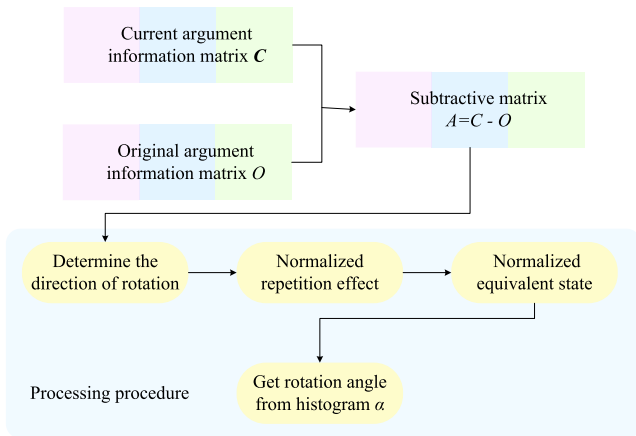


Fig. 8. Moment coefficient processing.

Step 2 is the key to eliminating the influence of repetition m , and the argument information matrix corresponding to the three channels is processed in the way of decreasing column by column, that is, in each channel PHFMs: {column($m = 2$)-column($m = 1$), column($m = 3$)-column($m = 2$), ..., column($m = m$)-column($m = m - 1$)}.

Step 3 is the final processing. After the end of the second step, there may be two states. One is that all the information in the processed matrix can reflect the rotation angle. The other

is that there are still equivalent states, and a clockwise rotation of α° and a counterclockwise rotation of $(360 - \alpha)^\circ$ are defined as a set of equivalent states that, although they have the same meaning, can still be normalized by a single processing. In the first case, the result is presented as a single peak, and in the second case, the result is presented as two peaks, as shown in Fig. 9. Although two peaks have the same meaning and can both explain the rotation change angle, in order to simplify the Angle estimation results, the double peak results are further processed to transform them into single peak, as shown in Fig. 10.

After the processing of Algorithm 2, all the PHFMs information calculated by any n and m can estimate the rotation angle, and perform the inverse transformation of the corresponding angle on the current image to get the corrected image.

C. Watermark Embedding Algorithm

Compared with the spatial watermarking method, frequency watermarking has better concealment and resistance to attack. However, frequency domain conversion is often targeted at a single image channel, so most of the watermarking algorithms based on color images embed the watermarking information into the Y channel after YCbCr transformation, in fact, the other two channels are not processed. This is fine, if only for

Algorithm 2: Rotate Angle Correction.

Input: Original argument information matrix O ,
Current argument information matrix C .
Any order n and any repetition m .

Output: Rotation angle α .

- Subtractive matrix $A = C - O$.
- Determine whether most of the coefficients are positive to normalized rotation direction:
 - if** $A(i, j) > 0$
 - $A(i, j) = A(i, j) - 360$;
 - else if**
 - $A(i, j) = A(i, j) + 360$;
 - end**
- Normalized repetition effect:
 - $B1 = A(1:n, 1:m)$;
 - $B2 = A(1:n, m+1:2m)$;
 - $B3 = A(1:n, 2m+1:3m)$;
 - for** $i = 1:n-1$
 - for** $j = 1:m$
 - $B1(:, i) = A(:, i+1) - A(:, i)$;
 - end**
 - end**
 - $B1 = B1(1:n, 1:m-1)$;
 - $B2$ and $B3$ are the same as above.
 - $B = [B1, B2, B3]$;
- Data distribution peak judgment to normalized equivalent state:
 - if** Double peak
 - $C = B$;
 - for** $i = 1:n$
 - for** $j = 1:3m-3$
 - if** $C(i, j) > 0$
 - $C(i, j) = C(i, j) - 360$;
 - end**
 - end**
 - end**
 - Get rotation angle from histogram;
 - else if**
 - Get rotation angle directly from histogram;
 - end**

the sake of image concealment. However, in the watermarking algorithm, the watermarking information is embedded into a known single channel, which does not make good use of multi-channel frequency domain information for color images. If the three-channel information can be used as the carrier of the watermarking algorithm, it is a better choice from the perspective of security and concealment. Therefore, this paper uses QDCT to realize frequency domain watermarking under quaternion theory and make full use of three-channel host information. According to Fig. 11, specific steps are as follows:

Step 1: Perform 8×8 QDCT transformation of the carrier image according to the effective calculation method to obtain the QDCT coefficient, that is, the component Q to be embedded in the watermark.

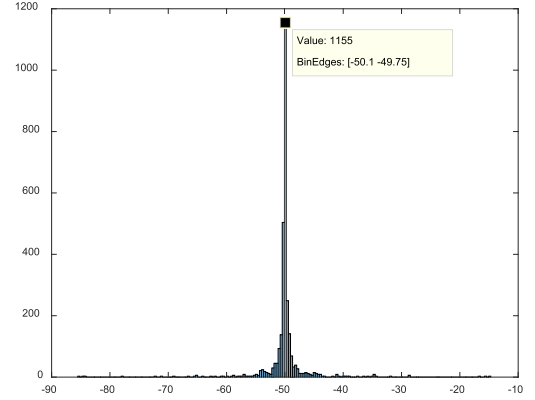


Fig. 10. Eliminate histogram results of equivalent states.

Step 2: Divide the component Q into 8×8 non-overlapping blocks B_i ($i = 1, 2, \dots, M \times N/64$), and subsequent operations are performed on each block.

Step 3: Performs singular value decomposition on block B_i ,

the S matrix diagonal element $\begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \cdots & \cdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_8 \end{bmatrix}$ as the

vector $X(\lambda_1, \lambda_2, \dots, \lambda_8)$ to be embedded in the watermark.

Step 4: Compute the parallel projection V of vector X : $V = X/\sqrt{\text{sum}(X^2)}$.

Step 5: Take the vector X and V into STDM quantization calculation: $S = X + (q(\Delta, \{01\}) - X^T V) \times V$.

Δ is the given quantization step, and the image quality and attack resistance of the image after embedding the watermark are also different from the step size set. For the embedded information 0 and 1, quantizer $q(x)$ generates two new dither quantizers, respectively:

$$\begin{cases} q_0(x) = q\left(x + \frac{\Delta}{4}\right) - \frac{\Delta}{4}, \\ q_1(x) = q\left(x - \frac{\Delta}{4}\right) + \frac{\Delta}{4}. \end{cases} \quad (16)$$

Step 6: The vector S embedded with the watermark is taken as the diagonal element of the new S_w matrix, and the inverse singular value decomposition is performed to obtain the image block embedded with the watermark: $B_{wi} = u \times S_w \times v'$.

Step 7: After all the blocks are processed, the inverse QDCT transform is carried out to obtain the carrier image embedded with a watermark.

D. Watermark Extraction Algorithm

The main idea of quantification is to divide the coordinate axes into A interval set and B interval set with the interval size of the step. According to the watermark value is 0 or 1, adjust the value of the watermark to be embedded so that it is equal to the middle value in the corresponding interval closest to itself. So, when detecting the watermark, only judge whether the value falls in the interval of set A or set B , and the corresponding watermark information can be obtained as 0 or 1.

The first two steps are basically the same:

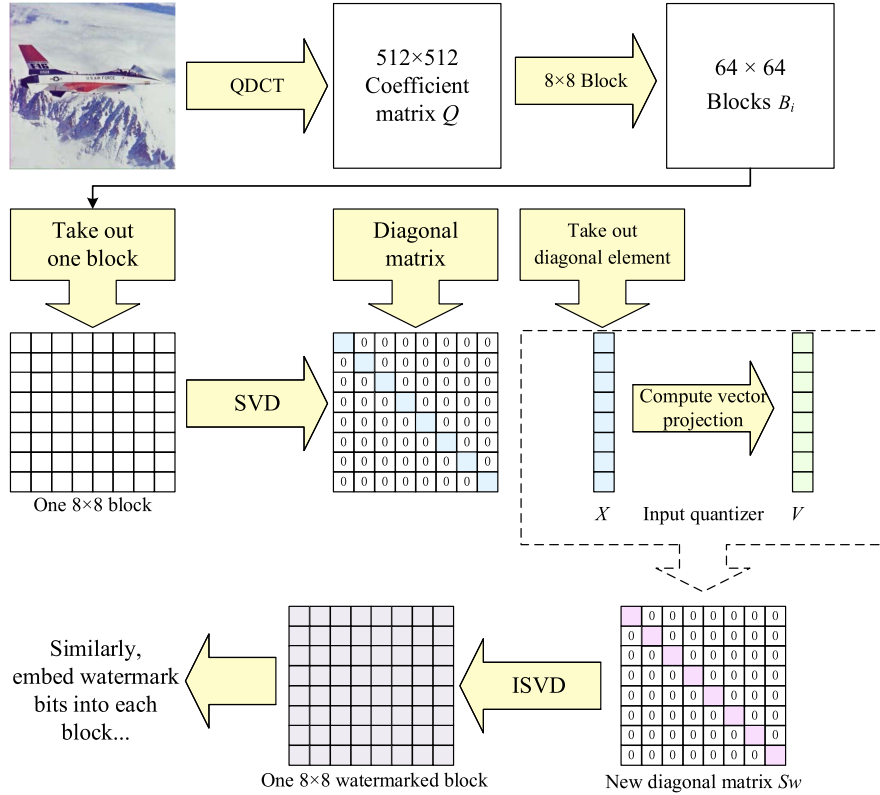


Fig. 11. Block diagram of watermarking.

Step 1: Restores the watermarked to its original size, and perform 8×8 QDCT transformation on the watermarked to obtain the current QDCT coefficient, that is, the watermark component to be extracted.

Step 2: The singular value vector and projection vector are calculated using the same method for each 8×8 subblock.

The watermark is decoded according to the principle of minimum distance above, the further explanation is as follows:

Step 3: Make the inner product of the current watermarking vector and the current projection vector to get the current coefficient p to be quantified.

Step 4: Input p respectively into the two quantizers $\{q_0(\cdot), q_1(\cdot)\}$ defined when embedding the watermark, and obtain the current quantization value $\{p_0, p_1\}$.

Step 5: Compare the current quantization coefficient p with the current quantization value $\{p_0, p_1\}$. If $\text{abs}(p_0 - p) < \text{abs}(p_1 - p)$, the watermark information corresponding to this block is 0; otherwise, it is 1.

Step 6: Traverse all blocks to obtain the complete watermark information.

It should be noted that in the complete watermarking process, the extracted watermark is still in the encrypted state at this time, and it is necessary to complete the decryption of the watermark with the help of S_2 and S_1 in turn.

Under the premise of great transparency, the STDM algorithm can better extract watermark information under noise, filtering and cropping attacks, and it can obtain less embedding distortion and has high robustness. However, the fly in the ointment is that the algorithm is not resistant to rotation attacks even at a very small rotation angle, as shown in Fig. 12. Therefore, if the

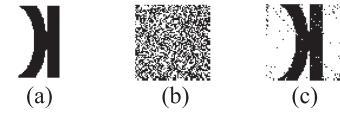
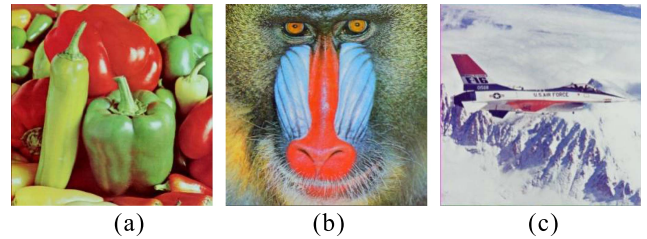

 Fig. 12. The effect of extracting watermark before and after rotation correction (5°): (a) Original watermark (b) Watermark extracted without correction (c) Watermark extracted after correction.


Fig. 13. Original images in the proposed method: (a) Peppers (b) Baboon (c) Airplane.

watermarked is subjected to rotation attack before the watermark extraction, the precorrection Algorithm 2 can improve the quality of the watermark extraction and eliminate the limitations of the algorithm.

IV. EXPERIMENTS FOR SIMULATION

In this section, we will test the performance of the proposed algorithm through simulation experiments, with the purpose of verifying the watermarks. All the processes proposed in this study were run with MATLAB 2016b, and the computer uses



Fig. 14. Watermark images in the proposed method: (a) Logo (b) Rose (c) Panda (d) Note.

Intel I5 CPU and 16.0 GB RAM. Color images in [25] were used as test subjects, as shown in Fig. 13. Binary logos with a resolution of “64×64” are used as the watermarks, as shown in Fig. 14. The test findings are unaffected by different watermarks. The reason is that the binary watermarks are scrambled before they are embedded in the images.

A. Imperceptibility Analysis

Peak signal-to-noise ratio (PSNR) is the most commonly used objective metric for evaluating image quality. It quantifies the difference between the original image and the processed image using mean square error (MSE), thus describing the differences between the watermarked and the original image. PSNR is calculated by comparing the MSE between two images and converting it to decibel units to indicate the degree of image quality difference. The MSE for two $m \times n$ grayscale images A and B is defined as (17). Based on this, PSNR is defined as (18), where the maximum value for each 8-bit is 255. In image watermarking, typical PSNR values range from 30 to 40 dB, with higher values indicating better quality.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [A(i, j) - B(i, j)]^2. \quad (17)$$

$$PSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{MSE} \right). \quad (18)$$

However, both MSE and PSNR focus only on the statistical characteristics of the image signal and do not align with the human visual system (HVS), thus failing to achieve a comprehensive subjective assessment. Weighted signal-to-noise ratio (WSNR) is an improved metric that incorporates some visual features by considering the error image (i.e., the difference between the original image and the tested image). It obtains a measurement value through contrast sensitivity function (CSF) filtering, referred to as signal-to-noise ratio (SNR), to achieve a closer subjective evaluation, as shown in:

$$WSNR = 10 \cdot \log_{10} \left(\frac{MAX_I^2}{\text{mean} \left(\text{mean} \left(E_{csf}^2 \right) \right)} \right). \quad (19)$$

$E(\cdot)$ represents the image obtained by filtering the difference between the two images with CSF. Unlike PSNR, WSNR takes into account the characteristics of the HVS by weighting different frequency components of the image or video, thus more accurately reflecting the sensitivity of the eye to image quality.

In addition to PSNR, the structural similarity (SSIM) index is also commonly used to measure the imperceptibility of watermark algorithms. It evaluates the degree of image quality

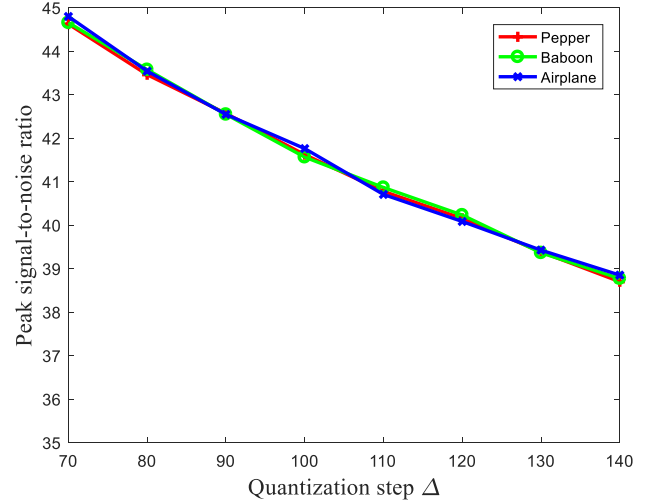


Fig. 15. PSNR at different step sizes.

loss by comparing the similarity of the structure, brightness, contrast, and other aspects between the original image and the processed image. SSIM combines information from the three aspects above, which better aligns with the eye’s perception of image quality. Equation (20) calculates the structural similarity between two images, considering the means, variances, and covariance of the images. The range of SSIM is -1 to 1, where a value of 1 indicates perfect similarity.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \quad (20)$$

where μ_x represents the mean of x , μ_y is the mean of y , σ_x represents the variance of x , σ_y is the variance of y , σ_{xy} is the covariance of x and y .

For color images typically composed of three channels, the average value for each channel is calculated experimentally, and the average values are taken as the final evaluation result. These metrics are widely applied in the field of image watermarking to evaluate the impact of different algorithms and techniques on host images, guiding and optimizing the watermark embedding process.

The same watermark is embedded into different host images, respectively, and different watermarks are embedded based on the same host image. The visual effects of watermarked images are observed in Tables II and III. The data show that the algorithm invisibility is somewhat related to the carrier image itself, but the watermark has almost no impact on the embedding effect, because the location correlation of different watermarks has been eliminated before embedding. At the same time, the watermark can be extracted lossless when the watermarked image is transmitted without any attack.

Finally, the experiment examined the invisibility index under asynchronous length by regulating the quantizer step size, as depicted in Figs. 15–17.

It can be observed from the figure that the value of PSNR is scarcely influenced by the host image, and there is no notable disparity among the four images. Regarding SSIM, although

TABLE II
PSNR, WSNR, AND SSIM OF WATERMARKED AND THE NC AND BER OF THE EXTRACTED WATERMARK

Watermarked Image	PSNR	WSNR	SSIM	NC	BER
Peppers	40.1566	0.9985	49.7744	1.0000	0.0000
Baboon	40.2324	0.9983	46.9510	1.0000	0.0000
Airplane	40.0846	0.9841	46.2803	1.0000	0.0000

TABLE III
PSNR, WSNR, AND SSIM OF WATERMARKED WITH DIFFERENT WATERMARKS AND THE NC AND BER OF THE EXTRACTED WATERMARK

Watermark	PSNR	WSNR	SSIM	NC	BER
Logo	40.0880	0.9987	51.4122	1.0000	0.0000
Rose	40.1220	0.9987	48.7468	1.0000	0.0000
Panda	40.1403	0.9987	52.1082	1.0000	0.0000
Note	40.0777	0.9987	50.2914	1.0000	0.0000

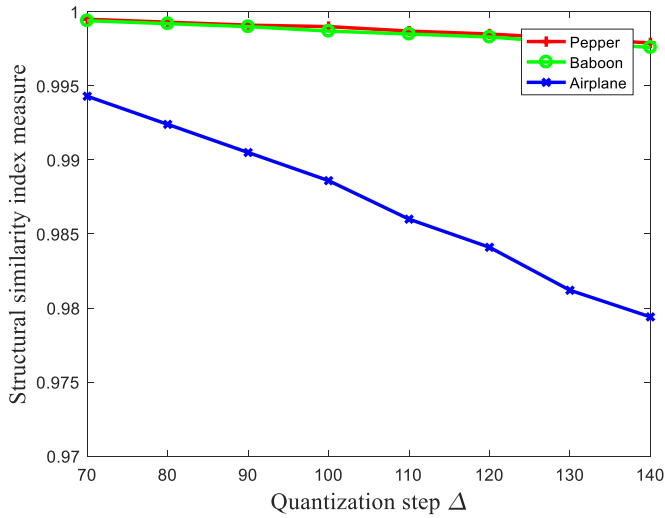


Fig. 16. SSIM at different step sizes.

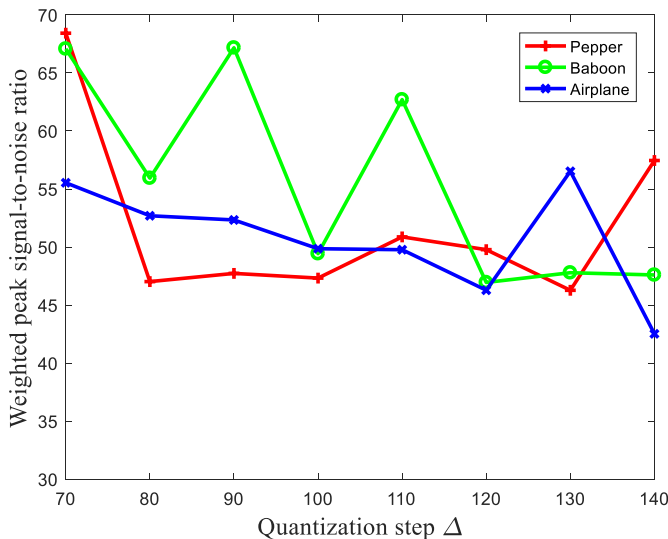


Fig. 17. WSNR at different step sizes.

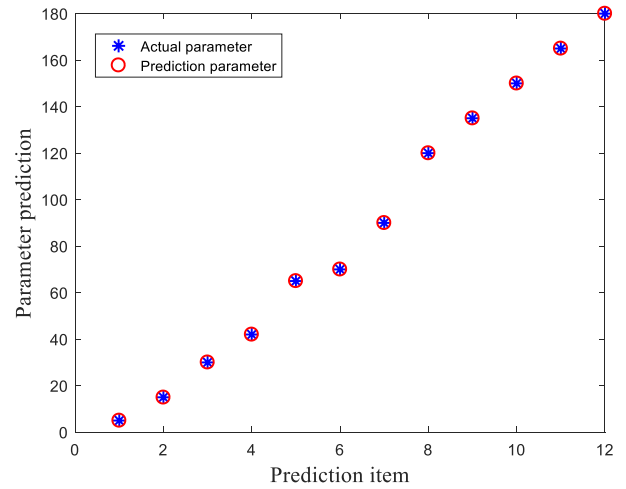


Fig. 18. Diagram of actual parameters and predictions.

there are certain differences between the airplane and the other three images, the value can still approach 0.98 or exceed it. The data of WSNR fluctuates significantly, ranging from 42 to 68 dB, and the appropriate step size can be determined based on the requirements of image quality to achieve superior robustness.

B. Correction Accuracy Analysis





























This section processes the test image using common rotation attack parameters and estimates the rotation angle using a correction algorithm based on continuous orthogonal moments, the results of which are shown in Fig. 18, and Table IV presents the specific data results for reference and comparison.

Based on the geometric invariance of image moments, the accuracy of the correction algorithm can reach 0.1. According to the experimental results, when the rotation angle is larger than 90°, the accuracy of the algorithm is improved to a certain extent, which makes the watermarked have the ability to completely correct and restore to the original when facing the flipping attack.

TABLE IV
THE ACTUAL ROTATION ANGLE AND THE ESTIMATED RESULT OF THE ALGORITHM

Rotate attacks						
Actual Parameter	5	15	30	42	65	70
Estimated Parameter	5.01	14.94	30.03	42.01	65.02	70.01
Actual Parameter	90	120	135	150	165	180
Estimated Parameter	90.00	120.00	135.00	150.00	165.00	180.00

TABLE V
ROBUSTNESS PERFORMANCE: EXTRACTED WATERMARKS FROM THE ATTACKED WATERMARKED IMAGES AND CORRESPONDING NCs AND BERS OF WATERMARKS ($\Delta = 120$)

Attacks	Rotate 5°	Rotate 15°	Rotate 45°	Rotate 90°	Rotate 180°	Rescale 0.5	Rescale 0.75
Watermark							
NC	0.9751	0.9295	0.9072	1.0000	1.0000	0.9849	0.9996
BER	0.0200	0.0558	0.0727	0.0000	0.0000	0.0122	0.0003
Attacks	Rescale 2	Rescale 4	JPEG 30	JPEG 50	JPEG 75	JPEG 90	JPEG 2000
Watermark							
NC	1.0000	1.0000	0.9010	0.9865	0.9996	1.0000	0.9998
BER	0.0000	0.0000	0.0784	0.0109	0.0003	0.0000	0.0000
Attacks	Gaussian Filter [3,3]	Wiener Filter [3,3]	Median Filter [3,3]	Gaussian noise 0.001	Salt & Pepper noise 0.001	Salt & Pepper noise 0.005	Poisson noise
Watermark							
NC	0.9990	0.9992	0.9686	0.9998	0.9952	0.9646	0.9713
BER	0.0081	0.0006	0.0253	0.0002	0.0039	0.0284	0.0231
Attacks	Speckle noise 0.001	Speckle noise 0.005	Sharpen (0.6)	Sharpen (0.8)	Crop (1/16)	Crop (1/8)	Crop (1/4)
Watermark							
NC	0.9998	0.9822	0.9614	0.9350	0.9741	0.9498	0.8943
BER	0.0002	0.0144	0.0311	0.0520	0.0208	0.0400	0.0831

C. Robustness Analysis

In watermarking, normalized correlation (NC) coefficient and bit error ratio (BER) are commonly used performance indicators to evaluate and measure the accuracy and robustness of watermark extraction processes.

NC is used to measure the detectability and robustness of the embedded watermark in the image by calculating the degree of correlation between the embedded watermark and the extracted watermark. A higher NC value indicates that there is a strong correlation between the embedded watermark and the extracted watermark, which can effectively detect and extract watermark. The maximum NC value of two identical watermarks is 1.

In the experiment, NC is used to evaluate the performance against various attacks or image processing. When the watermark size is $m \times n$, NC is defined as:

$$NC = \frac{\sum_{m=0}^{M-1} \sum_{n=0}^{N-1} W(m, n) W^*(m, n)}{\sqrt{\sum_{m=0}^{M-1} \sum_{n=0}^{N-1} W(m, n)^2} \sqrt{\sum_{m=0}^{M-1} \sum_{n=0}^{N-1} W^*(m, n)^2}} \quad (21)$$

BER is used to measure the accuracy of watermark extraction. It represents the ratio between the number of watermark bits with errors and the total number of watermark bits. A lower BER value indicates that the watermark extraction accuracy is high, and the integrity of the watermark is effectively protected, the corresponding watermarking has great robustness.

Equation (22) is usually used to calculate the bit error ratio, where W is the original watermark image, W^* representing the extracted watermark image, \oplus is the xor operation.

$$BER = \frac{\text{sum}(W \oplus W^*)}{\text{length}(W)} \times 100\% \quad (22)$$

The watermark is extracted after different degrees of attack and processing on the watermarked. Before extracting the watermark, the proposed correction algorithm is applied to correct the rotation processing, and the watermark still in the encrypted state is decrypted by using the chaotic key to improve the integrity and quality of the extracted watermark.

In Table V, NC and BER are used to evaluate the differences between the extracted watermark and the original, which shows the robustness of the watermarking algorithm.

TABLE VI
COMPARISON EXPERIMENT WITH RELEVANT STUDIES

Attacks	[11]		[12]		[13]	Proposed	
	NC	BER	NC	BER	BER	NC	BER
Rotate 45°	-	-	-	-	0.096	0.907	0.073
Rotate 60°	0.939	0.030	-	-	-	0.910	0.070
Vertical flipping	1	0	-	-	-	1	0
Horizontal flipping	1	0	-	-	-	1	0
Rescale 0.5	-	-	-	-	0.098	0.985	0.012
Rescale 0.8	0.891	0.083	0.992	0.009	-	0.931	0.055
Rescale 1.6	0.972	0.004	-	-	-	1	0
Crop (1/8)	-	-	0.885	-	-	0.950	0.040
Crop (1/4)	0.856	0.061	0.890	-	0.038	0.894	0.083
JPEG 50	-	-	0.971	0.038	-	0.987	0.011
JPEG 75	0.853	0.117	-	-	-	0.999	0
JPEG 90	0.995	-	0.995	0.007	0.008	1	0
SP noise 0.01	0.929	-	0.928	0.084	0.048	0.914	0.068
Gaussian noise 0.001	-	-	-	-	0.013	0.999	0
Gaussian Filter 3×3	0.904	0.039	0.989	0.014	0.035	0.999	0.008
Median Filter 3×3	-	-	0.927	0.085	0.096	0.969	0.025

TABLE VII
COMPARISON EXPERIMENT WITH RELATED ROTATION ANGLE STUDIES

	Rotate attacks								MSE	MAE
	5.1	13	27.3	37.4	45	51.9	62	72.6	-	-
Actual Parameter	5.1	13	27.3	37.4	45	51.9	62	72.6	-	-
Proposed	5.12	12.98	27.26	37.45	44.98	51.91	62.00	72.62	0.0095	0.0225
[6]	4.83	13.01	27.21	37.47	44.99	51.99	62.06	72.67	0.0401	0.0838
Actual Parameter	30.1		45.6		60.2		75.8		-	-
Proposed	30.04		45.62		60.18		75.77		0.0182	0.0325
[11]	29.95		45.62		60.18		75.73		0.0420	0.0650

D. Comparison Analysis

Tables VI–VII shows the comparative results of relevant studies in recent years, comparing the robustness indicators on the basis of comparable invisibility. Through the analysis and comparison of these indicators, the reliability and robustness of the watermarking algorithm can be continuously improved, so as to better meet the application requirements of watermark protection and authentication.

The comparative works are all robust digital watermarking algorithms based on color host images. Image processing based on the quaternion concept adopts methods such as QDCT and QWT. Reference [11] proposes a color image watermarking scheme based on holograms using QDCT. Compared with this algorithm, the proposed possesses the same capacity to resist rotation attack, flip attack, and noise, and the advantages in scaling, cropping, compression and filtering attack are more pronounced. Reference [12] employs quaternion wavelet transform (QWT) on color image watermarking, yet it does not discuss the solution for rotation attack. Compared with this algorithm, the proposed demonstrates superior performance in cropping attack, compression and filtering attack, but is not as effective as this algorithm in minimizing and noise attack. QDCT is also adopted in Reference [13], but the distinction lies in that the denoising convolutional neural network (DCNN) optimization algorithm

is also introduced, which renders the extracted binary watermark more visually recognizable. Compared with this algorithm, the proposed does not consume more time and space cost for model training and has better anti-geometric attack performance.

In Table VII, distortion detection algorithms based on synchronous correction [6] and Zernike moments [11] are respectively compared. The former uses relevant techniques of machine learning, and it takes a certain amount of time to train the machine to predict rotation distortion. The latter is a geometric distortion detection algorithm based on an invariant centroid proposed by Khotanzad in 1990 [26], and a geometric estimation method based on Zernike moments is proposed. According to the data provided by the references, the accuracy of the prediction is compared. Most of the data prove that the proposed is closer to the actual parameter than that of the comparison works. MSE and mean absolute error (MAE) are used to measure the progress of accuracy of angle prediction algorithm.

E. Security Analysis

The watermarking encryption process must exhibit both high sensitivity and security. In the case of an incorrect key, the decryption process should not proceed smoothly, resulting in a completely different decrypted watermark compared to the correct outcome.

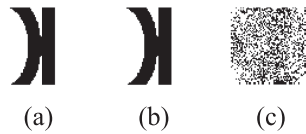


Fig. 19. (a) Original watermark (b) Correct key decryption watermark (c) False key decryption watermark.

During practical testing, when a key for a hyperchaotic map was modified, the process yielded only a minor alteration, with a discrepancy of 10^{-15} from the correct key. Fig. 19 serves as evidence that even a slight error cannot restore the correct watermark. Furthermore, the watermark obtained by decrypting the incorrect key contains minimal visual information, indicating the key sensitivity of the algorithm.

V. CONCLUSION

A rotation correction algorithm based on continuous orthogonal moments is put forward. Taking the polar harmonic Fourier moments as an instance, the results obtained for any order and repetition possess high accuracy. From the application perspective, it is highly suitable for quantization watermarking and ameliorates the limitation of quantization in rotation attack. The new chaotic system proposed in this paper realizes the chaotic enhancement of a one-way coupled mapping lattice system by introducing a one-dimensional mapping dynamic modulation coupling coefficient, and passes the NIST random test to guarantee the security of the entire watermarking algorithm, including the scrambling and encryption process, and is capable of resisting statistical analysis attacks. In addition, the quality of watermark extraction by quantization in the case of cropping attack is enhanced by eliminating the location correlation of pixels. However, there are still certain special attacks against which the algorithm is insufficient. For instance, histogram equalization and affine transformation, can be further investigated in future endeavors.

REFERENCES

- [1] G. Cao et al., "Improved FAST algorithm for non-uniform rotational distortion correction in OCT endoscopic imaging," *Opt. Exp.*, vol. 31, no. 2, pp. 2754–2767, Jan. 2023, doi: [10.1364/OE.474955](https://doi.org/10.1364/OE.474955).
- [2] Z. Li, S. Chen, and X. Cheng, "Dual video watermarking algorithm based on SIFT and HVS in the contourlet domain," *IEEE Access*, vol. 7, pp. 84020–84032, 2019, doi: [10.1109/ACCESS.2019.2899378](https://doi.org/10.1109/ACCESS.2019.2899378).
- [3] J.-H. Son, H.-G. Kim, H.-J. Han, and T. Kim, "Comparison of various frequency matching schemes for geometric correction of geostationary ocean color imager," *Sensors*, vol. 19, no. 24, Dec. 2019, Art. no. 5564, doi: [10.3390/s19245564](https://doi.org/10.3390/s19245564).
- [4] Z. Bian, M. Shao, A. Carass, and J. L. Prince, "DrDisco: Deep registration for distortion correction of diffusion MRI with single phase-encoding," *Image Video Process.*, vol. 12464, pp. 292–296, Apr. 2023, doi: [10.48550/arXiv.2304.00217](https://doi.org/10.48550/arXiv.2304.00217).
- [5] Y. Qiao and Y. Shi, "Unsupervised deep learning for FOD-based susceptibility distortion correction in diffusion MRI," *IEEE Trans. Med. Imag.*, vol. 41, no. 5, pp. 1165–1175, May 2021, doi: [10.1109/TMI.2021.3134496](https://doi.org/10.1109/TMI.2021.3134496).
- [6] Q. Wang, T. Wen, H. Yang, and X. Wang, "Synchronisation correction-based colour image watermarking using proximal classifier with consistency and multivariate generalised Gaussian model," *Signal Process.*, vol. 55, no. 24, pp. 1305–1307, Nov. 2019, doi: [10.1049/el.2019.2586](https://doi.org/10.1049/el.2019.2586).
- [7] M. Jiang, X. Feng, C. Wang, X. Fan, and H. Zhang, "Robust color image watermarking algorithm based on synchronization correction with multi-layer perceptron and Cauchy distribution model," *Appl. Soft Comput.*, vol. 140, Jun. 2023, Art. no. 110271, doi: [10.1016/j.asoc.2023.110271](https://doi.org/10.1016/j.asoc.2023.110271).
- [8] Z. L. Paola, L. S. Jesus, and H. Arroyo, "Christian, Rincon U. Sonia, correction of banding errors in satellite images with generative adversarial networks (GAN)," *IEEE Access*, vol. 11, pp. 51960–55190, 2023, doi: [10.1109/ACCESS.2023.3279265](https://doi.org/10.1109/ACCESS.2023.3279265).
- [9] Y. Wang, S. Ji, and Y. Zhang, "A learnable joint spatial and spectral transformation for high resolution remote sensing image retrieval," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 14, pp. 8100–8112, 2021, doi: [10.1109/JSTARS.2021.3103216](https://doi.org/10.1109/JSTARS.2021.3103216).
- [10] C. Wang, X. Wang, Z. Xia, and B. Ma, "Image description with polar Harmonic Fourier moments," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 12, pp. 4440–4452, Dec. 2019, doi: [10.1109/TCSVT.2019.2960507](https://doi.org/10.1109/TCSVT.2019.2960507).
- [11] J. Li, Q. Lin, C. Yu, X. Ren, and P. Li, "A QDCT- and SVD-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram," *Soft Comput.*, vol. 22, pp. 47–65, Aug. 2018, doi: [10.1007/s00500-016-2320-x](https://doi.org/10.1007/s00500-016-2320-x).
- [12] H. Zhang, Z. Li, X. Liu, C. Wang, and X. Wang, "Robust image watermarking algorithm based on QWT and QSVD using 2D Chebyshev-Logistic map," *J. Franklin Inst.*, vol. 359, no. 2, pp. 1755–1781, Jan. 2022, doi: [10.1016/j.jfranklin.2021.11.027](https://doi.org/10.1016/j.jfranklin.2021.11.027).
- [13] L. Hsu and H. Hu, "QDCT-based blind color image watermarking with aid of GWO and DnCNN for performance improvement," *IEEE Access*, vol. 9, pp. 155138–155152, 2021, doi: [10.1109/ACCESS.2021.3127917](https://doi.org/10.1109/ACCESS.2021.3127917).
- [14] C. Yu, X. Zhang, C. Qin, and Z. Tang, "Reversible data hiding in encrypted images with secret sharing and hybrid coding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 33, no. 11, pp. 6443–6458, Nov. 2023, doi: [10.1109/TCSVT.2023.3270882](https://doi.org/10.1109/TCSVT.2023.3270882).
- [15] C. Yu, X. Zhang, X. Zhang, G. Li, and Z. Tang, "Reversible data hiding with hierarchical embedding for encrypted images," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 2, pp. 451–466, Feb. 2022, doi: [10.1109/TCSVT.2021.3062947](https://doi.org/10.1109/TCSVT.2021.3062947).
- [16] C. Yu, X. Zhang, G. Li, S. Zhan, and Z. Tang, "Reversible data hiding with adaptive difference recovery for encrypted images," *Inf. Sci.*, vol. 584, pp. 89–110, 2022, doi: [10.1016/j.ins.2021.10.050](https://doi.org/10.1016/j.ins.2021.10.050).
- [17] W. Feng and B. Hu, "Quaternion discrete cosine transform and its application in color template matching," in *Proc. IEEE Congr. Image Signal Process.*, Sanya, China, May 2008, pp. 252–256, doi: [10.1109/CISP.2008.61](https://doi.org/10.1109/CISP.2008.61).
- [18] L. Teng, X. Wang, and Y. Xian, "Image encryption algorithm based on 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion," *Inf. Sci.*, 2022, vol. 605, pp. 71–85, doi: [10.1016/j.ins.2022.05.032](https://doi.org/10.1016/j.ins.2022.05.032).
- [19] L. Teng, X. Wang, F. Yang, and Y. Xian, "Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion," *Nonlinear Dyn.*, vol. 105, no. 2, pp. 1859–1876, 2021, doi: [10.1007/s11071-021-06663-1](https://doi.org/10.1007/s11071-021-06663-1).
- [20] K. Kaneko, "Pattern dynamics in spatiotemporal chaos: Pattern selection, diffusion of defect and pattern competition intermittency," *Physica D: Nonlinear Phenomena*, vol. 34, no. 1, pp. 1–41, Jan. 1989, doi: [10.1016/0167-2789\(89\)90227-3](https://doi.org/10.1016/0167-2789(89)90227-3).
- [21] X. Wang, L. Feng, S. Wang, C. Zhang, and Y. Zhang, "Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption," *IEEE Access*, vol. 6, pp. 39705–39724, Jun. 2018, doi: [10.1109/ACCESS.2018.2855726](https://doi.org/10.1109/ACCESS.2018.2855726).
- [22] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-allen and hamilton inc mclean va, 2001.
- [23] C. Singh and J. Singh, "A survey on rotation invariance of orthogonal moments and transforms," *Signal Process.*, vol. 185, Aug. 2021, Art. no. 108086, doi: [10.1016/j.sigpro.2021.108086](https://doi.org/10.1016/j.sigpro.2021.108086).
- [24] S. Pei, J. Ding, and J. Chang, "Efficient implementation of quaternion Fourier transform, convolution, and correlation by 2-D complex FFT," *IEEE Trans. Signal Process.*, vol. 49, no. 11, pp. 2783–2797, Nov. 2001, doi: [10.1109/78.960426](https://doi.org/10.1109/78.960426).
- [25] The standard color images from the Computer Vision Group at the University of Granada, Feb. 2018, [Online]. Available: <http://decsai.ugr.es/cv/gdbimagenes>
- [26] A. Khotanzad and Y. H. Hong, "Invariant image recognition by Zernike moments," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 12, no. 5, pp. 489–497, May 1990, doi: [10.1109/34.55109](https://doi.org/10.1109/34.55109).