A New RST-Invariant Watermarking Scheme Based on Texture Features

Shipu ZHENG, Yuesheng ZHU, and Xing WANG

The Key Laboratory of Integrated Microsystems, Shenzhen Graduate School

Peking University, Shenzhen, 518055, China. Phone: +86-755-26032316

E-mail: spzheng@sz.pku.edu.cn , zhuys@szpku.edu.cn, wangx@szpku.edu.cn

ABSTRACT

Robustness and imperceptibility are two fundamental criteria for digital watermarking algorithm. In this paper, we present a new RST-invariant (rotation, scaling, and translation) digital image watermarking scheme to embed and detect watermark in DFT domain, which is based on image texture features and the corresponding wedge curves. Experimental evaluations have demonstrated that the proposed scheme performs imperceptibility watermarking of images and the embedded watermark is good resilient to various common geometric attacks.

Keywords LPM, RST-invariance, digital watermarking, texture, standard deviation

1. INTRODUCTION

Digital watermarking is an effective tool to embed intellectual property and other security information to multimedia content, and has potential applications in distribution tracking, digital right management (DRM) of multimedia, and data authentication. Up to now, some progress in the algorithm research of digital watermarking has been achieved. There are two kinds of algorithms available; ones are operated directly by using LSB (least significant bits) substitution in spatial domain [3], [6]. These methods usually have features of small computation and large hidden information, and it can easily utilize the characteristics of HVS (human visual system) to hide watermark data well, but the drawback is with weak robustness. The others are based on the transformation techniques, such as, based on DCT domain [1][5][12][20][22], DFT domain [4][10][11][17], and DWT domain [8][13]-[15] etc. The latter becomes more popular due to the natural framework for incorporating perceptual knowledge into the embedded algorithm with conducive to achieve better perceptual quality and robustness.

With respect to actual applications, watermarking algorithms must fulfill better robustness to counteract various attacks. RST (rotation, scaling, and translation) attacks are considered more challenging than other attacks, because the image size and orientation would be changed after geometrical transformation attacks so that it would be very difficult to detect watermark information right even though subtle and slight changes. Therefore, some RST-invariant digital watermarking schemes have been proposed [2][7][18][19][21][22]. In literature 2, the features, such as the salient corner points, are extracted from the image based on image recognition. These points are used as the vertex and Delaunay tessellation, and then the image is divided into detached triangles based on these points. The watermarks are embedded into the triangles area. The geometrical distortions including the local nonlinear geometrical attacks will not change the alignments and relative positions of these points. However, these feature points are easily attacked with intention. A Radon transform based digital image watermarking algorithm was proposed [19] to withstand a variety of attacks including common geometric attacks, in which the RIT (Radial Integration Transform) is independent of scaling, and rotation only results in a shift of the RIT and the CIT (Circular Integration Transform) is independent of rotation and the scale of CIT is consistent with that of image scaled. Fourier Mellin transform (FMT) based watermarking algorithms and its modified algorithm, log-polar mapping (LPM), and can counteract geometric attacks but are difficult to implement and the image fidelity loss is serious [18][21]. Another strategy to detect watermark suffered attacks is template-identification methods presented in [9][16], the template functions lie in rectifying distortion of image after attacks and inverting them to the initial location, and then detect watermark. But these schemes are vulnerable to the template-attacked which makes difficulties locate initial location of watermark information.

In this paper, we present a new RST invariant watermarking solution in DFT domain, which mainly utilize orientation features of texture image as a mark of image's owner. The following sections are organized as follows. The proposed scheme is described in Section 2. The process of watermark embedding and detection is illustrated in Section 3. Section 4 gives the experimental results and the discussions. Section 5 is the conclusions.

2. THE PROPOSED SCHEME

It is well known, when an image is transformed into Fourier domain, the orientation distribution of its spectrum is relevant to that of texture in spatial domain. Moreover, two directions are upright mutually, e.g. a vertical line, observed from power spectrum in spectrum domain, responses to horizontal stripe texture in spatial domain. Considering watermark-related researches against RST invariant in digital image, we propose a digital image watermarking scheme based on the texture information, and the implementation scheme is shown in Fig.1,

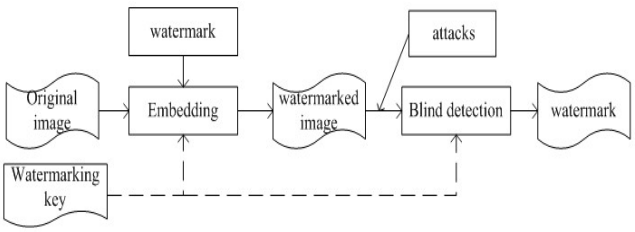

Fig 1. Watermarking scheme

e-Forensics 2008, January 21-23, 2008, Adelaide, Australia.

where watermarking key can control watermark embedding location.

According to texture image theory, texture features extraction can be achieved in spatial and transformation domain. We use Fourier transformation to implement features extraction. In order to present the solution simply and clearly, we use digital gray image to illustrate our new RST invariant watermarking, since it's easier to extend this scheme from gray image to colorful image and even video application. It's assumed that pixel gray of image at location (x, y) is $f(x, y)$, and its Fourier transformation is

$$F(u,v)=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)\exp[-2\pi i(\frac{u}{M}m+\frac{v}{N}n)] \quad , \quad (1)$$

with $u = 0,1,\cdots,M-1$ and $v = 0,1,\cdots,N-1$. The Power spectrum can be written as

$$\left|F(u,v)\right|^2 = F(u,v)F^*(u,v), \quad (2)$$

where $F^*(u,v)$ is conjugate value of Fourier transformation, since features of texture image are easier to be distilled in log-polar coordinate spectrum, so we can perform transformation from Cartesian plane to log-polar plane. Power distribution of image, along with angle θ, can be obtained from the Equ. 2 as follows

$$P(\theta)=\int_0^{+\infty}\left|F(u,v)\right|^2 dr \, . \quad (3)$$

and described it in discrete form as

$$P(\theta_i)=2\sum_{r=0}^{r_n}\left|F(u,v)\right|^2 \quad i=1,2,\cdots,n \quad . \quad (4)$$

$P(\theta_i)$ portrays wedge features and it makes up of a fan-shape in log-polar plane, the fan-shaped angle interval equals $\theta_{i+1}-\theta_i=\pi/n$.

As an example, we choose image Mandrill (512×512 pixels) as the original test image, shown in Fig.2 (a); Meanwhile, the watermark image is obtained with a two-dimensional discrete-space sinusoid, whose function form can be written as

$$\sin[2\pi(\frac{u}{M}m+\frac{v}{N}n)] \, . \quad (5)$$

Fig.2 (b) depicts a discrete-space sinusoid of dimensions 512× 512, that is M=N=512 and oscillating frequency with u=v=10. It has clear texture with special orientation. Fig.2 (c) and (d) present wedge features of the corresponding images power spectrum with internal texture distribution, respectively. Where x axis is angle degree from 0 to 180. From $P(\theta)$ curve of watermark texture image originated by two-dimensional discrete-space sinusoidal in Fig.2 (d), it is found that has sharp orientation characteristic located at 135 degree nearby. Observed from Fig.2 (b), it's consistent with rule that texture orientation is upright with power spectrum, i.e. the oscillation orientation with 45 degree in Fig.2 (b) has shifted 90 degree compared to Fig.2 (d). However, $P(\theta)$ in Fig.2 (c) shows that wedge features curve look like more random, it shows that main texture features of the mandrill image focus on 90 degree nearby. There are different wedge feature curves for various images. So we firstly should do image analysis when watermark embedding is performed in order to avoid the embedding watermark texture orientation superposing with that of hostage image. If texture features of watermark can be properly embedded into a given host image, meanwhile, it can't be removed lightly and still be easily detected after worse geometric attacks including others common attacks. This scheme will be available to achieve the goal against RST attacks efficiently.

3. EMBEDDING AND DETECTION OF WATERMARK

3.1 Watermark Embedding

The proposed watermarking scheme performs the watermark embedding in the following steps, and it's depicted in Fig.3 (a).

1) DFT of original image and watermark image is computed. The original image is given randomly, but it's compulsory that watermark with peculiar texture features is chosen properly, so that there is a good orientation distribution in wedge feature curve of power spectrum.

2) After a power spectrum of original image and watermark is obtained by DFT, we generate a man-made amplitude spectrum to find a watermark image with good texture orientation features according to amplitude spectrum feature of host image.

3) The watermark W_i is inserted in the DFT domain of image by setting the amplitude spectrum X_i in original image to X'_i, and the formula can be written as

$$X'_i = X_i + \alpha W_i \, , \quad (6)$$

where α is a scalar factor and it controls the watermark's embedded strength.

4) After finishing watermark embedded in amplitude frequency domain, then inverting the DFT, we keep phase information of original image unchanged, and reproduce new image with watermark.

3.2 Watermark Detection

Fig.3 (b) presents the detection steps of watermark, and this process can be conducted as follows:

1) The watermarked image with suffered attacks is transformed by DFT. Then referring to the approach of wedge spectrum in Section 2, we can get the wedge features distribution figures.

2) The standard deviation of point around the embedded watermark location is computed and given in Table 1 and 2 with various attacks. For only rotation attack or other attacks with rotation attack, as it has been pointed out in Section 2, the wedge orientation features of image in frequency domain are orthogonal to image's texture orientation in spatial domain. We do proper rectification to make it available to find out the location of special watermark information [16]. Rectification is also called as re-synchronization; one way of re-synchronization is to embed a template, which can be easily detected when watermarked image suffers the rotation-included attack, into the host image. Except for rotation-included attack, it's unnecessary to do re-synchronization for other geometric attacks, because the

orientation features of texture image keep unchanged in despite of scaling, translation, crop attack etc.

Table 1 Standard deviation of original and watermarked image

No-attack/ α	Standard deviation	No-attack/ α	Standard deviation
Original image/0	340.5709	Watermarked image/0.6	7.2871e+3

Table 2 Standard deviation under different Attacks/Level with $\alpha = 0.6$

Attacks/Level	Standard deviation	Attacks/Level	Standard deviation
Rotation/ 5°	3.9875e+3	Crop/[61 61 431 431]	3.0822e+3
Rotation/ 10°	4.0481e+3	Crop/[32 32 385 385]	2.0635e+3
Rotation/ 15°	4.0239e+3	Crop/[1 1 351 351]	1.8650e+3
Scaling/0.7	1.0781e+4	Pepper noise/0.05	3.5095e+3
Scaling/0.9	9.0174e+3	Pepper noise/0.07	9.2155e+3
Scaling/1.2	2.0343e+4	Pepper noise/0.10	9.0920e+3

(Crop [x1 y1 x2 y2] means the image pixel's location when crop)

3) Comparing the standard deviation of the watermarked image that suffered attacks with that of the original image, if their difference exceeds certain threshold, it's confirmed that image content surely belong to special owner. Observing from the wedge feature curve, if watermark information is embedded at the location with angle θ_i (θ_i ranges from 0 to 180 degree), then we can compute the standard deviation of θ_i nearby. We take three points ($P(\theta_{i-1}), P(\theta_i), P(\theta_{i+1})$) and apply them to the standard deviation evaluation at each embedded location as follows:

$$S = \sqrt{\frac{1}{3}\sum_{n=i-1}^{i+1}[p(\theta_n) - \overline{p(\theta)}]^2}\ , \qquad (7)$$

where $\overline{p(\theta)} = \frac{1}{3}\sum_{n=i-1}^{i+1} p(\theta_n)$ and n is the number of elements.

4. EXPERIMENTS AND RESULTS

In order to verify robustness of our new scheme based on texture information, we design various scenarios for testing under the condition of guaranteeing imperceptibility quality. Our first goal is to check the robustness of our new scheme against rotation, scaling, crop with different geometric attacks levels. Moreover, we have also tested an attack under common pepper noise situation; all these experiments show that our proposed scheme performs well against attacks listed above.

We choose the Mandrill as the original image shown in Fig.2 (a). The wedge feature curve $P(\theta)$ of watermark image is similar with that of Fig.2 (d), but we add the other orientation feature information into watermark image, so the final watermarked image is shown in Fig.4 (a). The embedded strength α is 0.6. Compared with original image, the imperceptibility of watermarked image is good, and it's difficult to discern the differences of two images with eyes, so the scheme proposed in Section 2 finely satisfies the requirements that quality of original image does not incur to degradation after it watermarked. The corresponding wedge feature curve $P(\theta)$ is shown in Fig.4 (b). The differences between original image's wedge feature curve and that of watermarked image lie in that there appear two sharp pulses at 45 and 135 degree, which means the watermark information with owner rights and interests, i.e. intellectual property.

A primary factor of a RST invariant watermarking scheme is that watermark information can be detected easily after geometric attacks. Fig.5 (e)-(h) intuitively shows the watermark detection results under different attacks respectively, these results are gotten with the same embedded strength $\alpha = 0.6$. It can be found that all curves of wedge features happen to part changes at some extent. The curves under rotation-attack and crop-attack change more serious than that of resize-attack and noise-attack. The noise-attack's effect on wedge feature curve is most slight. It denotes that the scheme performs well against common noise-attack. Moreover, we can approximately evaluate the possibility if there is watermark information and detect watermark more accurate.

With the corresponding standard deviations under various parameters are listed in the Table 1 and 2, two groups of test results shown in Fig.5. For the rotation attack, we assume that corresponding geometric rectification have been done before standard deviation computed, i.e. make corresponding angle shift in wedge features curve. From the values in Table 1 and 2, the original image's value is much less than that of watermarked image and image suffered attacks. However, both standard deviations of watermarked and attacked images are very close, this means that watermark information after suffered different attacks keeps perfect yet relatively, and can be detected correctly. So it's very good resilience to distortion incurred by geometric attacks.

To illustrate our watermark detection approach more clearly, Fig.6 presents the threshold detection curve which is plotted referenced to the data of Table 1 and 2 which are gotten by using logarithmic transformation, *S* is the standard deviation. We can also set proper threshold to determine whether watermark appears or not. In Our results shown in Fig.6 the threshold is set between 6 and 7.

5. CONCLUSIONS

A novel RST invariant digital image watermarking scheme is presented in this paper. Utilizing mainly the pattern recognition theory of image processing, we embed and detect watermark information by changing the image texture features in DFT domain. The experimental results have illustrated that watermark detection is resilient to geometric attacks, such as rotation, crop, scaling etc. and noise attacks and has good imperceptibility quality.

6. ACKNOWLEDGEMENTS

This work was supported by National Key Technology R&D Program of China under Grant No.2006BAH02A10 and by Science and Technology Program of Shenzhen Nanshan District under Grant No.2006083.

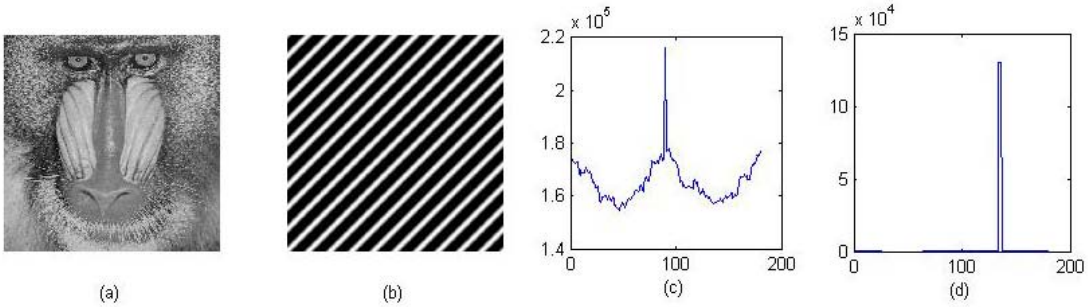

Fig 2. The corresponding wedge features curve of hostage and watermark image (a) host image (b) two-dimensional discrete-space sinusoidal (c) $P(\theta)$ curve of host image (d) $P(\theta)$ curve of watermark image.

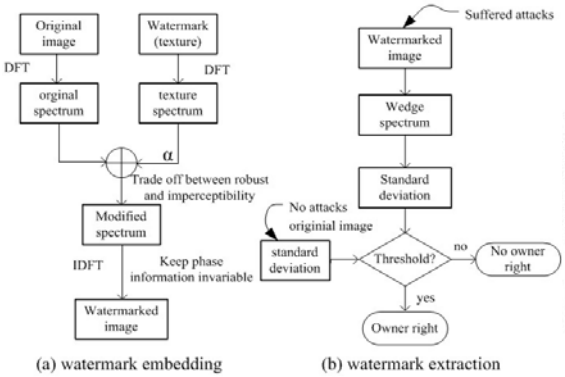

Fig 3. Schematic diagram of embedded and extracted watermark.

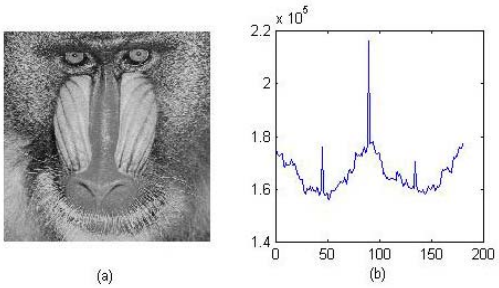

Fig 4. (a) Watermarked image and (b) wedge feature curve of watermarked image.

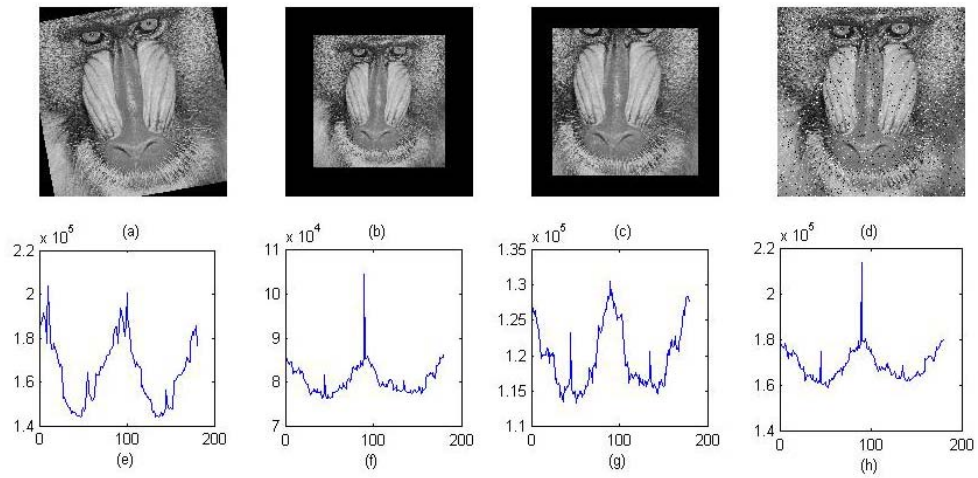

Fig 5. (a) Rotation-attacked image (b) resize-attacked image (c) crop-attacked image (d) pepper noise-attacked image (e) wedge feature curve after rotation-attack (f) wedge feature curve after scale-attack (g) wedge feature curve after crop-attack (h) Wedge feature curve after noise-attack.

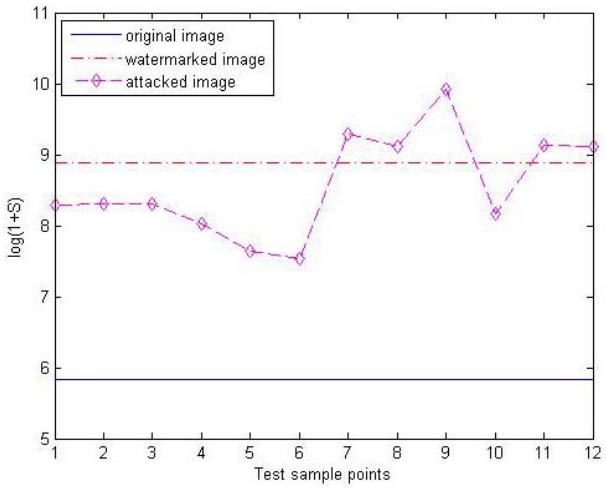

Fig 6. Watermark threshold detection

7. REFERENCES

[1] Alturki, F. and R. Mersereau. Robust oblivious digital watermarking using image transform phase modulation. 2000.

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

[3] Celik, M.U., et al., Lossless generalized-LSB data embedding. IEEE Transactions on Image Processing, 2005. 14(2): p. 253-266.

[4] Chi-Man, P. A Novel DFT-based Digital Watermarking System for Images. 2006.

[5] Cho, J.S., et al. Enhancement of robustness of image watermarks embedding into colored image, based on WT and DCT. 2000.

[6] Cvejic, N. and T. Seppanen, Increasing robustness of LSB audio steganography by reduced distortion LSB coding. Journal of Universal Computer Science, 2005. 11(1): p. 56-65.

[7] Dong, Z., L. Yan, and Z. Jiying. A Survey of RST Invariant Image Watermarking Algorithms. In Electrical and Computer Engineering, 2006. CCECE '06. Canadian Conference on. 2006.

[8] Emek, S. and M. Pazarci, Additive vs. image dependent DWT-DCT based watermarking, in Multimedia Content Representation, Classification and Security. 2006. p. 98-105.

[9] Herrigel, A., et al., Secure copyright protection techniques for digital images, in Information Hiding. 1998. p. 169-+.

[10] Kim, B.-S., et al., Robust digital image watermarking method against geometrical attacks. Real-Time Imaging, 2003. 9(2): p. 139-149.

[11] Kitamura, I., S. Kanai, and T. Kishinami. Copyright protection of vector map using digital watermarking method based on discrete Fourier transform. 2001.

[12] Langelaar, G.C. and R.L. Lagendijk, Optimal differential energy watermarking of DCT encoded images and video. Image Processing, IEEE Transactions on, 2001. 10(1): p. 148-158.

[13] Lou, D.C., J.M. Shieh, and H.X. Tso, A robust buyer-seller watermarking scheme based on DWT. International Journal of Pattern Recognition and Artificial Intelligence, 2006. 20(1): p. 79-90.

[14] Moon, H.S., M.H. Sohn, and D.S. Jang, DWT-based image watermarking for copyright protection, in Artificial Intelligence and Simulation. 2004. p. 490-497.

[15] Ni, J.Q., et al., A RST-invariant robust DWT-HMM watermarking algorithm incorporating Zernike moments and template, in Knowledge-Based Intelligent Information and Engineering Systems, Pt 1, Proceedings. 2005. p. 1233-1239.

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

[17] Qiang, C. and T.S. Huang. Optimum detection and decoding of multiplicative watermarks in DFT domain. 2002.

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

[19] Simitopoulos, D., D.E. Koutsonanos, and M.G. Strintzis, Robust image watermarking based on generalized Radon transformations. Circuits and Systems for Video Technology, IEEE Transactions on, 2003. 13(8): p. 732-745.

[20] Yi-Chong, Z., P. Soo-Chang, and D. Jian-Jiun. DCT-Based Image Protection using Dual-Domain Bi-Watermarking Algorithm. 2006.

[21] Zheng, D., J. Zhao, and A. El Saddik, RST-invariant digital image watermarking based on log-polar mapping and phase correlation. Circuits and Systems for Video Technology, IEEE Transactions on, 2003. 13(8): p. 753-765.

[22] Cox, I. J, et al. Secure spread spectrum watermarking for multimedia. Image Processing, IEEE Transactions on, 1997.6(12) p.1673-1687.