A GEOMETRICALLY ROBUST WATERMARKING SCHEME BASED ON SELF-RECOGNITION WATERMARK PATTERN

Hefei Ling, Zhengding Lu, Fuhao Zou, Wugang Yuan

School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, Hubei 430074,China

ABSTRACT

Presently, almost all of the watermarking algorithms resistant to geometric attacks are dependent on the synchronization. In this paper, a geometrically robust watermarking scheme, which is not sensitive to synchronization, is proposed based on self-recognition watermark pattern. The structure of watermark pattern is elaborately designed, which makes the pattern recognized by its structure. Different watermark corresponds to different watermark pattern. The watermark bits can be decoded by recognizing the structures of detected pattern. This method's complexity is very low because no additional work is needed to meet the synchronization requirement and no area partitioning and normalization are needed. Experimental results show that this scheme is not only robust against geometric attacks including rotation, scaling, cropping, aspect ratio changing etc., but also resist numeric processes including Gaussian additive noise, low-pass filtering and lossy compression etc.

1. INTRODUCTION

Although it has been made great progress in the research of robust watermarking recently, how to resist to geometric attacks is still a challenging problem and becomes one of the research focuses in the field of watermarking. Even if a slight geometric modification such as rotation, scaling, translation is added to the watermarked image by attacker, most watermark detectors cannot correctly extract the watermark information. Because the synchronization between the watermark embedder and detector is destroyed by geometric attacks, the watermark detector hardly extracts the watermark[1]. Moreover, the above-mentioned issues will be more serious in the case of multi-bits embedding.

Currently, the watermark schemes resistant to geometric attacks can be roughly categorized as follows: non-blind watermarking scheme[2], synchronization calibration-based watermarking scheme[3, 4], invariant domain-based watermarking scheme[5, 6], local content-based watermark scheme[7, 8]. For resorting to original image in the watermark extraction process, the application of the non-blind watermarking scheme is limited. The watermarking based on synchronization calibration can be divided into exhaustive search based scheme, synchronization template based scheme, auto-correlation based scheme [4]. In the case of synchronization template-based scheme, the synchronization template will decrease the capacity and fidelity [3] and is at the risk of template estimated attack [9]. So do the auto-correlation-based scheme. The invariant geometrical watermark can be classified into invariant domain-based watermarking[5] and invariant moments watermarking [6]. Although being resistant to RST attack, these methods cannot resist to cropping and aspect ratio changing. In addition, the computational complexity is very high because of constructing geometrical invariant domain. The disadvantages of invariant domain-based watermarking schemes are time consuming and sensitive to cropping and aspect ratio changing.

The local content-based watermark considered as the second generation watermarking[7, 8], which usually first extracts robust feature point, and then partitions the image into multi-area using the feature point as the centre, finally the watermark is repeatedly embedding into each area. The merit of this category method is resistant to local cropping, but their computational complexity is very high for the operation of feature point extraction, area partition and normalization. So it is impractical, especially in the application of video watermarking.

The above-mentioned watermarking methods have the same objective: resisting synchronization or recovering the detecting synchronization. It is evident that all geometrical resistant methods depend on synchronization. From other perspective, is there a method without depending on synchronization? In this paper, a geometrically robust watermarking method, which is not sensitive to synchronization, will be proposed based on self-recognition watermark pattern. The structure of watermark pattern is elaborately designed, thus make the pattern recognized by its structure. Different watermark corresponds to different watermark pattern. The watermark bits can be decided by recognizing the structures of detected pattern. Section 2 will introduce this method in detail. Section 3 presents experimental results and analysis. The conclusion is drawn in Section 4.

1-4244-0367-7/06/$20.00 ©2006 IEEE

2. ALGORITHM DESCRIPTION

Generally, for local content-based watermarking algorithms, the area partitioning and normalization processes are needed before watermark embedding and detection, which lowers the computational efficiency. Therefore, the proposed method avoids the area partitioning and normalization processes because it is not sensitive to synchronization. In this method, the structure of watermark pattern is elaborately designed, thus make the pattern easily recognized by its structure in the detector. Multi-bit detected watermark bits are reordered by the distance between the corresponding detected patterns and the feature point. The watermark embedding and detection processes are illustrated in Fig. 1. Firstly, the message is encoded into the watermark pattern constituted by a series of concentric circles. Then the watermark pattern is modulated into a noise pattern using the specific band-pass filter and a private key *K*, and the band-pass filter is specifically designed to make it very sensitive to the noise pattern. Thereafter, the noise pattern is repeatedly added into all the feature-point-depended local image regions. Thus produces the watermarked image. The design of band-pass filter should try to filter most information of the original images and keep the noise pattern unaffected. Moreover, the band-pass filter is dependent on the private key *K*, without which the noise pattern cannot be filtered by the band-pass filter.

The watermark message is assumed as W , for each watermark bit w_n , the corresponding pattern WP_n is defined as:

$$WP_n(r,\theta) = \begin{cases} +1, & (n-1)r_w < r - nt < nr_w \;\&\; w_n = 1 \\ -1, & (n-1)r_w < r - nt < nr_w \;\&\; w_n = 0 \\ 0, & otherwise \end{cases} \qquad (1)$$

where *r* denotes the radius of cirque pattern, θ denotes the angle of points in the cirque pattern, r_w is the width of cirque, *t* is the distance between two neighboring cirques. If multi-bit watermark message is inputted, the multi concentric cirques are arranged from inner to outer. For instance a watermark message is assumed as $\{011001\}$, the watermark pattern shown in Fig.2 is encoded according to (1). The method embedding such watermark pattern has two advantages: One is that the watermark pattern can be embedded anywhere in the image and the watermark detector needn't know the accurate location of watermark, which could lower the algorithm's computational complexity much because no additional steps are needed to acquire the synchronization. Another is the watermark pattern itself can resist common geometric attacks such as rotation, translation and scaling because the structure of pattern and the order relation between two neighboring cirques are invariant to RST attacks.

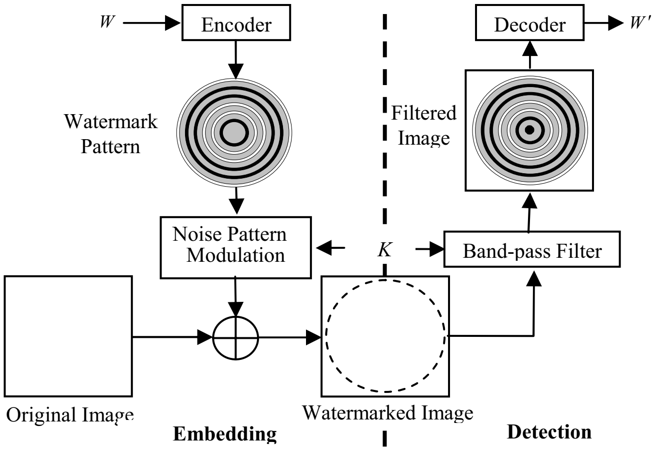

Fig. 1. The watermark embedding and detection processes for local image regions

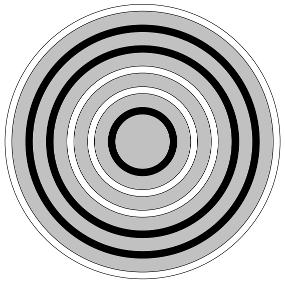

Fig. 2 A watermark pattern instance encoded as $W = \{011001\}$

Thereafter, the encoded watermark pattern is embedded into the local image region using (2), so that:

$$X_w(i,j) = \begin{cases} X(i,j) + \alpha \cdot \left(P_0(x,y \mid K) * WP(u,v)\right), & X(i,j) \in Pattern \\ X(i,j), & Otherwise \end{cases} \qquad (2)$$

where $X_w(i,j)$ denotes the pixels' value of watermarked image in local region, $X(i,j)$ denotes the pixels' value of original image in the same positions, α is the embedding scale factor. $P_0(x,y \mid K)$ is the key-dependent band-pass filter which is used to pick a spatial frequency band where the energy of the original image data is relatively lower compared to the energy of the noise pattern, then the noise pattern is added into the selected band. Considering the properties of the Human Visual System (HVS), if the maximal magnitude allowing modification for each pixel is denoted as $M(x,y)$, (2) should be modified as:

$$X_w(i,j) = \begin{cases} X(i,j) + \alpha \cdot M(x,y) \cdot \left(P_0(x,y \mid K) * WP(u,v)\right), & X(i,j) \in Pattern \\ X(i,j), & Otherwise \end{cases} \qquad (3)$$

The watermark detection process includes three steps: Firstly the watermarked image is filtered using band-pass filter P_1 . Then the concentric cirque pattern is detected using Hough Translation. Finally, the pixels are averaged in each concentric cirque and the detected watermark message is decoded.

The watermarked image is denoted as X_w, band-pass filter in the watermark detector is denoted as P_1, the filtered watermarked image as X_{wf}, so that

$$X_{wf}(i,j) = P_1(x,y \mid K) * X_w(i,j) \tag{4}$$

Substitute the expression (2) of X_w into (4), so that

$$\begin{aligned} X_{wf}(i,j) &= P_1(x,y \mid K) * X(i,j) \\ &\quad + \alpha\left(P_1(x,y \mid K) * P_0(x,y \mid K) * WP(u,v)\right),\ X_{wf}(i,j) \in Pattern \\ &= P_1(x,y \mid K) * X(i,j), \qquad \qquad otherwise \end{aligned} \tag{5}$$

It is obvious that the design of band-pass filter should pick one or more spatial frequency bands where the energy of the original image data is relatively lower compared to the energy of the noise pattern. In order to improve the performance of watermark detector, the band-pass filter P_1 in detector is often constructed as a convolution of a high-pass filter and P_0. The main function of high-pass filter is lessening the affection of host image signal.

Hough Translation is effective for curves detection, and has shown its robustness against any distortion of circle. Therefore, the concentric cirque pattern is detected using Hough Translation, and the pattern parameters can be estimated, thus acquire the spatial distribution position of each cirque. Then the inner and outer mean pixel value of each cirque are computed respectively, if the inner mean value is bigger than the outer mean value, then the detected bit is assigned to ‘1’, else ‘0’.

3. EXPERIMENTS AND DISCUSSION

We test the proposed method to see its performance in terms of watermark’s visual quality impact, capacity and robustness. The standard colorful images including “Lena”, “Bike”, “Bridge”, “Parrot”, “Temple” are used as test images. Their sizes are all equal to 720×512 pixels. The watermark pattern is encoded using (1), where the width of each cirque is set to 5 pixels (i.e., $r_w = 5$) and the distance between two neighboring cirques is set to 10 pixels (i.e., $t = 10$), and the embedding scale factor is set to 0.5 (i.e., $\alpha = 0.5$).

The visual quality can be assessed objectively by measuring the Peak Signal-to-Noise Ratio (PSNR) values of the watermarked image compared to the original image. The PSNR of each watermarked image varies with the embedding watermarks capacity. The experimental results are presented in Fig. 3. It shows the PSNRs decrease as the embedding capacity increases. As the embedding capacity increases to 12 bits, the average PSNR decreases to 37.2dB; As the embedding capacity increases further to be larger than 13 bits, the distortion is quite serious, the average PSNR value is less than 35.3dB.

In practice, watermarked images will be subjected to a variety of distortions before reaching the detector. Watermarks designed to survive legitimate and everyday usage of content, e.g. low-pass filtering, noise and JPEG compression, and all sorts of geometric attacks are referred to as robust watermarks. In order to benchmark the proposed method, we present robustness results for addition of Gaussian noise, low-pass filtering, JPEG compression, geometric distortions. For each class of distortion, the watermarked images were modified with a varying magnitude of distortion and the bit error rate (BER) was then computed. The experimental results are presented in Table. 1. From this table it appears the proposed method is not only robust to geometric attacks including rotation, scaling, cropping, aspect ratio changing etc., but also resists numeric processes including Gaussian noise, low-pass filtering etc. But it seems to be fragile to scaling with too large ratio, Gaussian noise with too large deviation and low-pass filtering with too large width.

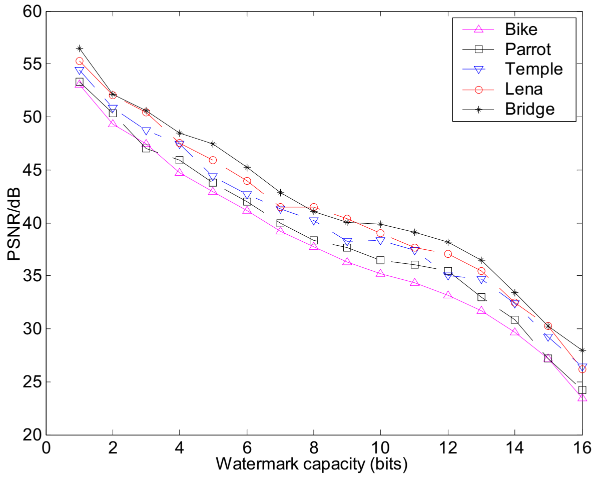

Fig. 3. The PSNR of each watermarked image varies with the embedding watermarks capacity

4. CONCLUSIONS

In our work, a geometrically robust watermarking method, which is not sensitive to synchronization, has been proposed based on self-recognition watermark pattern. We have presented the results of our investigation on the performance of the algorithm in terms of watermark visual quality, capacity and robustness. Based on these experimental results we can make the following conclusions:

This method’s complexity decreases much because no additional work is needed to meet the synchronization requirement and no area partitioning and normalization are needed.

It is robust to geometric attacks including rotation, scaling, cropping, aspect ratio changing and numeric processes including Gaussian additive noise, low-pass filtering, lossy compression.

The results of this work open up a path for future research work. Some of the most important challenges for our future research are as follows. One is how to optimize the watermark detector. Second, the security issues of the system needs to be enhanced. Relying solely on the key used to generate P_0 and P_1 may not be enough to prevent an attacker to use simple detectors to get some indication of the areas where the watermark patch has been embedded.

5. ACKNOWLEDGEMENT

This work is supported by the Natural Science Foundation of China under Grant No. 60502024, the Natural Science Foundation of Hubei Province under Grant No. 2005ABA267, the Electronic Development Fund of Ministry of Information Industry of China and the Innovation Fund for Technology Based Firms of Ministry of Science and Technology of China under Grant No. 04C26214201284.

TABLE I
THE BER VALUE OF WATERMARKED IMAGES AFTER ATTACKS

Attack		BER (%)				
Attack Type	Parameters	Lena	Bike	Bridge	Parrot	Temple
Aspect Ratio Change	4:3 → 16:9	0.5	1.1	0.8	1.2	0.9
	16:9 → 4:3	0.3	0.9	0.7	0.5	0.6
Scaling	50%	1.2	1.4	0.4	0.6	1.0
	75%	0.8	1.0	0.8	0.9	1.4
	150%	5.6	4.3	3.7	5.2	4.8
	200%	22.8	27.3	24.2	18.9	20.6
Rotation	1°	0	0	0	0	0
	2°	0	0	0	0	0
	5°	0	0	0	0	0
	10°	1.8	2.2	0	0.8	0.9
	90°	0.8	0.2	0.5	1.5	0.9
Cropping	50%	3.2	2.6	3.7	2.1	1.5
	25%	1.5	0.8	1.2	0.7	0.4
JPEG Compression	QF=60	0	0	0	0	0
	QF=40	1.8	2.7	1.2	0	0.6
	QF=20	10.4	12.6	12.1	11.7	10.9
Gaussian Noise	$\sigma = 5$	0	0	0	0	0
	$\sigma = 15$	0	0	0	0	0
	$\sigma = 25$	6.3	4.2	3.9	7.5	3.7
	$\sigma = 35$	26.2	28.7	22.6	30.4	24.5
Gaussian Low-pass Filtering	$\sigma_g = 0.5$	0	0	0	0	0
	$\sigma_g = 1.0$	0	0	0	0	0
	$\sigma_g = 1.5$	3.2	2.4	1.5	3.4	2.8
	$\sigma_g = 2.0$	15.6	19.4	20.1	13.2	12.7

Where QF is the quality factor, σ is the standand deviation, σ_g is the width.

5. REFERENCES

[1] Petitcolas, F.A.P., R.J. Anderson, and M.G. Kuhn, "Attacks on copyright marking systems", in *Proceedings of the Second International Workshop on Information Hiding*, SPRINGER-VERLAG BERLIN, Portland, pp. 218-238, 1998.

[2] Cheng, H, "A review of video registration methods for watermark detection in digital cinema applications", in *Proceeding of 2004 IEEE International Symposium on Circuits and Systems*, Institute of Electrical and Electronics Engineers Inc., Piscataway, United States, Vancouver, BC, Canada, pp. 704-707, 2004.

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

[4] Kutter, M, "Watermarking resisting to translation, rotation, and scaling", in *Proceedings of SPIE - Multimedia Systems and Applications*, Society of Photo-Optical Instrumentation Engineers, Bellingham, WA, USA, Boston, MA, USA, pp. 423-431, 1999.

[5] O'Ruanaidh, J. and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking", *Signal Processing*, 1998, 66(3): pp. 303-317.

[6] Xin, Y., S. Liao, and M. Pawlak, "A multibit geometrically robust image watermark based on Zernike moments", in *Proceedings of the 17th International Conference on Pattern Recognition(ICPR'2004)*, Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ 08855-1331, United States, Cambridge, United Kingdom, pp. 861-864, 2004.

[7] Kutter, M., S.K. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking schemes", in *Processing of IEEE International Conference on Image Processing (ICIP'99)*, Institute of Electrical and Electronics Engineers Computer Society, Los Alamitos, CA, USA, Kobe, Jpn, pp. 320-323, 1999.

[8] Tang, C.-W. and H.-M. Hang, "A feature-based robust digital image watermarking scheme", *IEEE Transactions on Signal Processing*, 2003, 51(4): pp. 950-959.

[9] Herrigel, A., S. Voloshynovskiy, and Y. Rytsar, "The watermark template attack", in *Proceedings of SPIE - Security and Watermarking of Multimedia Contents III*, Society of Photo-Optical Instrumentation Engineers, San Jose, CA, pp. 394-405, 2001.