International Journal of Innovative
Computing, Information and Control
Volume **16**, Number **1**, February **2020**

ICIC International ©2020 ISSN 1349-4198
pp. **367–384**

THE DIGITAL IMAGE WATERMARKING SCHEME USING LOW FREQUENCY CONSTRUCTION AND HISTOGRAM

Hang-Yu Fan[1], Zhe-Ming Lu[1,*] and Yongliang Liu[2]

[1]School of Aeronautics and Astronautics
Zhejiang University
No. 38, Zheda Road, Hangzhou 310027, P. R. China
*Corresponding author: zheminglu@zju.edu.cn

[2]Alibaba Group
No. 969, West Wen Yi Road, Hangzhou 311121, P. R. China
yongliang.lyl@alibaba-inc.com

Received June 2019; revised October 2019

Abstract. *In order to protect the copyright authority of important digital images, the non-blind watermarking scheme is allowed. In this paper, we propose a histogram based non-blind watermarking scheme with high robustness. We consider constructing or enhancing the feature of low frequency in the carrier image when embedding the watermark by modifying the value of pixels according to the histogram. In the traditional histogram based watermarking scheme, the selection of modified pixels often adopts the random selection method, which will cause the noise texture in the image. The traditional transform domain based watermarking scheme will also generate objectionable texture features in the carrier image. By calculating the weights of pixels at different positions, we choose the most suitable pixel to modify. The modified pixel will be equal or close to the surrounding pixels after the modifying. The region with equal or close pixel values can form a feature of low frequency. And the feature of low frequency is very robust to many attacks. Experiments show that the proposed method can effectively deal with compression, scaling, and noise attacks, and can resist rotation attacks in a certain extent.*

Keywords: Image watermarking, Robust watermarking, Histogram, Low frequency construction

1. **Introduction.** With the rapid development of the Internet, the speed of information dissemination is far faster than any previous period. As a common information carrier, the digital image is widely used in the digital information age [25]. For the digital images, they are very easy to be spread, copied, or falsified. Although researchers have proposed digital image watermarking technology, there are still many problems such as copyright attribution and anti-counterfeiting for digital images in practical using.

We are in a period of mobile Internet. The images are often compressed and scaled when they are transported in the mobile application. Compression and scaling facilitate the fast propagation of information, but they are serious attacks on digital images and watermarks in them. Most hidden information cannot preserve under high-intensity compression and scaling attacks. Because such attacks are real common in the daily life, if the problems caused by such attacks cannot be solved in time, the copyright protection of images will be greatly damaged. Thus, our scheme is proposed under this situation.

In the digital image watermarking technology, users embed some identification information into the digital image without affecting the use of the image. Digital image watermarking is an effective way to protect digital image about security, and it is also

DOI: 10.24507/ijicic.16.01.367

very useful for anti-counterfeiting traceability and copyright protection. From the point of view, there are visible and invisible digital watermarking. The invisible digital watermarking is not easy to be perceived by the naked eyes, and the utility is more extensive [1-4], so, in this paper, we mainly discuss the invisible watermark.

Today, there are many robust digital watermarking schemes. After consulting the relevant papers, we find that there are three main thoughts about robust watermarking: 1) embedding the information in the middle and low frequency coefficients in the transform domain [7-14]; 2) embedding the information uses the method of hybrid of the singular value decomposition (SVD) and transform domain [15-18]; 3) the embedding based on the statistics in the spatial domain, such as histogram embedding [19-22].

According to the perspectives of Cox and Huang [5,6], the most intuitive and simplest thought is to embed watermark into low frequency coefficients or DC components in the transform domain. Under the guidance of their thought, most anti-compressed image watermarking methods embed the watermark in the low frequency or DC component in the transform domain. In order to improve the robustness of these methods, it is necessary to increase the degree of modification, but it will cause the pixels in spatial domains change too much. When the embedding strength is increased, the peak signal-to-noise ratio (PSNR) of the images before and after embedding will be reduced, and a disgusting perception will be left on the carrier image, which can be shown in Figure 1.

(a) The original carrier image (b) The carrier image after the embedding

FIGURE 1. The carrier images comparison between the original and after embedding

Therefore, in order to achieve higher robustness and achieve better visual effects, we consider if there are some of the operations in the spatial domain that can construct the low frequency feature in the image, which can resist the severe attacks.

By analyzing the impact of compression on images, and in order to balance the perceptibility and the robustness of digital watermarking, we propose a high robust digital watermarking scheme based on histogram. Our idea is very simple. Different from the traditional transform domain and spatial domain embedding methods, we modify the pixels in the spatial domain to affect the low frequency feature. In the spatial domain, low frequency feature appears as the smooth and continuous pixel region. The larger the continuous pixel region, the more obvious the low frequency feature. According to this principle, we try to modify the pixel to make the surrounding region to be continuous. In the histogram based method, the modification of the pixel is easy to control, we use the histogram based method to locate the potential pixel, and select the pixels by a

dynamic pixel position selection scheme, which is proposed by us. Our scheme is very robust, but needs original carrier image for watermarking recovery. Nowadays, in order to protect valuable images, it is permissible to obtain the original image during watermark extraction.

In Section 2, the related works will be introduced. The detail embedding processes will be discussed in Section 3. In order to show the effects of our method, the experiments will be demonstrated in Section 4, and conclusion and future works will be explained in Section 5.

2. **Related Work.** Lin et al. studied the problem of watermark imperceptibility degradation caused by low frequency embedding, and proposed a watermarking method based on quantization method [12]. This method is designed for JPEG compression. First, the DCT coefficients of blocks need to be calculated, and each DCT coefficient is quantized based on the quantization table provided by the JPEG compression standard [23]. Then the blocks which contain most non-zeros quotients are selected as the embedded blocks, and the watermark is embedded into the low frequency coefficients in the blocks. This method works well and can resist a certain degree of compression attack. Similarly, Preda and Vizireanu proposed a digital watermarking method for JPEG compression [9]. This method also embeds the watermark into the DCT low frequency coefficients by quantization index modulation (QIM). About the choosing of quantization step size, it is necessary to set a JPEG compression quality factor at first, and then calculate the DCT coefficient quantization table according to the compression quality factor. These ideas are following the thought of Cox. In order to resist heavy attacks, the watermarking imperceptibility will decrease.

Das et al. proposed a method which embeds watermark into the difference of two DCT coefficients in two adjacent blocks, and the selected DCT coefficients belong to the middle and low frequency coefficients [7]. By introducing the difference, this method distributes the changes into two blocks, which improves the robustness and enhances the imperceptibility of the watermark. Parah et al. proposed an improved scheme based on this method [11]. By dividing some intervals, the difference will be adjusted to different interval according to the embedding information. These methods can resist varying degrees of compression attacks, but the shortcoming of these methods is that robustness and imperceptibility are difficult to balance.

There are a series of methods based on the SVD decomposition which claim their methods are very robust [8,15,17,18,24]. We find that such methods have the issue about using, and the watermark can be extracted from the original carrier image. This proves that these methods are not convincing, and they cannot prove which image contains the watermark, so it cannot be widely used.

The histogram based watermarking method based on image statistical features. This kind of methods is applicable and widely used in robust watermarking and fragile watermarking. Xiang et al. proposed a robust watermarking algorithm based on histogram [19], and in this method, the watermark is embedded into the low frequency features. First, Gaussian filtering is performed on the carrier image to obtain a low frequency image. Then, the histogram is obtained from the low frequency image, and the maximum pixel frequency is obtained. The embedded pixel range is determined according to one parameter and the pixel value with maximum frequency. The embedding process is performed by adjusting the pixel frequency ratio of two adjacent bins in the histogram, and the positions of modified pixels are randomly selected. Multiple bits can be embedded in one histogram. In the extracting process, the pixel value with the largest frequency in the image needs to be found. Then according to the pixel embedding interval, the

embedded bit is extracted according to the pixel frequency of the adjacent bins. This method has highly robustness against geometric attacks, but there are three unavoidable shortcomings. 1) It cannot resist severe compression attacks. 2) The embedded capacity of this method is limited. Theoretically, the embedding capacity of an image is up to 128 bits. The actual embedded capacity is about 20 bits. 3) This method is a blind watermarking scheme, but it needs to know the embedded content when extracting for exhaustive search. Although this method has some shortcomings, it gives us a lot of inspirations. As a method based on statistical features, the histogram method can obtain strong robustness according to the frequency relationship of pixels. Because the positions of the selected pixels are randomly selected, it appears as the feature of noise. After filtering or compression, the pixels carrying the watermark information will be tampered. Thus, we think about whether we can choose the position of the modified pixel so that the most modified pixel can still exist after being attacked by filtering or compression.

Transform domain based watermarking methods embed information by modifying the transform domain parameters. This can cause the degradation of the carrier. We hope to select the most suitable pixel position to modify, and actively construct the low frequency features in the spatial domain, so that the modified pixels can be surrounded by the close pixels, making the image smoother, and the modified content behaves as a feature of low frequency. In the following sections, we will elaborate our method.

3. Proposed Method.

In this section, the complete description of our scheme is given. The digital image watermarking is a useful tool for digital image copyright protection, and secret information will be embedded in the digital image without affecting the usage of the image. The proposed scheme consists of the improving histogram shifting method and low frequency construction method. The improved histogram shifting method is designed for embedding and extraction. In the process of embedding, some pixels will be modified, and these pixels are chosen by the low frequency construction method. The details of the methods are given in the following sub-sections.

3.1. Improved histogram shifting method.

Inspired by the method of Xiang et al. [19], we propose a simplified histogram shifting method for increasing the embedding capacity. The method of Xiang embeds the watermarking into one histogram, which is generated by the whole image. This method works by setting the frequency of adjacent bins in the histogram, and the extraction is comparing the frequency of adjacent bins. Because there is only one histogram in one image, an image can only embed 128 bits at most, and the embedding capacity is only tens of bits in reality.

Although the robustness against compression is not good, it has great potential. We consider dividing the image into non-overlapped blocks, and 1 bit is embedded in each block. The steps for watermark embedding for one block are as follows, and the process example is shown in Figure 2.

Step 0: Set threshold T, and the embedding range length l;

Step 1: Obtain the pixel histogram of the block; obtain the maximum frequency of pixels $F_{\max}$ and the corresponding pixel value $P_{\max}$ in the histogram; set two embedding range bin 1 and bin 2, and the pixel range of bin 1 is $[P_{\max}-l, P_{\max}-1]$, the pixel range of bin 2 is $[P_{\max}+1, P_{\max}+l]$; the frequency of the pixel in the bin 1 is a, and the frequency of the pixel in the bin 2 is b;

Step 2: If the embedded bit is 0, the relationship of a and b should be $b/a \geq T$; if the embedded bit is 1, the relationship of a and b should be $a/b \geq T$; if the relationship of a and b satisfies the inequality relationship, no adjustment needs to be performed. If the inequality relationship is not satisfied, the range of bin 1 and bin 2 needs to be adjusted:

1) If the embedded bit is 0, the pixel range of bin 1 is $[P_{\max} - l, P_{\max}]$, the pixel range of bin 2 is $[P_{\max} + 1, P_{\max} + l]$;
2) If the embedded bit is 1, the pixel range of bin 1 is $[P_{\max} - l, P_{\max} - 1]$, the pixel range of bin 2 is $[P_{\max}, P_{\max} + l]$;

Then, a, b should be updated according to the range of bins; according to the number of a, b and T, c pixels need to be modified from one bin to another; the equation of c is shown in Equation (1); the way of selecting the modified pixels is shown in next sub-section.

$$c = \begin{cases} \dfrac{a - Tb}{1 + T}, & (\text{EmbedBit} = 0,\ b/a < T) \\ \dfrac{Tb - a}{1 + T}, & (\text{EmbedBit} = 1,\ a/b < T) \end{cases} \tag{1}$$

Step 3: Determine whether the embedding is completed. If not, move to next block and perform Step 2; otherwise, the embedding process is completed.

The watermark extraction process for one block is as follows.

Step 0: Obtain the embedding range length $l \geq 1$; obtain the maximum frequency of pixels $F_{\max}$ and the corresponding pixel value $P_{\max}$ in the histogram in the block of the same position in the original carrier image.

Step 1: Obtain the pixel histogram of this block; according to $P_{\max}$, obtain two embedded ranges bin 1 and bin 2. The pixel range of bin 1 is $[P_{\max} - l, P_{\max} - 1]$, and the pixel range of bin 2 is $[P_{\max} + 1, P_{\max} + l]$; the frequency of pixels in bin 1 is a, and the frequency of pixels in bin 2 is b.

Step 2: If $a < b$, the extracted bit is 0; otherwise, it is 1.

In our method, one block can embed one bit, which has more capacity than that of Xiang method [19]. The incremental contribution of proposed method is that our method has more embedding capacity. What is more, our method is more flexible. If you need to resist the rotation attack, you only need to increase the size of the block. When combined with redundant embedding and scrambling, the robustness and security of the algorithm can be increased.

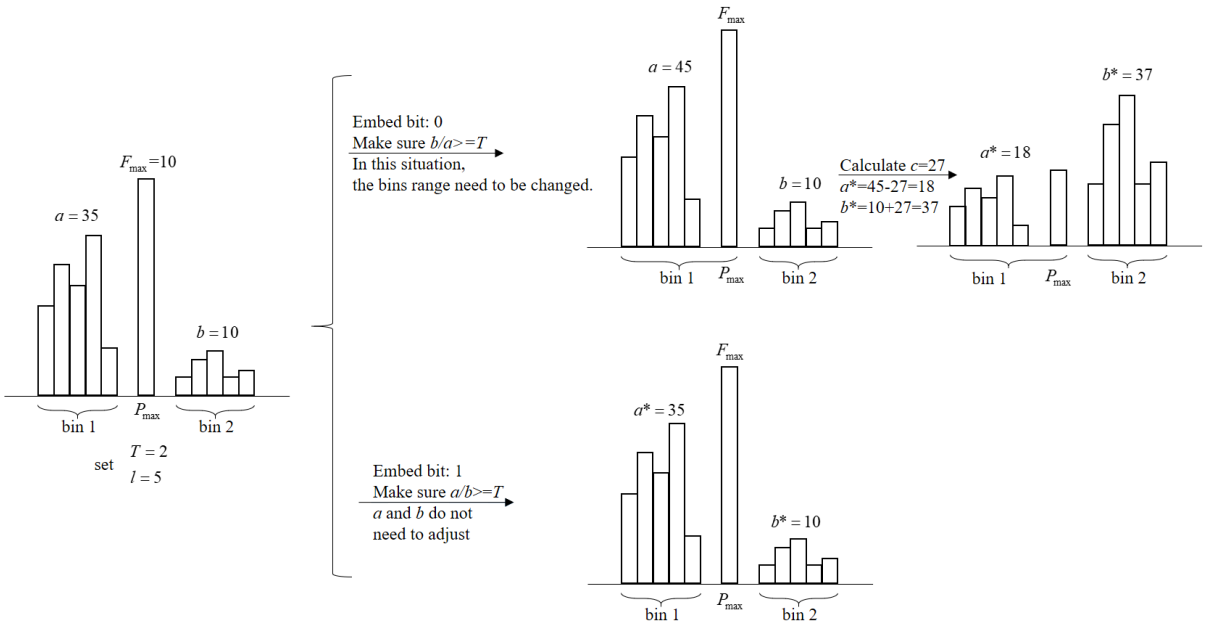


FIGURE 2. An example of improved histogram shifting method

3.2. **Low frequency construction method.** In the past digital watermarking method, transform domain watermarking method and spatial domain watermarking method are often not related. Watermark embedding in the transform domain affects all pixel in the spatial domain, so when the robustness is increased, the imperceptibility is degraded; on the other hand, the embedding in the spatial domain often does not consider the effects in the transform domain. The random selected pixel position causes the modified content like noise and will be filtered when passing through the low pass filter or compression.

Therefore, we propose a low frequency construction method on spatial domain. Our purpose is to select the pixel with best position to modify, so that the modified pixel is close or equal to the surrounding pixels. The steps for a block are as follows.

Step 0: Determine range $1 \in [\text{range\_1\_left}, \text{range\_1\_right}]$ as the pixel value range which needs to be modified, and range $2 \in [\text{range\_2\_left}, \text{range\_2\_right}]$ as the target pixel value range, there must be no overlap between the two ranges; determine the number of pixels c need to be modified, and counting variable $cn = 0$.

Step 1: Traverse all the pixels of the block. If one pixel value $p_{x,y}$ in the position of x, y in range 1, the adjacent 8 pixels are called surrounding pixels. In the surrounding pixels, the pixels whose value in range 2 are called neighbor pixels, the number of neighbor pixels is $neighbor_{x,y}$, and the mean value of neighbor pixels is $mean_{x,y}$, and the weight of $p_{x,y}$ is calculated in Equation (2).

$$weight_{x,y} = \frac{\exp(neighbor_{x,y})}{\text{abs}(mean_{x,y} - p_{x,y})} \tag{2}$$

Step 2: Select the pixel which has the maximum $weight_{x,y}$, and modify it to $\text{int}(mean_{x,y})$, then, the counting variable $cn = cn + 1$.

Step 3: Determine whether cn is equal to c. If they are equal, stop the modification process, otherwise jump to Step 1.

The entire process and example can be illustrated in Figure 3 and Figure 4.

We design the weight calculation equation in Equation (2). We hope the number of neighbor pixels can affect the weight more. Because the larger $neighbor_{x,y}$ indicates that the pixel in the position of x, y is surrounded by more pixels in range 2, and it is easier to be assimilated into the surrounding pixels after modification. The denominator of Equation (2) represents the difference before and after the modification of pixel. If the difference is larger, the PSNR of block before and after the embedding will rise. When implementing this method, the values of exp(0) to exp(8) can be calculated and stored in advance for saving computation time.

Through Figure 4, we can find that our method modifies the pixel which like the "island" at first, and then modifies the pixel like the "edge". After the modification, the feature of low frequency can be enhanced. In compression or low-pass filtering, both "island" pixels and "edge" pixels can be tampered easily, but after the processing of our method, these modified pixels can still remain with high probability after compression or low-pass filtering. This is why our scheme has strong robustness. In addition, using our method for embedding can avoid the disgusting texture caused by the modification of transform domain coefficients, and it can also avoid the noise feature caused by pixel position random selection which is used in the scheme of Xiang. The embedded image is smoother, and the imperceptibility is better. The example of the original image and embedded image can be shown in Figure 5.

3.3. **The watermarking scheme for the image.** After the above explanations, we know the watermark embedding steps for a block. In this subsection we introduce the

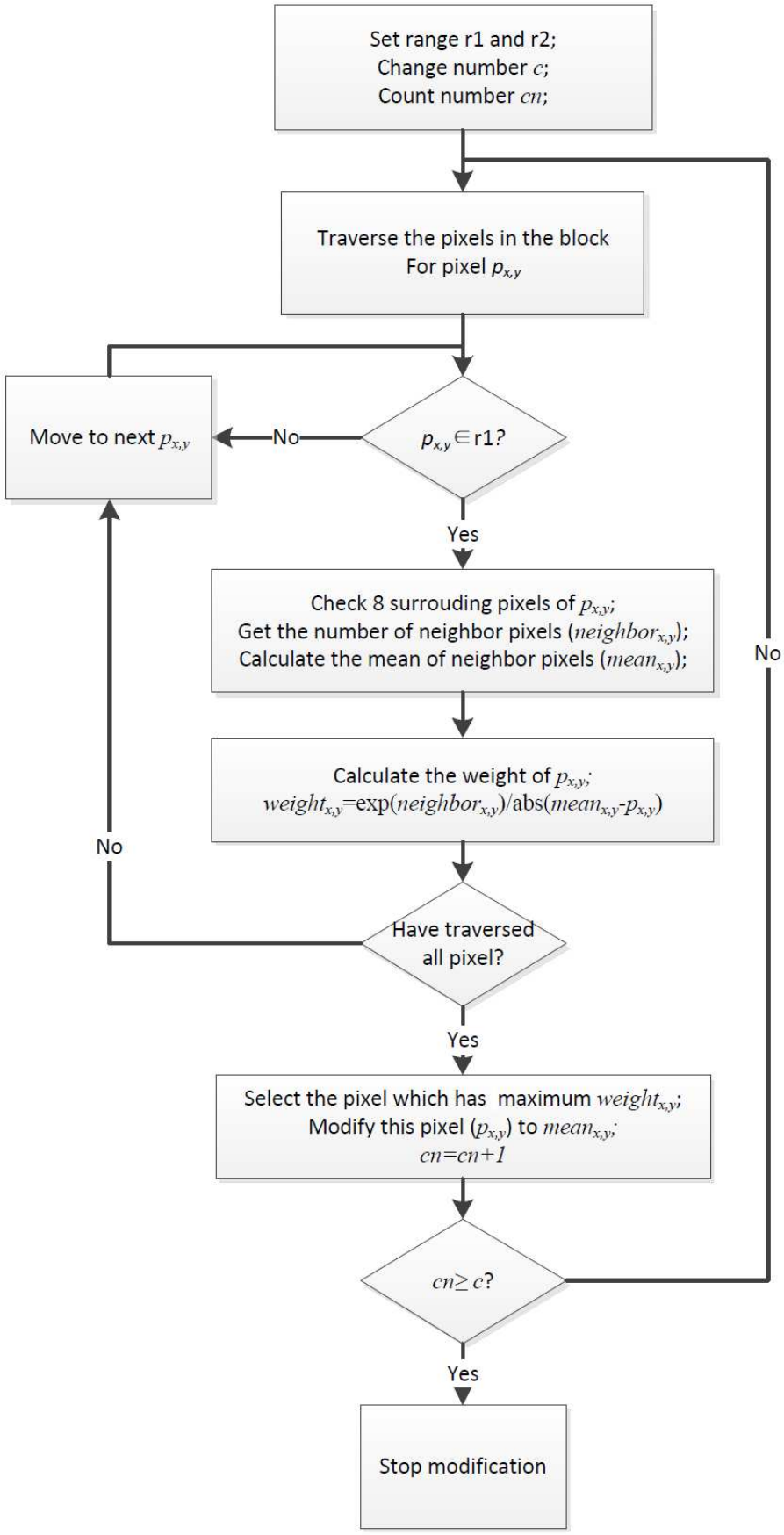
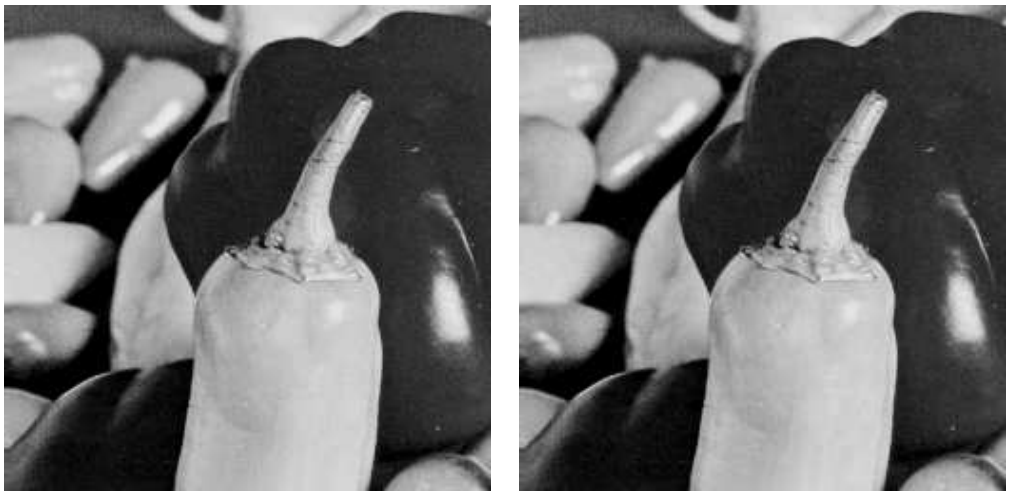


FIGURE 3. The flow chart of entire process

FIGURE 4. An example of low frequency construction in a block



(a) (b)

FIGURE 5. The original image (a) and the image with watermark (b)

watermark embedding and extraction scheme for an image. The embedding steps are as follows:

Step 0: Set the block size BS, set the embedding range length l, threshold T; adjustable parameter μ and initial value x_0 for chaotic Logistic map; prepare the watermark bit sequence $W = \{w_i | i = 1, \ldots, L_w\}$;

Step 1: Perform non-overlapping block divide on the image, the number of blocks is BN, and it is necessary to ensure $BN \geq L_w$; the watermark needs to be redundantly extended, and the extended watermark is $WR = \{w_i | i = 1, \ldots, BN\}$; the chaotic Logistic map is used to scramble the sequence WR to obtain a scrambled sequence $WSR = \{w_i | i = 1, \ldots, BN\}$;

Step 2: Use the methods in the previous two sub-sections to embed the WSR into blocks.

The steps of extraction are as follows:

Step 0: Obtain the block size BS, obtain the embedding range length l, threshold T; obtain adjustable parameter μ and initial value x_0 for chaotic Logistic map; obtain the watermark sequence length L_w;

Step 1: Restore the embedded information WSR^* using the methods mentioned in the above sub-sections;

Step 2: Use the chaotic Logistic map to descramble WSR^* to obtain WR^*;

Step 3: Restore W^* from WR^* according to the principle of majority.

Here, the chaotic Logistic map mentioned above needs to be explained. The chaotic Logistic map is generated by the chaotic equation $x_{n+1} = f(x_n)$. The chaotic Logistic map is sensitive to the initial value. It can generate a series of irregular values by providing the initial value x_0. According to the order of these values, a sequence can be generated. Using chaotic Logistic map to scramble the watermark can increase the security. The definition of the chaotic Logistic map used in this paper is given in Equation (3).

$$x_{n+1} = 1 - \mu x_n^2 \tag{3}$$

where μ is an adjustable parameter, and for any n, the obtained $x_n \in [0, 1]$ is fixed if the initial value x_0 is fixed. The sequence $\{x_i\}$, $i = 1, 2, \ldots$ can be sorted to obtain the order sequence $\{k_i\}$, $i = 1, 2, \ldots$. The original sequence can be scrambled by $\{k_i\}$; the scrambled sequence can be descrambled according to $\{k_i\}$.

The complete processes of the proposed scheme are described above. Different from the other traditional watermarking schemes, we consider the effects on the frequency domain, and modify the pixels in the spatial domain. The proposed improved histogram based watermarking method has larger capacity and better imperceptibility, and the low frequency construction method can enhance the robustness and imperceptibility. These are the main differences from other schemes.

4. **Experiment.** In order to exhibit the features of our scheme and the ability to resist some common attacks, we focus on the comparison of our scheme and others. In this section, besides our scheme, the schemes for comparing are: (1) embedding method based on histogram, which mentioned in sub-section 3.1 but selects the modified pixels randomly; (2) the histogram based scheme proposed in [19]; (3) the scheme proposed in [7]; (4) the scheme proposed in [15]; (5) the scheme proposed in [12]; (6) the scheme proposed in [9]. In order to ensure fairness, the schemes (2) and (5) have been modified as the non-blind extraction schemes to improve the robustness. The relevant parameters of the above schemes are shown in the following subsections. We use the peak signal-to-noise ratio (PSNR) to illustrate the degree of change of the carrier image before and after the embedding. The equation for calculating the PSNR is shown in Equation (4). Larger PSNR value denotes the higher similarity between the two images. In order to compare the robustness, we use the normalized correlation (NC) value to describe the relation between the original watermark and the extracted one. The equation about NC is shown in Equation (5), where w represents the original watermark, w^* represents the extracted watermark. The NC value is between 0 and 1, and larger NC value means the original

watermark and the extracted watermark are more similar.

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I(i,j) - I^*(i,j)]^2}}\right) \tag{4}$$

$$NC(w, w^*) = \frac{\sum_{i=0}^{M-1} w(i) \times w^*(i)}{\sum_{i=0}^{M-1} w(i)^2} \tag{5}$$

4.1. **Experiment 1.** In this experiment, we mainly discuss the robustness of our scheme and others under JPEG compression attacks. The PSNR about carrier images and the NC value about the watermarks are illustrated. We use 10 standard test images with the size of 512∗512 as the carrier images. These images are shown in Figure 6. In this experiment, the parameters of each scheme are shown in Table 1. For every scheme, the parameters are settled according to the empirical results. Under these parameters, every scheme has a good performance. Because the histogram-based scheme proposed by Xiang has limited embedding capacity [19], 20 bits are embedded for his scheme. The scheme (6) needs to set a compression quality factor in advance. For fair comparison, we use 30 as the quality factor. Under this parameter, the PSNR before and after the embedding is similar to that of our scheme. The PSNR values of the carrier images before and after the embedding are shown in Table 2. The NC values of the watermark before and after the attack are shown in Figure 7.

FIGURE 6. 10 standard test images. The name of these images are 0628, Baboon, F16, Goldhill, Lena, Luyu8g, Pepper, SONIC, Test8g, Woman from left to right.

By analyzing the experimental results, we can find that our scheme is not very effective for the images with much detailed features, such as 0628 and Baboon. The reason is that the histogram method relies on the characteristics of the image. For 0628 and Baboon, they are not smooth, and the histograms of these images are not continuous, thus, the number of adjusted pixels is too small. For images with less detailed features, this problem does not reappear. For scheme (1), we find that the robustness is similar to ours, but the PSNR is lower. Scheme (2) has a limited embedding capacity, and the robustness about JPEG compression is not good as well. Scheme (3) has strong robustness, but the PSNR of the carrier image before and after watermark embedding is very low, which means the imperceptibility of the scheme is not good. For scheme (3), if not use redundant

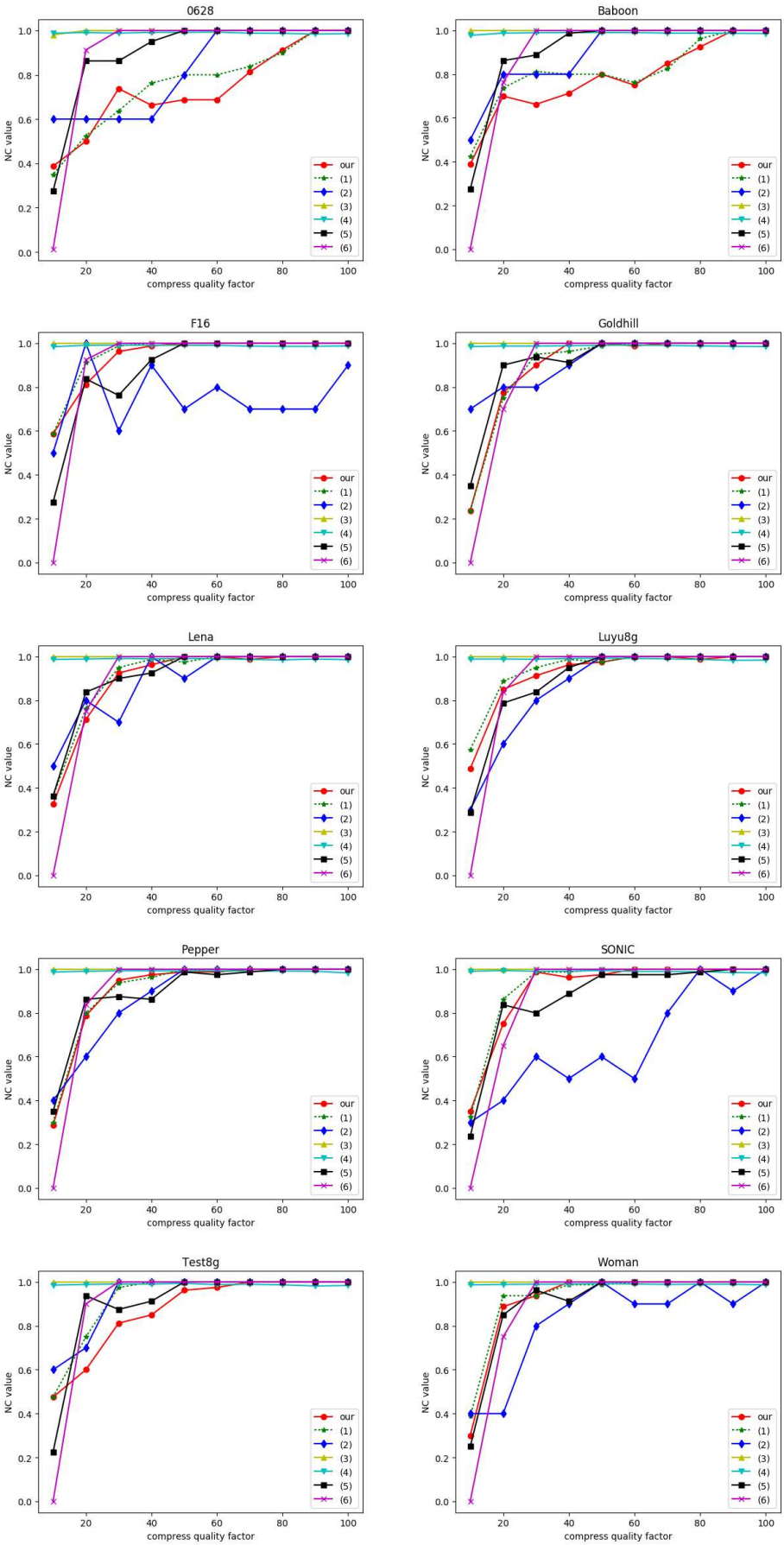


FIGURE 7. The NC values between the original watermark and the extracted watermark from the attacked images

TABLE 1. The parameters of each scheme

Scheme	Block size	Parameters	Embedding bit length	Redundant embedding
Ours	8∗8	$T = 14$	160 bits	yes
(1)	8∗8	$T = 14$	160 bits	yes
(2)	–	Range lambda = 0.55 Thresh = 14	20 bits	no
(3)	8∗8	Thresh = 80 $K = 12$	160 bits	yes
(4)	–	$\alpha = 0.1$	32∗32 binary image	no
(5)	8∗8	$M = 40$	160 bits	no
(6)	8∗8	Compress quality factor = 30	160 bits	yes

TABLE 2. The PSNR between the original image and embedded image

Scheme	0628	Baboon	F16	Goldhill	Lena	Luyu8g	Pepper	SONIC	Test8g	Woman
Ours	45.522	45.052	43.945	43.340	42.604	44.928	42.877	43.664	45.678	43.629
(1)	43.532	43.340	40.861	41.437	40.837	42.445	41.048	41.602	42.040	41.713
(2)	43.292	41.046	38.541	42.193	44.334	40.983	45.094	37.825	40.579	40.179
(3)	30.235	34.576	28.171	37.898	30.453	27.748	17.900	20.862	39.039	26.168
(4)	70.983	70.895	70.887	70.911	70.922	70.906	70.972	70.866	70.900	70.944
(5)	58.450	58.327	58.255	58.410	58.414	59.240	59.142	58.207	58.792	58.381
(6)	40.337	40.226	41.100	40.623	41.152	40.717	41.209	40.800	41.555	41.020

embedding, the PSNR of the carrier image before and after the embedding will become higher, but still below 40. For scheme (4), we can see that the performance of this method is quite excellent. However, since this type of schemes can extract information from the original carrier image, these schemes cannot be used in reality. Because such schemes have excellent performance and very common in academy, so we need to explain in our paper. Scheme (5) is a highly robust scheme for JPEG compression. In this scheme, some blocks are selected for embedding. For these selected blocks, the PSNR value about before and after embedding is very low, and the modified image blocks have the obvious texture features caused by the transform domain modification mentioned before, so the visual effects are not good. The scheme (6) has a similar robustness to our scheme, and the NC values are similar to that of ours, but this scheme cannot resist other attacks such as geometric attacks, and in Experiment 3 we will explain.

From this experiment, we can find that our scheme is not good for the image with too many details, but the overall performance is balance. The PSNR before and after the embedding is above 40, which ensures the invisibility of the watermark, and it has good robustness against compression attacks.

4.2. **Experiment 2.** This experiment illustrates the impact of the adjustment of parameters on the performance. We adjust block size BS and threshold T to observe the resistance about compression attack. In order to save space, in this experiment and experiment 3, we select two standard test images for display, which are Lena and Pepper. The PSNR values of the carrier images before and after the embedding are shown in Table 3. The NC values of the watermarks before and after attack are shown in Figure 8.

According to the experimental results, we can find that when a larger threshold is selected, the PSNR value is getting lower. When choosing a larger threshold, the number

TABLE 3. The PSNR values of the carrier image before and after the embedding

	Lena				Pepper			
BS \ T	2	4	8	16	2	4	8	16
8	47.190	44.628	43.307	42.462	47.408	44.802	43.529	42.741
16	47.615	44.842	43.525	42.870	47.969	45.240	43.943	43.313
32	49.710	46.831	45.504	44.829	50.269	47.366	46.047	45.418

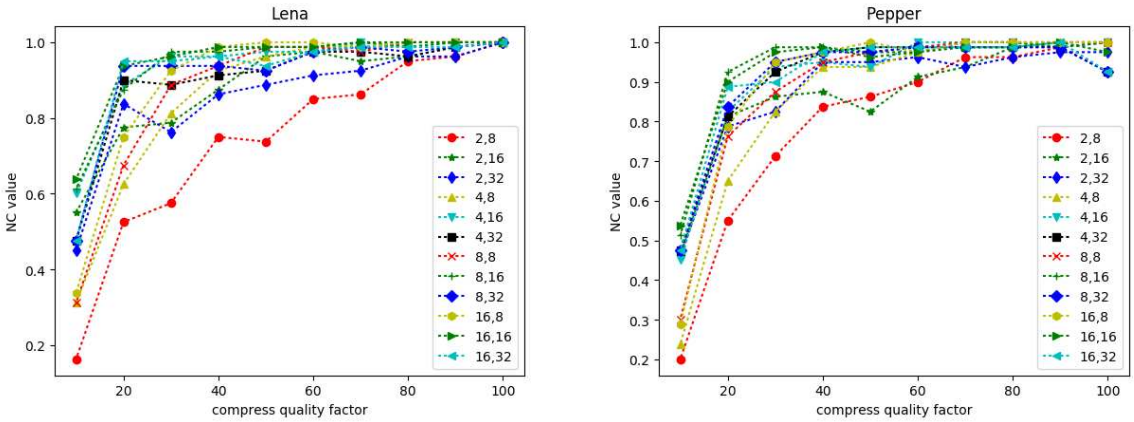


FIGURE 8. The NC values of the watermark before and after attack, the label format is (T, BS).

of modified pixels becomes more, so the value of PSNR will decrease. When a larger block size is selected, the PSNR values will increase. The main reason is that when a larger block size is selected, the capacity of the embedding bits is degraded, and the error correction capability is degraded due to the less redundant information. From the results of NC value, we can find that balanced parameters can resist severe attacks.

4.3. **Experiment 3.** In this experiment, we mainly illustrate the robustness of our scheme under some other attacks. Our method can adjust the parameters to resist different attacks. A larger block size can resist geometric attacks well. In this experiment, the block size is 32, threshold is 14. We do not adjust parameters of other schemes because of their design. In this section, rotation, scaling, and Gaussian noise attacks have been used. Because our scheme does not include synchronization, the tests about smear, tampering, and shear attacks are meaningless. So we do not test these attacks.

The experimental results are shown in Figure 9. Through these results, we can find that our scheme can resist a certain degree of rotation attack, severe scaling attack and noise attack. Scheme (2) is based on global histograms, so it can resist severe geometric attacks. Scheme (3) is the SVD-based method mentioned before, and it cannot be used in reality. And the other schemes are based on transform domain, so the robustness about geomatics attack is not good. The schemes based on transform domain can better deal with scaling attacks, such as the schemes (3) and (6). But overall, our scheme can handle multiple attacks.

4.4. **Experiment 4.** This experiment mainly shows the attacks on images which are caused by mobile applications, and the robustness of our scheme under such attacks. We select several popular mobile chat applications for image transmission. In these applications, the images may be compressed, scaled or format conversed to improve the speed of

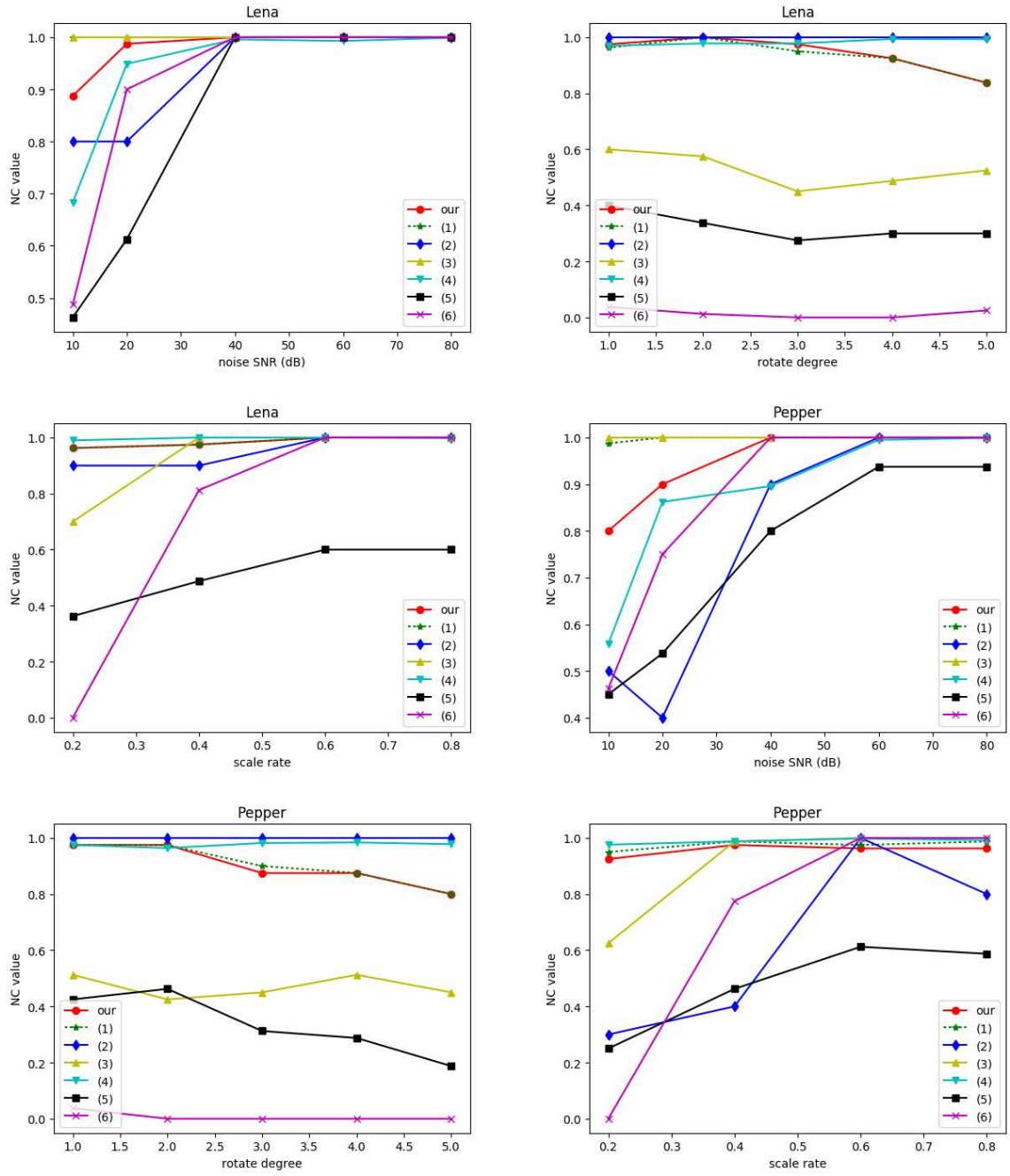


FIGURE 9. The NC values under different attacks

information transmission. The compression operations performed on images by different applications are also different. For us, the details of these attacks are unknown. The applications we selected are WeChat, DingDing, and Bullet Message. All transmitted images are color images. In order to ensure fairness and simulate the real situation, we perform Y-Cb-Cr decomposition on the color images and embed the watermark into the Y component of the images. During the test, we find that these applications compress and scale the images which have large size, while the small size images may not be compressed and scaled. Therefore, we select some large images for testing in this experiment. The parameters of these schemes are the same as those in Experiment 1. The test images

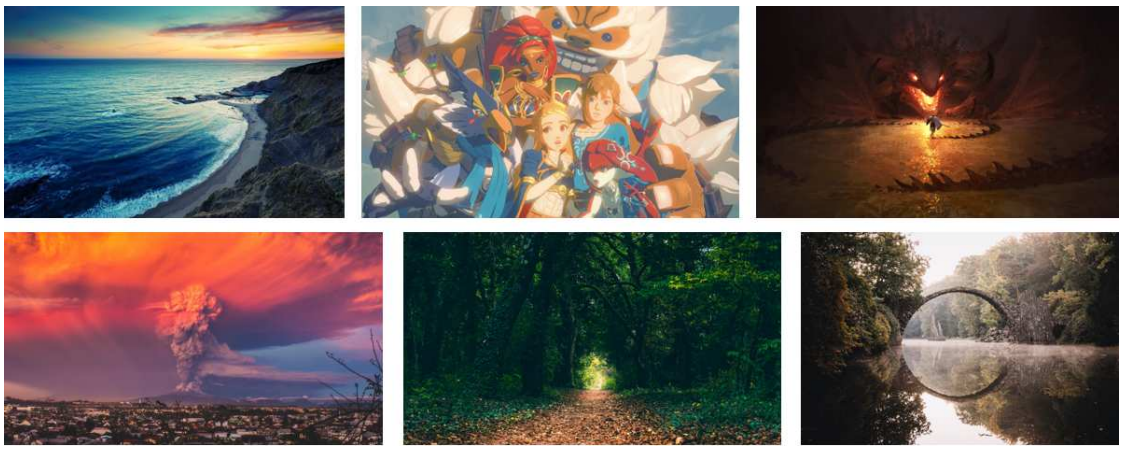


FIGURE 10. The test images in Experiment 4 (Image 1 to Image 6 are shown from left to right)

TABLE 4. The information about test images

	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6
Size	1920∗1200	1920∗1080	1920∗1121	1975∗1111	1920∗1080	2048∗1365
Format	JPEG	PNG	JPEG	JPEG	JPEG	JPEG
File size	652KB	2.0MB	216KB	444KB	554KB	1.07MB

TABLE 5. The image file information after transmission by mobile applications

		Image 1	Image 2	Image 3	Image 4	Image 5	Image 6
DingDing	Size	1200∗750	1200∗675	1200∗701	1200∗675	1200∗675	1200∗800
	Format	JPEG	JPEG	JPEG	JPEG	JPEG	JPEG
	File size	290KB	197KB	95.6KB	150KB	194KB	384KB
WeChat	Size	1920∗1080	1850∗1080	1920∗1080	1920∗1080	1620∗1079	1728∗1080
	Format	JPEG	JPEG	JPEG	JPEG	JPEG	JPEG
	File size	194KB	107KB	163KB	378KB	354KB	288KB
Bullet Message	Size	828∗466	828∗483	828∗466	828∗466	828∗552	828∗518
	Format	JPEG	JPEG	JPEG	JPEG	JPEG	JPEG
	File size	60.5KB	28.3KB	43.7KB	82.8KB	90.2KB	71.2KB

are shown in Figure 10, the information about test images are shown in Table 4, and the experimental results are shown in Table 5 and Figure 11.

From the results, our scheme works well for mobile application transmission attacks. The scheme (4) is meaningless, so we decide not to mention it in this experiment. The scheme (3) has strong robustness, but the imperceptibility is not good. The PSNR of the carrier image before and after embedding is below 40, which is difficult to use in practice. The robustness of other schemes is not good from Figure 9. Thus, we can say that our scheme can resist the mobile application transmission attacks.

5. **Conclusions and Future Work.** In order to deal with the problem that occurred in mobile application transmission, we have researched different schemes and designed our scheme in the end.

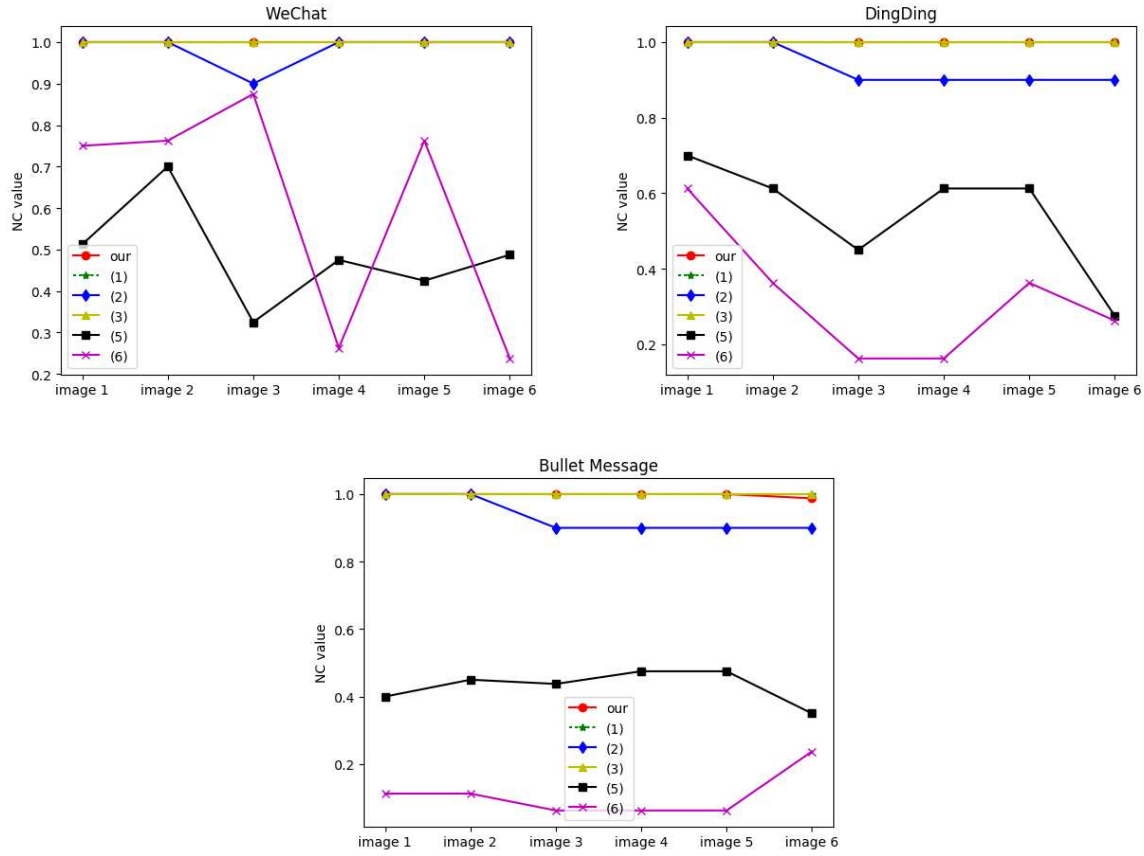


FIGURE 11. The test images in Experiment 4. The watermark NC values under different transmission.

The proposed histogram based watermarking method and low frequency construction method are our main contributions. By computing weights of the pixels, some most suitable pixels are selected, and after the modification, the low frequency feature of the image will be enhanced. Our scheme is an implementation of affecting low frequency feature in the spatial domain, and this is our biggest contribution.

The advantages of our scheme can be summarized as follows: 1) our scheme has good capacity; 2) our scheme has good robustness against many common attacks, such as JPEG compression attack and noise attack, and it can resist geometric attacks in a degree; 3) our scheme has good imperceptibility. There is no typical texture in the embedded images.

There are some common shortcomings about histogram based schemes. The most important point is that these schemes rely on the pixel statistical features. If an image consists of only a few pixel values, the histogram based watermarking scheme is difficult to be effective. Another problem about our scheme is that the embedding effectiveness is not good. Because the process of finding the best modified pixel position is a dynamic optimization process, after the modification of one pixel, the next optimal position needs to be recalculated. When a larger block size is set, the required time will increase. As the number of pixels in one block increases, the number of pixels that need to be modified also increases, the computation time also increases.

In the future, we will optimize the efficiency of our scheme. In addition, improve the way of weight calculation. We hope to find a way to express the weight more reasonable and improve the embedding more effective. And the histogram based method can be

updated for some hard samples, such as 0628 and Baboon, to get a broader application scenario.

REFERENCES

[1] X. M. Niu, Z. M. Lu and S. H. Sun, Digital watermarking of still images with gray-level digital watermarks, *IEEE Transactions on Consumer Electronics*, vol.46, no.1, pp.137-145, 2000.

[2] C. Honsinger, Digital watermarking, *Journal of Electronic Imaging*, vol.11, no.3, p.414, 2002.

[3] I. Cox, M. Miller, J. Bloom, J. Fridrich and T. Kalker, *Digital Watermarking and Steganography*, 2nd Edition, Morgan Kaufmann, San Francisco, Calif, USA, 2008.

[4] G. C. Langelaar, I. Setyawan and R. L. Lagendijk, Watermarking digital image and video data. A state-of-the-art overview, *IEEE Signal Processing Magazine*, vol.17, no.5, pp.20-46, 2000.

[5] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Transactions on Image Processing*, vol.6, no.12, pp.1673-1687, 1997.

[6] J. Huang, Y. Q. Shi and Y. Shi, Embedding image watermarks in DC components, *IEEE Transactions on Circuits and Systems for Video Technology*, vol.10, no.6, pp.974-979, 2000.

[7] C. Das, S. Panigrahi, V. K. Sharma and K. Mahapatra, A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation, *AEU – International Journal of Electronics and Communications*, vol.68, no.3, pp.244-253, 2014.

[8] A. K. Singh, M. Dave and A. Mohan, Hybrid technique for robust and imperceptible multiple watermarking using medical images, *Multimedia Tools and Applications*, vol.75, no.14, pp.8381-8401, 2016.

[9] R. Preda and D. Vizireanu, Watermarking-based image authentication robust to JPEG compression, *Electronics Letters*, vol.51, no.23, pp.1873-1875, 2015.

[10] X. Kang, J. Huang, Y. Q. Shi and Y. Lin, A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression, *IEEE Transactions on Circuits and Systems for Video Technology*, vol.13, no.8, pp.776-786, 2003.

[11] S. A. Parah, J. A. Sheikh, N. A. Loan and G. M. Bhat, Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing, *Digital Signal Processing*, vol.53, pp.11-24, 2016.

[12] S. D. Lin, S. C. Shie and J. Y. Guo, Improving the robustness of DCT-based image watermarking against JPEG compression, *Computer Standards & Interfaces*, vol.32, nos.1-2, pp.54-60, 2010.

[13] S. Das, M. Banerjee and A. Chaudhuri, An improved DCT based image watermarking robust against JPEG compression and other attacks, *International Journal of Image, Graphics and Signal Processing*, vol.9, no.9, pp.40-50, 2017.

[14] F. Chen, H. He and Y. Huo, Self-embedding watermarking scheme against JPEG compression with superior imperceptibility, *Multimedia Tools and Applications*, vol.76, no.7, pp.9681-9712, 2017.

[15] F. Liu and Y. Liu, A watermarking algorithm for digital image based on DCT and SVD, *IEEE Congress on Image and Signal Processing, CISP'08*, vol.1, pp.380-383, 2008.

[16] F. Liu, K. Han and C. Z. Wang, A novel blind watermark algorithm based on SVD and DCT, *IEEE International Conference on Intelligent Computing and Intelligent Systems, ICIS 2009*, vol.4, pp.283-286, 2009.

[17] N. M. Makbol and B. E. Khoo, Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, *AEU – International Journal of Electronics and Communications*, vol.67, no.2, pp.102-112, 2013.

[18] S. Fazli and M. Moeini, A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks, *Optik – International Journal for Light and Electron Optics*, vol.127, no.2, pp.964-972, 2016.

[19] S. Xiang, H. J. Kim and J. Huang, Invariant image watermarking based on statistical features in the low-frequency domain, *IEEE Transactions on Circuits and Systems for Video Technology*, vol.18, no.6, pp.777-790, 2008.

[20] B. Ou, X. Li, Y. Zhao, R. Ni and Y.-Q. Shi, Pairwise prediction-error expansion for efficient reversible data hiding, *IEEE Transactions on Image Processing*, vol.22, no.12, pp.5010-5021, 2013.

[21] C. C. Lo and Y. C. Hu, A novel reversible image authentication scheme for digital images, *Signal Processing*, vol.98, pp.174-185, 2014.

[22] I. C. Dragoi and D. Coltuc, Local-prediction-based difference expansion reversible watermarking, *IEEE Transactions on Image Processing*, vol.23, no.4, pp.1779-1790, 2014.

[23] G. K. Wallace, The JPEG still picture compression standard, *IEEE Transactions on Consumer Electronics*, vol.38, no.1, pp.xviii-xxxiv, 1992.

[24] M. Ali, C. W. Ahn and M. Pant, A robust image watermarking technique using SVD and differential evolution in DCT domain, *Optik – International Journal for Light and Electron Optics*, vol.125, no.1, pp.428-434, 2014.

[25] T. Hiraoka, H. Nonaka and Y. Tsurunari, A high-speed method for generating labyrinth images using smoothing filters with different window sizes, *ICIC Express Letters*, vol.13, no.8, pp.711-717, 2019.