IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 28 August 2023, accepted 21 September 2023, date of publication 27 September 2023, date of current version 3 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3319669

METHODS

A Robust Image Watermarking Scheme Based on Image Normalization and Contourlet Transform

SHAOBAO WU[1], **ZHIHUA WU**[1], **MEIXUAN HUANG**[1], **AND DONGSHENG SHEN**[2]
[1]School of Information and Electronic Engineering, Liming Vocational University, Quanzhou 362000, China
[2]College of Computer, Minnan Normal University, Zhangzhou 363000, China

Corresponding author: Shaobao Wu (shao1987.wu@gmail.com)

This work was supported in part by the Research Project of Liming Vocational University under Grant LMTD202101, and in part by the Fujian Educational Committee under Grant JAT220712.

ABSTRACT It is a challenging work to solve the geometric attack in the field of digital watermarking. In order to solve the synchronization between the host image and the watermark, image normalization is introduced. Firstly, the geometrically invariant space of image is constructed by using image normalization, and a region of interest (ROI) is obtained from the normalized image by utilizing the invariant centroid theory. Then, the contourlet transform is performed on the ROI. Low-pass sub-band coefficients are divided into non-overlapping blocks. Finally, as the energy of the blocks are not the same, an adaptive quantization step is used to embed the binary watermark information on the maximum singular value of the block. The experimental results demonstrate that the watermarked images exhibit high visual quality, and the scheme is effective against common image processing and geometric distortions.

INDEX TERMS Image normalization, region of interest, contourlet transform, adaptive quantization, geometric distortions.

I. INTRODUCTION

Nowadays multimedia data has become an important source for people to obtain information. When people are enjoying the convenience brought by digital technology, the tampering of multimedia data appears. Once tampered data is used in formal occasions, it will bring a huge negative impact on our lives. These digital assets need to be protected. As part of the solution, digital watermarking has made vital contributions to the identification of the authenticity and integrity of digital resources. In real application, digital images containing watermarks may be subject to various attacks, such as compression, cropping, tampering, rotation and scaling, etc., so robust watermarking techniques that can resist related attacks have emerged.

Robust image watermarking is an important branch of digital watermarking research [1]. Various algorithms and methods have been developed for authentication based watermarking, including spatial domain and transform domain techniques. These techniques employ sophisticated algorithms and mathematical models to effectively embed the watermark and robustly extract it in the presence of various attacks. They often utilize digital signal processing, data hiding, and cryptographic principles to ensure the security and reliability of the authentication process. In the early watermarking technologies, most of the watermarking schemes are based on the spatial domain. Least-Significant Bits (LSB) watermarking which develops from steganography [2] is the common spatial watermarking method. It directly modifies the image pixel value by utilizing the redundant characteristics of image pixels and the insensitivity of human eyes to slight pixel changes. As one of the earliest LSB watermarking works, Wang et al [3] investigate a genetic algorithm to hide the data into the rightmost k LSBs of host image. Based on the concept of perceptual modeling, the work has high embedding capability and good invisibility. Bamatraf et al. [4] embed two bits in the third and fourth LSB, the scheme shows more robust than the traditional LSB technique. Chen and Lu [5] make use of the Cb component of the YCbCr color space for LSB modification. In order to resist JPEG

The associate editor coordinating the review of this manuscript and approving it for publication was Yongjie Li.

compression and reduce image distortion, the work introduce quantization and DCT based JND model. Besides the LSB methods, there are some works based on the histogram of image. Coltuc and Bolon used the histogram specification to hide the watermark in the image well without causing obvious visual effects [6]. Ni et al. introduce zero or the minimum points of the image histogram, and embed data into host image by slightly modifying the pixel grayscale value [7]. In addition to a certain robustness, the work has the ability to be reversible and low computational complexity. Xiang et al. [8] take advantage of two statistical features of Gaussian filtered low-frequency component of images (histogram shape and mean), and design a watermarking scheme that can effectively resist cropping and random bending attacks.

Most of spatial-based schemes are fragile to resist image processing attacks, on the contrary, the transform domain watermarking techniques have large watermark capacity and strong robustness. Barni et al. [9] embed watermark information into DCT transform domain coefficients. For invisibility, the watermark is adapted to the image base on the human visual system. The work is robust to some image processing techniques. On the basis of this, researchers have proposed a number of digital image robust watermarking schemes based on DCT transform. In addition to using DCT transform, the transform methods used for robust digital image watermarking include Discrete Fourier Transform (DFT), Fourier Merlin Transform (FMT), Discrete Wavelet Transform (DWT), Hadamard Transform (HT), Singular Value Decomposition (SVD) and so on. In general, the effect of relying on a single transformation scheme is not as effective as using multiple transformation methods. Therefore, The transform domain schemes always use combined transform methods, such as DCT and DWT, DWT and SVD, etc. Deb et al. [10] describe a robust and imperceptible watermarking scheme which combined DWT-DCT technique. The work embeds watermark bits into DCT coefficients of DWT sub-band. The weighted correction is introduced for image visual quality. A color image watermarking algorithm based on DWT-SVD is proposed by Yin et al. [11]. The green component of color image is decomposed at Nth levels with DWT. SVD is performed on the scrambled watermarking and the wavelet coefficients for embedding course. A multiple watermarking algorithm based on DWT, DCT and SVD is proposed for medical applications [12]. Hasan et al. [13] introduce an encryption-based image watermarking scheme combining 2DWT and DCT. The method achieves robustness against various attacks and maintains high imperceptibility by using the same random bit sequence as the watermark and seed for embedding zone coefficients. A watermarking approach [14] using DWT-DCT-SVD and LWT-DCT-SVD, in which the image is divided into sub-bands via multilevel DWT or LWT. DWT provides high/low-frequency bands, LWT employs smaller structures for faster processing. DCT is applied to sub-bands, followed by SVD. In [15], the sender side applies DWT to the cover image, performing eigendecomposition on HH components, and repeats for the watermark image. Matrices combine into a watermarked image via iDWT. Diagonal component transmits securely. At the receiver, the watermark image is recovered from the watermarked image and original image's diagonal.

The table 1 highligt the pros and cons associated with different domain watermarking methods.

TABLE 1. pros and cons of different watermarking methods.

Watermarking Approach	Pros	Cons
Spatial Domain[3-8]	Simple implementation	Susceptible to geometric and signal processing attacks
	No additional transformation required	Limited embedding capacity
Transform Domain[9-15]	Robust against geometric attacks	Additional computational complexity
	Can achieve higher embedding capacity	Vulnerable to certain signal modifications

The above-mentioned watermarking algorithms can resist the common image processing attacks, but they have poor abilities of resisting geometric attacks. As geometric attacks are easy to destroy the synchronization of watermark and image, the watermark which is embedded into host image can not be correctly extracted. Therefore, it is a challenging work to design watermarking algorithms against geometric attacks. The image normalization [16] is a widely used technique in the fields of computer vision and pattern recognition. The so-called image normalization, through a series of transformations, the original image will be processed to the only standard form. Because the standard form is not changed for image translation, rotation, scaling, this makes the development of resistance to geometric attacks image watermarking algorithm is possible.

In this paper, an authentication based watermarking scheme that aims to provide a robust and imperceptible solution for verifying the authenticity and integrity of digital images is proposed, in which the image normalization and contourlet transform are utilized. Firstly, the image normalization is performed on the image. The region of interest (ROI) into which the watermark will embed is obtained from the normalized image by use of invariant centroid theory. Then, the Contourlet transform is applied for ROI. According to the energy of the blocks of low-pass sub-band coefficients are not the same, an adaptive quantization step is used to embed the binary watermark information on the maximum singular value of the block.

The rest of the paper is organized as follows. Related works about image normalization and contourlet transform are described in Section II. Section III is the process of watermarking embedding and decoding, including watermark information preprocessing, watermark embedding, adaptive quantization method, watermark extraction, etc. Section IV are results of simulation which show the invisibility and robustness of our scheme. Finally, conclusions are given in Section V.

II. THEORETICAL BACKGROUND

A. IMAGE NORMALIZATION AND DETERMINE THE ROI

In order to obtain the standard form, it is necessary to compute the geometric moments of the image. Define the Cartesian moment m_{pq}, and central moment μ_{pq} of image $f(x, y)$ of size $M \times N$ as:

$$m_{pq} = \sum_{x=1}^{M} \sum_{y=1}^{N} x^p y^q f(x, y)$$

and

$$\mu_{pq} = \sum_{x=1}^{M} \sum_{y=1}^{N} (x - \bar{x})^p (y - \bar{y})^q f(x, y)$$

where $\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}}$, and $(\bar{x}, \bar{y})$ is the centriod of the image.

Based on the above geometric moments and some matrix operations, the procedure of normalizing an image includes four steps:

a) Re-center the image. In order to eliminate the influence of translation transformation on the original image, the coordinates of the original image are centered according to (1):

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} d_1 \\ d_2 \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - d \tag{1}$$

where $d = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$, $d_1 = \bar{x}$, $d_2 = \bar{y}$. The re-centered image is represented as $f_1(x_1, y_1)$.

b) X-shearing normalization. According to (2), the image $f_1(x_1, y_1)$ after coordinate centering is subjected to x-shearing normalization processing.

$$\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \tag{2}$$

where $\beta = -\frac{\mu_{11}^{(1)}}{\mu_{02}^{(1)}}$, $\mu_{pq}^{(1)}$ is the central moment of the centered image $f_1(x_1, y_1)$. $f_2(x_2, y_2)$ represents the x-shearing normalized image.

c) Scaling normalization. The x-shearing normalized image $f_2(x_2, y_2)$ is transformed according to formula (3).

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} \tag{3}$$

where $\alpha = \pm\sqrt{\frac{1}{\mu_{20}^{(2)}}}$, $\delta = \pm\sqrt{\frac{1}{\mu_{02}^{(2)}}}$. $\mu_{pq}^{(2)}$ is the central moment of the x-shearing normalized image $f_2(x_2, y_2)$. Its sign depends on constraints $\mu_{50}^{(3)} > 0$ and $\mu_{05}^{(3)} > 0$ ($\mu_{pq}^{(3)}$ is the central moment of the scaled normalized image $f_3(x_3, y_3)$).

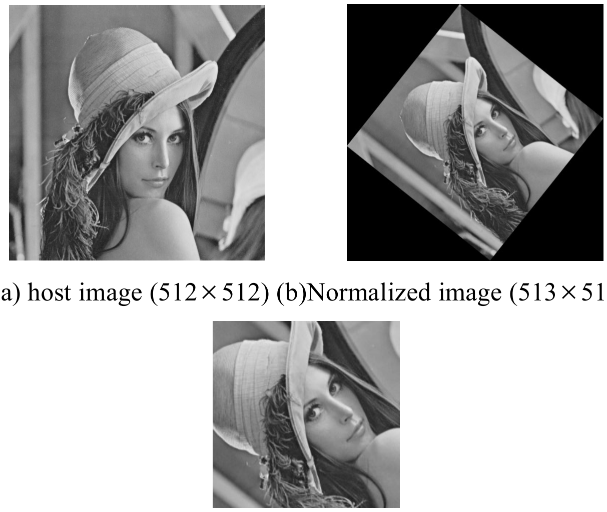
d) Rotation normalization. The scaled normalized image $f_3(x_3, y_3)$ is transformed according to formula (4).

$$\begin{pmatrix} x_4 \\ y_4 \end{pmatrix} = \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix} \cdot \begin{pmatrix} x_3 \\ y_3 \end{pmatrix} \tag{4}$$

where $\psi = \arctan\left(-\frac{\mu_{30}^{(3)}+\mu_{12}^{(3)}}{\mu_{03}^{(3)}+\mu_{21}^{(3)}}\right)$, $\mu_{pq}^{(3)}$ is the central moment of the scaled normalized image $f_3(x_3, y_3)$. $f_4(x_4, y_4)$ is the result of the rotation normalization of $f_3(x_3, y_3)$.

After these four steps, the standard position of the image $f_4(x_4, y_4)$ is obtained. It is invariant to affine transformations (including translation, rotation, flipping, scaling, etc.). Fig 1.(a) is the original Lena image, Fig 1.(b) is the normalized image. Due to the redundancies of normalized image (the black part as show in the Fig 1.(b)), the inverse normalized image yield to the information loss. Therefore, our proposed work introduce the regional invariant centroid theory, and extract regions of interest which is used for watermark embedding from the normalized image.

The invariant centroid C_c can be computed as follows: (1)The centroid (x_0, y_0) of the entire normalized image $I(x, y)$ is first computed as $x_0 = \bar{x} = m_{10}/m_{00}$ and $y_0 = \bar{y} = m_{01}/m_{00}$. (2)A circular region of radius r and centered at (x_0, y_0) is extracted from the image $I(x, y)$ and a new centroid point (x_1, y_1) is computed. (3)A circular region of the same radius but now centered on (x_1, y_1) is extracted from the image $I(x, y)$ and a new centroid point (x_2, y_2) is again computed. (4)Terminate the procedure if convergence to a unique point C_c with co-ordinates (x_c, y_c) is obtained, otherwise let $x_1 = x_2$ and $y_1 = y_2$ and repeat (3).



(a) host image (512×512) (b)Normalized image (513×512)

(c)ROI (256×256)

FIGURE 1. Image normalization and determine the ROI.

Then, select a $S_1 \times S_2$ rectangular area around the centroid (x_c, y_c) in the normalized image as the ROI (Fig 1.(c))which will embed watermark information.

B. CONTOURLET TRANSFORM

Do and Vetterli have proposed the contourlet transform in [17], it is a new high-dimensional signal singularity analysis tools. As the wavelet transform applied to two-dimensional image information, can not be optimally expressed the singularity curve, and the image can only be decomposed into horizontal direction, vertical and diagonal directions by the wavelet transform, which is unable to embody the anisotropic characteristics of the image and effectively capture the image contour information. Therefore, wavelet analysis is not the best or most sparse function representation, whereas contourlet transform not only has good directionality and anisotropy, but also to efficiently capture the image geometric structure.

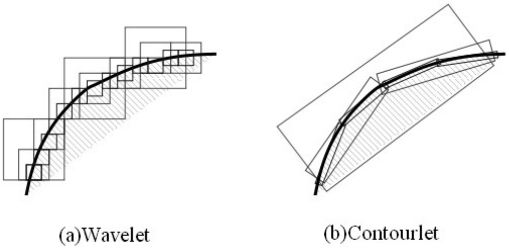


FIGURE 2. **(a) The representation of curve by wavelet,(b) the representation of curve by contourlet.**

The decomposition process of the Contoutlet transformation can be divided into two steps: First, the image is decomposed at multi-resolution by Laplacian Pyramid Filters, and each layer of transformation will obtain a low-frequency image and a difference image. Secondly, the directional filter is used to combine singular points distributed in the same direction into one coefficient, and each layer decomposes the frequency domain into 2^{n} directional sub-bands (n is the number of decomposed layers). Figure 3 shows the sub-bands of each direction of the image Pepper after the Contourlet transformation.

C. SINGULAR VALUE DECOMPOSITION THEORY

For any image, its singular values can be used to describe its internal features. Since the singular values show good stability, when there is a certain degree of interference in the image, the singular values can still maintain a good stable feature. According to this feature, by SVD processing the image, the matrix can be diagonalized to obtain the singular value of the image, and then add a watermark on it. At this time, even if there is an external attack, the watermark can still be restored well. In addition, the singular value represents the brightness information, and the addition of watermark will not affect the subjective effect and geometric properties of the image. SVD is described in detail as follows:

Let A be an image of size $N \times M$, and the singular value decomposition is:

$$A = USV^T \tag{5}$$

where $A \in R^{N\times M}$, $U \in R^{N\times N}$, $S \in R^{N\times M}$, $V^T \in R^{M\times M}$, U and V are left and right singular matrices, and they are both orthogonal matrices. Matrix $S = diag(\sigma_1, \sigma_2, \ldots, \sigma_r)$, where $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r > 0$, r is the rank of A, $\sigma_i(i = 1, \ldots, r)$ is the singular value of matrix A. The watermark is often embedded in the singular value of image to resist various attacks to the watermarked image.

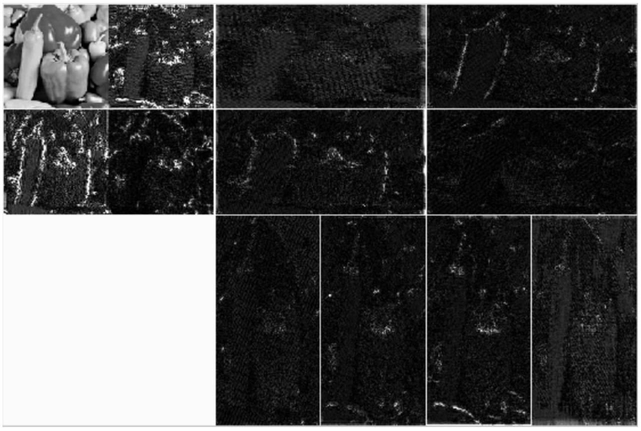


FIGURE 3. **Contourlet transform of Pepper (decomposition level 3).**

III. IMPLEMENTATION OF THE WORK

In this paper, the image is first normalized, then ROI is determined by using the invariant centroid, and Contourlet transform is performed on the ROI for extracting the low-frequency sub-bands. The low-frequency sub-bands are subjected to 4×4 block SVD. Scrambled watermark information is adaptively embedded into the largest singular value of the block, and the image includes the watermark information is obtained by inverse Contourlet transform. Finally, a watermarked image is obtained. The process is shown in Figure 4.

A. PREPROCESSING OF WATERMARK BITS

In order to improve the robustness of the algorithm and the security of embedded watermark information, Arnold Cat Map is selected to scramble the watermark information to realize the image preprocessing step. In the Arnold transform, the position of each pixel is shuffled by iterating over the pixels of the image. At the same time, the number of scrambled images can be used as the secondary key of the watermarking system, and can also reduce the storage space during remote transmission. Therefore, using Arnold transform to scramble the watermark and eliminate the spatial correlation of pixels can make the original image into an image that is not sensitive to white noise, so as to realize the hiding of watermark information. Although the attacker can extract the watermark, without the specific information of the Arnold transform algorithm, the original watermark information cannot be recovered, so the Arnold transform improves the security of the watermark information and the robustness of the scheme. The Arnold transform is defined as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N \tag{6}$$

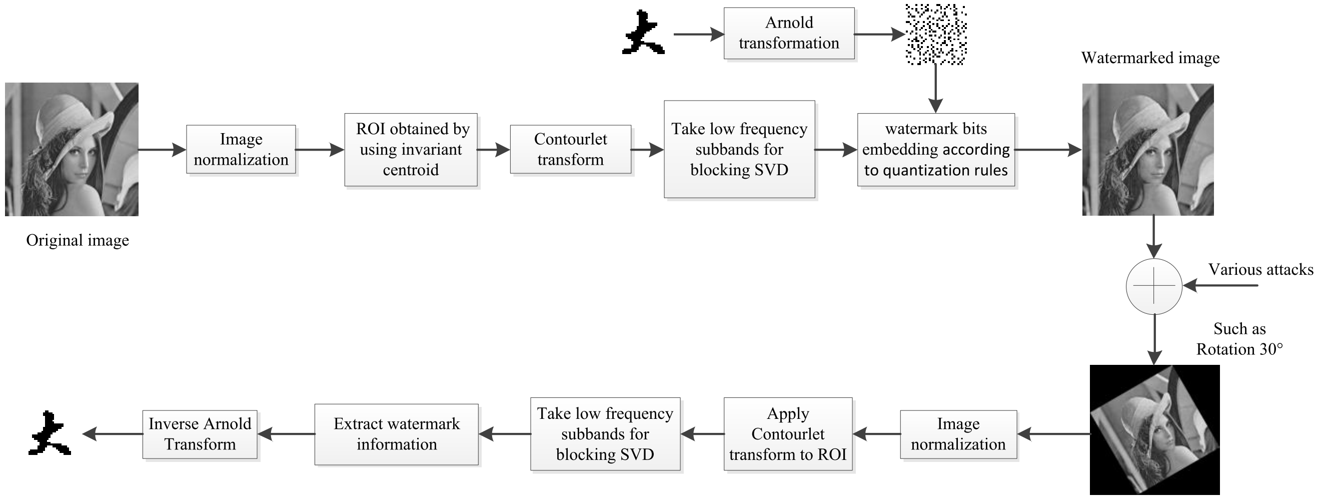

Arnold transformation
Watermarked image
Original image
Image normalization
ROI obtained by using invariant centroid
Contourlet transform
Take low frequency subbands for blocking SVD
watermark bits embedding according to quantization rules
Various attacks
Such as Rotation 30°
Inverse Arnold Transform
Extract watermark information
Take low frequency subbands for blocking SVD
Apply Contourlet transform to ROI
Image normalization

FIGURE 4. **Overview of the proposed scheme.**

where (x', y') is the pixel coordinates of the watermark image after n iterations, a, b, c, d are positive integers.

N is the watermark image width or height. Since the Arnold transformation is periodic, if the position (x', y') is transformed for T iterations, it returns to the original position. T is the transformation period, that is, the number of iterations, which depends on the parameters a, b, c, d. When these values change, the correlation between pixels will also change, so these parameters can be used as key.

B. WATERMARK EMBEDDING

The pseudocode representation of the watermark embedding steps as follows:

Algorithm 1 The Watermark Embeding Steps

```
Input: Host image and Binary watermark image
Output: watermarked_image
  Step 1: Perform Arnold transformation on the watermark image;
  Step 2: Normalize the host image and extract regions of interest (ROI); Apply one-scale contourlet transform to ROI and select low-frequency subband;
  Step 3: Divide low-frequency coefficients into non-overlapping blocks (block_size is $4 \times 4$); Quantization step based on block energy and embedding of watermark information
for block in blocks:
      CalculateQuantizationStep(block)
      singular_values=embedding_strength* watermark_bits
  Step 4: Obtain new low-frequency contourlet coefficients with embedded watermark
  Step 5: Inverse contourlet transform and obtain new normalized image
  Step 6: Apply pre-distortion compensation strategy [18] to obtain watermarked image
```

C. RULES OF QUANTIZATION

1) SELECTION OF QUANTIZATION STEP

In this paper, the quantization step is adaptively selected according to the different energy of the low-frequency subband blocks. Taking the low-frequency region in the contourlet domain as an example, the i-th block adaptive quantization step size is:

$$\Delta = \log_2(E_{blk} \times 1000)/1000 + \Delta_0,$$

$$E_{blk} = \sum_{p=1}^{4}\sum_{q=1}^{4} \{LL(i)_{pq}\}^2/16$$

where Δ_0 is the basic quantization step size, and $LL(i)_{pq}$ is the coefficient of the low frequency region in the Contourlet domain.

2) RULES OF QUANTIZATION

Watermark information is embedded according to the following rules to the image:

$$Z = mod(round(S(1,1)/\Delta), 2),$$

$$\begin{cases} S(1,1)' = round(S(1,1)/\Delta) \times \Delta + \Delta/2 & if\ Z = W(i,j) \\ S(1,1)' = round(S(1,1)/\Delta) \times \Delta - \Delta/2 & if\ Z \neq W(i,j) \end{cases}$$

where mod $(\bullet, 2)$ is modulus 2 arithmetic, $round(\bullet)$ is rounding operation, Δ is the block quantization step, $S(1, 1)$ is the largest singular value of block, $S(1, 1)'$ is the new largest singular value which is embedded watermark. Substitute $S(1, 1)'$ for $S(1, 1)$ and multiply with the respective U and V^T of each block to obtain the low-frequency coefficients of the watermark information of each block $U \times S(1, 1)' \times V^T \rightarrow LLw(i)$.

D. WATERMARK EXTRACTION

The pseudocode representation of the watermark extraction steps as follows:

Algorithm 2 The Watermark Extraction Steps

```
Input: watermarked_image
Output: final_watermark
    Step 1: Perform normalization and extract ROI using invariant centroid theory
    Step 2: Apply one-scale contourlet transform to ROI and select low-frequency coefficients
    Step 3: Divide low-frequency contourlet coefficients into non-overlapping blocks;
for block in blocks:
    ExtractWatermarkBit(largest_singular_value)
    Step 4: Perform anti-scrambling on the extracted watermark bits
```

According to the parity of largest singular value $S(1, 1)'$, combining with the block quantization step, extract the watermark information $W1$ as follows:

$$Z' = ceil(S(1, 1)'/\Delta),$$

$$W1 = \begin{cases} 0 & if\ \ mod(Z', 2) = 1 \\ 1 & else\ mod(Z', 2) = 0 \end{cases}$$

E. COMPUTING COMPLEXITY

Table 2 shows the time complexity of watermark embedding and extraction process. The size of the host image in discussion is n=m×m, and the size of the watermark image is w=k×k.

TABLE 2. Time complexity of our scheme.

Step	Operation	Embedding	Extraction
1	Arnold transformation	O(w)	O(w)
2	Normalize	O(1)	O(1)
3	Contourlet Transform	O(n)	O(n)
4	Watermark embedding/extraction	O(w)	O(w)
5	Inverse Contourlet Transform	O(n)	-
	Total	O(w)+O(n)+ O(1)	O(w)+O(n)+ O(1)

IV. RESULTS OF EXPERIMENT

The experiment is under MATLAB 2010a environment, all the host images are 512 × 512 bit images which seclect from USC-SIPI image database, the size of the watermark and ROI are 32×32 and 256×256 respectively. The basic quantization step Δ_0 is set to 48. Both the LP filter and the DFB filter in the Contourlet transform select the "pkva" filter.

Peak Signal to Noise Ratio (PSNR) is a metric for evaluating image quality. It is used to measure the difference between two images, such as a watermarked image and the original image. The larger the PSNR, the less image distortion.The definition is as follows:

$$PSNR = 10\lg \frac{M * N * 255^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I'_\phi(i,j) - I_\phi(i,j)\right]^2}$$

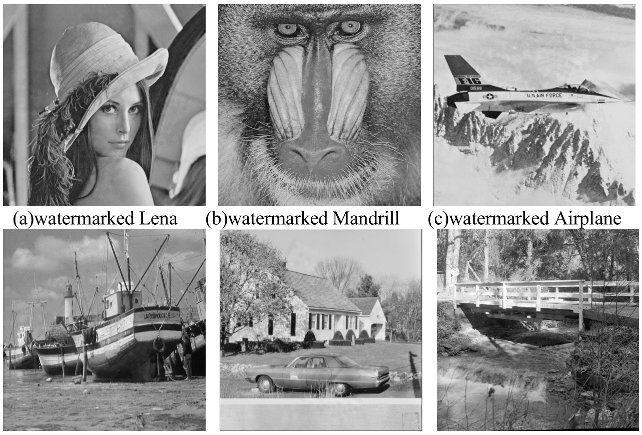
Among them, $I_\phi(i,j)$ is the original images, $I'_\phi(i,j)$ is the watermarked image,and the size of image is $M \times N$. The normalized correlation (NC) is mainly to evaluate the similarity between the extracted watermark and the original watermark. If the NC value is high, it indicates that the similarity between the two watermarks is high, and it can also reflect that the scheme is more robust and less susceptible to attacks. The definition is as follows:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(s,t)\cdot W'(s,t)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W^2(s,t)}\cdot\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W'^2(s,t)}}$$

Among them, $W(s, t)$ is the original watermark, $W'(s, t)$ is the extracted watermark, and the watermark size is $M \times N$.

A. INVISIBILITY TEST

As shown in Fig. 5(a) - (f) are the watermarked images obtained by using our method. From the Fig. 6, the PSNRs of the proposed scheme are above 40.00 dB for the different images. It can be observed that the our scheme has high transparency. That is, the watermarked image has less distortion after host image is embedded with watermark information.


(a)watermarked Lena (b)watermarked Mandrill (c)watermarked Airplane

(d)watermarked Fishingboat (e)watermarked House (f)watermarked Bridge

FIGURE 5. The watermarked images.

B. ROBUSTNESS TEST

In order to test the robustness of our scheme, various attacks are performed on the watermarked image. It can be seen from Table 3 and Table 4, the proposed scheme against JPEG compression and image rotation has good results. In addition, the NC values extracted from watermarked images after various attacks are given in this part. The test image and watermark

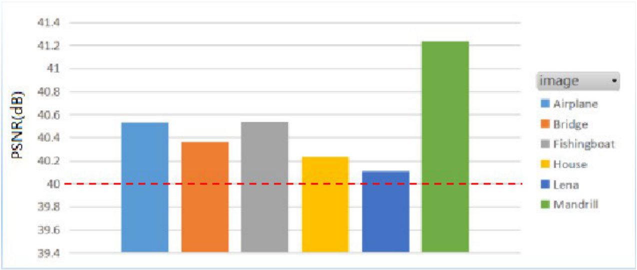
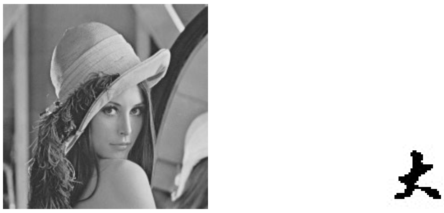


FIGURE 6. PSNRs of different watermarked images.

image as shown in Fig.7, we take Lena as host image, and chinese character as watermark.



(a)host image (b) binary watermark image

FIGURE 7. The test image and watermark image.

TABLE 3. Extract the watermarks against JPEG compression.

Quality	90	70	50	30	10
Extracted watermark					
NC	0.9699	0.9811	0.9525	0.8484	0.8376

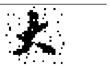
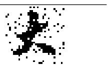
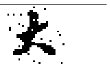
TABLE 4. Extract the watermarks against image rotation.

Rotation	10°	30°	50°	70°	90°
Extracted watermark					
NC	0.9281	0.8252	0.8993	0.8760	0.8605

The remark of table 5 (Change ratio of length and width: the watermarked image 2 times magnification along the y direction, the x direction remain unchanged. Scaling:the watermarked image is reduced by half and then 2 times magnification. Salt & Pepper noise: the noise density is 0.01. Gaussian noise: zero mean with 0.005 variance. Affine transformation: the template is [1 0 0;0.5 1 0; 0 0 1]).

From the table 5, we can see that our scheme has high NC values under different attacks with different size of watermark. It is robust to common image processing attacks, especially, it is also effective for geometric attacks such as affine transformation.

TABLE 5. The NC values under other attacks.

Attack type	Size of watermark	NC	Extracted watermark
No attack	32×32	1.0000	
	16×16	1.0000	
Change ratio of length and width	32×32	0.8530	
	16×16	0.9064	
Scaling	32×32	0.9693	
	16×16	0.9974	
Flip left-right	32×32	0.8357	
	16×16	0.8599	
Salt & Pepper noise	32×32	0.9537	
	16×16	0.9570	
Gaussian noise	32×32	0.9442	
	16×16	0.9706	
Affine transformation	32×32	0.9555	
	16×16	0.9705	
3×3 Gaussian filter	32×32	0.9842	
	16×16	0.9920	
3×3 Average filter	32×32	0.8171	
	16×16	0.8950	
7×7 Wiener filter	32×32	0.8113	
	16×16	0.9947	

C. COMPARISON WITH OTHER METHODS

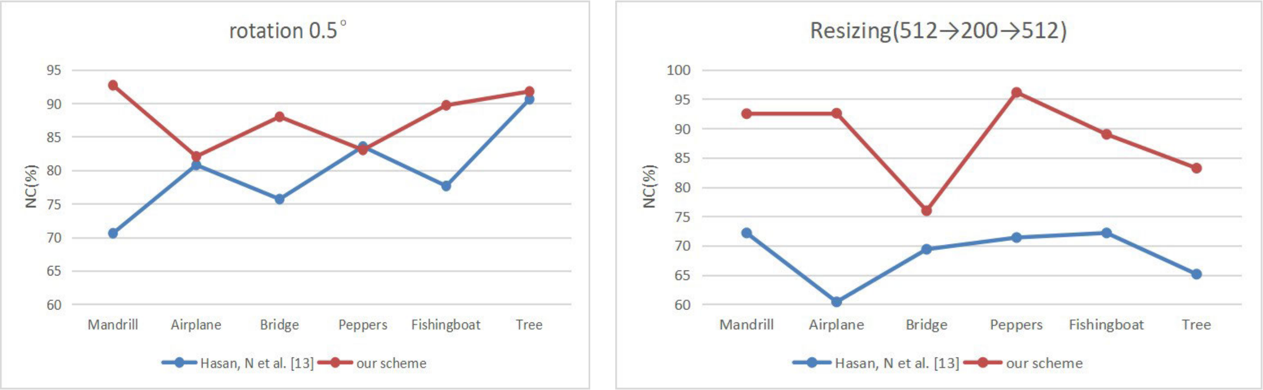
To assess the watermark's perceptual quality, Table 6 presents a comparative analysis of several watermarking algorithms based on their average PSNR values. According to our method, the average PSNR value obtained is higher than the existing methods. As can be seen from Table 7, the method exhibits robustness against common image attacks. In Fig. 8, the experiments are designed to scrutinize the resilience of the method against the geometric distortions. (a) represents a rotation attack, while (b) represents a resizing attack. Both

TABLE 6. Comparison of average PSNR (dB) values of the proposed with existing schemes.

Escalante-Ramírez B et al. [19]	Abdulrahman, A.K. et al. [20]	Lang, J et al. [21]	Hu, H.-T et al. [22]	Guo, J et al. [23]	Our scheme
39.8981	37.0035	40.021	40.48	40.321	**40.5020**

TABLE 7. Comparison of NC (%) values for common image attacks.

Attack	Ferda et al. [24]	Feng et al. [25]	Jiang et al. [26]	Mardolkar et al. [27]	Our scheme
JPEG compression 20	49.80	69.80	50.88	59.37	**83.39**
JPEG compression 30	71.97	78.40			**84.84**
JPEG compression 40	83.50	89.20	76.95	69.85	**90.94**
Gaussian noise(0.01)	**99.06**	87.50	70.41	68.26	86.27
Salt and Pepper(0.01)	**99.17**		79.98	81.74	95.93
Median Filter(3×3)	99.01	97.10			**99.52**



(a)rotation attack

(b)resizing attack

FIGURE 8. Comparison of NC (%) values for geometric image attacks.

our method and the approach in reference [13] have been compared against these two types of geometric attacks. From the results, it is evident that our method indeed exhibits outperformance in countering geometric attacks. The method exhibits a balance between maintaining watermark invisibility and countering geometric manipulations.

V. CONCLUSION

In this paper, we have presented a watermark algorithm based on image normalization and the contourlet transform. Our proposed algorithm addresses the synchronization problem of watermark information through the introduction of image normalization. Additionally, to enhance the invisibility of the watermark, we have incorporated adaptive quantization steps during the watermark embedding process. The experimental results have demonstrated the effectiveness of our scheme in terms of its robustness and invisibility. Specifically, our algorithm exhibits resilience against image compression attacks and geometric attacks. Future research directions we will focus on exploring advanced techniques that consider color correlations and spatial dependencies to further enhance the performance of our algorithm.

REFERENCES

[1] W. Wan, J. Wang, Y. Zhang, J. Li, H. Yu, and J. Sun, "A comprehensive survey on robust image watermarking," *Neurocomputing*, vol. 488, pp. 226–247, Jun. 2022.

[2] C.-C. Chang, J.-Y. Hsiao, and C.-S. Chan, "Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy," *Pattern Recognit.*, vol. 36, no. 7, pp. 1583–1595, Jul. 2003.

[3] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm," *Pattern Recognit.*, vol. 34, no. 3, pp. 671–683, Mar. 2001.

[4] A. Bamatraf, R. Ibrahim, and Mohd. N. B. M. Salleh, "Digital watermarking algorithm using LSB," in *Proc. Int. Conf. Comput. Appl. Ind. Electron.*, Dec. 2010, pp. 155–159.

[5] T. Chen and H. Lu, "Robust spatial LSB watermarking of color images against JPEG compression," in *Proc. IEEE 5th Int. Conf. Adv. Comput. Intell. (ICACI)*, Oct. 2012, pp. 872–875.

[6] D. Coltuc and P. Bolon, "Robust watermarking by histogram specification," in *Proc. Int. Conf. Image Process.*, 1999, pp. 236–239.

[7] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar. 2006.

[8] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 6, pp. 777–790, May 2008.

[9] M. Barni, F. Bartolini, V. Cappellini, and A. Piva, "A DCT-domain system for robust image watermarking," *Signal Process.*, vol. 66, no. 3, pp. 357–372, May 1998.

[10] K. Deb, Md. S. Al-Seraj, Md. M. Hoque, and Md. I. H. Sarkar, "Combined DWT-DCT based digital image watermarking technique for copyright protection," in *Proc. 7th Int. Conf. Electr. Comput. Eng.*, Dec. 2012, pp. 458–461.

[11] C.-Q. Yin, L. Li, A.-Q. Lv, and L. Qu, "Color image watermarking algorithm based on DWT-SVD," in *Proc. IEEE Int. Conf. Autom. Logistics*, Aug. 2007, pp. 2607–2611.

[12] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools Appl.*, vol. 77, no. 4, pp. 4863–4882, Feb. 2018.

[13] N. Hasan, M. S. Islam, W. Chen, M. A. Kabir, and S. Al-Ahmadi, "Encryption based image watermarking algorithm in 2DWT-DCT domains," *Sensors*, vol. 21, pp. 5540–5569, Aug. 2021, doi: 10.3390/s21165540.

[14] D. Awasthi and V. K. Srivastava, "LWT-DCT-SVD and DWT-DCT-SVD based watermarking schemes with their performance enhancement using Jaya and particle swarm optimization and comparison of results under various attacks," *Multimedia Tools Appl.*, vol. 81, no. 18, pp. 25075–25099, Jul. 2022.

[15] S. E. Naffouti, A. Kricha, and A. Sakly, "A sophisticated and provably grayscale image watermarking system using DWT-SVD domain," *Vis. Comput.*, vol. 39, no. 9, pp. 4227–4247, Sep. 2023.

[16] J. Wood, "Invariant pattern recognition: A review," *Pattern Recognit.*, vol. 29, no. 1, pp. 1–17, Jan. 1996.

[17] M. N. Do and M. Vetterli, "The contourlet transform: An efficient directional multiresolution image representation," *IEEE Trans. Image Process.*, vol. 14, no. 12, pp. 2091–2106, Dec. 2005.

[18] W. X. Yang, Z. D. Dan, and Y. H. Ying, "Image normalization based robust digital watermarking scheme in contourlet domain," *J. Chin. Comput. Syst.*, vol. 30, no. 11, pp. 2272–2276, 2009.

[19] B. Escalante-Ramírez and S. L. Gomez-Coronel, "A perceptive approach to digital image watermarking using a brightness model and the Hermite transform," *Math. Problems Eng.*, vol. 2018, pp. 1–19, Jan. 2018, doi: 10.1155/2018/5463632.

[20] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 17027–17049, Jun. 2019.

[21] J. Lang and Z.-G. Zhang, "Blind digital watermarking method in the fractional Fourier transform domain," *Opt. Lasers Eng.*, vol. 53, pp. 112–121, Feb. 2014.

[22] H.-T. Hu, J.-R. Chang, and L.-Y. Hsu, "Robust blind image watermarking by modulating the mean of partly sign-altered DCT coefficients guided by human visual perception," *AEU-Int. J. Electron. Commun.*, vol. 70, no. 10, pp. 1374–1381, Oct. 2016.

[23] J. Guo, P. Zheng, and J. Huang, "Secure watermarking scheme against watermark attacks in the encrypted domain," *J. Vis. Commun. Image Represent.*, vol. 30, pp. 125–135, Jul. 2015.

[24] F. Ernawan and M. N. Kabir, "A robust image watermarking technique with an optimal DCT-psychovisual threshold," *IEEE Access*, vol. 6, pp. 20464–20480, 2018, doi: 10.1109/ACCESS.2018.2819424.

[25] L. P. Feng, L. B. Zheng, and P. Cao, "A DWT-DCT based blind watermarking algorithm for copyright protection," in *Proc. 3rd Int. Conf. Comput. Sci. Inf. Technol.*, Chengdu, China, vol. 7, Jul. 2010, pp. 455–458.

[26] Y. Jiang, Y. Zhang, W. Pei, and K. Wang, "Adaptive spread transform QIM watermarking algorithm based on improved perceptual models," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 8, pp. 690–696, Aug. 2013.

[27] S. B. Mardolkar and N. Shenvi, "A blind digital watermarking algorithm based on DWT-DCT transformation," *Int. J. Innov. Res. Elect., Electron., Instrum. Control Eng.*, vol. 4, no. 2, pp. 212–216, Apr. 2016, doi: 10.17148/IJIREEICE/NCAEE.2016.42.

SHAOBAO WU received the M.Sc. degree from Minnan Normal University, Zhangzhou, China, in 2013. He is currently a Lecturer with the School of Information and Electronic Engineering, Liming Vocational University. His research interests include image forensic, digital image watermarking, and steganography.

ZHIHUA WU received the B.S. and M.S. degrees in manage information system and electronic communication engineering from Huaqiao University, Quanzhou, China, in 1998 and 2010, respectively. He is currently a Professor with the School of Electronic Information Engineering, Liming Vocational University. His research interests include cyber security, digital image processing, and network communication technology.

MEIXUAN HUANG received the B.S. degree in educational technology from Fujian Normal University, in 2005, and the M.S. degree in computer science and technology from Huaqiao University, in 2010. She is currently an Associate Professor with the School of Information and Electronic Engineering, Liming Vocational University. Her research interests include digital image processing and network communication technology.

DONGSHENG SHEN received the B.S. and M.S. degrees from Fujian Normal University, Fuzhou, China, in 1987 and 1993, respectively. He is currently an Associate Professor with the College of Computer and the Deputy Director of the Information and Network Center, Minnan Normal University. His research interests include multimedia security, image processing, and data mining.