A FEATURE-POINT-BASED RST RESISTANT WATERMARKING SCHEME

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

ABSTRACT
This paper presents a feature-point-based rotation, scaling, and translation (RST) resistant digital watermarking scheme. The improved Harris detector locates the robust and important feature points, which are further used by the acute triangle matching to determine the possible geometric attacks for reducing synchronization errors. The human visual system compatible mid-frequency embedding strength is also adaptively determined using the modified modulation transfer function. The blind spread-spectrum-based error correcting coded watermark embedding and retrieval scheme is finally applied to each 8×8 discrete cosine transform (DCT) subblock of the host image. Experimental results demonstrate the proposed system is more robust against geometric and common image processing attacks than other feature-point-based and template-based approaches.

KEY WORDS
Digital watermarking, feature-point-based restoration, human vision system, and rotation, scaling, translation attacks.

1. Introduction

The protection of multimedia information, especially its copyright, has attracted more and more attention during the past few years since the publicly exposed digital information can be easily transferred, copied, and tampered. Identifying the genuine ownership or copyright after the distortions is one of the major challenging issues. Consequently, digital watermarking emerges as one possible and popular solution. This technique generally requires several properties including transparency, robustness, universality, blind detection, and so on [1].

A variety of watermarking techniques have been proposed in the literature. However, a few techniques focus on the robustness to geometric distortions, which can easily magnify synchronization errors between the extracted and embedded watermarks and therefore make the verification task unreliable. These geometric distortion-focused watermarking schemes can be roughly divided into four categories: moment-based [2-4], template-based [5, 6], invariant-domain-based [7, 8], and feature-point-based [9-11] approaches. Among these techniques, feature-point-based schemes are the best in resisting geometric distortions. In general, they utilize the Harris detector [9] or the Mexican hat wavelet [10, 11] to extract features and further use the Delaunay tessellation [9], Voronoi diagrams [10], or normalized disks [11] to define the embedding regions. However, they depend on the capacity of the detector to preserve feature points after distortions. Furthermore, they do not consider the fact that human eyes are not equally sensitive to different spatial frequencies. Even though several watermarking systems [12, 13] utilize the characteristics of the human visual system (HVS) for robust embedding, they are not robust to the severe geometric attacks.

In this paper, we develop an oblivious yet highly robust watermarking scheme which achieves the image authentication under various geometric distortions. First, a universal and reliable feature-point-based acute triangle matching is utilized to synchronize the image for resisting RST attacks. Second, a HVS compatible adaptive embedding scheme is explored in DCT domain to achieve the robustness and invisibility. Third, an error correcting coding and a blind spread spectrum (SS) watermark embedding and retrieval scheme are combined to ensure a more reliable and convenient watermarking system. The reminder of the paper is organized as follows:

- Section 2 presents the embedding procedure.
- Section 3 elaborates on the feature-point-based image restoration technique.

- Section 4 details the proposed watermark extraction and detection scheme.
- Section 5 shows the experimental results.
- Section 6 draws conclusions.

2. Watermark Embedding

The proposed watermark embedding scheme is shown in Fig. 1. An error correcting coded (ECC) bipolar watermark bit sequence is spread by a permutation of the SS using the pseudo-noise (PN) sequence. The resulting message is adaptively embedded into each 8×8 JPEG compatible DCT subblock based on the characteristics of the HVS. The inverse DCT (IDCT) is applied to each watermark embedded subblock to obtain the watermarked image. Several important procedures are detailed in the following subsections.

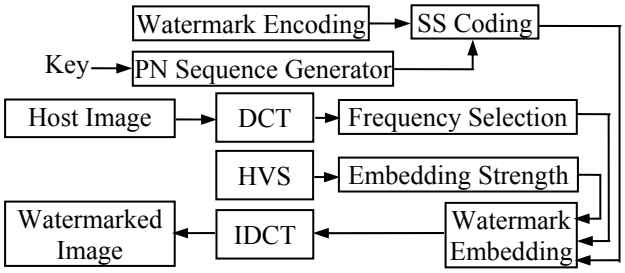


Fig. 1: The Embedding Process

2.1 Watermark Encoding

The original bipolar watermark message is coded by the Hamming error correction method [14]. The length of the encoded watermark depends on the number of mid-frequencies chosen for embedding. In our system, this length is set to be 22 and is capable of correcting at most 3-bit errors.

2.2 Frequency Selection

The middle frequency of each 8×8 DCT subblock is selected as the embedding area, which is indicated by 22 gray cells in Fig. 2. This mid-frequency spectrum is empirically chosen to ensure good invisibility and robustness since low-frequency watermark (noise) is usually more noticeable and high-frequency watermark is easily to be eliminated by lossy compression. Furthermore, we specifically make the length of ECC watermark sequence equal the number of embedding positions (i.e., 22) in each DCT subblock to facilitate the blind SS-based embedding and retrieval.

2.3 Embedding Strength

The modified modulation transfer function (MTF) used in compression [15] is adopted here for generating the embedding strength at each mid-frequency position $P_{i,j}$. These adaptive strengths enhance the watermark invisibility and robustness since they effectively measure the relative importance of each spatial frequency in DCT domain according to the HVS [16]. The optimized weight associated with each position $P_{i,j}$ is computed by using MTF and is shown in Fig.2. These weights are used to construct an embedding strength vector $\beta_{1\times l} = [\ \beta_1\ \beta_2\ \ldots.\ \beta_l]^T$ where $l = 22$, and β_1 through β_l are computed by 0.5 dividing the weight at each position taken from left to right and top to bottom.

$p_{20,k}$		$p_{5,k}$	$p_{6,k}$	$p_{1,k}$	$p_{2,k}$	$p_{3,k}$	$p_{4,k}$	
1	1	1	1	.9045	.7839	.6536	.5029	
1	1	1	.9490	.8569	.7403	.6177	.5015	
1	1	.9001	.8040	.7142	.6176	.5190	.4251	
1	.9490	.8040	.6458	.5401	.4607	.3896	.3233	
.9045	.8569	.7142	.5401	.4113	.3297	.2724	.2260	
.7839	.7403	.6176	.4607	.3297	.2435	.1893	.1523	
.6536	.6177	.5190	.3896	.2724	.1893	.1369	.1041	
.5295	.5015	.4251	.3233	.2260	.1523	.1041	.0742	

Fig. 2: Mid-Frequencies and Weights in DCT

2.4 Watermark Embedding

The blind SS-based embedding is used in our system to grant good noise tolerance to the watermark itself and to ensure the blind retrieval of the embedded watermark. The detailed procedure is:

1. Each bit of the ECC watermark sequence w, whose length is l, is spread by a secret key based m-bit PN sequence p, where m is equal to the number of DCT subblocks. This spread scheme can be achieved by:
$$[W]_{l\times m} = [w_1\ \ w_2 \ldots w_l]^T \cdot [p_1\ \ p_2 \ldots p_m] \qquad (1)$$
where w_i is the ith bit of the ECC watermark message and p_i is the ith bit of the PN sequence.
2. The resulting SS coded ECC watermark message will be further embedded into the mid-frequency spectrum of each 8×8 DCT subblock of the host image. The DCT values associated with these embedding positions can be expressed by an $l\times m$ matrix $E = [\{e_{i,j}\}]_{l\times m}$ with $e_{i,j}$ indicating the DCT value at the ith mid-frequency embedding position in DCT subblock j ($P_{i,j}$ in Fig. 2), where $i = 1, 2, \ldots, l$ and $j = 1, 2, \ldots, m$. The embedding function can be expressed as:

$$\hat{E} = E + \alpha * |E| * W$$
$$= \begin{bmatrix} e_{1,1}+\alpha_1|e_{1,1}|w_1p_1 & e_{1,2}+\alpha_1|e_{1,2}|w_1p_2 & \ldots & e_{1,m}+\alpha_1|e_{1,m}|w_1p_m \\ e_{2,1}+\alpha_2|e_{2,1}|w_2p_1 & e_{2,2}+\alpha_2|e_{2,2}|w_2p_2 & \ldots & e_{2,m}+\alpha_2|e_{2,m}|w_2p_m \\ \ldots & \ldots & \ldots & \\ e_{l,1}+\alpha_l|e_{l,1}|w_lp_1 & e_{l,2}+\alpha_l|e_{l,2}|w_lp_2 & \ldots & e_{l,m}+\alpha_l|e_{l,m}|w_lp_m \end{bmatrix} \qquad (2)$$

where:

- * denotes the entry-by-entry multiplication;

- α is the embedding strength matrix which is constructed by columnwisely copying $\beta_{1\times l}$ (i.e., the values indicated in Fig. 2) m times;
- $|E|$ represents the absolute value of each element in E; and
- $\hat{E}$ represents the watermarked DCT values.

3. Feature Point Based Restoration

In our system, the feature-point-based image restoration is used for the synchronization of the embedded and extracted watermarks after various attacks. The main idea is to look for feature points that are perceptually significant and can thus resist various attacks. These feature points are further used as synchronization markers during the detection process.

We improve the Harris corner detector to exclusively locate important feature points (IFPs) in the image. The detection procedure is:

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 image center based 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. This threshold T is a predefined threshold value to extract a desired number of corner points. It is empirically set to be 10^6 in our scheme. The size of this neighborhood depends on the image textures, i.e., the higher the texture, the larger the size.

In our proposed approach, the circular neighborhood size is adaptive to the image size and thus helps to control the number of feature points. Image textures are roughly classified as high, medium, low, and extremely low, based on the ratio of the feature points to the total number of pixels in an image. These feature points are obtained by using our improved Harris corner detector with a fixed 3×3 neighborhood window. The image texture classification is performed as follows:

$$image = \begin{cases} \text{high texture} & \text{if ratio} \geq 0.01 \\ \text{medium texture} & \text{if ratio} \geq 0.002 \\ \text{low texture} & \text{if ratio} \geq 0.0001 \\ \text{extremely low texture} & \text{if ratio} < 0.0001 \end{cases} \quad (3)$$

The diameter of the circular window is calculated:

$$D = \frac{\sqrt{wh}}{np} \quad (4)$$

where:

- Integers w and h respectively represent the width and height of the image;
- Integer p is an empirical value (i.e., p = 5) for obtaining a reasonable number of feature points for images with large homogeneous areas;
- Integer n is the window size quantizer, which depends on the texture of the image. It is set to be 2, 2.5, 3, and 5 for images with high, medium, low, and extremely low textures, respectively.

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. The intersection operation is applied on all the restored pre-attacked images. In our proposed system, rotation and scaling attacks are selected as the pre-attacks for obtaining the robust IFPs since most IFPs surviving one of the RST transformations can survive the others if they are not cropped. Fig. 3 demonstrates the final preserved robust IFPs of six images with different textures. The proposed approach effectively eliminates some unreliable feature points which fail to be detected after certain geometric attacks. Moreover, the proposed approach ensures sufficient enough IFPs are located for all kinds of different textured images unlike all the other approaches, which suffer from finding a small number of feature points in the less textured images and a large number of feature points in the highly textured images.

Fig. 3: Robust Important Feature Points

Table 1 further summarizes the adaptive parameters for these six different textured images, where:

- *Ratio* is the factor for classifying image textures;
- *Type* is the texture type decided by (3);
- D is the diameter of the circular window used by our improved Harris corner detector.

In general, D is determined based on the texture of the image. This is, the more complicate the texture, the lager the diameter.

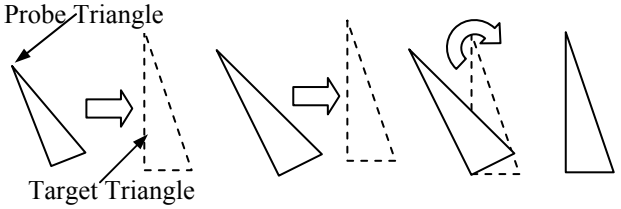
Table 1: Several Image Texture Dependant Parameters

	Lena	Peppers	Baboon	Plane	Beach	Textures
Ratio	0.002	0.0013	0.01	0.0033	0.0000267	0.014
Type	Med	Low	High	Med	Ex. Low	High
D	41	34	51	41	20	51
SNum	3	4	9	6	2	9

All the possible acute triangles based on the robust IFPs will be located and saved for the image restoration. The IFP-based acute triangles of the probe and original images will be utilized to find the matched triangle pairs. This acute-triangle-based matching criterion is based on the angle radians. That is, if two triangles have very similar angle radians (i.e., the angle difference is less than 0.01 radian), these two triangles are claimed to be possibly matched. The possible geometric transformations are further determined from the matched triangle pairs since the IFPs-based triangles in an image undergo the same transformation as the image itself. The detailed steps are:

1) Calculate the scaling factor *SF* by resizing the probe triangle to the same size as the target matched triangle saved in the embedding procedure.
2) Calculate the translation factor *TF* by registering one of the vertices of the matched triangle pair.
3) Calculate the rotation factor *RF* by aligning the other two unregistered vertices of the matched triangle pair.

These factors form a 3-element tuple (*SF*, *TF*, *RF*) where *SF* measures the scaling ratio up to a precision of 1/10, *TF* measures the translation in pixel numbers, and *RF* measures the rotation angle in an integer degree. Fig. 4 illustrates the above three steps by using the right triangle as an example. The 3-tuple to represent this transformation is (1.5, 15, 26°).



(a) (b) (c) (d)

Fig. 4: The Illustration Diagram for Finding the Geometric Transformation. (a) The Matched Triangle Pair. (b) Resizing Result. (c) Translation Result. (d) Rotation Result.

Since the image and the within triangles undergo exactly the same transformation, the transformation obtained from the triangle matching can restore the probe image to be aligned with the host image.

4. Watermark Detection

The watermark extraction and detection is performed after the feature-point-based image restoration. In specific, the value at each embedding position is obtained by applying the frequency selection onto each 8×8 DCT subblock. These values will be arranged to a matrix $\widetilde{E}_{l\times m}$ based on the layout of *E*. The watermark can be blindly extracted as follows:

1) Element-by-element multiply the same secret key based *m*-bit PN sequence *p* with each row of $\widetilde{E}$, i.e., $\widetilde{E}_{i,[1:m]}$ where i = 1, 2, … *l*. The result *R* is:

$$R=\widetilde{E}_{i,[1:m]}*p\approx\hat{E}_{i,[1:m]}*p=E_{i,[1:m]}*p+\alpha*\left|E_{i,[1:m]}\right|*W_{i,[1:m]}*p$$
$$=\begin{bmatrix} e_{1,1}p_1+\alpha_1\left|e_{1,1}\right|w_1p_1^{\,2} & \dots & e_{1,m}p_m+\alpha_1\left|e_{1,m}\right|w_1p_m^{\,2} \\ e_{2,1}p_1+\alpha_2\left|e_{2,1}\right|w_2p_1^{\,2} & \dots & e_{2,m}p_m+\alpha_2\left|e_{2,m}\right|w_2p_m^{\,2} \\ \dots & \dots & \dots \\ e_{l,1}p_1+\alpha_l\left|e_{l,1}\right|w_lp_1^{\,2} & \dots & e_{l,m}p_m+\alpha_l\left|e_{l,m}\right|w_lp_m^{\,2} \end{bmatrix} \quad (5)$$

2) Group each row *i* in R, where *i* ranges from 1 to *l*.

$$group(R_i)=\sum_{j}^{m}e_{i,j}p_j+\alpha_i w_i\sum_{j=1}^{m}\left|e_{i,j}\right|p_j^{\,2} \quad (6)$$

Since $e_{i,j}$ and p_j are statistically uncorrelated, the value of the first item in (6) is much smaller than the second item. As a result,

$$sign(group(R_i))\approx sign(\alpha_i w_i\sum_{j=1}^{m}\left|e_{i,j}\right|p_j^{\,2})=sign(w_i) \quad (7)$$

That is, the sign of the correlation sum is equivalent to the extracted ECC watermark bit, which should be highly correlated with the embedded ECC watermark.

The watermark detection is carried out after applying the ECC scheme to correct the possible mistakes in the extracted ECC watermark bit. The high correlation between the extracted and embedded watermark bits indicates the presence of watermark. This high correlation value is determined to be at least 0.6 based on the statistically computed false-alarm rate.

5. Simulation Results

To evaluate the performance of the proposed watermarking scheme, a variety of experiments have been performed to test on images with distinct textures using different kinds of attempting attacks.

5.1 Watermark Invisibility

The watermark invisibility is shown in Fig. 5. It clearly shows that there is no obvious visual distortion in watermarked images by using adaptive and fixed embedding. Based on the PSNR values, we conclude that

our HVS-based adaptive embedding scheme allows stronger changes on the host image than the fixed embedding scheme where the embedding strength is 0.5 for all the mid-frequency embedding positions.

(a) (b) (c)

Fig. 5: The Invisibility in the Watermarked Images (a) Original Image (b) Adaptive Embedding: PSNR = 34.5 db (c) Fixed Embedding: PSNR = 35.62 db

The PSNRs of the other watermarked images, namely, Pepper, Baboon, and Plane, are 43.33, 44.06, and 37.62, respectively**.**

5.2 Simulation Results

Simulation results for different attacks are shown in Table 2. The results of Tang's method [11] applied on three images (i.e., Lena, Pepper, and Baboon) are also included in Table 2 for fair comparison. It is clear that our method outperforms theirs under different distortions with higher detection rates. We have also tested on several attacks that Tang's method cannot handle, namely 10 random relatively large rotations, croppings, and any combination of RST attacks. The watermark has been correctly identified with high detection rates as shown in the last four rows in Table 2.

Table 2: Detection Rates Under Different Attacks (Ours vs. Tang's method [11])

	Lenna		Pepper		Baboon		Plane
	Ours	Tang	Ours	Tang	Ours	Tang	Ours
R1°+ cropping	1	3/8	1	2/4	1	3/11	1
R5°+ cropping	1	0/8	1	0/4	1	0/11	1
Linear transform (1.007,.01,.01,1.012)	0.43	5/8	0	1/4	0.65	4/11	0
Histogram equal.	1	7/8	1	1/4	1	4/11	1
Median 2x2	0.74	1/8	0.74	1/4	1	6/11	1
Sharpening	1	4/8	1	4/4	1	4/11	1
Gaussian filtering	1	5/8	1	1/4	1	8/11	1
JPEG 40	1	3/8	1	1/4	1	5/11	1
JPEG30	1	2/8	1	0/4	1	4/11	1
Scaling 0.8	0.65	N/A	1	N/A	1	N/A	0.74
Translation [15,15]	1	N/A	1	N/A	1	N/A	1
Translation [0,25]	1	N/A	1	N/A	1	N/A	1
Mean 2x2	1	N/A	1	N/A	1	N/A	0.74
10 random rotations	1	failed	1	failed	1	failed	1
Cropping 0.05	1	failed	1	failed	1	failed	1
Cropping 0.1	1	failed	1	failed	1	failed	1
Cropping 0.15	1	failed	1	failed	1	failed	1

Our method can also successfully detect the watermarks under all the attacks listed in [9]. Since only simple detection results (yes/no) are shown in [9], we do not include these attacks here. 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, which cannot be handled in [9]. The watermark has also been correctly identified with high detection rates.

Finally, we compare our system with the template approach [5], Digimarc, and Suresign by performing the same tests as shown in Table 3. It clearly shows that our system outperforms the other schemes for all attacks except the shearing and non-linear geometric distortions provided in Stirmark in terms of the detection rates.

Table 3: Detection Rates Under Different Attacks (ours vs. Template Approach [5])

	Proposed	Template	Digimarc	Suresign
Enhancement	1	1	1	1
Compression	1	0.74	0.81	0.95
Scaling	0.8747	0.78	0.72	0.95
Cropping	1	0.89	1	1
Shearing	0	0.89	1	1
Rotation	1	1	0.5	0.5
Row/column removal	1	1	1	1
Stirmark geometric attacks	0	0	0.33	0

6. Conclusions

In this paper, we propose a novel and effective feature-point-based RST resistant watermarking scheme, which inserts watermark into the mid-frequency of each 8×8 DCT subblock using HVS-based adaptive embedding strength values. The major contributions consist of:

- Adaptive HVS-based embedding strength selection.
- Robust watermark embedding and detection based on blind SS coding in DCT domain.
- Error correcting coding for correcting at most 3-bit possible errors in the extracted watermark bits.
- Improved robust important feature points extraction.
- Acute-triangle-based image restoration.

Our watermark scheme shows good resistance to RST (especially for rotation and cropping) and common image processing attacks as indicated in the experimental results. In particular, it is more robust to JPEG compression and the combination of the geometric distortions than other feature-point-based and template-based techniques.

References

[1]. G. Voyatzis & I. Pitas, Protecting digital image copyrights: a framework, *IEEE Comput. Graph. Appl*., 19(1), 1999, 18-24.

[2] M. Alghoniemy & A.H. Tewfik, Image watermarking by moment invariants, *Proc. IEEE Int. Conf. on Image Processing*, vol. 2, 2000, 73-76.

[3] M. Alghoniemy & A.H. Tewfik, Geometric invariance in image watermarking, *IEEE Trans. on Image Processing*, 13(2), 2004, 145-153.
[4] H.S. Kim & H.K. Lee, Invariant image watermark using Zernike moments, *IEEE Trans. on Circuit and Systems for Video Technology*, 13(8), 2003, 766-775.
[5] S. Pereira & T. Pun, Robust template matching for affine resistant image watermarks, *IEEE Trans. on Image Processing*, 9(6), 2000, 1123-1129.
[6] Digimarc Corporation, US patent 5,822,436, *Photographic Products and Methods Employing Embedded Information*.
[7] J. J. K. O'Ruanaidh & T. Pun, Rotation, scale, and translation invariant spread spectrum digital image watermarking, *Signal Processing*, 66(3), 1998, 303-317.
[8] C.Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, & Y. Liu, Rotation, scale, and translation resilient watermarking for images, *IEEE Trans on Image Processing*, 10(5), 2001, 767-782.
[9] P. Bas, J. M. Chassery & B. Macq, Geometrically invariant watermarking using feature points, *IEEE Trans. on Image Processing*, 11(9), 2002, 1014-1028.
[10] M. Kutter, S. K. Bhattacharjee & T. Ebrahimi, Toward Second generation watermarking schemes, *Proc IEEE Int. Conf. on Image Processing*, vol. 1, 1999, 320-323.
[11] C. W. Tang & H. M. Hang, A feature-based robust digital image watermarking scheme, *IEEE Trans. on Signal Processing*, 51(4), 2003, 950-959.
[12] A. Briassouli & M. G. Strintzis, Optimal watermark detection under quantization in the transform domain, *IEEE Trans. on Circuits and Systems for Video Technolgoy*, 14(12), 2004, 1308-1319.
[13] Y-S Kim, O-H Kwon & R-H Park; Wavelet based watermarking method for digital images using the human visual system, *Proc. ISCAS*, 4, 1999, 80-83.
[14]. R. Hamming, *Coding and Information Theory*, Prentice-Hall, Englewood Cliffs, 1980.
[15] S. Daly, Application of a noise adaptive contrast sensitivity function to image data compression, *Proc. SP*IE, 1077, 1989, 217-227.
[16]. Eyadat, M, Factors that affect the performance of the DCT-block based image watermarking algorithms, *Proc. ITCC*, 1, 2004, 650-654.