A Histogram Based Watermarking Algorithm Robust to Geometric Distortions

Xuefeng Hu[1, 2, a], Daoshun Wang[1, 2, b]

[1]Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

[2]State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093

[a]huxf12@mails.tsinghua.edu.cn, [b]wangdaoshun@gmail.com

Keywords: Digital watermark, Histogram modification, Geometric distortions, HVS.

Abstract. Most of the histogram-based watermarking methods focused on the geometric invariance feature more while paying less attention to the robustness to some common image processing attacks like JPEG compression. In this paper, we propose a new histogram modification scheme considering the visual quality of the watermarked image while combining block dividing and histogram statistics for the first time in watermarking scheme. We use the mean pixel value of divided blocks to calculate histogram and the mean square error to select blocks to be modified based on HVS. We can obtain a good trade-off between robustness to geometric attacks and common image processing attacks by adjusting the block size. Finally the complete embedding and extracting algorithms are given. The experiment shows that the proposed approach has an excellent robustness against geometric attacks and some normal attacks, such as adding noise and JPEG compression.

Introduction

How to resist geometric attacks has become one of the most popular research directions, especially in digital watermarking field. The most common watermarking methods related can be divided into three categories: inverse transformation methods, geometric invariance domain methods and feature area embedding methods. *Inverse transformation methods* inverse the attacked image to the form of the original image before the watermark extraction procedure. Exhaustive search [1] and embedding template in addition to the watermark [2] fall into this category. *Geometric invariance domain methods* will first use mathematical transformation on the input image before embedding and extracting procedure. The transformation achieves the same result even the image has been geometrically attacked. The most common geometric invariance transformation methods are as follows: the Fourier-Mellin transform [3], the Zernike moments [4] and image normalization methods [5]. *Feature area embedding methods* usually extract feature points of an image firstly and then construct feature areas, which can be exactly reconstructed. Lots of well-known feature point extraction methods have been presented, such as Harris corner detector [6] and SIFT point detector [7] and so on.

There is another special kind of solutions that use the statistic features of an image. The histogram is mainly employed based on the fact that the histogram shape is only related to the pixel count of each grayscale, not the position of pixels. So Xiang et al. [8] presented the well-known grey level histogram method using mean and histogram shape of a Gaussian filtered image. Then Deng et al [9] and He et al [11] both proposed new histogram modification methods based on Xiang et al.'s scheme. Besides, Fang and Zhao [10] also presented an algorithm which used quantization index modulation (QIM) to modify the histogram of an image.

Among these histogram-based algorithms, Xiang et al.'s method was proved that it can achieve a certain degree of robustness to not only geometric attacks but also some common image processing attacks. Xiang el al.'s method is analyzed in this paper. The experimental result shows that this scheme has two obvious problems that should be optimized. The first one is that the visual quality will be seriously reduced in some smooth area when the bins width increases. The second one is

that the scheme works not very well when the image is under JPEG compression attacks, which needs to be improved. Based on the analysis, we will give two optimization methods from the histogram modification and the pixel modulation respectively. In the end, our embedding and extracting algorithms are proposed and some experiment results are given. The experimental results indicate that our watermarking scheme is robust to geometric attacks (rotation, scaling and translation) as well as common image processing and outperforms Xiang et al.'s representative method in some cases.

The rest of this paper is organized as follows. Section 2 briefly reviews Xiang et al.'s method and then analyzes the reason of two drawbacks. In section 3, we will introduce two optimization methods first and then the complete embedding and extracting procedures are presented. Experimental results and analysis are given in section 4 and section 5 gives the conclusion finally.

Background and Motivation

As we all know, the histogram of an image is calculated by dividing the image pixel values into equal-sized bins and counting the number of pixels into each bin. Suppose there is an image $I = \{I(\mathrm{m},\mathrm{n})|\mathrm{m} = 1,2,\dots,R,\ \mathrm{n} = 1,2,\dots,C\}$, then the histogram can be described by:

$$H = \{h(i) \mid i = 1,2,\dots \mathrm{N}\} \tag{1}$$

where N defines the number of equal-sized bins, and $h(i)$ represents the number of pixels in the ith bin and it satisfies $Sum = \sum_{i=1}^{N} h(i) = R \times C$. When the image is under geometric attack, the size and spatial position of the image may change, but the ratio of each bin, that is $\frac{h(i)}{Sum}$, stays stable.

In Xiang et al.'s method, the histogram embedding range $[(1-\lambda)\bar{A}, (1+\lambda)\bar{A}]$ is determined by the mean $\bar{A}$ of the image firstly. Then each two bins that fall into this range are merged into a group. The watermark bits are embedded into these groups. Suppose the pixel number of two adjoining bins in one group is a and b respectively. The embedding rules are as follows:

$$\begin{cases} \frac{a}{b} \geq T & if\ \ W(i) = 1 \\ \frac{b}{a} \geq T & if\ \ W(i) = 0 \end{cases} \tag{2}$$

where T is a trade-off threshold between the visual quality and the robustness of the algorithm. If a and b of the original image meet the conditions in (2), no change will be made to image pixels. Otherwise, some modification will be made to let the pixel in one bin jump into the other. The modification degree of each pixel depends on the size M of each bin.

After some experimental tests on Xiang et al.'s scheme, we have found two problems that need to be solved. Firstly, when increasing the bin's size M, the visual quality of some smooth area will be seriously reduced. Figure 1 gives an example in which the bin's size M is set to 3. We can find a '*waterlogging*' situation in the upper left corner area after watermark embedding. The reason of this situation is that when the bin's size M is set to 3, pixels need to be modified will add or minus 3 pixel values too. Besides, the pixels to be modified are selected randomly, so in some smooth area, the situation will occur as the example shows.

Fig. 1 Original image and the upper left corner area after embedding procedure

Another drawback of the histogram-based scheme is that the robustness to JPEG compression attacks is weak relatively for the reason that the JPEG compression will smooth the histogram of embedded image as Figure 2 shows. In JPEG compression, the low-and-middle frequency energy will be reserved and some high frequency energy may be lost. On the contrary, the energy that histogram-based algorithms introduce belongs to high frequency part precisely. In order to solve

this problem, Xiang et al. used the Gaussian filtered low-frequency component to calculate the histogram. This approach has obtained some certain effect, but the result shows that it is still not so ideal.

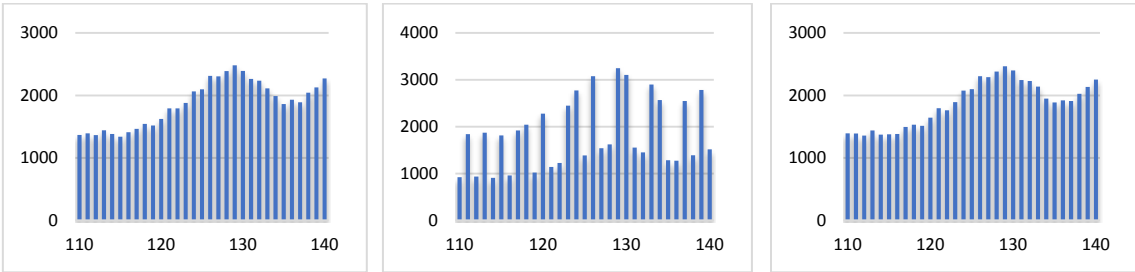

Fig. 2 Histograms of original image, watermarked image and JPEG attacked image

So, in the next section, we will give our optimization methods to deal with above two problems.

The proposed Algorithm

Histogram Modification. To solve the first problem mentioned above, this paper extends the group size to 3 bins without increasing the modification degree of each pixel. The modification procedure is shows as Figure 3.

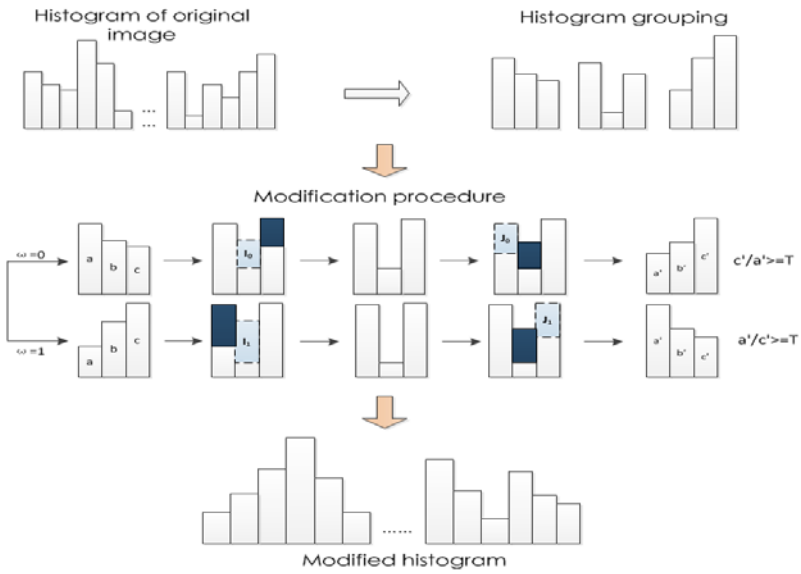

Fig. 3 Histogram modification procedure

Suppose the pixel number of three consecutive bins (bin_1, bin_2 and bin_3) in one group is a, b and c respectively. The embedding rules are described as follows.

a. the bit to be embedded is '1';

If $\frac{a}{c} \geq T$, no pixels will be modulated. Otherwise, I_1 pixels in bin_2 are chosen to be modified firstly so as to make them fall into bin_1 (The method of choosing pixels will be described in next subsection *Pixel Modulation*); then J_1 pixels in bin_3 are chosen to be modified so as to make them fall into bin_2. To make sure the modification degree of each pixel is M, the order of above two steps should not be changed because the pixels chosen from bin_2 should not contain those that has been modulated from bin_3. The modification degree of some pixels may be $2M$ if the order is exchanged. I_1 and J_1 are defined as follows:

$$J_1 = \mathrm{c} - \left\lfloor \frac{a}{T} \right\rfloor \tag{3}$$

$$I_1 = \begin{cases} T \cdot J_1 & if \ \ \mathrm{b} \geq T \cdot J_1 \\ b & else \end{cases} \tag{4}$$

The verification is as follows:

$$a' = a + I_1 = a + T\left(\mathrm{c} - \left\lfloor \frac{a}{T} \right\rfloor\right) = cT \tag{5}$$

$$c' = c - J_1 = c - \left(\mathrm{c} - \left\lfloor \frac{a}{T} \right\rfloor\right) = \frac{a}{T} \tag{6}$$

$$\frac{a'}{c'} = T^2 \frac{\mathrm{c}}{a} > T^2 \cdot \frac{1}{T} = T \tag{7}$$

b. the bit to be embedded is '0';

If $\frac{c}{a} \geq T$, no pixels will be modulated. Otherwise, I_0 pixels in bin_2 are chosen to be modified firstly so as to make them fall into bin_3; then J_0 pixels in bin_1 are chosen to be modified so as to make them fall into bin_2. The order of above two steps cannot be exchanged too for the same reason as mentioned above. I_0 and J_0 are defined as follows:

$$J_0 = a - \left\lfloor \frac{c}{T} \right\rfloor \tag{8}$$

$$I_0 = \begin{cases} T \cdot J_0 & if \ \ \mathrm{b} \geq T \cdot J_0 \\ b & else \end{cases} \tag{9}$$

The verification is as follows:

$$a' = a - J_0 = a - \left(a - \left\lfloor \frac{c}{T} \right\rfloor\right) = \frac{c}{T} \tag{10}$$

$$c' = c + I_0 = c + T\left(a - \left\lfloor \frac{c}{T} \right\rfloor\right) = aT \tag{11}$$

$$\frac{c'}{a'} = T^2 \frac{a}{c} > T^2 \cdot \frac{1}{T} = T \tag{12}$$

Pixel Modulation. In Xiang et al.'s method, to deal with some common image processing attacks like JPEG compression, Gaussian filtering was used before calculating the histogram. In this paper, we divide the image into blocks as statistic units after filtering to achieve better performance in robustness against common image processing attacks. Besides, Xiang et al. chose pixels to be modulated by random selecting. In this paper, we calculate the mean square error (MSE) to represent the smoothness of the block. When pixels need to be selected, we choose those blocks whose MSE are larger based on the texture cover feature of HVS (human visual system) to ensure the visual quality of the watermarked image.

To sum up, we divide the image into blocks and calculate the mean of each block for histogram calculation and the MSE for pixel modulation. When it comes to pixel modulation step, we choose blocks with largest MSE and then modify all the pixels in one block with the same degree.

Suppose the image size is $\mathrm{R} \times \mathrm{C}$ and the block size is $\mathrm{n} \times \mathrm{n}$, the mean and the MSE are calculated as follows where $p = 1,2, \ldots \ldots \frac{\mathrm{R}}{\mathrm{n}}$, $q = 1,2, \ldots \ldots \frac{\mathrm{C}}{\mathrm{n}}$.

$$m(p,q) = \frac{1}{n \times n} \sum_{i=1}^{n} \sum_{j=1}^{n} I(i,j) \tag{13}$$

$$e(p,q) = \sqrt{\frac{1}{n \times n} \sum_{i=1}^{n} \sum_{j=1}^{n} (I(i,j) - m(p,q))} \tag{14}$$

Embedding Algorithm.

Input: image I with size $R \times C$, watermark information $W \epsilon \{0,1\}$ with length L_w

Output: embedded image

Embedding procedure:

1. Divide the input image I into $\mathrm{n} \times \mathrm{n}$ blocks, and calculate the mean $m(p,q)$ and the MSE $e(p,q)$ of each block, where $p = 1,2, \ldots \ldots \frac{\mathrm{R}}{\mathrm{n}}$, $q = 1,2, \ldots \ldots \frac{\mathrm{C}}{\mathrm{n}}$;
2. Calculate the mean $\bar{A}$ of all blocks, and the embedding range $\mathrm{B} = [(1-\lambda)\bar{A}, (1+\lambda)\bar{A}]$ that with length L, where $\mathrm{L} \geq 3L_w$;
3. Divide B into $3L_w$ equal-sized bins. Every consecutive 3 bins fall into one group. Suppose the pixel numbers in each bin are a, b and c respectively, the embedding rules are as follows:

$$\begin{cases} \frac{a}{c} \geq T & if \ \ W(i) = 1 \\ \frac{c}{a} \geq T & if \ \ W(i) = 0 \end{cases} \tag{15}$$

   Where T is a threshold to make a trade-off between visual quality and robustness.
4. According to above subsection *Histogram modification* to modify the histogram shape of each group. When modulating the pixel value, choose blocks with larger MSE.

5. Follow the steps above until all the L_w bits have been embedded to the $3L_w$ bins.

Extracting Algorithm.

Input: watermarked image I_W
Output: extracted watermark information $\mathrm{W}^{'}$
Extracting procedure:

1. Calculate the histogram $H^{'}$, the mean $\bar{A}'$ and the embedding range $B^{'}$ with the same way as embedding algorithm. Divide the range into L_w groups with 3 bins in each group.
2. Suppose the numbers of three bins in the ith group are a', b' and c'. Then the ith bit is:

$$\mathrm{W}^{'}(i) = \begin{cases} 1 & if \ \frac{\mathrm{a}'}{c'} \geq 1 \\ 0 & otherwise \end{cases} \tag{16}$$

3. Follow step 2 until all the bits are extracted.
4. If the extracted sequence is matched with W, the extracting process is completed. Otherwise, keep the best matching sequence as $\mathrm{W}_{temp}^{'}$ and let $\bar{A}' = \bar{A}' + \Delta$ or $\bar{A}' = \bar{A}' - \Delta$ to repeat step 1 until the algorithm has found a best matching sequence $\mathrm{W}^{'}$.

Experiment and Analysis

In this section, the watermark imperceptibility and robustness are tested by using four benchmark grayscale images including Lena, Barbara, Peppers and Baboon. The watermark is a random 20-bits binary sequence.

Imperceptibility. The algorithm parameters in the experiment are as follows: the threshold $\mathrm{T} = 5$, the bin's width $\mathrm{M} = 2$, and the block size $\mathrm{n} = 4$.

The extraction accuracy rates of test images in the experiment are all 100%. And table 1 gives the testing result of PSNR values of four watermarked images. It can reveal the imperceptibility of the proposed watermarking scheme.

Table 1 PSNR values of watermarked images

Test Image	Proposed	Xiang et al.
Lena	43.65dB	49.68dB
Barbara	46.35dB	49.18dB
Peppers	46.08dB	49.17dB
Baboon	39.33dB	41.68dB

The result shows that all watermarked images for testing get an ideal PSNR that is above 35dB and the PSNR of watermarked images is a little lower than Xiang et al.'s method for the reason of block-based modification. But with block selecting method proposed and algorithm parameter adjustment we can assure the visual quality of human eyes. So we can get the conclusion that the watermarked images are perceptibly similar to the original image. Besides, all bits embedded can be extracted exactly when the watermarked image is under no attack. It proves that the algorithm can be used for digital watermarking.

Robustness. In the robustness test, the software Stirmark 4.0 (Petitcolas, 2000) is used to simulate the different attacks on test images. Figures 5-9 show the test results of the proposed scheme and the comparison with Xiang et al.'s method for six different attacks including common image processing and geometric distortions. The result uses BER (bit error rate) to measure the robustness of the algorithm. Detail test contents are as follows:

1. JPEG compression: compression coefficients count from 10 to 100 with interval 10. Results are referenced by Fig 4;
2. Additive noise: coefficients count from 1 to 10 with interval 1. Results are referenced by Fig 5;
3. Rotation: rotation angles count from 3° to 30° with interval 3°. Results are referenced by Fig 6;
4. Scaling: scaling ratios count from 0.6 to 1.5 with interval 0.1. The width and height of images are scaled with the same ratio. Results are referenced by Fig 7;

5. Translation: translate from -5 to 5 along the x-axis with interval 1. Negative numbers represent translating the left while positive numbers represent translating to the right. Results are referenced by Fig 8.

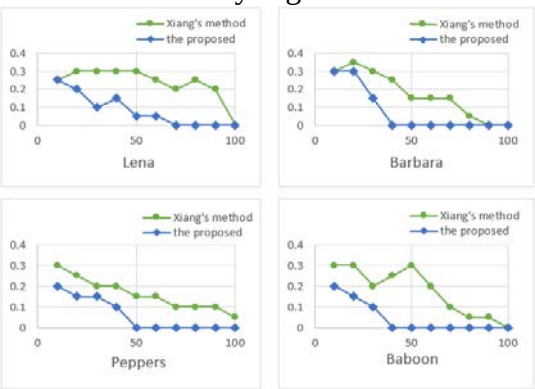

Fig. 4 BER test of images under JPEG compression

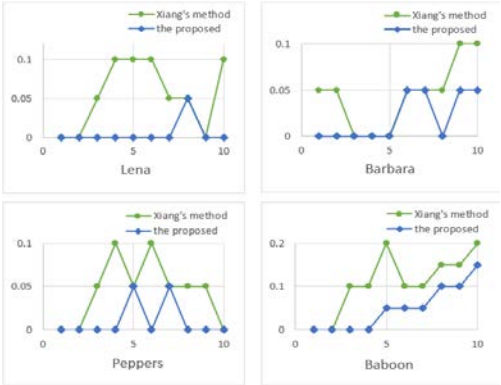

Fig. 5 BER test of images under additive noise

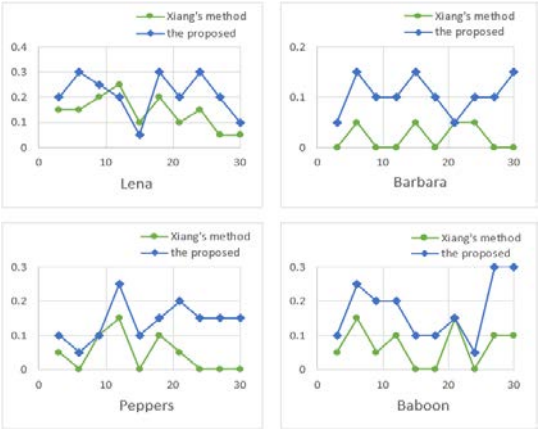

Fig. 6 BER test of images under rotation attacks

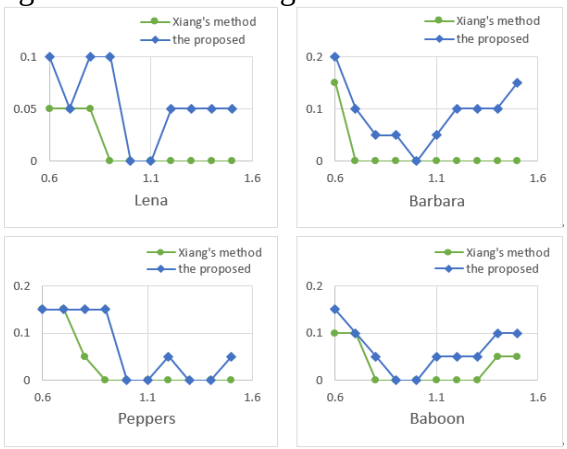

Fig. 7 BER test of images under scaling attacks

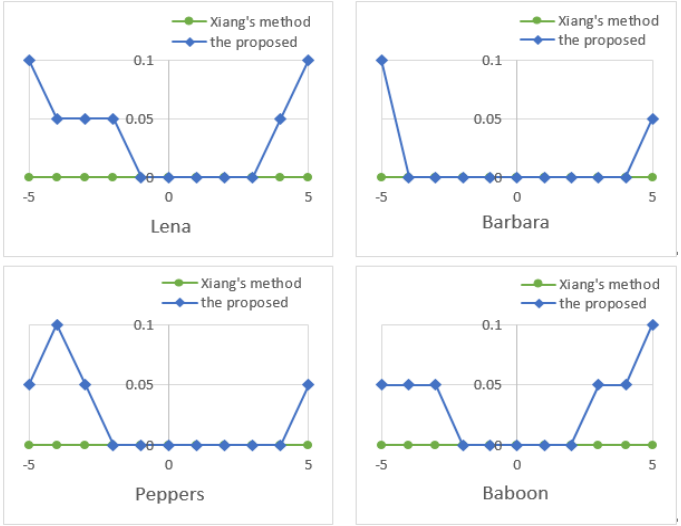

Fig. 8 BER test of images under translation attacks

The experimental result above shows that the algorithm proposed in this paper has a good robustness to geometric attacks as well as common image processing operations. In particular, the robustness to JPEG compression and additive noise attacks is proved to be obviously better than Xiang et al.'s representative watermarking scheme while the BERs of extracted watermarks under rotation and scaling attacks are slightly higher than Xiang et al.'s method for the reason that the block based method has introduced a synchronization issue. However, we can achieve a better trade-off result between traditional signal processing attacks and geometric distortions by adjusting relevant parameters such as the block size n.

Conclusions

In this paper, we propose an image watermarking scheme robust to geometric distortions as well as common image processing operations based on histogram modification. In the proposed scheme, we have presented two optimization methods based on Xiang et al.'s method from histogram modification and pixel modification respectively. The experimental results have proved that the watermarked images get a good visual quality and are resistant to various attacks including geometric distortions and traditional image processing attacks.

Acknowledgment

This research was supported in part by the National Natural Science Foundation of China (Grant Nos. 61170032, and 6173020), and was also supported in part by State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences (Grand No.2015-MS-13).

References

[1] Lichtenauer J F, Setyawan I, Kalker T, et al. Exhaustive geometrical search and the false positive watermark detection probability. Electronic Imaging 2003. International Society for Optics and Photonics, 2003: 203-214.

[2] Pereira S, Pun T. Robust template matching for affine resistant image watermarks. Image Processing, IEEE Transactions on, 2000, 9(6): 1123-1129.

[3] Ruanaidh J J K O, Pun T. Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal processing, 1998, 66(3): 303-317.

[4] Yuan X C, Pun C M, Chen C L P. Geometric invariant watermarking by local Zernike moments of binary image patches. Signal Processing, 2013, 93(7): 2087-2095.

[5] Dong P, Brankov J G, Galatsanos N P, et al. Digital watermarking robust to geometric distortions. Image Processing, IEEE Transactions on, 2005, 14(12): 2140-2150.

[6] Bas P, Chassery J M, Macq B. Geometrically invariant watermarking using feature points. Image Processing, IEEE Transactions on, 2002, 11(9): 1014-1028.

[7] Lee H Y, Kim H, Lee H K. Robust image watermarking using local invariant features. Optical Engineering, 2006, 45(3): 037002-037002-11.

[8] Xiang S, Kim H J, Huang J. Invariant image watermarking based on statistical features in the low-frequency domain. Circuits and Systems for Video Technology, IEEE Transactions on, 2008, 18(6): 777-790.

[9] Deng C, Gao X, Peng H, et al. Histogram modification based robust image watermarking approach. International Journal of Multimedia Intelligence and Security, 2010, 1(2): 153-168.

[10] Fang Z, Zhao Y. Image Watermarking Resisting to Geometrical Attacks Based on Histogram. Intelligent Information Hiding and Multimedia Signal Processing, 2006. IIH-MSP'06. International Conference on. IEEE, 2006: 79-82.

[11] He X, Zhu T, Yang G. A geometrical attack resistant image watermarking algorithm based on histogram modification. Multidimensional Systems and Signal Processing, 2013: 1-16.