Geometrical attack resistant watermarking algorithm using the invariability of the histogram

Song-Chun Pang*, Jong-Pil Sim, Son-Myong Hwang

Faculty of Information Science, Kim Il Sung University, Pyongyang,

Democratic People's Republic of Korea

Abstract: With the rapid development of the Internet, multimedia communication and authorization become more and more important. In order to avoid geometric distortions in watermark embedding, this paper proposes a geometrical attack resistant image watermarking algorithm based on histogram modification. The watermark information is embedded into the original image by modifying the number of the gray samples of the image histogram. One bit of the watermark is embedded by changing the number of samples of the three adjacent grey levels in the histograms and the same watermark repeatedly embedded into each of the four histograms. Watermark detection is an inverse process of watermark embedding. Watermark information is detected based on the relationship of the number of samples of the three successive gray levels. The experimental results show that our algorithm is robust to both geometrical attacks and those conventional signal processing attacks and achieves high detection rate.

Keywords: Image watermarking, histogram, geometrical attack

***Song-Chun Pang,** E-mail: bsc197842@star-co.net.kp

1 Introduction

With the rapid development of multimedia and Internet technology, a great deal of information has become available [1-3]. Meanwhile, they have become the greatest tool for malicious user to attack and pirate the digital media [4-6]. In order to protect copyright and prevent illegal copying, digital watermarking is a potential solution to this issue [7, 8]. Digital Watermarking is a technique that inserts some information into carrier without degrading its quality [9-11].

Image watermarking has gained considerable research. Compared with the common signal processing attacks, geometrical attacks can change the spatial position of pixels and the physical position of watermark [12, 13].

To improve the watermarking algorithm's robustness against the geometrical distortions, some useful methods have already been presented. A DWT–DFT (discrete wavelet transform - discrete Fourier

transform) composite image watermarking algorithm [6] is robust against both affine transformation and JPEG compression, however, the robustness of the watermark against median filtering and random bending needs to be improved.

Some image watermarking algorithms based on histogram have been proposed to improve its performance against geometrical attacks. Geometric invariant watermarking schemes for gray-level images based on histogram in DWT domain [14, 15], using block-based histogram and intensity-level histograms were proposed to resist geometric distortion. These two methods can effectively resist JPEG compression, image cropping, scaling, but their robustness against image rotation is defective.

In order to enhance the secret information security, a reversible blind image watermarking algorithm [7] was proposed that utilized histogram rotation to embed a binary watermark in discrete fractional random transform (DFRT) domain. However, because of the randomness of DFRT, the algorithm is difficult to retrieve the watermark.

For color images, a HSV (Hue, Saturation, Value) image watermarking scheme [16] was proposed. The watermark embedding is based on the histograms of HSV planes.
Although this method can withstand geometric attacks, when the variance of the additive Gaussian noise is more than 0.1, the extracted watermark had severe distortion. An invariant image watermarking scheme [17] utilized the histogram shape and the mean in the Gaussian filtered low-frequency components of images to resist geometric attacks.

Watermark robustness to some geometric attacks is still challenging in the image watermarking research. When an image has undergone geometric attacks, the position of all or some of its pixels may be modified, the number of its pixels may be decreased or increased, and the value of its pixels will be distorted due to interpolation errors during geometric attacks.

Histogram shapes are not only invariant to the scaling, but also resistant to rotation, translation and random bending attacks due to their property to be independent of the position of pixels in the image plane [18]. Consequently, the image watermarking algorithm based on histogram can provide tradeoff between robustness and security.

In this paper, we are going to focus on the image watermarking algorithm robust to geometric attacks and common signal processing manipulations. In general, it is very difficult to make an image watermarking algorithm robust to not only geometric attacks but also common image processing operations. To solve the problem, we propose an image watermarking algorithm based on histogram modification to resist geometric attacks and common signal processing attacks.

A novel watermark embedding rule is established that conceals the watermark in the image by modifying numbers of samples of gray levels of the histogram. First, a fixed gray value range is chosen to embed the watermark and the three consecutive gray levels are divided into a group to embed one bit of

watermark. Next, numbers of sample value of a gray level are modified to the sample value of the neighbor gray level to insert the watermark, the modified histogram is mapped to the watermarked image. Because the embedding rule is reversible, the watermark is easily extracted by judging the relationship of the number of samples of the three consecutive gray levels.

2 Watermarking algorithm based on histogram modification

In general, image histogram shapes are not only invariant to the scaling, but also resistant to geometric attacks such as rotation, translation and random bending due to their property to be independent of the position of pixels. In special, image histogram shapes corresponding to low-frequency components are more resistant to geometric attacks. Therefore, before watermark embedding, the use of Gaussian filter-based preprocessing for extracting the robust feature is necessary [17]. The input image is filtered with a Gaussian low-pass filter for removing the high-frequency information. Suppose that the image has been filtered, we will mainly consider the watermark embedding process.

2.1 Watermark embedding method

2.1.1 Decision of watermark length

In this paper, we adopt the 256 gray-level image histogram. If the original image is color, its color space is converted into gray scale. Gray histogram is one simple but very important statistical feature of an image and it has been commonly used in image processing. Histogram of a gray image can reflect the relationship between the image gray level and the number of pixels in this level. A 256 gray-level image histogram can be represented as

$$H(k) = \{h(k)\}$$

where $h(k)$ represents the number of pixels corresponding to the kth gray level.

In case the image is rotated, only the pixel number of zero intensity value is changed, the pixel number of other pixel value remains basically unchanged, so the statistical curve is essentially coincident with the original histogram. Scaling and shearing attacks reduce the pixel number, the attacked histogram curves are below the curve of original histogram, but the corresponding relationship of the statistical characteristic of histogram keeps mostly unchangeable.

In this paper we use binary sequence as watermark information. The length of the watermark is decided according to the number of sub-image gray level and should be less than the number of gray - levels of the histogram.

In this paper, we use three consecutive gray levels to embed one bit of watermark. Therefore, the range of gray-level value R should not be less than $3L$ in order to embed the whole watermark sequence:

$$L < \frac{R}{3} \qquad (1)$$

The watermark sequence of length L is repeatedly embedded in the 4 sub-images of the original image.

2.1.2 Watermark embedding principle

In general, when some gray values are changed to adjacent gray values in the image, the original image produces very little distortion. Based on this fact, in this paper, the watermark is embedded into the sub-image through modifying the number of samples of the image histogram.

Starting with the minimum gray level of each sub-image, every three consecutive gray levels (bin_1, bin_2 and bin_3) are combined into a group to embed one bit of watermark. Denote the original number of pixels in three consecutive gray levels by *a, b* and *c*, respectively. We can embed one bit of watermark by modifying number of three consecutive gray level samples into a group

$$\begin{cases} \frac{2b}{a+c} \geq V & (w_i = 1) \\ \frac{2b}{a+c} < V & (w_i = 0) \end{cases} \qquad (2)$$

where *V* is a threshold value controlling the number of modified samples. The bigger the *V*, the more the distortion due to the more samples being modified, the stronger the robustness. A desired *V* value is to make a good trade-off between the robustness and imperceptibility. In general, imperceptibility of the watermark expressed with the peak signal-to-noise ratio (PSNR) value is ensured to be over a particular value by adaptively modifying the *V* value. When the watermark bit $w_i = 1$ or $w_i = 0$, the watermarking process is as follows.

When the watermark bit $w_i = 1$ and $\frac{2b}{a+c} \geq V$, no operation is needed. When the watermark bit $w_i = 1$ and $\frac{2b}{a+c} < V$, the numbers of samples in the three consecutive gray level, *a, b* and *c*, are reassigned to satisfy

$$\frac{2b_1}{a_1+c_1} \geq V \qquad (3)$$

where a_1, b_1 and c_1 are the numbers of samples in the three consecutive gray level after changed. To satisfy formula (4), we randomly choose Δ_{12} samples from bin_1 and Δ_{32} samples from bin_3 and move those samples to bin_2 (Fig. 1). After that, the number of samples of bin_1 is $a_1 = a - \Delta_{12}$, that of bin3 is $c_1 = c - \Delta_{32}$ and that of bin2 is $b_1 = b + \Delta_{12} + \Delta_{32}$. Hence,

$$\begin{cases} G_{1,k}^{(1)} = G_{1,k} + 1, & (1 \leq k \leq \Delta_{12}) \\ G_{3,k}^{(1)} = G_{3,k} - 1, & (1 \leq k \leq \Delta_{32}) \end{cases} \qquad (4)$$

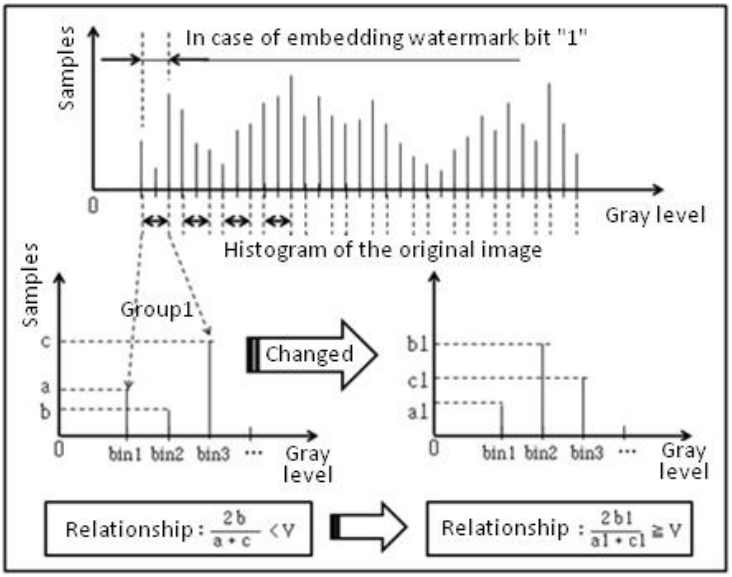

Fig. 1 The numbers of samples changed according to watermark bit "1"

where $G_{1,k}$ and $G_{3,k}$ denote the kth modified sample value in bin1 and bin3, respectively, $G_{1,k}^{(1)}$ and $G_{3,k}^{(1)}$ are the kth modified versions of $G_{1,k}$ and $G_{3,k}$, respectively. Thus, (3) can be expressed as

$$\frac{2(b+\Delta_{12}+\Delta_{32})}{a+c-\Delta_{12}-\Delta_{32}} \geq V \qquad (5)$$

Without loss of generality, let Δ denote the total number of modified samples, from (5) we can easily get

$$\Delta = \Delta_{12} + \Delta_{32} \geq \frac{V(a+c)-2b}{2+V} \qquad (6)$$

The modified number of samples is proportionate to the original number of samples in the bin, that is,

$$\frac{a}{c} = \frac{\Delta_{12}}{\Delta_{32}} \qquad (7)$$

From (7), we have the following deduction,

$$c\Delta_{12} = a\Delta_{32} \Rightarrow c(\Delta_{12} + \Delta_{32}) = (a+c)\Delta_{32} \Rightarrow$$

$$c\Delta = (a+c)\Delta_{32}$$

$$c\Delta_{12} = a\Delta_{32} \Rightarrow (a+c)\Delta_{12} = a(\Delta_{12} + \Delta_{32}) \Rightarrow (a+c)\Delta_{12} = a\Delta$$

Thus, the modified numbers of samples are as follows:

$$\begin{cases} \Delta_{12} = \Delta\frac{a}{a+c} \\ \Delta_{32} = \Delta\frac{c}{a+c} \end{cases} \qquad (8)$$

When the watermark bit $w_i = 0$ and $\frac{2b}{a+c} < V$, no operation is needed. When the watermark bit $w_i = 0$ and $\frac{2b}{a+c} \geq V$, the numbers of samples in the three consecutive gray level, *a, b* and *c*, are reassigned to satisfy

$$\frac{2b_0}{a_0+c_0} < V \qquad (9)$$

where a_0, b_0 and c_0 are the numbers of samples in the three consecutive gray level after changed. To satisfy (9), we randomly choose Δ_{21} and Δ_{23} samples from bin2 to move to bin1 and bin3 (Fig. 2).

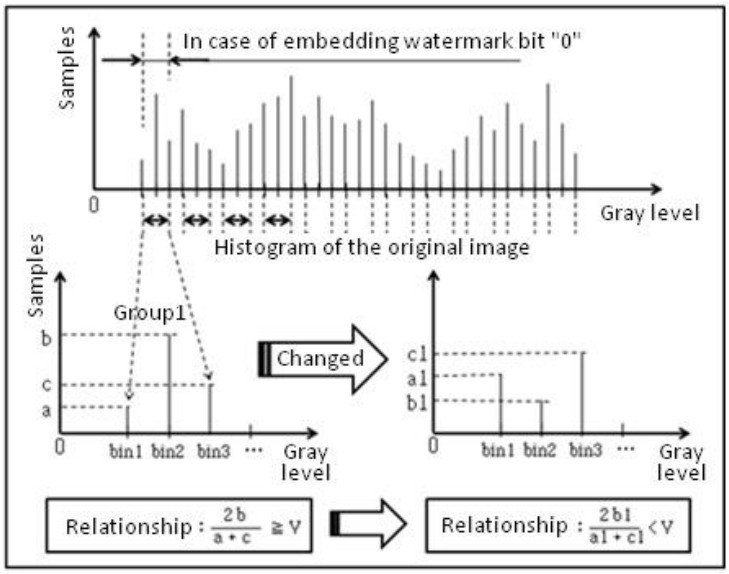

Fig. 2 The numbers of samples changed according to watermark bit "0".

After that, the number of samples of bin1 is $a_0 = a + \Delta_{21}$, that of bin3 is $c_0 = c + \Delta_{23}$ and that of bin2 is $b_0 = b - \Delta_{21} - \Delta_{23}$.

$$\begin{cases} G_{2,i}^{(1)} = G_{2,i} - 1, & (1 \le i \le \Delta_{21}) \\ G_{2,j}^{(1)} = G_{2,j} + 1, & (1 \le j \le \Delta_{23}) \end{cases} \qquad (10)$$

where $G_{2,i}$ and $G_{2,j}$denote the *i*th and the *j* th modified sample value in bin2, $G_{2,i}^{(0)}$and $G_{2,j}^{(0)}$ are the *i*th and the *j* th modified versions of $G_{2,i}$ and $G_{2,j}$, respectively. Thus (9) can be expressed as

$$\frac{a+c+\Delta_{21}+\Delta_{23}}{2(b-\Delta_{21}-\Delta_{23})} \ge V \qquad (11)$$

From (11) we can get the total number Δ of modified samples

$$\Delta = \Delta_{21} + \Delta_{23} \ge \frac{2Vb-(a+c)}{1+2V} \qquad (12)$$

The modified numbers of samples from bin2 are as follows:

$$\begin{cases} \Delta_{21} = \Delta \dfrac{a}{a+c} \\ \Delta_{23} = \Delta \dfrac{c}{a+c} \end{cases} \qquad (13)$$

This process is repeated until the whole watermark sequence is embedded. The modified histogram is the histogram of the watermarked image.

2.2 Watermark extraction method

Since the watermark embedding rule is reversible, the watermark extraction process can be easily implemented.

First, we generate a histogram for watermarked image. Now, let's consider how to detect the watermark from one sub-image. We select the same range $B = [G_m, G_M]$ $(0 < G_m, G_M < 256)$ of gray-level value of the histogram to extract the watermark sequence. In this range, the histogram levels are divided into groups, the three consecutive gray levels as a group.

Next, for each group we can extract one bit of the watermark. Suppose that the numbers of samples in three consecutive gray levels area', b', c', respectively. By computing the ratio between b' and $a' + c'$, one inserted bit is extracted.

$$\begin{cases} \hat{w}_i = 1 & \left(\frac{2b'}{a'+c'} \geq V\right) \\ \hat{w}_i = 0 & \left(\frac{2b'}{a'+c'} < V\right) \end{cases} \tag{14}$$

where $\hat{w}_i$ is the estimate value of the watermark bit. Denote the watermark estimate value sequence extracted from all groups as

$$W' = \left\{\hat{w}_i, \quad i = 1,2,\ldots,L\right\}$$

The process is repeated until all bits ara extracted.

If the detected sequence W' is matched with the embedded sequence W, the searching process is completed.

3 Experimental results

In order to measure distortion and similarity between the original watermark W and the extracted watermark W', the following quality metrics are used: PSNR and normalized cross-correlation (NC).

In the experiments 3 images of size 512×512 and 256 gray levels *woman*, *peppers* and *Lena* were taken as the host images.

In the experiments, important parameter is the threshold V. Watermark imperceptibility is used to measure the distortion amount due to the inserted message.

In the histogram-based watermarking schemes, the distortion is related to the embedding threshold V and the length L of the inserted watermark sequence.

In the experiments, we measure the watermark imperceptibility with the PSNR value. The greater the V, the lower the PSNR value because the more samples are modified. For the watermark image, the PSNR value must be over 40 dB, thus, in general, the range of the threshold V is in [1, 2].

The host images and watermarked images are shown in fig. 3 and fig.4, respectively.

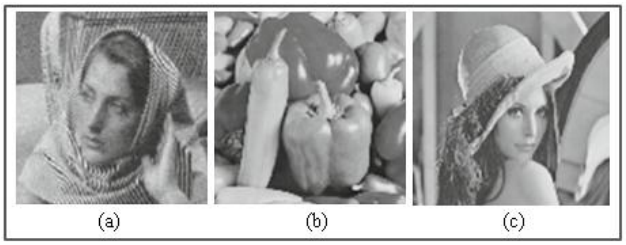

Fig. 3 Original images (a) *woman* (b) *peppers* (c) *Lena*

Under no attacking environment, the PSNR of original and watermarking image of *woman* is 60.25 dB, the PSNR of *peppers* is 60.20 dB, and the PSNR of *Lena* is 60.21 dB.

The results demonstrate that the watermark imperceptibility with the proposed algorithm is excellent. The robustness of the proposed algorithm is tested by applying conventional signal processing operations on thewatermarking images and then retrieving thewatermark.

Table 1 shows the results of watermark extraction after adding different types of noise, filtering and compression process.

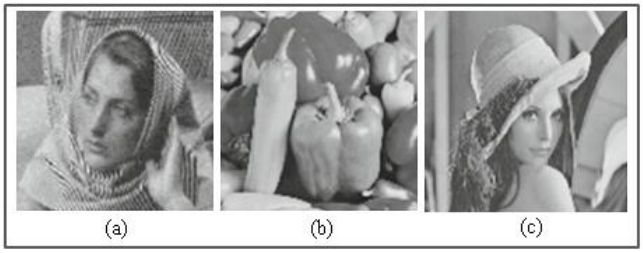

Fig. 4 Watermarked images (a) *woman* (b) *peppers* (c) *Lena*

Table 1 The results of conventional attacks

Attacks	NC		
	Woman	*Peppers*	*Lena*
Gaussian noise $(m = 0, v = 0.01)$	1	1	1
Gaussian noise $(m = 0, v = 0.02)$	1	0.9833	1
Gaussian filter $(m = 0.2, \quad 3 \times 3)$	1	1	1
Gaussian filter $(m = 0.3, \quad 3 \times 3)$	1	1	1
Wiener filter (3×3)	1	0.9906	1
Median filter (3×3)	1	1	1
JPEG(Q=10)	1	1	0.9763
JPEG(Q=30)	0.9621	0.8069	0.8271

As depicted in Table 1, the original images are affected by Gaussian noise with mean *(m)* and variance

(v). Then we have tested the performance of the proposed algorithm after applying filtering process by Gaussian (with mean $m = 0.2$) low-pass, Wiener and median filters using mask of size 3×3. To test the performance of resisting to geometrical attacks, the watermarking images are counterclockwise rotated at an angle, cut a certain proportion from left side, enlarged or reduced, moved their pixels horizontally and vertically, respectively.

Table 2 lists the results of applying rotation, cropping, scaling and translation between the original watermark and the extracted one. From Table 2 we can see that the proposed algorithm is robust to geometrical attacks. Those results demonstrate that our algorithm is robust to geometric attacks as well as general signal processing attacks.

Table 2 The results of geometrical attacks

Attacks	NC		
	Woman	*Peppers*	*Lena*
Rotation 10°	1	1	1
Rotation 20°	1	1	1
Rotation 30°	0.9833	1	1
Crop 1/16	1	1	1
Crop 1/12	1	1	1
Crop 1/8	1	1	1
Scaling by factor 1/16	1	1	1
Scaling by factor 1/8	1	1	1
Scaling by factor 3/2	1	1	1
Translation 10 pixels	1	1	1
Translation 20 pixels	1	1	1
Translation 40 pixels	0.9763	1	0.9833

4 Conclusion

In this paper, we use affine immutability of the histogram to embed and extract the watermark information.

One bit of the watermark is embedded by changing the number of three adjacent grey level sample in the histograms.

The experimental results demonstrate that our algorithm is robust to both geometrical attacks and those conventional signal processing attacks and achieves high detection rate.

In the future research, we will establish new ways so that a longer watermark sequence can be inseted.

References

[1] Ali, H. A. and Khamis, S. A. K. Robust digital image watermarking technique based on histogram analysis, *World of Computer Science and Information Technology Journal* 2(5) 163–168(2012).

[2] Cao, J., and Huang, J. Controllable secure watermarking technique for tradeoff between robustness and security, *IEEE Transactions on Information Forensics and Security* 7(2) 821–826(2012).

[3] Li M, Xiao D, Zhang Y. Attack and Improvement of the Fidelity Preserved Fragile Watermarking of Digital Images, *Arabian Journal for Science and Engineering* 41(3) 941-50(2016).

[4] Coltuc, D. Lowdistortion transform for reversible watermarking, *IEEE Transactions on Image Processing* 21(1) 412–417(2012).

[5] Singh, D., and Singh, S. K. DCT based efficient fragile 526 watermarking scheme for image authentication and restoration, *Multimedia Tools and Applications* 76(1) 953-977(2017).

[6] Y. Yang, Novel Zero. Watermarking Scheme Based on DWT-DCT, *China Communications*, vol 13 no.7 pp. 122-126(2016).

[7] Lee, Y., and Kim, J. Histogram rotation-based image watermarking with reversibility, *Internationa Journal of Security and Its Applications* 6(2) 197–201(2012).

[8] Nguyen TS, Chang CC, Yang XQ. A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain, *AEU-International Journal of Electronics and Communications* 70(8) 1055-61(2016).

[9] Martinez-Noriega, R., and Nakano, M. High payload audio watermarking: toward channel characterization of MP3 compression, *Journal of Information Hiding and Multimedia Signal Processing* 2(2) 91–107(2011).

[10] Pal, K., Ghosh, G., and Bhattacharya, M. Reversible digital image watermarking scheme using bit replacement and majority algorithm technique, *Journal of Intelligent Learning Systems and Applications* 2012(4) 199–206(2012).

[11] B. Behera and V. Govindan, Improved Multimodal Biometric Watermarking in Authentication Systems Based on DCT and Phase Congruency Model, *International Journal of Computer Science and Network* vol. 2 issue 3 pp. 123-129(2013).

[12] Surekha, B. and Swamy, G. N. Sensitive digital image watermarking for copyright protection, *International Journal of Network Security* 15(1) 95–103(2013).

[13] Zhang, X., Wang, S., Qian, Z., and Feng, G. Reference sharing mechanism for watermark selfembedding, *IEEE Transactions on Image Processing* 20(2), 485–495(2011).

[14] Pun, C.-M., and Yuan, X.-C. Geometric invariant digital image watermarking scheme based on histogram in DWT domain, *Journal of Multimedia* 5(5) 434–442(2010).

[15] Pun, C.-M., and Yuan, X.-C. Robust and geometric invariant watermarking scheme using block and gray-level histograms, *International Journal of Digital Content Technology and its Applications* 4(3) 171–183(2010).

[16] Zaghloul, R. I., and Al-Rawashdeh, E. F. HSV Image watermarking scheme based on visual cryptography, World Academy of Science. *Engineering and Technology* 44 482–485(2008).

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

[18] Cheng, Deng., Xinbo, Gao., and Xuelong, Li. Local histogram based geometric invariant image watermarking, *Signal Processing* 90(6) 3256–3264(2010).

.