IMAGE CONTENT-BASED GEOMETRIC TRANSFORMATION RESISTANT WATERMARKING APPROACH

Xiaojun Qi and Ji Qi

xqi@cc.usu.edu and jiqi@cc.usu.edu
Computer Science Department
Utah State University
Logan, UT 84322-4205

ABSTRACT

This paper presents a content-based RST (Rotation, Scaling, and Translation) resistant image copyright protection method. The image content is represented by IFPs (Important Feature Points) obtained by the robust Harris detector-based feature extraction method. These IFPs are further used by the acute triangle matching method to determine the possible geometric attacks for reducing synchronization errors. The spread-spectrum-based blind watermark embedding and retrieval scheme is applied in the DFT (Discrete Fourier Transform) domain of each perceptually highly textured sub-image. The multiplicative scheme is used to embed the blind watermark at highly secure mid-frequency positions generated by one-way hash functions. The watermark detection decision is based on the number of matched bits between the recovered and embedded watermarks in embedding sub-images. Experimental results demonstrate that our algorithm yields good perceptual invisibility, adaptability, and security. It is also more robust to geometric and common image processing attacks than other peer approaches.

1. INTRODUCTION

Digital watermarking is one particular approach to solving copyright protection problems in the digital information world (i.e., audio, video, or images). The watermark is embedded in the original image and then extracted to verify the right of the owner. However, synchronization errors between the extracted and embedded watermarks can be easily magnified by geometric attacks. As a result, several approaches have been developed to counterattack geometric distortions. These approaches can be roughly divided into four categories. 1) Invariant-domain-based watermarking [1, 2]: Embed watermarks and maintain synchronization in a geometric invariant domain. 2) Template-based watermarking [3, 4]: Add additional structured templates in the frequency domain for identifying the geometric transformation and assisting synchronization. 3) Moment-based watermarking [5-7]: Employ geometric moments to normalize the image for maintaining the geometric invariance. 4) Feature-based watermarking [8-11]: Utilize salient region or object features for the recovery of geometric attacks.

In general, feature-based watermark algorithms, which belong to the second generation watermarking, are the best approaches to resisting geometric distortions. Bas et al. [8] use the Harris detector to extract features and Delaunay tessellation to define watermark embedding regions. Kutter et al. [9, 10] use the Mexican hat wavelet to extract features and Voronio diagrams to define watermark embedding regions. Tang and Hang [11] also use the Mexican hat wavelet to extract feature points. Watermarks are embedded in the normalized disks centered at the feature points. However, the robustness of these methods depends on the capacity of the detector to preserve feature points after geometric transformation, especially on images with more texture and images with less texture and large homogeneous areas.

In this paper, we develop a robust second generation watermarking scheme to resist geometric distortions. This scheme combines the advantages of robust feature extraction and acute-triangle-based matching methods to reduce the watermark synchronization errors. Section 2 describes the proposed robust feature extraction method. Section 3 presents the theory of spread-spectrum-based blind watermark embedding and retrieval scheme. Section 4 covers the details of our watermark embedding and detection method. Section 5 shows the experimental results. Section 6 draws conclusions and presents future research directions.

2. ROBUST FEATURE EXTRACTION METHOD

Feature extraction is the most important step in the proposed watermarking scheme. In order to detect watermarks without access to the original image, we look for feature points that are perceptually significant and can

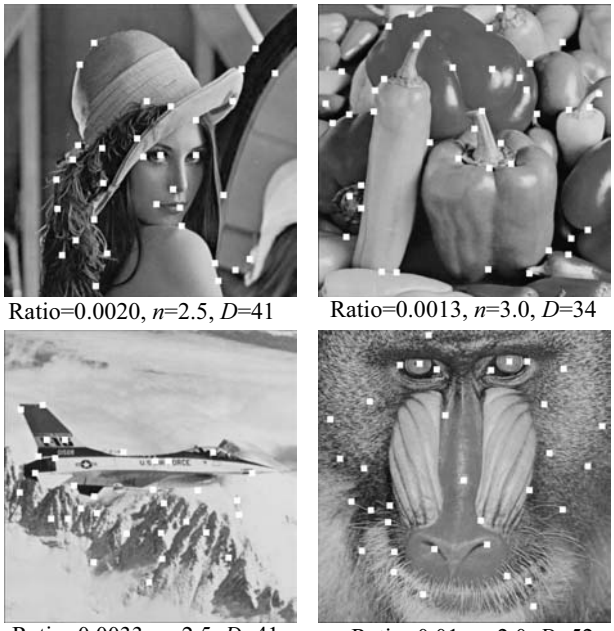
thus resist various types of common signal processing and geometric distortions. These image-content-bounded feature points can be further used as synchronization markers during the detection process. In our scheme, we improve the Harris corner detector [12] to exclusively extract IFPs as follows: 1) Apply a Gaussian low-pass filter to the original image to avoid corners due to image noise. 2) Calculate the corner response image within a circular window to reduce the effect of rotation attacks on the performance of the corner detector. This circular window centers at the image center and covers the largest area of the original image. 3) Apply a Gaussian low-pass filter to the corner response image to achieve the robustness against compression and interpolation. 4) Find the IFPs based on the local maxima within a circular neighborhood centered at each filtered corner response whose value is greater than threshold T.

The diameter of the circular neighborhood is:

$$D=wh/np \quad (1)$$

where integers w and h respectively represent the width and height of the image; integer p is an empirical value for obtaining a reasonable number of feature points for images with large homogeneous areas. It is set to be 2500 in our implementation; and integer n is the window size quantizer, which depends on image textures. It is set as 2, 2.5, 3, and 5 for images with large textured areas, some homogeneous and textured areas, relatively large homogeneous areas, and very large homogeneous areas, respectively. The image texture classification is performed based on the ratio of the IFPs in an image. That is: ratio $\geq$ 0.01→high texture; ratio $\geq$ 0.002→medium texture; ratio $\geq$ 0.0001→low texture; ratio<0.0001→extremely low texture.

We further apply several rotation and scaling attacks on the image to find a group of preserved IFPs. These IFPs are obtained from an intersection operation and are more robust against geometric attacks since they can survive all attacks. Rotation and scaling attacks are selected as the pre-attacks for obtaining the robust IFPs since most IFPs surviving one of the transformations, such as the rotation, scaling, translation, and cropping, can survive the others if they are not cropped. Fig. 1 demonstrates the final preserved robust IFPs by applying our method on four images with different textures. The proposed approach effectively eliminates some unreliable feature points which fail to be detected after certain geometric attacks.



Ratio=0.0020, n=2.5, D=41 Ratio=0.0013, n=3.0, D=34

Ratio=0.0033, n=2.5, D=41 Ratio=0.01, n=2.0, D=52

Fig 1: Robust important feature points

3. BLIND WATERMARK EMBEDDING AND RETRIEVAL

It is desirable to construct a watermark so the detection is independent of the original image. We adopt the blind watermark embedding and retrieval scheme in the DCT (Discrete Cosine Transform) domain [13] in our system. That is, the spread-spectrum-based embedding procedure is modified to be applied in the DFT domain as follows:

$$F\hat{I}_i = FI_i + G \times W_i \times p_i \quad (2)$$

where FI_i is the original sequence (DFT coefficients), $F\hat{I}_i$ is the watermarked sequence, G is the embedding strength, p_i is a bipolar m-sequence, and W_i is the watermark information bit sequence obtained by repeating w_i by a factor s such that $W_i = w_j$ for $js \leq i < (j+1)s$. The factor s is a spread spectrum parameter called spreading factor or chip rate.

The blind retrieval can be achieved by de-spreading the watermarked sequence using the correlation detector. The same embedding m-sequence p_i is now applied to multiply the possibly watermarked sequence.

$$W_i' = p_i F\hat{I}_i \quad (3)$$

The W_i' is further grouped into blocks of size s where each block is computed as:

$$\sum_{i=js}^{(j+1)s-1} p_i F\hat{I}_i = \underbrace{\sum_{i=js}^{(j+1)s-1} p_i FI_i}_{S_1} + \underbrace{G \sum_{i=js}^{(j+1)s-1} p_i^2 W_i}_{S_2} \quad (4)$$

For large values of s, S_2 is usually much larger than S_1, where $S_1 \approx 0$ since FI_i is uncorrelated with p_i. Therefore, the sign of the correlation sum is equivalent to the extracted watermark bit w'_j. That is:

$$w'_j \approx sign\left(G \sum_{i=js}^{(j+1)s-1} p_i^2 W_i \right) \quad (5)$$

4. WATERMARK EMBEDDING AND DETECTION

Fig. 2 illustrates the block diagram of our proposed watermark embedding and detection scheme.

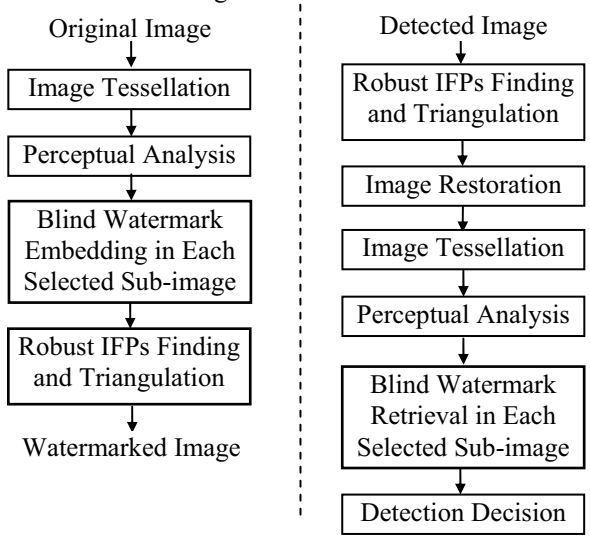


Fig. 2: Watermark embedding and detection scheme

4.1. Watermark embedding method

Each block involved in the watermark embedding process is detailed as follows:

Image Tessellation: Divide the original image into 3x3 non-overlapping sub-images. The last several non-divisible rows and columns are not used for embedding.

Perceptual Analysis: Apply the Harris corner detector to find all possible feature points in the original image by using a 3x3 window. Choose the sub-images with a large number of feature points to be the embedding blocks. These blocks are perceptually highly textured.

Blind Watermark Embedding: The blind retrievable watermark W_i will be embedded into the DFT domain image FI_i of each selected embedding sub-image I_i. The embedding positions are generated in the mid-frequencies in the upper half plane of FI_i using one-way hash functions with two secrete keys [14]. The same changes are also carried out at center-based symmetric positions due to the constraints in the Fourier domain for obtaining a real value image. After embedding, the inverse DFT is applied to obtain the watermark embedded sub-image $I_i^{'}$, which replaces the original sub-image I_i.

Robust IFPs Finding and Triangulation: Apply our robust feature extraction method to find all possible robust IFPs in the watermarked image. Save all robust IFPs-based acute triangles for the detection procedure.

4.2. Watermark detection method

The watermark detector does not need the original image. The blocks uniquely involved in the watermark detection process are detailed as follows:

Image Restoration: Use the angle degrees and statistics information to perform triangle matching on both saved and detected triangles, which are obtained from the previous block. The matched triangle pairs will be further used to determine the possible transforms that these triangles have undergone. The detailed steps for finding the geometric transforms to align the best matched triangle pair (i.e., the detected and target triangles) are as follows: 1) Calculate the scaling factor by resizing the detected triangle to the same size as the target matched triangle saved in the embedding procedure. 2) Calculate the translation factor by registering one of the vertices of the detected and target matched triangles. 3) Calculate the rotation factor by rotating the detected image centered at the registered vertex to align the other two vertices with the corresponding vertices in the target matched triangle. Since the triangles within the detected image undergo exactly the same geometric transformation as the detected image, the transformation obtained from the triangle matching can be further applied to the detected image to restore it to be aligned with the original image.

Blind Watermark Retrieval: The blind retrieval scheme is applied to each restored perceptually highly textured sub-image to extract watermark bits $w_i^{'}$.

Detection Decision: The number of matched bits between the embedded watermark w and the extracted watermark $w^{'}$ determines whether the detected image contains the watermark. In general, watermark is present in the detected image if $w = w^{'}$ for any embedding sub-image or if the total number of matched bits extracted from any two embedding blocks exceeds T, which is determined based on the false alarm probability:

$$P = \sum_{\substack{k_1=T_1,k_2=T_2 \\ k_1+k_2 \geq T}}^{n} \left(\frac{1}{2}\right)^n \cdot \left(\frac{n!}{k_1!(n-k_1)!}\right)\left(\frac{1}{2}\right)^n \cdot \left(\frac{n!}{k_2!(n-k_2)!}\right) \quad (6)$$

where k_i is the number of matched bits in sub-image i and n is the length of the watermark bit sequence. For instance, if the length of the watermark is 14, choosing T as 24 will lead to false alarm probability of $P = 6.59\times10^{-5}$.

5. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on various images with different textures and different kinds of attempting attacks.

Watermark invisibility is evaluated on images of Lena (L), Peppers (Pe), Plane (Pl), and Baboon (B). The PSNRs of these four watermarked images are 42.74, 43.78, 40.73, and 36.62, respectively. These PSNR

values are all greater than 35.00 db, which is the empirical value for the image without any perceivable degradation.

Simulation results for geometric distortions and common signal processing attacks are shown in Table I. The results of Tang's method [11] applied on three images (Lena, Pepper, and Baboon) are also included in Table I for fair comparison. It is clear that our method outperforms theirs under different geometric distortions in terms of the fraction of correctly detected watermark embedding sub-images (i.e., detection rates). We have also tested on several attacks that Tang's method cannot handle, namely 20 random relatively large rotations and any combination of RST attacks. The watermark has been correctly identified with high detection rates. An example of this combination is listed in the last row of Table I.

Table I: Fraction of correctly detected watermark embedding sub-images under different attacks

	L		Pe		B		Pl
	Ours	Tang	Ours	Tang	Ours	Tang	Ours
R1°+ Cropping	3/3	3/8	3/4	2/4	9/9	3/11	5/6
R5°+ Cropping	3/3	0/8	2/4	0/4	9/9	0/11	5/6
Cropping 0.1	2/3	2/8	3/4	2/4	8/9	2/11	4/6
Linear Transform .(1.007,0.01,0.01,1.012)	3/3	5/8	1/4	1/4	4/9	4/11	2/6
Histogram Eq	3/3	7/8	4/4	1/4	8/9	4/11	6/6
Median 2x2	3/3	1/8	4/4	1/4	9/9	6/11	6/6
Sharpening	3/3	4/8	4/4	4/4	9/9	4/11	6/6
Gaussian Filtering	2/3	5/8	4/4	1/4	9/9	8/11	6/6
JPEG 40	3/3	3/8	4/4	1/4	9/9	5/11	5/6
JPEG30	3/3	2/8	2/4	0/4	9/9	4/11	4/6
Scaling 0.8	3/3	N/A	2/4	N/A	9/9	N/A	4/6
Translation [15,15]	3/3	N/A	4/4	N/A	9/9	N/A	5/6
Translation [0,25]	3/3	N/A	4/4	N/A	7/9	N/A	6/6
Mean 2x2	3/3	N/A	4/4	N/A	9/9	N/A	6/6
R10°+T[0,25] +Scaling0.8	2/3	N/A	1/4	N/A	9/9	N/A	3/6

Our method is further compared with the method in [8]. It can successfully detect the watermarks under all the attacks listed in [8]. Since only simple detection results (yes/no) are shown in [8], we do not include these attacks here due to the page limitation. We have further tested on attacks of lower than 80% scaling on highly textured images and attacks of compression with a quality factor of lower than 40. The watermark has also been correctly identified with high detection rates while the method in [8] failed to detect watermarks under these attacks.

6. CONCLUSIONS AND DISCUSSIONS

In this paper, we propose a novel and effective content-based RST-invariant watermarking approach. The major contributions consist of:

- Improved robust important feature points extraction.
- Image dependent perceptually highly textured sub-image selection for embedding.
- Spread-spectrum-based blind watermark embedding and retrieval in the DFT domain.
- Acute-triangle-based image restoration.

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 the combination of the geometric distortions than other feature-based watermarking techniques. Our approach can be further improved by developing a more reliable feature extraction method under severe geometric distortions and a more efficient and accurate triangle matching method.

7. REFERENCES

[1] J. J. K. O'Ruanaidh and T. Pun, "Rotation, Scale, and Translation Invariant Spread Spectrum Digital Image Watermarking," *Signal Processing*, vol. 66, no. 3, pp. 303-317, 1998.

[2] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, "Rotation, Scale, and Translation Resilient Watermarking for Images," *IEEE Trans on IP*, vol. 10, no. 5, pp. 767-782, May 2001.

[3] S. Pereira and T. Pun, "Robust Template Matching for Affine Resistant Image Watermarks," *IEEE Trans. on IP*, vol. 9, no. 6, pp. 1123-1129, June 2000.

[4] Digimarc Corporation, US patent 5,822,436, Photographic Products and Methods Employing Embedded Information.

[5] M. Alghoniemy and A. H. Tewfik, "Image Watermarking by Moment Invariants," *Proc. IEEE ICIP*, vol. 2, pp. 73-76, 2000.

[6] M. Alghoniemy and A. H. Tewfik, "Geometric Invariance in Image Watermarking," *IEEE Trans. on IP*, vol. 13, no. 2, pp. 145-153, Feb. 2004.

[7] H. S. Kim and H. K. Lee, "Invariant Image Watermark using Zernike Moments," *IEEE Trans. on Circuit and Systems for Video Technology*, vol. 13, no. 8, pp. 766-775, August 2003.

[8] P. Bas, J. M. Chassery, and B. Macq, "Geometrically Invariant Watermarking Using Feature Points," *IEEE Trans. on IP*, vol. 11, no. 9, pp. 1014-1028, Sept. 2002.

[9] S. Bhattacharjee and M. Kutter, "Compression Tolerant Image Authentication," *Proc. IEEE Int. Conf. Image Process*, vol. 1, pp. 435-439, 1998.

[10] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Toward Second Generation Watermarking Schemes," *Proc. IEEE ICIP*, vol. 1, Kobe, Japan, pp. 320-323, 1999.

[11] C. W. Tang and H. M. Hang, "A Feature-Based Robust Digital Image Watermarking Scheme," *IEEE Trans. on Signal Processing*, vol. 51, no. 4, pp. 950-959, April 2003.

[12] C. Harris and M. Stephen, "A Combined Corner and Edge Detector," *Proc. 4th Alvey Vision Conf.*, Manchester, pp. 147-151, 1988.

[13] S. Pranata, Y. L. Guan, and H. C. Chua, "BER Formulation for the Blind Retrieval of MPEG Video Watermark," *Lecture Notes in Computer Science*, vol. 2613, pp. 91 -104, 2003.

[14] M.S.Hwang, C.C.Chang, and K.F.Hwang, "A Watermarking Technique Based on One-Way Hash Functions," *IEEE Trans on IP,* vol. 45, no. 2, pp.286-294, 1999.