A LOCALIZED GEOMETRIC-DISTORTION RESILIENT DIGITAL WATERMARKING SCHEME USING TWO KINDS OF COMPLEMENTARY FEATURE POINTS

Xiaojun Qi and Jiyuan Wang

Xiaojun.Qi@usu.edu and jywang.08ms@gmail.com
Department of Computer Science, Utah State University, Logan, UT 84322-4205

ABSTRACT

We propose a novel localized geometric-distortion resilient digital watermarking scheme to embed two invisible messages to images. Our scheme utilizes local circular region- (LCR) based and block DCT-based techniques to hide two watermarks in two kinds of regions and extract these two embedding sequences from their individual regions. Specifically, we use the histogram and mean statistically independent of pixel positions to embed one watermark in LCRs, whose centers are SIFT feature points that are robust against various attacks. We also use Watson's DCT-based visual model to embed the other watermark in several rich textured regions not covered by any embedding LCR. Our experimental results demonstrate the proposed system achieves better performance than several peer systems in the literature.

Index Terms**—** Digital watermarking scheme, local circular region, Watson's DCT-based visual model

1. INTRODUCTION

Watermarking emerges as a popular solution to resolve the strong need for protecting digital information. It has been developed as an important technology for image forensics, copyright protection, authentication, and fingerprinting. It requires properties such as transparency, robustness, trustworthy detection, and computational efficiency.

Geometric-distortion resilient watermarking techniques are the most challenging and can be roughly classified into search-based, invariant domain-based, template-based, and feature-based techniques, where the last technique [1] uses image dependent features as a content descriptor to represent invariant reference points for embedding and detection. Feature-based techniques can be further divided into moment-based, histogram-based, and feature point (FP)-based techniques. Here, we briefly review the last two techniques which are related to the proposed technique.

Histogram-based watermarking techniques utilize histograms to measure global features in an image to solve the geometric invariance problem. Xiang *et al.* [2] propose an invariant image watermarking by using the histogram shape and mean in the Gaussian filtered low-frequency component of images. Lin *et al.* [3] present a histogram-oriented blind watermarking algorithm to resist various attacks. However, they cannot resist local transformations. Therefore, Deng *et al.* [4] use histogram in a range to embed a watermark in circular regions centered on FPs.

FP-based watermarking techniques use FPs to form local regions for embedding and extracting watermark. Li *et al.* [5] embed a watermark into multi-scale SIFT FP-based local regions to achieve robustness. Seo and Yoo [6] use the synchronization of Harris-Laplacian FPs to achieve resilience against geometric distortions. Tang and Hang [7] apply the Mexican-hat wavelet scale interaction technique to extract FPs and embed watermark in normalized FP centered circular regions. Bas *et al.* [8] apply Delaunay tessellation on Harris FPs to obtain unique triangles to embed and extract a watermark.

In this paper, we present a novel geometric-resilient watermarking scheme to hide two watermarks in two kinds of regions and extract these two sequences from their individual embedding regions. It combines advantages of SIFT FP extraction, local histogram computing, and blind watermark embedding and extraction in the spatial domain to resist geometric distortions. It also utilizes advantages of Harris FP extraction, triangle tessellation and matching, human visual system (HVS), and spread spectrum-based blind watermark embedding and extraction in the DCT domain to resist image processing attacks and reduce the watermark synchronization problem at the same time. The rest of the paper is organized as follows: Section 2 presents the proposed watermarking scheme. Section 3 shows experimental results. Section 4 concludes the paper with future directions.

2. THE PROPOSED GEOMETRIC-RESILIENT WATERMARKING SCHEME

The proposed geometric resilient watermarking scheme is a robust technique capable of resisting geometric attacks and common image processing attacks.

2.1. Watermark embedding procedure

The watermark embedding procedure uses LCR-based and block DCT-based techniques. A secret private key *pk* is used to generate two watermarks. We first generate a 20-bit pseudo-random bipolar sequence to be embedded into two 20-bin histograms in each chosen LCR. We then generate a 25-bit pseudo-random sequence to be embedded into rich textured 80×80 regions outside of embedded LCRs.

2.1.1. LCR-based embedding technique

The LCR-based embedding technique consists of robust SIFT FP extraction, histogram bin quality-based LCRs extraction, and histogram relationship-based embedding.

Robust SIFT FP extraction: We extract SIFT FPs and apply a series of operations to remove a large number of non-robust FPs. We first remove relatively non-robust FPs whose scales are smaller than 4 or larger than 8. We then remove non-robust FPs near the image border. Finally, we pre-attack the original image by performing a combined rotation, scaling, and compression attack. For each pre-attacked image, we find matched relatively robust FPs between original and pre-attacked images. The intersection of matched FPs across pre-attacked and original images keeps robust FPs for embedding watermark.

Histogram bin quality-based LCRs extraction: LCRs are circular regions centering on each of robust FPs. The radius of LCR depends on the scale σ of its FP and is set as $\tau \cdot [\sigma]$ where $[\cdot]$ is a rounding operation and τ equals 8. We then design a histogram bin quality-based strategy to choose the best non-overlapping LCRs for embedding watermark. We first split each LCR into two concentric circles with equal areas, where C_1 represents the outer circular ring and C_2 represents the inner circle. We then compute a local 20-bin histogram of pixels falling in the range of $B = [(1-\lambda)A, (1+\lambda)A]$ for two areas C_1 and C_2, where A is LCR's average intensity, and λ (0.6) controls the histogram width and the quality of the watermarked image.

After computing the local histogram for C_1 and C_2, we sort all LCRs based on the number of good quality bins which contain more than 80 pixels in descending order. We then sort on the previously sorted LCRs based on the total number of pixels in all bins in descending order. In other words, the LCR with all bins as good quality bins and the maximum pixels in all bins is the best LCR for embedding watermark. We select this LCR at first and find the second best LCR that does not overlap with the best LCR. The same process is iteratively used to find all the other LCRs.

Histogram relationship-based embedding: We utilize the relationship between groups of two adjacent bins in C_1 and C_2 to embed a watermark bit. Specifically, we use the histogram and mean statistically independent of the pixel position to embed watermark in each LCR, where HC_1 is the 20-bin histogram in C_1 area, $HC_1(i)$ is the ith bin of HC_1, $HC_1(i+1)$ is the i+1th bin of HC_1, a_i is the number of pixels in $HC_1(i)$, and a_{i+1} is the number of pixels in $HC_1(i+1)$. We sequentially choose two consecutive bins in HC_1 to embed a watermark bit as follows: 1) If embedded bit is 1 and $a_i / a_{i+1} \geq T$, no operation is performed. 2) If embedded bit is 1 and $a_i / a_{i+1} < T$, randomly select I_1 pixels from $HC_1(i+1)$ and subtract these pixel intensities by the width of histogram bin. 3) If embedded bit is 0 and $a_{i+1} / a_i \geq T$, no operation is performed. 4) If embedded bit is 0 and $a_{i+1} / a_i < T$, randomly select I_0 pixels from $HC_1(i)$ and add these pixel intensities by the width of histogram bin.

The same embedding strategy is applied on the histogram bins in C_2 area to embed the remaining half of the watermark bits. Here, I_1 and I_0 are computed as follows:

$$I_1 = \frac{T \times a_{i+1} - a_i}{1+T} \ \ and \ \ I_0 = \frac{T \times a_i - a_{i+1}}{1+T} \tag{1}$$

2.1.2. HVS-based block DCT domain embedding technique

The HVS-based embedding technique consists of robust Harris FPs extraction, highly textured embedding regions extraction, and HVS-based DCT domain embedding.

Robust Harris FPs extraction: We use the improved Harris corner detector [9] to find several robust Harris FPs.

Highly textured embedding regions extraction: We divide the original image into 80×80 non-overlapping blocks. We then find blocks that do not overlap with any LCRs and keep such blocks that contain at least one robust Harris FP for embedding the second watermark.

HVS-based DCT domain embedding: We divide each candidate block into 8×8 non-overlapping sub-blocks and embed a watermark bit in each sub-block. First, we separately apply DCT on each sub-block to form a DCT domain sub-block. We then group every 4 adjacent sub-blocks as one embedding unit to embed a watermark bit in the DC component of each sub-block. The watermarked i^{th} DC value of the k^{th} embedding unit, $DC_{k,i}'$, is calculated :

$$\begin{array}{ll} DC_{k,i}' = DC_{k,i} - (DC_{k,i} \bmod \alpha) + \frac{3}{4}\alpha, & \text{if } w_k = 1 \text{ and } (DC_{k,i} \bmod \alpha) \geq \frac{1}{4}\alpha \\ DC_{k,i}' = \left[DC_{k,i} - \frac{1}{4}\alpha\right] - \left[\left(DC_{k,i} - \frac{1}{4}\alpha\right) \bmod \alpha\right] + \frac{3}{4}\alpha, & \text{if } w_i = 1 \text{ and } (DC_{k,i} \bmod \alpha) < \frac{1}{4}\alpha \\ DC_{k,i}' = DC_{k,i} - (DC_{k,i} \bmod \alpha) + \frac{1}{4}\alpha, & \text{if } w_i = 0 \text{ and } (DC_{k,i} \bmod \alpha) \leq \frac{3}{4}\alpha \\ DC_{k,i}' = \left[DC_{k,i} + \frac{1}{2}\alpha\right] - \left[\left(DC_{k,i} - \frac{1}{2}\alpha\right) \bmod \alpha\right] + \frac{1}{4}\alpha, & \text{if } w_i = 0 \text{ and } (DC_{k,i} \bmod \alpha) > \frac{3}{4}\alpha \\ & i = 1 \ldots 4;\ k = 1 \ldots N \end{array} \tag{2}$$

where N is the watermark length, $DC_{k,i}$ is the original i^{th} DC value of the k^{th} embedding unit, and α is the embedding strength. We use Watson's DCT-based visual model as the HVS model [10] to estimate the sensitivity of human eyes to changes in each DCT sub-block. For sensitive sub-blocks, we set α as 45. For less sensitive sub-blocks, we set α as 90.

2.2. Watermark detection procedure

Due to possible geometric distortions, the probe image must be re-synchronized for successful detection and verification. We use the same key *pk* to generate watermarks.

2.2.1. LCR-based watermark detection technique

The LCR-based detection technique first extracts SIFT FPs whose scales are between 3.5 and 10. This larger scale range ensures most FPs used in embedding are approximately located. It then applies the same formula $\tau \cdot [\sigma]$ to compute the radius of each LCR and splits each LCR into two concentric circles (C_1 and C_2). It finally computes the 20-bin local histogram in the range of B in C_1 and C_2. Let a_i' and a_{i+1}' be the number of pixels in two adjacent bins in C_1 or C_2. The watermark is sequentially extracted from each pair of adjacent bins in C_1 and C_2 by:

$$w' = \begin{cases} 1 & if \ a_{i+1}'/a_i' \geq 1 \\ 0 & otherwise \end{cases} \tag{3}$$

At last, it applies the verification technique to decide the presence of watermark. The extracted watermark is compared with the secret key generated embedded watermark sequence. A ratio of matched watermark bits and the total number of watermark bits is computed for each probe LCR. We consider LCRs with a ratio of larger than 0.84 (at most a 3-bit difference) containing a watermark. If at least three LCRs contain a watermark, we claim watermark exists in the probe image.

2.2.2. HVS-based block DCT domain watermark detection

The HVS-based detection technique first extracts robust Harris FPs as did in embedding process. Second, it applies the Delaunay tessellation on FPs to generate a set of unique, non-overlapping triangles. Third, it applies Delaunay tessellation on the stored FPs of the original image to generate another set of unique, non-overlapping triangles. Fourth, it performs Delaunay triangle matching on these two sets of triangles to find matched triangles. The matching criterion is as follows: If two triangles have similar angle radians (the angle difference is less than 0.01 radian), they are claimed to be matched. Fifth, it determines possible geometric transformations from matched triangle pairs since triangles in an image undergo the same transformation as the image. The estimated parameters are utilized to restore the probe image to be aligned with the original image.

After restoring the probe image, the following steps are applied to extract the second watermark. 1) The aligned probe image is divided into 80×80 non-overlapping blocks. 2) Each block is divided into 8×8 non-overlapping sub-blocks and each sub-block is transformed into DCT sub-block. 3) For each block, every four adjacent sub-blocks are grouped together to extract one watermark bit by modularly dividing each of four DC values by α. That is:

$$\tilde{w}_{k,i}' = \begin{cases} 1 & if \ DC_{k,i}' \bmod \alpha \geq \frac{1}{2}\alpha \\ 0 & if \ DC_{k,i}' \bmod \alpha < \frac{1}{2}\alpha \end{cases} \quad i = 1 \ldots 4, k = 1 \ldots N \tag{4}$$

where $\tilde{w}_{k,i}'$ is one of the extracted bits in group k, and N is the watermark length. The final watermark bit $\hat{w}_k'$ is decided by the majority value $\tilde{w}_{k,j}'$ in group k.

A similar verification technique is used to decide the presence of watermark. We consider blocks with a ratio of larger than 0.84 (at most a 3-bit difference) containing a watermark. If at least two blocks contain a watermark, we claim that watermark exists in the probe image.

3. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed watermarking scheme, we conduct a variety of experiments on various standard images using different kinds of attempted attacks.

3.1. Watermark invisibility test

We evaluate watermark invisibility on four benchmark images (e.g., Baboon, Lena, Pepper, and Airplane). Their PSNRs are 41.80, 46.62, 43.37, and 41.17, respectively.

3.2. Simulation results

Tables 1 through 3 respectively summarize watermarking detection results under compression, scaling, and rotation/translation attacks. In Table 1, successful results are shown bolded based on two predefined thresholds. It shows the scheme is resistant to JPEG compression quality factor (QF) down to 40%. Table 2 shows block-based and LCR-based schemes complement each other to achieve decent resistance to scaling attacks in the range of 0.85 to 1.1. Table 3 shows that our scheme is resistant to all rotation attacks (3 cases marked as italic and bold fail on the block-based scheme) and translation attacks.

Table 1. Ratios under compression (LCR, block)

QF	Baboon	Lena	Pepper	Airplane
80%	**(5/10, 4/7)**	**(4/7, 5/5)**	**(4/10, 8/8)**	**(5/9, 4/5)**
70%	(2/10, **7/7)**	(2/7, **5/5)**	(1/10, **8/8)**	**(3/9, 4/5)**
60%	(2/10, **2/7)**	(1/7, **5/5)**	(2/10, **8/8)**	(0/9, **4/5)**
50%	(0/10, **2/7)**	(0/7, **5/5)**	(1/10, **8/8)**	(2/9, **4/5)**
40%	(0/10**, 7/7)**	(1/7, **5/5)**	(1/10, **8/8)**	(0/9, **4/5)**

Table 2. Ratios under scaling (LCR, block)

Scaling	Baboon	Lena	Pepper	Airplane
0.85	(0/10, **2/7)**	**(3/7, 2/5)**	**(5/10, 4/8)**	(2/9, 1/5)
0.9	(1/10, **7/7)**	(1/7, 0/5)	**(4/10,** 0/8)	(1/9, **3/5)**
0.95	(0/10, **4/7)**	(2/7, **2/5)**	**(5/10, 4/8)**	(1/9, **3/5)**
1.05	**(3/10,** 1/7)	**(5/7, 2/5)**	**(5/10, 6/8)**	**(5/9,** 1/5)
1.1	(2/10, **2/7)**	**(3/7,** 0/5)	**(5/10, 5/8)**	**(3/9, 2/5)**

Table 3. Ratios under rotation/translation (LCR, block)

Rotation	Baboon	Lena	Pepper	Airplane
5°	(9/10, 4/7)	(5/7, 5/5)	(8/10, ***1/8***)	(9/9, 2/5)
10°	(8/10, 4/7)	(4/7, 4/5)	(7/10, 2/8)	(10/9, 2/5)
15°	(9/10, ***0/7***)	(5/7, 2/5)	(3/10, 4/8)	(9/9, 3/5)
30°	(9/10, 4/7)	(4/7, 3/5)	(4/10, 3/8)	(9/9, 2/5)
45°	(9/10, 4/7)	(4/7, 3/5)	(5/10, 2/8)	(9/9, ***0/5***)
60°	(9/10, 4/7)	(5/7, 4/5)	(6/10, 4/8)	(9/9, 2/5)
75°	(10/10, 4/7)	(4/7, 2/5)	(6/10, 4/8)	(8/9, 2/5)
Shift 25 rows	(9/10, 6/7)	(5/7, 5/5)	(7/10, 5/8)	(10/9, 4/5)
Shift 40 rows	(9/9, 6/7)	(6/7, 5/5)	(7/10, 5/8)	(10/9, 4/5)
Shift 80 rows	(6/10, 9/7)	(4/7, 5/5)	(7/10, 5/8)	(10/10,4/5)

3.3. Comparison with other methods in the literature

Table 4 compares our system in terms of LCR and block ratios with Deng's method using Deng's experiments [4]. It shows our results are comparable with Deng's except for 4 detections shown in bold. However, our system has a higher payload and is more efficient since we embed two watermarks in two kinds of regions and Deng's detection searches for FP's small neighborhood to find best match.

Table 4. Comparison of our method with Deng's method [4]

Attack	Baboon		Lena		Pepper		Plane	
	Ours	[4]	Ours	[4]	Ours	[4]	Ours	[4]
1	8/10, 5/7	10/17	4/7, 3/5	7/13	6/10,7/8	7/18	5/9,4/5	5/14
2	**2/10,1/7**	11/17	4/7,5/5	10/13	4/10,8/8	13/18	3/9,4/5	8/14
3	9/10,0/7	8/17	5/7,5/5	5/13	8/10,1/8	10/18	9/9,2/5	6/14
4	9/10,0/7	8/17	4/7,3/5	5/13	4/10,3/8	7/18	9/9,2/5	6/14
5	8/10,2/7	7/17	7/7,5/5	7/13	9/10,8/8	8/18	10/9,4/4	6/14
6	2/10,7/7	8/17	7/7,5/5	5/13	5/10,8/8	11/18	6/9,4/5	6/14
7	6/10,3/7	12/17	7/7,5/5	7/13	7/10,8/8	16/18	10/9,4/5	10/14
8	0/10,6/7	6/17	1/7,4/5	7/13	3/10,3/8	8/18	0/9,3/5	6/18
9	2/10,7/7	7/17	2/7,5/5	7/13	1/10,8/8	8/18	3/9,4/5	6/14
10	7/10,7/7	16/17	5/7,5/5	12/13	5/10,8/8	17/18	10/9,4/5	13/14
11	2/10,7/7	15/17	2/7,5/5	12/13	1/10,8/8	17/18	3/9,4/5	12/14
12	**0/10,1/7**	15/17	0/7,5/5	11/13	1/10,8/8	15/18	2/9,4/5	12/14
13	**1/10,0/7**	14/17	0/7,5/5	10/13	1/10,8/8	16/18	**0/9,1/5**	11/14

Table 5 compares our system in terms of LCR and block ratios with Tang's method using Tang's experiments [7]. It shows our method fails under 4 attacks (11, 13, 17, 21) and Tang' method fails under 4 attacks (13, 16, 17, 20). However, our ratios are generally larger than Tang's, which indicates our system is more likely to extract watermarks from embedded regions. In addition, our method can resist larger rotation angles than Tang's method.

Table 5. Comparison of our method with Tang's method [7]

Attack	Lena		Baboon		Pepper	
	Ours	[7]	Ours	[7]	Ours	[7]
1	(7/7, 5/5)	7/8	(9/10,7/7)	10/11	(8/10,8/8)	4/4
2	(3/7, 2/5)	1/8	(1/10,2/7)	6/11	(5/10,2/8)	1/4
3	(7/7, 5/5)	1/8	(6/10,3/7)	2/11	(7/10 ,8/8)	1/4
4	(7/7, 5/5)	5/8	(2/10,7/7)	8/11	(5/10,8/8)	1/4
5	(7/7,5/5)	5/8	(8/10,7/7)	6/11	(8/10,8/8)	4/4
6	(7/7,5/5)	4/8	(8/10,7/7)	4/11	(7/10,8/8)	2/4
7	(6/7.5/5)	1/8	(8/10,7/7)	5/11	(8/10,8/8)	1/4
8	(4/7,5/5)	6/8	(5/10,4/7)	9/11	(4/10,8/8)	3/4
9	(2/7,5/5)	7/8	(2/10,7/7)	11/11	(1/10,8/8)	3/4
10	(1/7,5/5)	6/8	(2/10,2/7)	7/11	(2/10,8/8)	1/4
11	(0/7,5/5)	5/8	***(0/10,1/7)***	7/11	(1/10,8/8)	3/4
12	(1/7,5/5)	3/8	(0/10,7/7)	5/11	(1/10,8/8)	1/4
13	(0/7,5/5)	2/8	***(1/10,0/7)***	4/11	(1/10,8/8)	***0/4***
14	(1/7,5/5)	5/8	(0/10,7/7)	8/11	(2/10,8/8)	2/4
15	(5/7,0/5)	3/8	(9/10,4/7)	3/11	(9/10,2/8)	2/4
16	(4/7,0/5)	***0/8***	(8/10,4/7)	4/11	(4/10, 3/8)	2/4
17	(3/7, 2/5)	***0/8***	***(1/10,0/7)***	***0/11***	(5/10, 5/8)	***0/4***
18	(7/7,5/5)	3/8	(9/10,7/7)	6/11	(8/10,8/8)	3/4
19	(2/7,5/5)	4/8	(2/10,7/7)	6/11	(1/10,8/8)	3/4
20	(5/7,0/5)	***0/8***	(8/10,4/7)	3/11	(9/10,8/8)	1/4
21	***(1/7,0/5)***	1/8	(0/10,4/7)	3/11	(3/10, 1/8)	1/4

Experiments show our system achieves better scaling and JPEG compression resistance than Bas's system [8].

4. CONCLUSIONS AND FUTURE DIRECTIONS

We propose a novel and robust geometric distortion resilient watermarking approach. Major contributions are: 1) Apply pre-attacks to select robust SIFT FPs. 2) Apply a histogram bin quality-based strategy to find best non-overlapping embedding LCRs. 3) Apply a histogram relationship-based strategy to embed watermark using the histogram and mean statistically independent of pixel positions. 4) Apply a DCT-based HVS model to embed watermark in textured blocks chosen by Harris FPs. 5) Apply Delaunay tessellation and matching to restore the probe image for re-synchronization.

Our method achieves comparable performance to its peers and is more robust against rotation/translation attacks than its peers. It works well under scaling attacks except for high textured images and under a JPEG QF down to 40%. Our approach can be further improved by developing a more reliable feature extraction method and a more stable embedding function under combined geometric distortions.

5. REFERENCES

[1] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, "Towards second generation watermarking scheme," *Proc. of ICIP*, pp. 320–323, 1999.

[2] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 6, pp. 777–790, 2008.

[3] C. Lin, D. Chan, H. Su, and W. Hsieh, "Histogram-oriented watermarking algorithm: color image watermarking scheme robust against geometric attacks and signal processing," *IEE Proc. Vis. Image Signal Process.*, vol. 53, no. 4, pp. 483–492, 2006.

[4] C. Deng, X. Gao, X. Li, and D. Tao, "Local histogram based geometric invariant image watermarking," *Signal Processing*, vol. 90, no. 12, pp.3256-3264, 2010.

[5] L. Li, J. Qian, and J. Pan, "Characteristic region based watermark embedding with RST invariance and high capacity," *Int. J. of Electronics and Communications*, vol. 65, pp. 435-442, 2011.

[6] S. Jeo and C. Yoo, "Localized image watermarking based on feature points of scale-space representation," *Pattern Recognition*, vol. 37, pp. 1365–1375, 2004.

[7] C. Tang and H. Hang, "A feature-based robust digital image watermarking scheme," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 950-959, 2003.

[8] P. Bas, J. M. Chassery, and B. Macq, "Geometrically invariant watermarking using feature points," *IEEE Trans. Image Process.*, vol. 11, no. 9, pp. 1014-1028, 2002.

[9] X. Qi and J. Qi, "A robust content-based digital image watermarking scheme," *Signal Processing*, vol. 87, pp. 1264-1280, 2007.

[10] H. Tsai and L. Chang, "Highly imperceptible video watermarking with the Watson's DCT-based visual model," *Proc. of ICME*, pp. 1927-1930, 2004.