Tamper Detection in Watermarked Images Using NROI-Based Circular-Harmonic-Fourier Moments

Jitao Yan
School of Surveying and Urban Spatial Informatics, Henan University of Urban Construction, Pingdingshan 467036, Henan, China
E-mail: yjthncj@163.com

Keywords: circular-harmonic-fourier moments, image tampering watermarking, information tampering detection, masking keys, perceptibility

Received: February 28, 2025

In view of the lower discretization of image tampering watermark, the overall block-level operation characteristics are easy to trigger the square effect. The watermark-containing region has the attribute of multiple sub-blocks, there is a watermark-containing region with poor perceptibility, the watermarking information is not visible. The interference resistance and robustness are poor, for this reason, we propose a tamper detection method in watermarked images using NROI-based circular-harmonic-fourier moments. The NROI sub-block is selected, the circular-harmonic-Fourier moments of each sub-block are calculated. The smoothing sub-block in the polar coordinate system is decomposed orthogonally, the geometric invariance of the circular-harmonic-Fourier moments is embodied in the magnitude of the moments. The low-order circular-harmonic-Fourier moments are selected to superimpose and sum up the products of the circular-harmonic-Fourier functions of the same level, so that the reconstruction of image is realized; Take the sub-block circular-harmonic-Fourier low-order moments of the image reconstruction result in the NROI region as feature vectors. Determine the robust transformation coefficients by defining the robust coefficient selection rules to obtain the watermark tampering location to avoid the occurrence of the square effect; The complete watermark sequence is extracted by comparing the amplitude variation of all the moments with the domain values. The extracted binary watermark sequence is compared with the original watermark stored in the NORI location to verify whether the image has been tampered or not, through the implementation of the corrosion operation and expansion operation, the image region that matches the actual tampering is sensed. The experimental results show that this method can resist attacks such as white noise, rotation, and scaling for image samples with strong concealment of watermark images, and maintain clear and distinguishable watermark information. The PSNR of watermark information is higher than 40, SSIM index is higher than 0.9, and JND index is lower than 5, demonstrating excellent anti-interference and robustness. The detection accuracy of this method for tampering with image watermark information under different attack states is higher than 94%, the detection time is less than 8ms, and the detection efficiency is relatively good.

Povzetek: Metoda zazna posege v digitalne vodne žige s pomočjo NROI območij in nizkorednih krožno-harmoničnih Fourierjevih momentov, kar omogoča robustno, tončno in hitro zaznavo sprememb.

1 Introduction

The rapid development of digital technology makes digital images become the core of information dissemination, but the accompanying problems of image copyright protection, content confirmation and data integrity have become more and more prominent [1]. Image watermarking technology, as an advanced information hiding technology, by embedding tiny marks in the image that are difficult to find, provides strong support for the tracking and protection of multimedia content. These watermarks are in various forms, such as text, logos, small drawings, etc., after careful design and coding, skillfully integrated into the image, to ensure that the image source, use and modify the history of the traceability, effectively safeguard the rights and interests of the creators and the authenticity of the data [2]. However, this technology also faces the risk of tampering, unauthorized modification will threaten the integrity and validity of the watermark, weakening copyright protection, content confirmation and data integrity. Once the watermark is tampered with or deleted, the source and use of the image cannot be accurately traced, seriously infringing on the rights and interests of the creator and jeopardizing the authenticity of the data [3]. In the face of this urgent challenge, the development of efficient and reliable image watermark tampering detection techniques has become particularly critical [4]. Many scholars are actively engaged in this field of research, with a view to developing technical means that can accurately identify whether the image watermark has been tampered with, so as to effectively deal with the copyright protection and content authenticity verification problems in digital image dissemination.

Salama et al. used a combination of Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and

Blowfish cryptography in image watermark tampering detection [5]. This method generates an encrypted blue component by separating the given RGB main image into red, green and blue components, applying DWT and DCT to the green component and tampering with the watermarked logo in it, the blue component is encrypted by Blowfish encryption to generate an encrypted blue component, interchanging the lowest valid bit of the encrypted blue component with the lowest significant bit of the red component of the host image, generating a new red component, interchanging the green component with the red component with the watermark, the original image with the watermark, the original image with the watermark, and the original image with the watermark, the blue component with the watermark. The green component with watermark, the original blue component and the newly formed red component are merged to produce a watermarked image with watermark information and tampering detection capability. DCT is usually used to divide the image into small blocks (e.g., 8x8) for processing, which may lead to the square effect of the image after compression or watermark tampering. At high compression ratios or strong watermark tampering intensity, this effect affects the visual quality of the image. Mahto et al. proposed a fused secure watermarking algorithm [6]. This algorithm utilizes non-subsampling contour wave transform (NSCT) technique to generate a fuzzy watermarked image containing copyright or authentication information. Using methods such as random singular value decomposition (RSVD), this watermarked image is fused with the blue channel of the original image and encrypted to compute the hash value of the original cover image, which is then embedded into the green channel of the host image. By extracting the the embedded watermark and hash value, and compare it with the original watermark and hash value to determine whether the image has been tampered with. Although the hash value provides verification of the image integrity, the method may not be effective in detecting tampering if the attacker is able to modify the image through sophisticated tampering techniques without changing the hash value. Loc et al. introduced deep neural networks in their study of the task of protecting QR codes from tampering and verifying their authenticity through watermarking techniques [7]. Using error correcting code to encode secret features, deep neural network is utilized to generate QR code image with watermark by hiding the encoded information into the QR code. A neural network based on Siamese network architecture is developed to extract the secret features from the QR code to be verified, and combined with the similarity measurement results and watermark extraction results, a comprehensive judgment is made on whether the QR code has been tampered with or not. However, deep neural networks mainly process information through local sensing, and may not be able to handle well the scenarios that need to be analyzed as a whole, which may lead to the limitation of the performance of deep neural networks when the area containing watermarks is large or when global features are involved. Prasad et al. used a fragile watermarking technique in image watermarking information tampering detection [8]. This technique splits the image into (1 x 2) pixel chunks and for each chunk, block level authentication codes are extracted from the highest valid bits of both pixels using averaging and modulo operations. These authentication codes are encrypted by a chaotic key sequence based on logical mapping. The encrypted authentication codes are embedded back into the pixels of the corresponding block. The authentication codes in the watermarked image are extracted and compared with the recomputed authentication codes. If the two do not match, the image may have been tampered with. However, fragile watermarking techniques are usually very sensitive to small changes in the image, which helps detect tampering, but also means that it may not be able to resist some of the normal processing operations in the watermarked area, such as compression, filtering, and so on. This limits the usefulness of fragile watermarking in some application scenarios. The above analysis of the current relevant methods is shown in Table 1.

Table 1: Current relevant technical analysis.

Method name	The technology used	Robustness to attacks	Computational efficiency	Main limitations
Method in Literature [5]	DWT+DCT	It exhibits block effects under compression attacks, affecting the visual quality of the image.	The DCT division processing method is relatively cumbersome, leading to insufficient computational efficiency.	The DCT division processing may cause the image to exhibit block effects after compression or watermark tampering. Under high compression ratios or strong watermark tampering intensities, this effect can impact the visual quality of the image.
Method in Literature [6]	NSCT+RSVD	It relies on hash values and has limited robustness when the hash	The calculation of hash values for large-scale images is complex, and the computational	If an attacker can modify the image through sophisticated tampering techniques without changing the hash values, this method may not effectively detect the tampering.

		values remain unchanged.	efficiency needs to be improved.	
Method in Literature [7]	CNN+QR Code	It has poor robustness when the watermark area is large or involves global features.	CNN processes more slowly when dealing with large watermark areas or global features.	CNN's performance is limited when the watermarked area is large or involves global features, and it has poor perceptibility for the watermarked area.
Method in Literature [8]	Fragile Watermarking Technique + Logical Mapping Chaotic Encryption	It has poor robustness under compression and filtering attack conditions.	It has insufficient application efficiency in compressing and filtering processed images.	Fragile watermarking techniques cannot resist normal processing operations in the watermarked area, such as compression and filtering.

According to Table 1, existing methods are affected by multiple image compressions, cropping, or filtering, making it difficult to accurately detect tampering information using damaged watermarks. Therefore, we propose a tamper detection method in watermarked images using NROI-based circular-harmonic-fourier moments. NROI (Non-Region of Interest) has stable features, is not easy to be affected by geometric attacks such as rotation, scaling, etc., and is able to maintain the integrity of the watermark in complex scenarios. The circular-harmonic-Fourier moments, as a kind of image moments with rotation, scaling and translation invariance, circular harmonic Fourier moments can extract key watermark features after being tampered with by complex techniques such as high-intensity compression and filtering. This paper introduces NROI and circular harmonic Fourier moments to solve the problem of difficulty in accurately detecting tampered information in image watermarks after complex tampering processing and physical transformation. It maintains the visual quality of watermark information under extreme image degradation, effectively locates tampered areas, and improves the adaptability of watermark detection. Moreover, based on non regions of interest, it is possible to remove watermarks and redundant features, which improves computational efficiency when the watermarked area is large or global feature extraction occurs.

2 Tamper detection method in watermarked images

2.1 Non-Region of Interest (NROI) sub-block selection

In the field of image processing, ROI (Region of Interest) carries the main information and key features of an image, and is the focus of image analysis [9]. In contrast, it is the part of the image other than the ROI, whose information is often not regarded as the core content of the analysis. In order to avoid interference with the main information of the image, to ensure that the original function of the image is not affected, but also to achieve the purpose of copyright protection or tampering detection, the need to tamper with the watermark information in the NROI of the image to add an additional layer of security for the image, that is, the watermark information in the ROI due to a variety of reasons and lost, you can still rely on the watermark information in the NROI to detect tampering with the image.

According to the information entropy of image sub-blocks in the safe region for sub-block selection [10], the internal region of the image is divided into ROI and NROI: ROI corresponds to the large information entropy value of the texture sub-blocks, the texture information of these sub-blocks is more complex, tampering with the watermark will affect the diagnostic details of distortion; NROI corresponds to the smaller information entropy value of the smooth sub-blocks, these sub-blocks are mostly located in the background area, and tampering with the watermark information will not affect the overall visual quality of the image. In terms of security, attackers usually target high entropy areas for tampering, ignoring the watermark in low entropy smooth areas. Therefore, embedding watermark information in areas with lower information entropy can reduce the risk of active removal. And the moment features of low entropy regions have approximate invariance to geometric attacks such as rotation/scaling, making them tamper resistant. The information entropy of the image is calculated by the following Eq. (1):

$$G(B) = -\left[Q_1 \lg(Q_1) + Q_2 \lg(Q_2) + Q_3 \lg(Q_3) + \ldots + Q_n \lg(Q_n)\right] = -\sum_{k=1}^{255} Q_k \lg(Q_k) \quad (1)$$

Where: B represents the input image; Q_k denotes the proportion of the pixels for the gray value k in the image, and $Q_k \in [0,1]$, $\sum_{k=1}^{n} Q_k = 1$. In order to facilitate the later selection of the watermark tampering region, the image is divided into sub-blocks that do not overlap each other, and the information entropy of each block is expressed as follows Eq. (2):

$$g_i\left(b\right)=-\sum_{k=1}^{255}Q_k\lg\left(Q_k\right) \tag{2}$$

In order not to destroy the integrity of the image, the watermark information is embedded in the smoothing sub-block. According to the information entropy of the image, the image is divided into texture sub-block and smoothing sub-block [11], and are denoted as Eq. (3) and Eq. (4), respectively $C^W\left(b\right)$ and $C^H\left(b\right)$:

$$\left[g_i^v,g_i^e\right]=sort\left(g_i\right) \tag{3}$$

$$C_i^f=\begin{cases} f=W, & g_i>g_{1024}^v \\ f=H, & g_i\le g_{1024}^v \end{cases} \tag{4}$$

Where: $sort$ is the sorting function; g_i^v denotes the index sequence obtained by ordering the entropy values from smallest to largest, i indicates the sub-block order. g_i^e indicates the sub-block index position, which is used as the basis for tampering with the watermark sub-block selection. The sub-blocks with less texture information, i.e., the first 1024 sub-blocks with smaller entropy value, are selected as NROIs to tamper with the watermark information.

The sub-block selection method is used to form the mask key, which is used as the basis for embedding and extracting the watermark. The mask key is generated as follows: set an all-zero matrix as the transition matrix, according to the sub-block index g_i^e to mark the position of NROI sub-block $C^H\left(b\right)$, the mask g_i^e of the pixel matrix corresponding to the tampered position as 1 to obtain a mask key of the same size as the original image, enhancing the imperceptibility of the watermark and improving image security.

2.2 Image reconstruction based on smoothing sub-block with circular harmonic-Fourier moment algorithm

Although the Zernike moment has rotational invariance, it needs to be normalized by the amplitude of the moment, which increases computational complexity and reduces detection efficiency. The Chebyshev moment is based on the Cartesian coordinate system and is sensitive to rotation attacks, which can lead to geometric errors. Legendre moments are based on polynomials in Cartesian coordinate systems and are sensitive to rotation. The rotation operation will completely change the moment value, which can easily introduce detection errors. Therefore, this article adopts the CHFM method for tampering detection.

Under the complex geometric transformation, the image features are easy to change, and it is difficult to ensure the stability and detectability of the watermark, while the circular harmonic-Fourier moment algorithm effectively solves these problems. This algorithm is based on polar coordinates and decomposes smooth sub blocks into radial and angular robust transformation coefficients. Through the robust transformation coefficients, the image is orthogonally decomposed to obtain circular harmonic Fourier moments. Among them, the low-order moments contain the main structure and contour information of the image, which can reflect the overall features, and serve as the basis for watermark tampering location. Therefore, after selecting the NROI sub-block, the low-order moments are calculated and selected as feature vectors, and the image can be reconstructed approximately by superimposing the low-order moments and the product of the same level of circular harmonic-Fourier function, the more levels the higher the degree of approximation, so as to distinguish between the watermark tampering and the process of tampering [12], and to analyze the degree of rotation, scaling, and translation of the individual sub-block. Image tampering usually manifests as low-frequency structural damage, and low order moments are sufficient to sensitively capture such changes. Higher order moments, based on high-frequency details, are susceptible to noise interference, which in turn reduces robustness. The amplitude of low order moments is approximately invariant to geometric attacks such as rotation and scaling (due to energy concentration at low frequencies), while the phase of high-order moments is sensitive to geometric deformation, which can easily introduce false positives and require more integration operations and frequency domain sampling, resulting in increased computational complexity but slightly weaker improvement in detection performance. Therefore, this method uses low order moments as feature vectors. Low order moment-based image reconstruction may lose texture details, but the mean/variance of the tampered area does not match the surrounding low entropy background. Low order moment differences can mark tampering without analyzing texture details, so it does not significantly affect subsequent tampering detection results.

In the polar coordinate system $\left(r,\alpha\right)$ of the image NROI sub-block region $C^H\left(b\right)$, define the function system $R_{ps}\left(r,\alpha\right)$, including the radial function $J_p\left(r,\alpha\right)$ and angular functions $\exp\left(qs\alpha\right)$ these two parts:

$$R_{ps}\left(r,\alpha\right)=J\left(r,\alpha\right)\exp\left(qs\alpha\right) \tag{5}$$

When $p=0$:

$$J\left(r,\alpha\right)=\left(\sqrt{r}\right)^{-1} \tag{6}$$

When p is odd numbers:

$$J\left(r,\alpha\right)=2\left(\sqrt{r}\right)^{-1}\sin\left((p+1)\pi r\right) \tag{7}$$

When p For an even number:

$$J\left(r,\alpha\right)=2\left(\sqrt{r}\right)^{-1}\cos\left(p\pi r\right) \tag{8}$$

In the Eq. (5)-Eq. (8), r is the radius. α represents the angular component in the polar coordinate system; q is an imaginary number. p is the order of the Fourier transform; S is the number of times the circular harmonic Fourier transform is performed. The complex exponential function $\exp(qs\alpha)$ represents the Fourier factor in the direction of the indicated angle; The function system $R_{ps}(r,\alpha)$ in the unit circle $(0 \le r \le 1, 0 \le \alpha \le 2\pi)$ is orthogonal, i.e Eq. (9):

$$\int_0^{2\pi}\int_0^1 R_{ps}(r,\alpha)R_{ps}^*(r,\alpha)rdrd\alpha = c\times\kappa_{ps} \quad (9)$$

Among them, κ_{ps} is the Kronecker symbol for defining the orthogonality of vectors. $R_{ps}^*(r,\alpha)$ is the conjugate of $R_{ps}(r,\alpha)$; c is a constant. $r=1$ is the maximum size of the object encountered in a given situation.

The smooth sub-block $h(r,\alpha)$ in the polar frame can be orthogonally decomposed by the function system $R_{ps}(r,\alpha)$, so that the image rotation, scaling and other geometric transformations can be reflected in the magnitude of the moment. The orthogonal decomposition process is shown in Eq. (10):

$$h(r,\alpha) = \sum_{p=0}^{\infty}\sum_{s=-\infty}^{+\infty}\zeta_{ps}J_p(r)\exp(qs\alpha) \quad (10)$$

Among them:

$$\zeta_{ps} = \int_0^{2\pi}\int_0^1 h(r,\alpha)J_p(r)\exp(-qs\alpha)rdrd\alpha \quad (11)$$

In Eq. (11), ζ_{ps} is defined as the circular-harmonic-Fourier moment of the smoothed sub-block $h(r,\alpha)$.

Select the appropriate number of low-order circular harmonic - Fourier moments and the same level of the circular harmonic - Fourier function of the product of the superposition of the summation, you can approximate the reconstruction of the original image, the more levels selected, the higher the degree of approximation, as shown in Eq. (12):

$$\tilde{h}(r,\alpha) \approx \sum_{p=0}^{P}\sum_{s=-S}^{S}\zeta_{ps}J(r)\exp(qs\alpha) \quad (12)$$

Among them, $\tilde{h}(r,\alpha)$ is the image reconstruction results.

2.3 Image reconstruction results in NROI region watermark tampering detection

When the image watermark information is tampered with, it means that the watermark information is subject to geometric transformation in the image, but the NROI region of the image reconstruction result can maintain the maximum invariance, comparing the initial image and the image reconstruction result of the watermark in the NORI position, we can perceive the image region that matches with the actual tampering, i.e., by applying the geometrical invariance of the circular-harmonic-Fourier moments to the image reconstruction result of the NROI region, each sub-block of circular-harmonic-Fourier low-rank moments is taken as a feature vector, and after corrosion operation and expansion operation, we can complete the detection of tampering of watermark information of image tampering.

The carrier image with size $E\times L$ is Eq. (13):

$$T = \{h(x,y), 0 \le x < E, 0 \le y < L\} \quad (13)$$

Set the binary watermark image with the size $F\times V$ as Eq. (14):

$$Z = \{z(i,j), 0 \le i < F, 0 \le j < V\} \quad (14)$$

Among them, $z(i,j)\in[0,1]$. In order to enhance the imperceptibility of the method, prevent key leakage and brute force attacks on the code key, and fully destroy the pixel spatial relationship of the binary watermark, Arnold mapping is introduced to obfuscate the binary watermark. Where, the Arnold mapping is Eq. (15):

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}(\bmod A) \quad (15)$$

Among them, (x,y) represents the pixel coordinates of the binary watermark; (x',y') is the pixel coordinates of the obfuscated binary watermark; A is the order of the moments of the watermarked image; mod is the modulo operation.

Since the circular-harmonic-Fourier transform makes it difficult to compute circular eigenregions $O_k(k=0,1,2,...,e-1)$ directly, to that end, by obtaining the outer quadrilateral of these $O_k(k=0,1,2,...,e-1)$, evolving it into a square block $U_k(k=0,1,2,...,e-1)$, whose size is $2r_k\times 2r_k$, k is an integer index, which is used to distinguish different circular feature regions. Then according to the computational procedure in subsection 2.2, the decomposition is performed for all square blocks $U_k(k=0,1,2,...,e-1)$ to obtain a series of transformation coefficients [13-15].

Among all the circular-harmonic-Fourier transform coefficients, not all of them are suitable for watermark tampering. In order to enhance the robustness of the method, a robust coefficient selection rule is defined to find out the robust transform coefficients as the watermark tampering feature vectors.

First, the square blocks of the initial image $U_k(k=0,1,2,...,e-1)$ is decomposed using the circular-harmonic-Fourier transform, to obtain the corresponding transformation coefficient $\vartheta_i\left(i=0,1,2,...,N\right)$, of which, N is the total number of transform coefficients; Subsequently, the square block corresponding to the image $U'_k\left(k=0,1,2,...,e-1\right)$ attacked by the geometric transform is decomposed using the circular-harmonic-Fourier transform, the transformation coefficients of the formed $\vartheta'_i\left(i=0,1,2,...,N\right)$ is obtained; Calculate the variance σ of ϑ_i and ϑ'_i, if $\sigma<2\%$, then select from the coefficients, otherwise, discard; combine the magnitudes of these circular-harmonic-Fourier transform coefficients into a set of $\left\{T_{l_i,e_i}\ |, i=0,1,2,...,N-1\right\}$.

The mask key of the same size as the original image obtained through subsection 2.1 is applied to the watermark tampering detection process. The mask key is a binary image with the same dimensions as the original image, where the NROI region is labeled as 1 and other regions are labeled as 0. When tampering with the watermark, only the selected coefficients located within the NROI are modified.

Again, according to $\left\{T_{l_i,e_i}\ |, i=0,1,2,...,N-1\right\}$, design the watermark tampering detection methods Eq. (16):

$$T'_{l_i,e_i}=\begin{cases}2\Delta\square round\left(\dfrac{T_{l_i,e_i}}{2\Delta}\right)+\dfrac{\Delta}{2}, z\left(i\right)=1\\ 2\Delta\square round\left(\dfrac{T_{l_i,e_i}}{2\Delta}\right)-\dfrac{\Delta}{2}, z\left(i\right)=0\end{cases} \tag{16}$$

Where, $i=0,1,2,...,N-1$, Δ is the quantization step; T'_{l_i,e_i} is the amplitude of the circular-harmonic-Fourier transform coefficients after tampering with the watermark; $z\left(i\right)$ is the watermark information of the i th embedded coefficients. Embedding the watermark information into the amplitude of the circular-harmonic-Fourier moments of the binary watermarked image, after obfuscation by Eq. (15), in the NROI region, can ensure the stability and detectability of the watermark after various processes. If the amplitude T'_{l_i,e_i} value of the circular harmonic Fourier transform coefficient calculated by formula (16) after tampering with the watermark is 1, it indicates that the watermark information has been tampered with, and a value of 0 indicates that it has not been tampered with, completing the detection.

The NROI in the image to be detected is matched with the NROI in the original image, i.e., the circular harmonic-Fourier moments are extracted from the image to be detected and meticulously compared with the original watermarking information [16], which analyzes whether the primitive features of the initial image have been damaged and accurately locates the possible tampering regions [17], as shown in Figure 1.

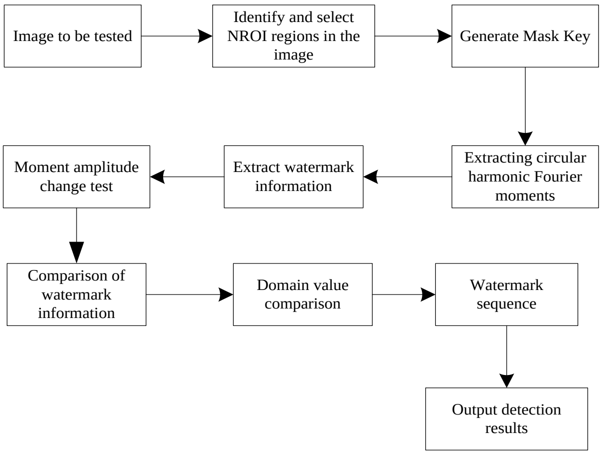


Image to be tested
Identify and select NROI regions in the image
Generate Mask Key
Extracting circular harmonic Fourier moments
Extract watermark information
Moment amplitude change test
Comparison of watermark information
Domain value comparison
Watermark sequence
Output detection results

Figure 1: Watermark detection steps

The $P\times S$ order circular-harmonic-Fourier moment of the inspected image was calculated, find the individual moments corresponding to those in the key, and compute the amount of change in the magnitude of the respective corresponding moments with respect to the key, and set the value $\varepsilon_{p,\mathrm{s}}$ of the domain of variation of the individual moments, the magnitude of change greater than $\varepsilon_{p,\mathrm{s}}$ is determined as 1 of the watermark sequence; less than or equal to $\varepsilon_{p,\mathrm{s}}$ is determined as 0 of the watermark sequence, and the method is as follows:

$$z'\left(i\right)\begin{cases}=1 \quad abs\left(\left|\zeta_{p,s}\right|-\left|\zeta'_{p,s}\right|\right)>\varepsilon_{p,\mathrm{s}}\\ =0 \quad abs\left(\left|\zeta_{p,s}\right|-\left|\zeta'_{p,s}\right|\right)\le\varepsilon_{p,\mathrm{s}}\end{cases} \tag{17}$$

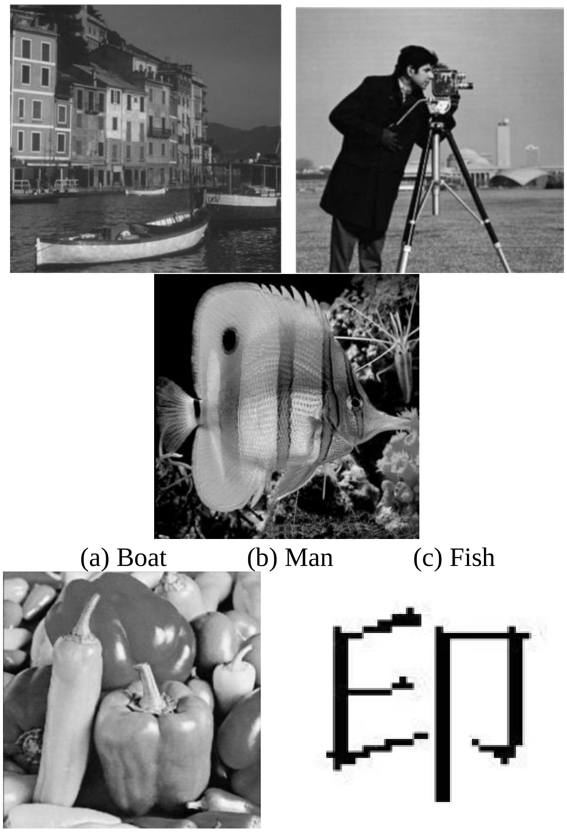
In the Eq. (17), $z'\left(i\right)$ is the watermark sequence, $abs\left(\ \right)$ function represents taking the absolute values.

According to the original watermark and the extracted watermark to obtain the watermark difference image, this difference image reflects the change of the watermark information in the image. Using the scanning line detection method to measure the sum of the distances of the white pixel points (error detection pixels) in each row of the difference image, and then divided by the total number of white pixels in the difference image to obtain the average distance M between neighboring white pixel points, and performed on the difference image $M\times M$ of median filtering removes noise interference caused by false detections [18]. The mathematical morphological expansion operation [19] is implemented on the structural elements $M\times M$ of the watermark to connect the "voids" formed by the watermark detection errors. Define a structural element (a 3x3 square). Let this structural element slide on the image, and mark the center point as tampered as long as it covers an area with at least one tampered pixel. The small tampered areas that were originally broken will be connected, and isolated voids will also be filled. Further, using a structure element of size $\left(M+2\right)\times\left(M+2\right)$ of structural elements to implement the corrosion operation in order to eliminate the possible boundary widening effect caused by the expansion [20]. Using the same structural element (such as a 3x3 square), slide the structural element so that the center point remains tampered with only when all the pixels it covers are tampered with. Through the above operation, the excessively expanded edges after expansion will be 'trimmed', restoring more accurate tampered boundaries. A complete watermark sequence is extracted by comparing the magnitude variation of all moments with the domain values. The extracted watermark sequence is compared with the original watermark stored in the NORI location. If the two match exactly, it indicates that the image has not been tampered with and is complete. If they do not match, the image watermark information has been tampered with, locate the image area that matches the actual tampering.

3 Experiment

Considering the generality and representativeness of the carrier images, a large number of different types of images were selected from the USC-SIPI image library as the test objects, and four natural images of 512 × 512 pixels with 8-bit depth were randomly selected as the main carrier image descriptions (shown in Figure 2(a) to (d)), which were in the BMP format to ensure lossless storage of the image quality and accuracy of processing.

The experimental platform is configured with Intel Core i7-13700K processor with 32GB DDR5 4800MHz RAM running on the computer, with NVIDIA GeForce RTX 4070Ti discrete graphics card, to ensure that the graphics processing power to meet the experimental needs. The experiment is based on Python 3.9 programming language, combined with scientific computing libraries such as NumPy 1.23.5, OpenCV 4.6.0 and SciPy 1.10.1. For the noise interference that may be involved in the experiments, in order to simulate the mild noise interference that may occur in actual transmission, the noise intensity is set to 0.01. In order to effectively remove noise while preserving image details to the greatest extent possible, a 3X3 filtering kernel is used. Using a 256 × 256 grayscale image as the carrier image for watermark tampering, the calculation order of the circular harmonic Fourier moment is set to P=40 and S=40. The experimental samples and the binary watermarking schematic are shown in Figure 2.

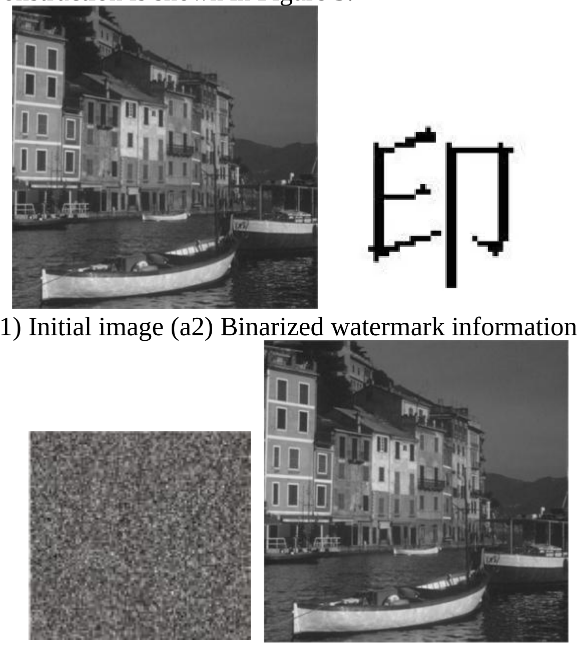


(a) Boat (b) Man (c) Fish

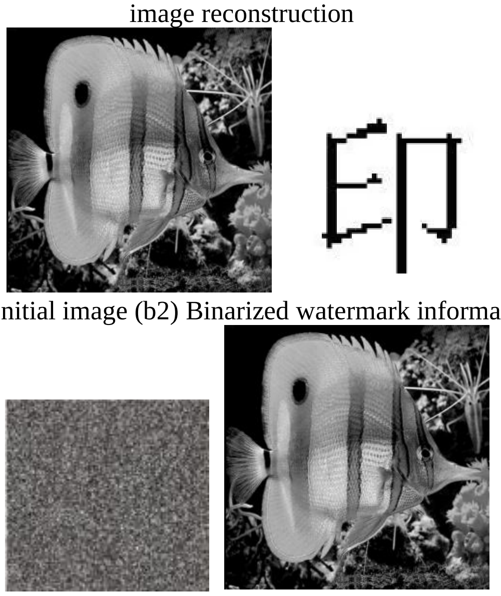
(d) Peppers (e) Authentication watermarking

Figure 2: Carrier image and binary watermark image

Two carrier images, Boat and Fish, are embedded with watermarking information to analyze whether an optimal balance can be found between guaranteeing the robustness of the watermarking algorithm and imperceptibility. The embedding strength is set to 0.03, and zero watermark information is embedded into the NROI of the images in group a, and a set of watermark information is tampered with in group b. The binarized display effect under strong steganographic image reconstruction is shown in Figure 3.



(a1) Initial image (a2) Binarized watermark information (a3) Schematic of binarized encryption (a4) Result of image reconstruction



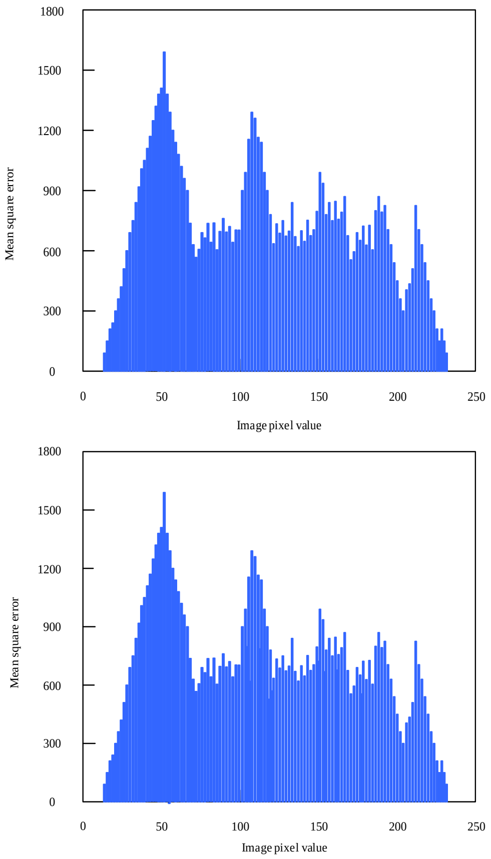
(b1) Initial image (b2) Binarized watermark information

(b3) Schematic of binarized encryption (b4) Reconstruction result of tampered image

Figure 3: Binarization display effect under strong concealment image reconstruction

In Figure 3, after the obfuscation process of Eq. (15), the image reconstruction results are obtained, in which none of the information about the binary watermark appears, and there is almost no difference with the original image visually, which conforms to the actual situation of the zero-watermark information embedding, and indicates that the image reconstruction results will not change the initial features of the original image after the reconstruction. Analyze the randomness of the image after Arnold mapping obfuscation processing, measure the linear correlation between adjacent pixels in Figure 3 (a1) and Figure 3 (b3), with a correlation value of 0.0001, close to 0, indicating good obfuscation effect.

Taking Figure 3(b1) and (b2) as samples, histograms are plotted to objectively assess the perceptibility of the watermark-containing region and measure the difference between the image reconstruction results and the initial image, as shown in Figure 4.

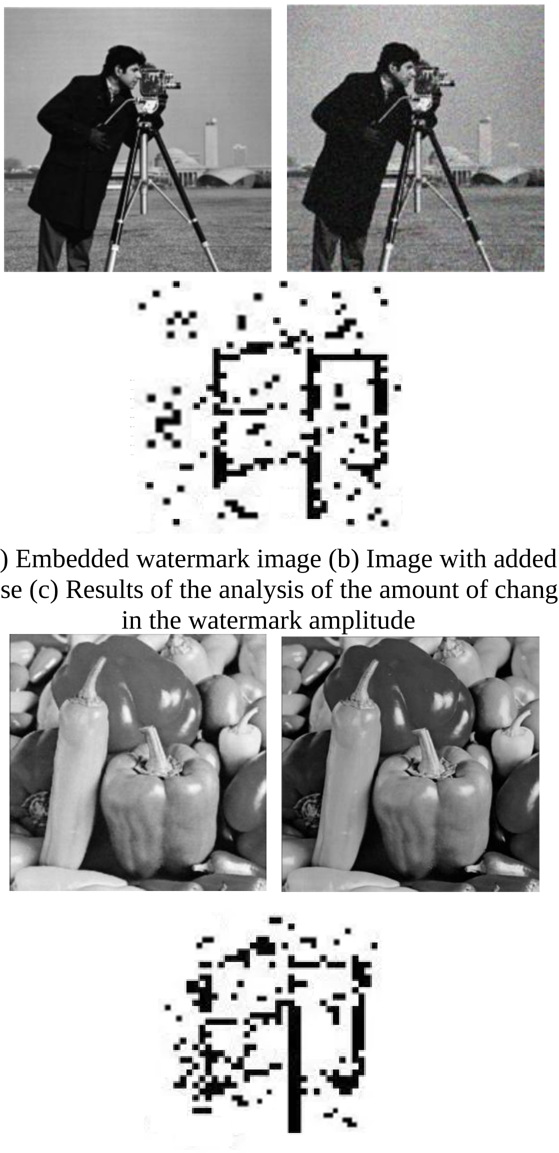


(a) Histogram of the initial image (b) Histogram of the image reconstruction result

Figure 4: Differences between the image reconstruction results and the initial images

As can be seen from Figure 4, the histograms of the tampered watermarked image and the initial image are very close to each other, indicating that the results of image reconstruction maximally retain the original characteristics of the initial image.

In order to analyze the anti-jamming and robustness, two groups of image processing processes are designed to simulate the white noise interference that may be caused by the image in the transmission or storage process, and the watermark amplitude change amount is analyzed for a certain image watermarking information tampering region, the experimental results are shown in Figure 5.



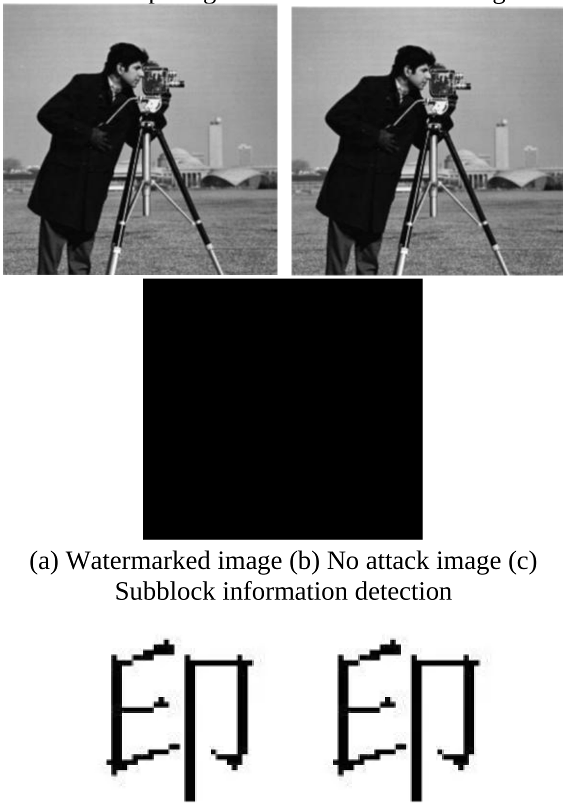
(a) Embedded watermark image (b) Image with added noise (c) Results of the analysis of the amount of change in the watermark amplitude

(d) Embedded watermark image (e) Image with added noise (f) Results of the analysis of the amount of change in the watermark amplitude

Figure 5: Effectiveness analysis of watermark magnitude change volume analysis

As shown in Figure 5(a)~(c), the quality of the image after adding white noise decreases significantly, and the watermark is extracted from the image after adding white noise, and the watermark amplitude change is low, although the extracted watermark image is blurred compared with the original watermark, the watermark information can still be clearly recognized. It shows that the method in this paper has certain anti-interference ability and robustness, and after median filtering, the watermark information is more integrated with the image background, while the watermark information is still retained in the filtered image.

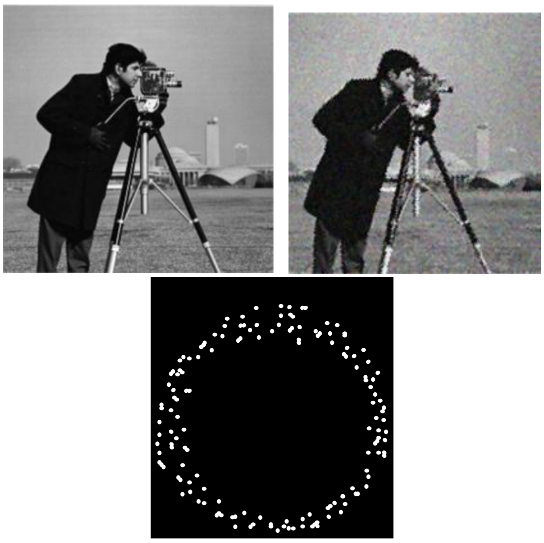
Compare the quality of watermark information extraction and tampering detection results under different attack conditions (tampering means), i.e., four types of attacks are designed, namely: no attack, as a control group, directly extracting watermark information. Sharpening attack, sharpening the watermarked image; shearing attack, randomly shearing part of the watermarked image; rotation and scaling attack, rotating and scaling the watermarked image. The rotation parameter is 30° and the scaling ratio is 10%. With a watermarked image as the detection object, the results of image watermark information tampering detection are shown in Figure 6-9.



(a) Watermarked image (b) No attack image (c) Subblock information detection

(d) Extracted watermark image(e) Original embedded watermark

Figure 6: No attack detection



(a) Watermarked image (b) Sharpened image (c) Subblock information detection

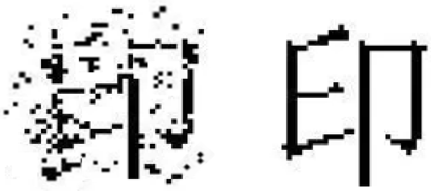
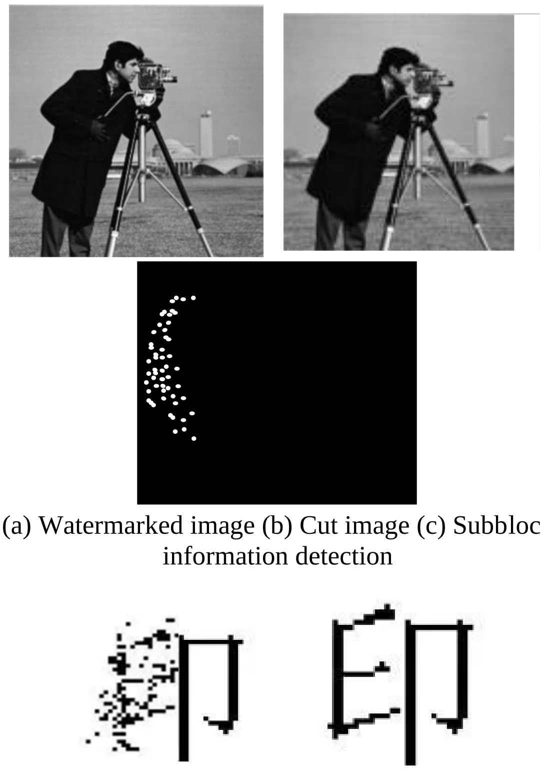


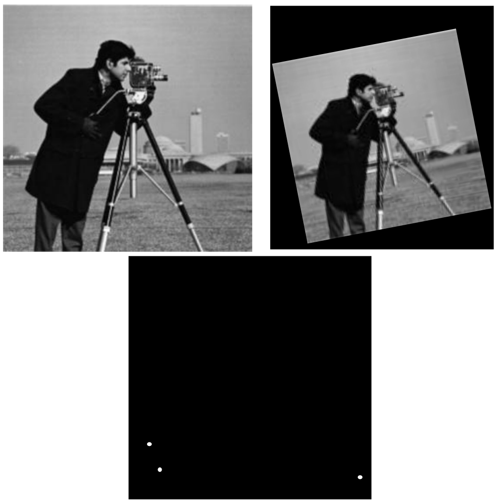
Figure 7: Sharpening attack detection results



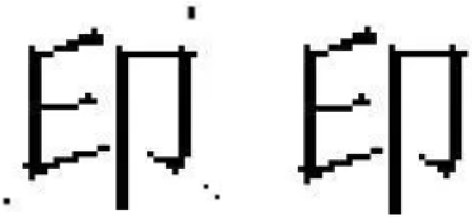
(a) Watermarked image (b) Cut image (c) Subblock information detection

(d) Extracted watermark image (e) Original embedded watermark

Figure 8: Cut attack detection results



(a) Watermarked image (b) Rotate and scale the image (c) Subblock information detection



(d) Extracted watermark image (e) Original embedded watermark

Figure 9: Rotation scaling attack detection results

The following information can be obtained by observing the sub-images in Figures 6 to 9. Figure 6(b) shows an unattacked image containing watermark. From Figure 6(c), it can be seen that the sub-blocks of the tampered watermark information remain intact, and the watermark information can be detected accurately and correctly, as shown in Figure 6(d), which is not different from the initial image in Figure 6(e). When the watermark-containing image suffers from high-intensity sharpening attack, as shown in Figure 7(b), some sub-blocks containing watermark information are tampered with, as shown in Figure 7(c), resulting in distortion of the extracted watermark image, as shown in Figure 7(d). Figure 8 shows the detection of watermarked images after shear attack. As shown in Figure 8(b), when the watermarked image is sheared, the watermark information in the corresponding position is lost, as shown in Figure 8(c). The detection results show that the location of the watermark information is lost and the location of the image under attack coincides exactly. As can be seen from the sub-plots in Figure 9, the position of the watermark information is only slightly disturbed when the image is attacked by rotation and scaling because the watermark information is embedded in the inner circle of the carrier image. This is due to the excellent geometric invariance of the circular-harmonic-Fourier moment watermark tampering method, including rotation invariance and scaling invariance. Even after the image has been rotated and scaled, the circular-harmonic-Fourier moments maintain their stability, which ensures that the watermark information can be extracted more accurately. The experimental results show that the results of tampering detection are highly consistent with the results of watermark extraction, which fully proves that the method in this paper can accurately locate the watermarked sub-blocks that have been tampered with.

Traditional DCT method, DWT method, Zernike moment, and the method in reference [6] were used as comparative methods and applied to tamper detection of 100 watermarked images. Set no attack state, add white noise state, image rotation state, image scaling state, image sharpening state, high-resolution actual scene, and image cropping state, and record the average detection accuracy and detection time under different conditions, as shown in Table 2.

Table 2: Comparison of tamper detection performance.

Test condition	Detection accuracy /%					Testing time/ms				
	DCT method	DWTmethod	Literature [6] method	This paper's method	Zernike quadrature	DCTmethod	DWTmethod	Literature [6] method	This paper's method	Zernike quadrature
No attack state	88.8	82.6	83.4	98.2	84.5	18.8	13.6	16.5	5.3	16.6
Enter the white noise state	84.4	76.9	80.2	96.5	79.4	24.8	25.4	20.8	6.1	20.9
Image rotation status	82.8	73.6	78.8	95.3	78.6	23.7	24.2	25.3	5.6	23.2
Image zoom status	84.8	75.4	80.8	96.1	80.9	29.7	27.3	26.9	7.4	18.8
Image sharpening status	83.7	74.2	79.3	95.5	76.2	23.2	25.6	19.2	6.7	19.1
High resolution actual scene	89.7	87.3	86.9	99.4	86.8	19.4	14.1	17.2	5.8	16.9
Image cropping status	83.2	75.6	79.2	94.7	79.1	22.8	23.6	18.8	5.3	18.6

According to Table 2, compared with other methods, the detection accuracy of our method varies slightly under different image conditions, and remains above 94%. However, the detection accuracy of other methods decreases significantly due to image attack processing, all below 90%, proving that our method has better detection accuracy. In terms of computational time efficiency, this method also has advantages, with a response time consistently below 8ms and better detection efficiency.

Test the resistance robustness of traditional DCT method, DWT method, Zernike moment, and our proposed method to different attack conditions such as white noise state, image rotation state, image scaling state, image sharpening state, high-resolution actual scene, and image cropping state in 100 image tampering detection. The robustness is evaluated by PSNR, SSIM, and JND, and the mean values of different indicators are recorded separately, as shown in Table 3.

Table 3: Robustness testing of methods under different conditions.

Test condition	PSNR				SSIM				JND			
	DCT method	DWTmethod	Zernike quadrature	This paper's method	DCT method	DWTmethod	Zernike quadrature	This paper's method	DCT method	DWTmethod	Zernike quadrature	This paper's method
No attack state	36	34	37	48	0.86	0.85	0.88	0.93	4.9	5.1	4.8	4.1
Enter the white	32	31	34	45	0.81	0.79	0.81	0.92	5.3	5.5	5.1	4.2

noise state												
Image rotation status	33	30	35	44	0.79	0.76	0.78	0.91	5.6	5.9	5.3	4.2
Image zoom status	34	31	33	46	0.78	0.74	0.79	0.92	5.5	6.4	5.2	4.3
Image sharpening status	31	32	33	43	0.81	0.85	0.82	0.91	5.9	6.5	5.6	4.5
High resolution actual scene	39	38	40	51	0.87	0.86	0.89	0.94	4.8	5.2	4.7	4.2
Image cropping status	28	29	30	43	0.76	0.72	0.78	0.90	6.3	6.9	5.5	4.4

According to Table 3, compared with traditional methods, this method has strong resistance and robustness under specific conditions such as introducing white noise, rotation processing, scaling processing, sharpening processing, high-resolution real scenes, and image cropping processing. The robustness index PSNR is higher than 40, which can ensure the visual quality of image watermark information extraction. The SSIM index is higher than 0.9, and the brightness, contrast, and structural similarity of the NROI sub block information in the image watermark are relatively high. The JND index is below 5, indicating a low level of visual distortion and ensuring image quality. However, the robustness indicators of other traditional methods are not ideal and are greatly affected by attacks such as white noise, rotation processing, and scaling processing.

4 Conclusion

In this paper, we propose a tamper detection method in watermarked images using NROI-based circular-harmonic-fourier moments. The results are as follows:

(a) According to the information entropy of the image sub-block in the safe area for the sub-block selection, the internal region of the image is divided into ROI (information entropy value of large texture sub-block) and NROI (information entropy value of smaller smooth sub-block), and the watermark information is embedded in the smooth sub-block, and the image reconstruction is realized by selecting the superposition and summation of the product of low-order circular-harmonic-Fourier moments and circular-harmonic-Fourier function of the same order, and the change of the watermark amplitude is low, the watermark information is still retained in the filtered image, and this method provides a new perspective and means for the image analysis and processing, which helps to capture the image features more accurately.

(b) The circular-harmonic-Fourier low-order moments of each sub-block in the NROI region of the image reconstruction result are used as feature vectors, and Arnold mapping is introduced to complete the binary watermark obfuscation, and the robust transformation coefficients are determined by defining the robust coefficients selection rule, so as to obtain the watermark tampering location. This innovation effectively solves the problem of square effect, and the result of tampering detection is highly consistent with the result of watermark extraction, which improves the accuracy and stability of watermark tampering detection.

(c) The complete watermark sequence is extracted by comparing the amplitude changes of all moments with the threshold value, and the extracted binary watermark sequence is compared with the original watermark stored in the NORI location to analyze whether the image watermark information has been tampered with, and effectively locate the tampered watermark-containing region, which exhibits good anti-interference and robustness, and is able to locate the location of the watermark-containing sub-block which has suffered tampering.

(d) However, the method in this paper only optimizes static images, and the efficiency of watermark detection for video streams or dynamic contents will be reduced. Future research can be combined with optical flow analysis to extend to video watermark detection and maintain the ability of temporal consistency detection.

Funding

Henan Provincial Education Reform Project: Exploration and Practice of the "O2O" Operation and

Management Model of Big Data Empowerment Application-oriented Undergraduate University Entrepreneurship Park (NO. 2024SJGLX1102).

References

[1] Mohammadi, H., Ghaderzadeh, A. & Sheikhahmadi, A. (2024). A new hybrid method for secure data transmission using watermarking based on fuzzy encryption in iot. IETE journal of research, 70(4), 3493-3514. DOI:10.1080/03772063.2023.2198989.

[2] Khaldi, A., Redouane, K. M. & Bilel, M. (2023). A medical image watermarking system based on redundant wavelets for secure transmission in telemedicine applications. Wireless Personal Communications, 132(2), 823-839. DOI:10.1007/s11277-023-10636-5.

[3] Purnima, Ahuja, R. & Gautam, N. (2023). Motion-frames based video watermarking scheme for copyright protection using guided filtering in wavelet domain. Traitement du Signal, 40(1), 187-197. DOI:10.18280/ts.400117.

[4] Hosny, K. M., Magdi, A., Elkomy, O. & M., H. H. (2024). Digital image watermarking using deep learning: a survey. Computer science review, 53(Aug.), 1.1-1.12. DOI ： 10.1016/j.cosrev.2024.100662.

[5] Salama, A. S., Shoitan, R., Abdallah, M. S., Cho, Y. I. & Nagm, A. M. (2023). A robust algorithm for digital image copyright protection and tampering detection: employing dwt, dct, and blowfish techniques. Traitement du Signal, 40(5), 2019-2027. DOI:10.18280/ts.400520.

[6] Mahto, D. K., Singh, O. P. & Singh, A. K. (2024). Fusiw: fusion-based secure rgb image watermarking using hashing. Multimedia tools and applications, 83(22), 61493-61509. DOI:10.1007/s11042-022-13454-2.

[7] Loc, C. V., Viet, T. X., Viet, T. H., Thao, L. H. & Viet, N. H. (2023). Deep learning based-approach for quick response code verification. Applied Intelligence, 53(19), 22700-22714. DOI:10.1007/s10489-023-04712-3.

[8] Prasad, S., Pal, A. K. & Paul, S. (2022). A block-level image tamper detection scheme using modulus function based fragile watermarking. Wireless Personal Communications, 125(3), 2581-2619. DOI:10.1007/s11277-022-09675-1.

[9] Balasamy, K., Krishnaraj, N.& Vijayalakshmi, K. (2022). An adaptive neuro-fuzzy based region selection and authenticating medical image through watermarking for secure communication. Wireless Personal Communications, 122(3), 2817-2837. DOI:10.1007/s11277-021-09031-9.

[10] Gaudencio, A. S., Hilal, M., Cardoso, J. M., Humeau-Heurtier, A. & Vaz, P. G. (2022). Texture analysis using two-dimensional permutation entropy and amplitude-aware permutation entropy. Pattern recognition letters, 159(Jul.), 150-156. DOI: 10.1016/j.patrec.2022.05.017.

[11] Ngo, D. & Kang, B. (2024). A novel pipelined architecture of entropy filter. Journal of Real-Time Image Processing, 21(4), 118.1-118.10. DOI:10.1007/s11554-024-01498-6.

[12] Atallah, A. M., Mahmoud, I. I. & Ali, H. S. (2024). Robust dense-field based copy-move forgery localization using generic radial harmonic fourier moment invariants. Journal of forensic sciences, 69(1), 139-152. DOI:10.1111/1556-4029.15420.

[13] Sebastian B, Duivenvoorden A J, Julien C ,et al. cunuSHT : GPU accelerated spherical harmonic transforms on arbitrary pixelizations[J].RAS Techniques and Instruments, 2024,3(1):711–721.

[14] Dai K, Mao D, Chen Y, et al. Harmonic dichromatic soliton molecules in synchronous mode-locked fiber lasers. Optics & Laser Technology, 2025, 184(000):711-721. DOI: 10.1016/j.optlastec.2025.112527.

[15] Nguyen S C, Ha K H, Nguyen H M. A Robust Image Watermarking Scheme Based on the Laplacian Pyramid Transform. Informatica, 2020, 44(1):75-84. DOI:10.31449/INF.V44I1.2042.

[16] Sharma, S., Zou, J. & Fang, G. (2022). A single watermark-based scheme for both protection and authentication of identities. IET Image Process, 16(12), 3113-3132. DOI:10.1049/ipr2.12542.

[17] Sunitha, K., Krishna, A. N. & Prasad, B. G. (2022). Copy-move tampering detection using keypoint based hybrid feature extraction and improved transformation model. Applied Intelligence, 52(13), 15405-15416. DOI:10.1007/s10489-022-03207-x.

[18] Boumezbeur I, Benoughidene A, Harkat I, et al. BACP-LRS: Blockchain and IPFS-based Land Record System. Acta Informatica Pragensia, 2024, 14(1):42–62. DOI: 10.18267/j.aip.252

[19] Vanini C, Hargreaves C, Breitinger F. Evaluating tamper resistance of digital forensic artifacts during event reconstruction. 2024, 17(12):12814.1-12814.9.

[20] Ma Y, Yang J, Su X, et al. Crack propagation characterization of concrete under non-uniform corrosion of steel strand using digital image correlation. Construction and Building Materials, 2024,455(13):139166.1-139166.15. DOI: 10.1016/j.conbuildmat.2024.139166.