A Modified Moment-Based Image Watermarking Method Robust to Cropping Attack

Tianrui Zong, Yong Xiang, and Suzan Elbadry
School of Information Technology
Deakin University, Burwood Campus
Melbourne, Australia
Email: {tzong, yxiang, suzan.elbadry}@deakin.edu.au

Saeid Nahavandi
Centre for Intelligent Systems Research
Deakin University, Waurn Ponds Campus
Geelong, Australia
Email: saeid.nahavandi@deakin.edu.au

***Abstract*—Developing a watermarking method that is robust to cropping attack is a challenging task in image watermarking. The moment-based watermarking schemes show good robustness to common signal processing attacks and some geometric attacks but are sensitive to cropping attack. In this paper, we modify the moment-based approach to deal with cropping attack. Firstly, we find the probability density function (pdf) of the pixel value distribution from the original image. Secondly, we reshape and normalize the pdf of the pixel value distribution (PPVD) to form a two dimensional image. Then, the moment invariants are calculated from the PPVD image. Since PPVD is insensitive to cropping, the proposed method is robust to cropping attack. Besides, it also has high robustness against other common attacks. Experimental results demonstrate the effectiveness of the proposed method.**

***Index Terms*—Image watermarking, cropping, moment invariants, probability density function.**

I. Introduction

In recent years, there has been increasing research interest in the protection of digital media concerning intellectual property rights. Digital watermarking is a promising technique to solve this problem. From the technical aspect, digital watermarking aims to embed proprietary data (such as signature, logo, ID number, etc.) into the media object. When necessary, the owners can extract these data to declare their copyright [1]. While digital watermarking can be applied to various multimedia data such as audio [2], [3], image [4]-[9] and video [10], this paper limits its attention to image watermarking.

For image watermarking methods, one of the most important properties is their robustness to common attacks, including signal processing attacks (e.g., compression, filtering and additive noise attacks) and geometrical attacks (e.g., rotation, scaling, cropping, and affine attacks). Compared to signal processing attacks, geometric attacks are more difficult to tackle as they can cause de-synchronization between the watermark embedder and receiver.

Over the last decade, much efforts have been made to develop effective image watermarking methods robust to geometric attacks. These watermarking schemes can be divided into three categories, which are invariant domain-based schemes, template-based schemes and moment-based schemes. The invariant domain-based schemes embed watermarks in invariant domains. In [4], the watermarks are embedded in a domain by using Fourier Mellin transform but this method is difficult to implement. In [5], Zheng *et al.* developed a watermarking scheme using phase correlation spectrum in the invariant domain generated by log-polar map, whose implementation is simple and feasible. However, the methods in [4] and [5] are highly sensitive to cropping and rotation attacks. The template-based schemes embed a template with the watermark sequence [6], [7]. At the detection end, the template in the received image is exploited to estimate the attacks and then the inverse transforms are applied in order to extract the watermark sequence. One of the major drawbacks of the watermarking schemes in [6] and [7] is that the templates can be estimated from the watermarked image and then removed, which will disable these watermarking schemes. The moment-based schemes utilize the statistical property of an image. By exploiting the affine geometric moment invariants, Alghoniemy and Tewfik proposed a watermarking scheme which modifies the moment invariants into a predefined interval [8]. This scheme is robust to rotation and scaling. In [9], the orthogonal Legendre moment invariant was employed to cope with affine attacks. However, the moment-based schemes are highly vulnerable to cropping attack. Specifically, the moment invariants can be badly distorted if part of the image is cut because the moment invariants are extracted from all pixels. In summary, all of the above-mentioned watermarking schemes are unable to cope with cropping attack.

Cropping is a common geometric attack. By cutting some part of the image, the synchronization between the transmitter and the receiver can be destroyed without degrading the perceptual quality significantly. Moreover, with some image processing tools, cropping can be easily operated nowadays even by a person who does not have much knowledge about image watermarking. In this paper, we propose a moment-based image watermarking method to tackle cropping attack. In the proposed method, we first obtain the probability density function (pdf) of the pixel value distribution of an image. Then, we reshape and normalize the pdf of the pixel value distribution (PPVD) to construct a two dimensional image. Finally, the moment invariants are calculated from the PPVD image for watermark embedding. The proposed method is robust to cropping attack because cropping has little impact on PPVD. It is also robust to other geometric attacks and signal

978-1-4673-6322-8/13/$31.00

processing attacks.

The remainder of the paper is organized as follows. Section II introduces moment invariants. The new image watermarking method is presented in Section III. Experimental results in Section IV show the robustness of the our method against varies attacks. Finally, Section V concludes the paper.

II. Moment Invariants

The $(p+q)$th order geometric moments n_{pq} of a gray scale image $I(x,y)$ are defined as

$$n_{pq} = \int_1^R \int_1^C x^p y^q I(x,y) dxdy \tag{1}$$

where R and C are the number of rows and columns of the image I, respectively. The central moments μ_{pq} can be described as

$$\mu_{pq} = \int_1^R \int_1^C (x-\bar{x})^p (y-\bar{y})^q I(x,y) d(x-\bar{x}) d(y-\bar{y}) \tag{2}$$

where

$$\bar{x} = n_{10}/n_{00} \quad \text{and} \quad \bar{y} = n_{01}/n_{00}. \tag{3}$$

In [11], Hu proposed seven functions invariant to orthogonal transformations, which are

$$\begin{aligned}
\psi_1 &= \mu_{20} + \mu_{02} \\
\psi_2 &= (\mu_{20} - \mu_{20})^2 + 4\mu_{11}^2 \\
\psi_3 &= (\mu_{30} - 3\mu_{12})^2 + (3\mu_{21} - \mu_{03})^2 \\
\psi_4 &= (\mu_{30} + \mu_{12})^2 + (\mu_{21} + \mu_{03})^2 \\
\psi_5 &= (\mu_{30} - 3\mu_{12})(\mu_{30} + \mu_{12}) \\
&\quad \times [(\mu_{30} + \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2] \\
&\quad + (3\mu_{21} - \mu_{03})(\mu_{21} + \mu_{03}) \\
&\quad \times [3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2] \\
\psi_6 &= (\mu_{20} - \mu_{02})[(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2] \\
&\quad + 4\mu_{11}(\mu_{30} + \mu_{12})(\mu_{21} + \mu_{03}) \\
\psi_7 &= (3\mu_{21} - \mu_{03})(\mu_{30} + \mu_{12}) \\
&\quad \times [(\mu_{30} + \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2] \\
&\quad - (\mu_{30} - 3\mu_{12})(\mu_{21} + \mu_{03}) \\
&\quad \times [3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2].
\end{aligned} \tag{4}$$

Table I shows the value of

$$\psi_i^* = |log_{10}\psi_i|, \quad i = 1, 2, \ldots, 7 \tag{5}$$

for the widely used image $Lena$ after common signal processing and geometric attacks. It can be seen from Table I that $\psi_1^*, \psi_2^*, \ldots, \psi_7^*$ are robust against many signal processing and geometric attacks but not robust against cropping attack.

III. Proposed Method

A. PPVD

For an 8-bit gray scale image I, it contains 256 gray levels. For any pixel, its value will be within $[0, 255]$. The pixel value distribution H can be defined as

$$H = \{h(i) | i = 0, 1, \ldots, 255\} \tag{6}$$

where $h(i)$ is the number of pixels whose values are i. Then the PPVD of the image I is described as

$$P = \frac{H}{RC} = \{p(i) | i = 0, 1, \ldots, 255\} \tag{7}$$

where

$$p(i) = \frac{h(i)}{RC}. \tag{8}$$

This means that given the image I, the corresponding PPVD can be obtained using (7) and (8). Fig. 1 shows the PPVDs of the original image $Lena$ and its counterparts after rotation, scaling and cropping attacks, versus different pixel values. We can see from Fig. 1 that these PPVDs curves are almost identical. This means that PPVD is insensitive to these attacks. Next, the special feature of PPVD will be employed to develop a new image watermarking method robust to cropping and other common attacks.

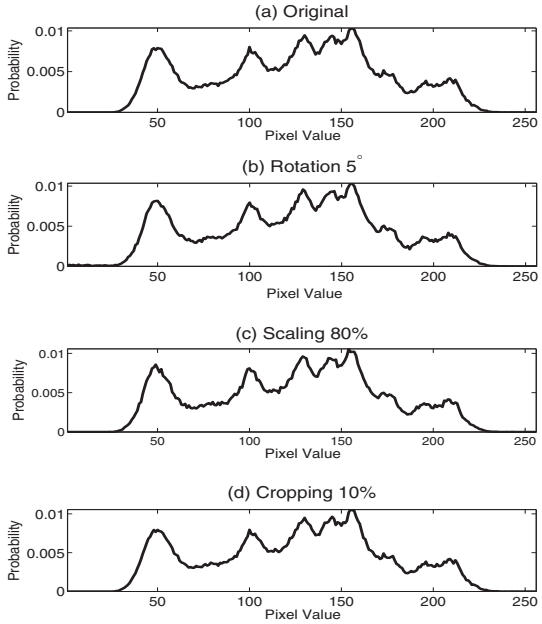

Fig. 1. PPVDs of the image $Lena$ before and after attacks. (a) Original, (b) rotation $5°$, (c) scaling 80%, and (d) cropping 10%.

B. Watermark Embedding

The process of watermark embedding is shown in Fig. 2. Firstly, the 1×256 vector P containing PPVD information is extracted from the original image I by using (7) and (8), followed by reshaping the vector P into a 16×16 matrix. Then, the elements of the matrix are further normalized to

TABLE I
MOMENT INVARIANTS ψ^* FOR IMAGE LENA

Attack	ψ_1^*	ψ_2^*	ψ_3^*	ψ_4^*	ψ_5^*	ψ_6^*	ψ_7^*
Original Image	6.6219	18.8256	27.4747	25.2049	54.6461	34.8360	51.6415
Median Filtering	6.6209	18.8004	27.4167	25.1842	54.3421	34.8023	51.5823
Gaussian Noise	6.6219	18.8279	27.4812	25.2044	54.6279	34.8373	51.6441
Salt & Pepper Noise	6.6218	18.8376	27.4864	25.2189	54.7230	34.8556	51.6682
JPEG 20%	6.6218	18.8269	27.4779	25.2050	54.6851	34.8367	51.6432
Rotation 1°	6.6219	18.8260	27.4781	25.2053	54.6115	34.8365	51.6439
Scaling 50%	6.6219	18.8256	27.4745	25.2049	54.6501	34.8360	51.6415
Scaling 110%	6.6222	18.8349	27.5710	25.2024	54.5427	34.8420	51.6863
Cropping 10%	6.5835	16.9721	24.0447	25.0950	49.7906	33.9937	51.1459

$[0, 255]$ to obtain a PPVD image I_P. After that, we calculate the moment invariants $\psi_1^*, \psi_2^*, \ldots, \psi_7^*$ from the PPVD image I_P using (4) and (5) and construct a function $f(\Psi^*)$ as follows [8]:

$$f(\Psi^*) = \alpha_1\psi_1^* + \alpha_2\psi_2^* + \cdots + \alpha_7\psi_7^* \tag{9}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_7$ are the weight factors determined by a secret key. It has been shown in Table I that for each ψ_i^*, the robustness to varies attacks is different. If there is certain information about the potential attacks, one can adjust the values of $\alpha_1, \alpha_2, \cdots, \alpha_7$ to enhance the robustness against specific attacks. Otherwise, we equally choose the α values by $\alpha_i = \{\frac{1}{7}, i = 1, 2, \ldots, 7\}$, which are used in this paper.

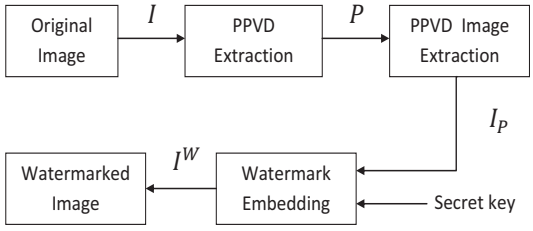

Fig. 2. Process of watermark embedding.

In the embedding process, we will modify P such that $f(\Psi^*)$ equals a predefined value M. We start with taking neighboring S pixel values as a bin to form L bins. In this paper, we choose $S = 8$ as it gives a 52dB peak signal-to-noise ratio (PSNR), ensuring high perceptual quality. The relationship between S and L can be shown as

$$L = \begin{cases} \frac{256}{S}, & \text{if Mod}\left(\frac{256}{S}\right) = 0 \\ \lfloor \frac{256}{S} \rfloor + 1, & \text{otherwise} \end{cases} \tag{10}$$

where Mod$(\cdot)$ is the modulus function and $\lfloor . \rfloor$ is the floor function. Without changing the total probability in one bin, we equalize the probabilities of all pixel values in this bin. Here, we use a simple example to explain the equalization process. Assume that there are two pixel values in a bin, which are PV_1 and PV_2. Denote the probabilities that the pixels in the bin take values PV_1 and PV_2 by a and b, respectively. If $a > b$, the probability of taking value PV_1 is reduced by

$$E_{ab} = \frac{a - b}{2} \tag{11}$$

and the probability of taking value PV_2 is increased by E_{ab}. This modification can be achieved by randomly selecting $E_{ab}RC$ pixels whose value is PV_1 and then change the value of these pixels from PV_1 to PV_2.

Denote the probabilities relating to PV_1 and PV_2 after the modification by a' and b', respectively. Clearly, $a' = a - E_{ab}$ and $b' = b + E_{ab}$. Further, we have

$$\begin{aligned} a' &= a - E_{ab} \\ &= \frac{a + b}{2} \\ &= b + \frac{a - b}{2} \\ &= b + E_{ab} \\ &= b'. \end{aligned} \tag{12}$$

The equation $a' = b'$ means that the number of pixels with value PV_1 is now the same as the number of pixels with value PV_2. This completes the equalization process. If $a < b$, we can equalize the corresponding probabilities in a similar manner.

After the equalization process, we consider two neighboring bins as a group and the group number G is expressed as

$$G = \begin{cases} \frac{L}{2}, & \text{if Mod}\left(\frac{L}{2}\right) = 0 \\ \lfloor \frac{L}{2} \rfloor, & \text{otherwise.} \end{cases} \tag{13}$$

Denote the two bins in a group by Bin_1 and Bin_2, and assume that the pixel values in Bin_1 are smaller than those in Bin_2. Let c and d be the total probabilities of Bin_1 and Bin_2, respectively. If $c > d$, we randomly pick $E_{cd} = \beta \cdot \lfloor \frac{c-d}{S} \rfloor RC$ pixels for each pixel value in Bin_1, and add S to their pixel values to shift the probability to that of Bin_2, where $\beta \in [0, 1]$. If $c < d$, the process will be similar. After this final modification, $f(\Psi^*)$ will be adjusted to M, which is set to be 14.5 in this paper. Note that when $\beta = 0.5$, the last modification is the same as the equalization. The original image $Lena$ and its watermarked version are shown in Fig. 3.

Fig. 3. The image $Lena$ and its watermarked counterpart. (a) Original and (b) watermarked.

C. Watermark Detection

Fig. 4 shows the process of watermark detection. By using the same procedures in Section III-B, we first extract the PPVD information P' from the received image I'. Then the PPVD image I'_P is generated from P'. After that, we calculate the moment invariants $f'(\Psi^*)$ from I'_P with the help of the secret key and obtain the distance between $f'(\Psi^*)$ and M by

$$\varepsilon = |f'(\Psi^*) - M|. \tag{14}$$

If ε is smaller than a predefined threshold T, the watermark can be claimed as detected. Same as other moment-based image watermarking schemes, the proposed watermarking method is a one-bit scheme. Since the original image is not needed at the detection phase, the new watermarking method is blind. The value of ε should be decided by the strength of the possible attacks. In this paper, $\varepsilon = 0.2$ is experimentally determined.

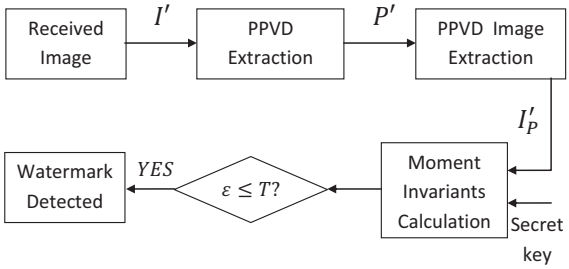

Fig. 4. Process of watermark detection.

IV. Experimental Results

In the experiments, we applied several common attacks to the watermarked $Lena$ image to test the robustness of the proposed watermarking method, in comparison with the method in [9]. The attacks we used include filtering, JPEG compression, noise, rotation, scaling, affine, and cropping attacks. The two affine attacks were generated by MATLAB using two transform matrices

$$\begin{bmatrix} 1.1 & 0.1 \\ 0.2 & 0.8 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -1.2 & 0.4 \\ 0.3 & -0.6 \end{bmatrix}.$$

The experimental results are shown in Table II. From Table II, we can observe that the proposed method is robust to common signal processing and geometric attacks, especially cropping. It is known [8] that traditional moment-based methods are sensitive to cropping attack and they will usually fail if the cropping rate is more than 5%. In contrast, the proposed method still works when the cropping rate has reached 30%. The reason is that PPVD is adopted in the proposed watermarking method. As we have shown before, PPVD is insensitive to cropping.

TABLE II
Robustness of the Proposed Method and the Method in [9] Against Common Attacks

Attack	Proposed Method		Method in [9]
	PSNR 52 dB		PSNR 45 dB
	$\lvert f'(\Psi^*) - 14.5\rvert$	Detection outcome	Detection outcome
Median Filtering	0.0271	Pass	Pass
JPEG 20%	0.0296	Pass	Pass
Gaussian Noise	0.0196	Pass	Pass
Salt & Pepper Noise	0.0630	Pass	Pass
Rotation 45°	0.1135	Pass	Pass
Scaling 80%	0.0618	Pass	Pass
Affine1	0.0604	Pass	Pass
Affine2	0.0433	Pass	Pass
Cropping 10%	0.0852	Pass	Fail
Cropping 20%	0.1330	Pass	Fail
Cropping 30%	0.1784	Pass	Fail

V. Conclusion

Traditional moment-based image watermarking schemes are robust to common signal processing attacks and some geomet-

ric attacks but they are highly vulnerable to cropping attack. In this paper, the moment-based watermarking approach is modified to tackle cropping attack. In the proposed watermarking method, PPVD is first extracted from the original image and then reshaped and normalized to generate a PPVD image. Based on the obtained PPVD image, the invariant moments are calculated and used in watermark embedding and detection. Since PPVD is robust to cropping, the proposed method shows good resistance to cropping, as well as other common signal processing attacks and geometric attacks.

REFERENCES

[1] Y. Xiang, D. Peng, I. Natgunanathan, and W. Zhou, "Effective pseudonoise sequence and decoding function for imperceptibility and robustness enhancement in time-spread echo based audio watermarking," *IEEE Trans. Multimedia*, vol. 13, no. 1, pp. 2–13, Feb. 2011.

[2] I. Natgunanathan, Y. Xiang, Y. Rong, W. Zhou, and S. Guo, "Robust patchwork-based embedding and decoding scheme for digital audio watermarking," *IEEE Trans. Audio, Speech and Language Process.*, vol. 20, no. 8, pp. 2232–2239, Oct. 2012.

[3] Y. Xiang, I. Natgunanathan, D. Peng, W. Zhou, and S. Yu, "A dual-channel time-spread echo method for audio watermarking," *IEEE Trans. Inf. Forensics and Security*, vol. 7, no. 2, pp. 383–392, Apr. 2012.

[4] C. Y. Lin, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767–782, May 2001.

[5] D. Zheng, J. Zhao, and A. El Saddik, "RST-invariant digital image watermarking based on log-polar mapping and phase correlation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 753–765, Aug. 2003.

[6] S. Pereira, J. J. K. O. Ruanaidh, F. Deguillaume, G. Csurka, and T. Pun, "Template based recovery of Fourier-based watermaks using log-polar and log-log maps," in *Proc. Int. Conf. Multimedia Computing Systems, Special Session Multimedia Data Security Watermarking*, Jun. 1999.

[7] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans. Image Process.*, vol. 9, no. 6, pp. 1123–1129, Jun. 2000.

[8] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 145–153, Feb. 2004.

[9] H. Zhang, H. Z. Shu, G. Coatrieux, J. Zhu, Q. M. J. Wu, Y. Zhang, H. Q. Zhu, and L. M. Luo, "Affine legendre moment invariants for image watermarking robust to geometric distortions," *IEEE Trans. Image Process.*, vol. 20, no. 8, pp. 2189–2199, Aug. 2011.

[10] H. Huang, C. Yang, and W. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," *IEEE Trans. Inf. Forensics and Security*, vol. 5, no. 4, pp. 625-637, Dec. 2010.

[11] M. K. Hu, "Visual pattern recognition by moment invariants," in *Proc. IRE*, vol. 49, pp. 1428, Sept. 1961.