IMPROVED AFFINE RESISTANT WATERMARKING BY USING ROBUST TEMPLATES

Xiaojun Qi and Ji Qi

Computer Science Department
Utah State University
Logan, UT 84322
Xiaojun.Qi@usu.edu and jiqi@cc.usu.edu

ABSTRACT

This paper proposes an improved affine resistant watermarking over the template matching-based watermarking method. A one-way hash function is utilized to generate the highly secure embedding positions in the mid-frequencies against position attacks. A spread spectrum watermark is embedded into these positions in the frequency domain based on the local perceptual capability. Two structural template lines are then added in the polar coordinate system for detecting any combination of the geometrical distortions. The watermark is detected based on the correlation between the recovered and embedded watermarks. The experimental results demonstrate the robustness of the method against some common image processing operations such as JPEG compression, enhancement, and any combination of the geometrical distortions.

1. INTRODUCTION

The common frequency-based watermarking techniques include Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT). They are robust to attacks such as JPEG compression, filtering, and noise addition, yet they lack robustness to geometrical attacks. To solve this problem, two classes of methods have been proposed to exploit the invariant properties of the DFT. They include Fourier-Mellin transform-based Watermarking (FMW), and Template Matching-based Watermarking (TMW).

The FMW methods [1-4] are theoretically robust to geometrical attacks due to the translation-invariant property of the 2D DFT, the scaling-invariant property based on the cyclic shift after applying Log-Polar-Maps (LPM) on the 2D DFT, and the rotation-invariant property based on the cyclic shift after applying another DFT on the LPM. However, generating LPM requires interpolation of neighboring magnitudes with a large dynamic range. As a result, such interpolation is robust under geometrical attacks with a high computational cost. However, the forward conversion from the frequency to LPM domain for embedding a watermark and the inverse conversion from the LPM to frequency domain for detecting a watermark double the chances of the degradation of the image due to the interpolation.

The TMW methods [5, 6] embed a template at certain 2D DFT magnitude as the local peaks for correcting geometrical distortions. A binary message is embedded afterwards. By finding the positions of the template, the geometrical distortion can be corrected and the watermark can be extracted. However, the template can easily disappear under geometrical attacks due to the blurring of the magnitudes by interpolation. As a result, even if the watermark remains, it cannot be extracted.

In this paper, we propose an improved template matching method for affine and compression resistant image watermarking. A one-way hash function is used to generate 1023 highly secure watermark embedding positions in the mid-frequency spectrum. A spread spectrum watermark with the same length is adaptively embedded into these positions in the Fourier domain. Two template lines with special structures are added in the polar coordinate system of the Fourier domain to find the geometrical distortions even under the blurring of the magnitudes by interpolation. The correlation between inserted and recovered watermarks is compared with the empirical threshold for watermark detection once the two template lines are detected. The remaining sections of this paper are organized as follows: Section 2 describes the watermark and template embedding approach and the corresponding detection method. Section 3 shows the experimental results. Section 4 draws conclusions.

2. EMBEDDING METHOD

Our embedding procedure includes two steps. The first step is to embed a watermark. The second step is to embed two special structural templates.

2.1 Watermark Embedding Process

In order to ensure the locations of the watermark are not obvious and resistant to position attacks, we apply a one-way hash function [7] with a secrete key K to generate 1023 (i.e., $2^{10}-1$) highly secure watermark embedding positions in the mid-frequency spectrum between F_1 and F_2. The one-way hash function is chosen because it is easy to compute and difficult to invert. The mid-frequency spectrum is chosen since low-frequency watermark (noise) is usually more noticeable and high-frequency watermark is easily to be eliminated by lossy compression schemes. To ensure the attackers cannot find out the watermark embedding positions by comparing several watermarked copies, different K's are used to generate the embedding positions for different images.

An m-sequence *Watermark* with the length of 1023, which is generated by Linear Feedback Shift Registers (LFSR), is used to decide the change at each embedding position in the Fourier frequency domain. This special spread spectrum is chosen due to its robustness against noise and its capability to achieve error free transmission near or at the limits set by Shannon's noisy channel coding theorem [8]. This m-sequence is converted to a new sequence by mapping 0→-1 and 1→ +1. This newly converted m-sequence is sequentially paired with the embedding positions generated by the one-way hash function. The new magnitude at each embedding position (x_i, y_i) is calculated by:

$$Magnitude \times (1 + \alpha_1 \times Watermark(i)) \quad \text{for } i = 1, ..., 1023 \tag{1}$$

where α_1 is the watermark strength, and *Magnitude* is the original value at $(x_i, y_i)'s$. The watermark strength is empirically set to be 0.1 and is used to calculate the changes at each position to ensure the perceptual fidelity based on the assumption that the large magnitudes are less sensitive to additives than small magnitudes. The changes are also carried out at those positions that are symmetric to the embedding positions due to the symmetric constraints in Fourier domain. The original magnitudes of the DFT image at the embedding positions (i.e., *MagVector(i)*'s) are stored for detection.

2.2 Template Embedding Process

The template contains no information but is merely a tool for recovering possible transformations applied to the image. We introduce special structures into the template which can be exploited during the recovery phase to find a general linear transformation.

We choose two template lines (8 points and 8 symmetric points per line) in the polar coordinate system of the Fourier mid-frequency domain at angles θ_1 and θ_2 with radii varying between F_1=50 and F_2=100. Thirty-two template points are experimentally proven to provide a good balance between visual quality and robustness since more template points introduce more image distortions. The two angles are chosen randomly by a secret key and $|\theta_1 - \theta_2|$ is less than 90º. The template line with a larger angle is referred to as a reference line T_1. The other template line T_2 corresponds to rotate T_1 by $|\theta_1 - \theta_2|$ in a clockwise direction.

Two different structures are applied to these two template lines to make the detection more robust to a variety of the geometrical operations. We only need to generate 8 points per line due to the symmetric property. The 8 points on T_1 are concentric, equal distance points. The distance between the adjacent points is experimentally set to be 10 pixels so the local peaks do not disappear under the blurring of the magnitudes resulted from the geometrical operations. The 8 points on T_2 are uniformly distributed points, whose radii are determined randomly by another secret key.

The strength of the template at each point $(x_i, y_i) = (R_i \sin\theta, R_i \cos\theta)$ is adaptively determined by:

$$LocalMean + \alpha_2 \times std \quad \text{for } i = 1, ..., 8 \tag{2}$$

where *LocalMean* is the average magnitude of the 120 neighborhood pixels of (x_i, y_i), *std* is the standard deviation of the FTed watermarked image, and α_2 is the embedding template strength. We find that a good compromise between visibility and robustness during the decoding yields when α_2 is between 1 and 2. Similar to the watermark embedding process, template points in the high frequencies are inserted less strongly.

3. DETECTION METHOD

Our detection procedure includes two steps. The first step is to detect the two templates. The second step is to detect the watermark if the two templates have been detected.

3.1 Template Detection Process

The algorithm for detecting the two templates is:

1) Calculate the FT of the image.
2) Extract the positions of all local peaks (P_x, P_y). These local peaks satisfy the following condition:
$$Magnitude - LocalMean - k \times Std \geq 0 \tag{3}$$
where *Magnitude* is the value at $(P_x, P_y)'s$; *LocalMean* is the average magnitudes of 120 neighborhood pixels of (P_x, P_y); *Std* is the standard deviation of the FTed image; k is the detection template strength. This template strength, which is initially set as 0.5, is adaptively increased until the number of local peaks is less than an experimental threshold. This threshold is determined based on a compromise between the computational cost and the

possibilities to miss template points for a robust detection.

3) Map the positions of the peaks to polar coordinates.
4) Sort the radii of the peaks in an ascending order to 360 bins, each of which corresponds to an angle of 1º. This sorted information is stored in a look-up table so any integer rotation angle can be detected.
5) For each angle bin, if there are at least 5 peaks that match the radius patterns of one of the two template lines by searching the look-up table, we consider it as a matched line.
6) For all combinations of sets of matched lines, choose two template lines T_1 and T_2 which satisfy the following:
   - The angle difference is $|\theta_1 - \theta_2|$;
   - Template T_2 should be at the direction of clockwisely rotating T_1 by $|\theta_1 - \theta_2|$.
7) If template pairs are detected, proceed to the watermark detection process. Otherwise, we conclude that there is no watermark in the image.

3.2 Watermark Detection Process

Several template pairs may be obtained from the template detection process. For each template pair, the following watermark detection procedure is applied:

1) Restore the image to its original size due to the possible scaling distortions.
2) Calculate the rotation angle θ based on the difference between the original and detected template pairs since the rotation in the spatial domain corresponds to the same rotation in the frequency domain and the DFT is invariant to the translation.
3) Rotate the restored detected image by $|\theta|$ in an inverse direction.
4) Generate the embedding positions and the watermark by using the same one-way hash function and LFSR as utilized in the embedding.
5) For each embedding position (x_i, y_i), determine the value of the recovered watermark by:

$$WM(i) = \frac{Magnitude - MagVector(i)}{\alpha_1 \times MagVector(i)}$$

$$\text{if } WM(i) > 0 \text{ then } \operatorname{Recover}(i) = 1 \qquad (4)$$

$$\text{else } \operatorname{Recover}(i) = -1$$

6) Calculate the similarity score by [9]:

$$Score = \frac{\sum_{i=1}^{m} Watermark(i) \times \operatorname{Recover}(i)}{\sqrt{\sum_{i=1}^{m} \operatorname{Recover}(i) \times \operatorname{Recover}(i)}} \qquad (5)$$

where high score means strong correlation between the recovered and original watermarks. That is, high score indicates a high possibility to have the watermark embedded.

7) The watermark is detected and the detection step is stopped if *Score* > 4, where 4 is an empirically determined threshold for the spread spectrum message detection. Otherwise, apply these 7 steps to another template pair until all the template pairs are tested.

4. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on various standard images and different kinds of attempting attacks. Some of the most significant results are shown in this section.

Watermark invisibility is evaluated on Lena, Peppers, Baboon, and Airplane images. The four original images are presented in Fig.1 (a) and the corresponding watermarked images are shown in Fig.1 (b). The PSNRs of the four watermarked images are 40.02, 39.20, 35.84, and 40.27 db, respectively.

(a) Original images

(b) Watermarked images

Fig. 1: Original and watermarked images

Different kinds of attempting attacks are evaluated. The testing results on JPEG compression at different Quality Factors (QFs) between 10% and 80% are summarized in Fig. 2. The algorithm is successful against JPEG down to a level of 20% quality factor since the corresponding similarity scores are above the threshold for all testing images. The testing results on scaling factors are summarized in Fig. 3. The watermark is successfully detected in the range 0.7 to 2.5. Table I shows some sample results after the attacks such as translation, rotation, cropping, histogram equalization, and combinations of the geometrical operations, histogram equalization, and cropping. In all the cases, the watermark can be correctly detected except for the histogram equalization operation and the cropping of 50%, where the similarity scores indicated by the upper asteroid are less than the threshold 4. Table II compares the performance of the proposed method with the LPM method [4] in terms of the similarity scores. The TMW [5, 6] methods are not included in the comparison since their implementation details cannot be reproduced and

their results do not show the detailed parameters for each attack. Our experimental results indicate that the watermarks are successfully detected with the larger threshold and similarity scores than the ones in [4].

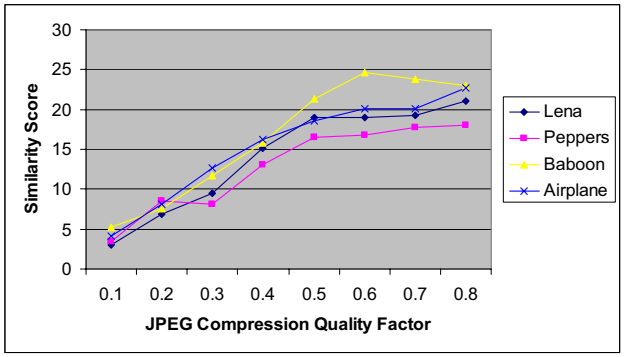

Fig. 2: Robustness against JPEG compression

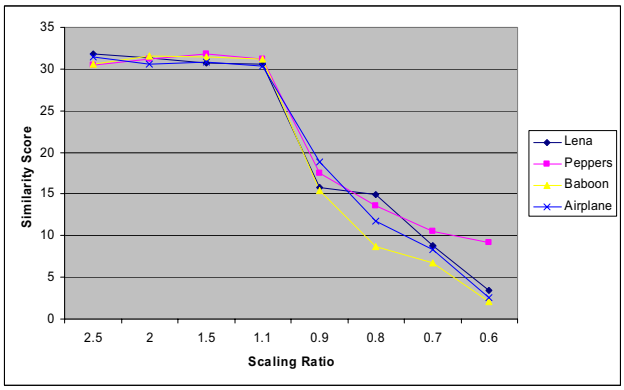

Fig. 3: Robustness against scaling

Table I: Robustness against other attacks

	Similarity Scores			
	Lena	Peppers	Baboon	Airplane
Translation	25.8564	16.1641	19.2907	24.2306
Rotation 13º	13.6004	11.4118	9.1607	13.913
Rotation 46º	10.0987	5.534	7.5975	9.3483
Cropping 0.1	15.4763	6.0342	6.8456	12.2247
Cropping 0.5	6.722	3.9077*	3.0962*	5.8466
Histogram	6.4094	8.4729	3.7023*	8.6605
H+R10º	6.9722	7.1597	5.0337	8.0352
R10º+C 0.1	12.0977	8.4104	8.1597	10.2237
R10º+S(0.9)	9.9111	10.1612	8.8481	11.2242

Table II: Comparison with LPM method [4]

	LPM Method	Our Method
Rotation 10º	~ 4.2	13.6004
Rotation 15º	~ 4.3	11.6619
Compression QF 0.3	~ 3.7	6.9096
Compression QF 0.5	~ 4.2	18.978
Translation 10 pixels	~ 4.3	25.8564
Translation 30 pixels	~ 4.0	25.6688
Scaling 0.5	~ 3.2	10.1312
Scaling 2	~ 5.0	31.6092

4. CONCLUSIONS

In this paper, we propose an improved affine resistant watermarking algorithm over the TMW method [6]. The major improvement consists of:

- A one-way hash function is used to generate 1023 highly secure embedding positions to resist position attacks.
- A spread spectrum with the length of 1023 is embedded at these positions to ensure a large measure of security against unintentional or intentional attacks.
- Two special structures are added to the two template lines to reduce the blurring of the magnitudes by interpolation. These two structures are utilized in the detection procedure to obtain a fast and robust algorithm.
- The correlation between the recovered and embedded message is utilized for detecting the watermark instead of comparing the two messages pairwisely.

The proposed method is robust against a wide variety of tests as indicated in the experimental results. In particular, it is more robust against JPEG compression and any combination of the geometrical distortions than the TMW and FMW methods.

5. REFERENCES

[1] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale, and translation invariant digital image watermarking," *Proceedings of ICIP*, Vol. 1, pp. 536-539, 1997.

[2] J. J. K. O'Ruanaidh and T. Pun, "Rotation, scale, and translation invariant spread spectrum digital image watermarking," *Signal Processing*, Vol. 66, pp. 303-317, 1998.

[3] C. Y. Lin, M. Wu, et. al., "Rotation, scale, and translation resilient watermarking for images," *IEEE Trnas on Image Processing*, Vol. 10, No. 5, pp. 767-782, 2001.

[4] B. S. Kim, J. G. Choi, et. Al., "Robust digital image watermarking method against geometrical attacks," *Real-Time Imaging*, Vol. 9, pp. 139-149, 2003.

[5] S. Pereira, J. J. K. O'Ruanaidh, *et. al.*, "Template based recovery of Fourier-based watermarks using log-polar and log-log map," *Proceedings of ICMCS*, Vol. 1, pp. 870-874, 1999.

[6] S. Pereira and T. Pun, "Robust template matching for affine resistant image watermarks," *IEEE Trans on Image Processing*, Vol. 9, No. 6, pp. 1123-1129, 2000.

[7] M. S. Hwang, C. C. Chang, K. F. Hwang, "A watermarking technique based on one-way hashing functions," *IEEE Transactions on Consumer Electronics*, Vol. 45, No. 2, pp. 286-294, 1999.

[8] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread spectrum communications – A tutorial," *IEEE Trans on Communications*, Vol. 30, No. 5, pp. 855-884, 1982.

[9] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," NEC Research Institute, Technical Report, 95-10.