6.1-6

Copyright Protection through Feature-based Watermarking using Scale-invariant Keypoints

Hae-Yeoun Lee and Heung-Kyu Lee, *Member, IEEE*

***Abstract*--This paper presents a feature-based watermarking method based on scale-invariant keypoints for copyright protection. We extract feature points by using scale-invariant keypoint extractor and then these points are decomposed into a set of disjoint triangles. The triangles are watermarked by an additive way. Our method is compared with previous methods.**

I. INTRODUCTION

Digital watermarking is an efficient solution to protect copyright of multimedia. Most previous algorithms, however, suffer from geometric distortion attacks that desynchronize the location of the inserted copyright information, *the watermark*. One solution to synchronize the watermark location is to use image features. This paper proposes a new feature-based watermarking method based on scale-invariant keypoints. We perform an intensive simulation to evaluate our method against signal processing attacks and geometric distortion attacks in comparison with other feature-based watermarking methods.

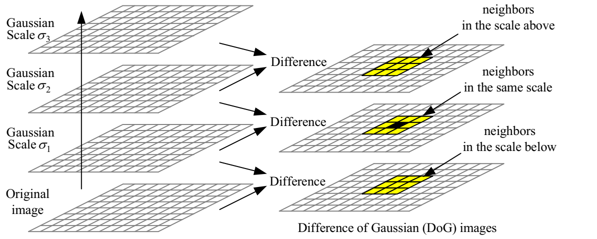
Gaussian Scale σ_3
Gaussian Scale σ_2
Gaussian Scale σ_1
Original image
Difference
Difference
Difference
neighbors in the scale above
neighbors in the same scale
neighbors in the scale below
Difference of Gaussian (DoG) images

Fig. 1. Scale-space from difference of Gaussian function and the closest neighborhoods of a pixel

II. SCALE-INVARIANT KEYPOINT EXTRACTOR

Features should be carefully selected to achieve robust watermarking. We use an affine-invariant feature called as scale-invariant keypoints [1] that is highly distinctive and matched with high probability against a large case of image distortions.

Scale-invariant keypoint extractor considers local image characteristics. The basic idea of the scale-invariant keypoint extractor is detecting features through a staged filtering that identifies stable points in the scale-space. First, we generate a scale-space using difference of Gaussian function, where we successively smooth the image with a variable scale Gaussian filter and calculate the scale-space images by subtracting two successive smoothed images. In these scale-space images, all local maximums and minimums are searched by checking eight closest neighborhoods in the same scale and nine neighborhoods in the scale above and below (see Fig. 1). These extrema are candidates for keypoints. Candidates that have low contrast or are poorly localized are removed by measuring the stability at their location and scale. Scale-invariant keypoints obtained through this process are invariant to rotation, scaling, translation, and partly illumination changes of images and useful to design robust watermarking.

III. PROPOSED WATERMARKING METHOD

We first describe the way to synchronize the watermark location and then explain watermark insertion and detection.

A. *Watermark synchronization*

Feature points extracted by the scale-invariant keypoint extractor should be relatively related to generate the patches for watermark insertion and detection. We decompose feature points into a set of disjoint triangles by Delaunay tessellation. In order to control the distribution of feature points, we apply a circular neighborhood constraint and then feature points whose strength is the largest are selected [2].

Although attacks result in a different tessellation by modifying the relative position of feature points, several patches match. Therefore, we can synchronize successfully the location for watermark insertion and detection.

B. *Watermark insertion*

The first step for watermark insertion is analyzing image contents to extract the patches, and then the watermark is inserted repeatedly into all patches (see Fig. 2).

The shape of the watermark is a right-angled triangle. Because the shape of the patches and the watermark is different, we warp the triangular watermark according to the shape of the patches. Watermark insertion must not affect the perceptual quality of images and hence we consider human visual system. Finally, we insert imperceptibly the watermark by an additive way on the spatial domain, where the pixels of the warped watermark are added to the pixels of image.

C. *Watermark detection*

The first step for watermark detection is analyzing contents to find the patches. The watermark is then detected from all patches (see Fig. 3).

There are several patches in an image and we try to detect the watermark from all patches. Because the watermark is inserted into contents as noise, we apply a Wiener filter to calculate this noise and regard it as the retrieved watermark. To measure similarity between the reference watermark generated during watermark insertion and the retrieved watermark, the retrieved watermark is converted into the shape of the reference watermark. We calculate normalized correlation between the reference watermark and the retrieved watermark. If this correlation value exceeds a pre-defined threshold, we can be

0-7803-9459-3/06/$20.00 ©2006 IEEE

satisfied that the reference watermark has been inserted. If the watermark is detected from at least one patch, we can prove ownership successfully. It is highly likely that the proposed method will detect the watermark even after attacks, because we insert the watermark multiple times into several patches, not just one.

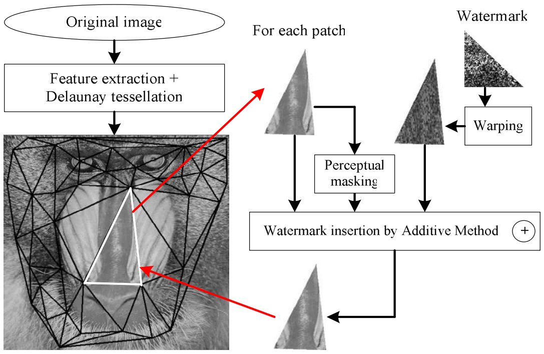
Original image
Feature extraction + Delaunay tessellation
For each patch
Watermark
Warping
Perceptual masking
Watermark insertion by Additive Method
+

Fig. 2. Watermark insertion process

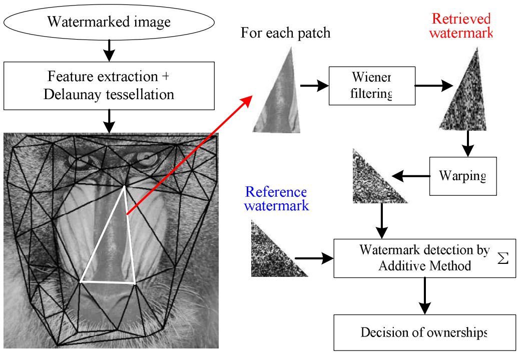

Fig. 3. Watermark detection process

IV. Simulation Results

Using 100 randomly collected images, we compared our method with other feature-based watermarking methods: Kutter method [3, 4] and Bas method [2]. We applied signal processing and geometric distortion attacks listed in Stirmark 3.1. Tables I and II show the number of images where the watermark was detected correctly and the mean of their correlation.

Bas method showed lower performance than others in signal processing attacks, but outperformed in scaling attacks. Kutter method performed better than other methods in signal processing attacks, but showed severe weakness in scaling attacks. Our method showed higher performance than Bas method in signal processing attacks and performed better than other methods against most geometric distortion attacks except scaling attacks. Overall performance of our method was acceptable because we could prove ownership successfully if the watermark was detected from more than one patch.

V. Conclusion

In order to resist geometric distortion attacks, the location of the watermark should be synchronized during watermark insertion and detection. This paper proposed a feature-based watermarking based on the scale-invariant keypoints for copyright protection.

TABLE I
PERFORMANCE UNDER SIGNAL PROCESSING ATTACKS

	Kutter method		Bas method		Our method	
	# img.	Corr.	# img.	Corr.	# img.	Corr.
No attack	100	0.78	99	0.60	100	0.70
Median 2×2	100	0.62	91	0.41	97	0.47
Median 3×3	99	0.59	93	0.39	99	0.45
Median 4×4	96	0.48	83	0.32	85	0.36
Gaussian filter	99	0.64	96	0.39	98	0.50
Additive uni. noise	100	0.45	91	0.28	95	0.33
JPEG compress. 50	99	0.41	78	0.26	83	0.30
JPEG compress. 70	100	0.57	92	0.34	99	0.43
JPEG compress. 90	100	0.73	99	0.51	100	0.62

TABLE II
PERFORMANCE UNDER GEOMETRIC DISTORTION ATTACKS

	Kutter method		Bas method		Our method	
	# img.	Corr.	# img.	Corr.	# img.	Corr.
Crop 5%	99	0.59	99	0.54	100	0.62
Crop 15%	99	0.50	97	0.51	100	0.53
Crop 25%	96	0.40	94	0.46	95	0.46
Linear trans. 1.008	98	0.52	99	0.48	100	0.51
Linear trans. 1.011	98	0.51	98	0.49	97	0.52
Linear trans. 1.012	99	0.51	96	0.48	99	0.51
Random bending	99	0.52	99	0.49	99	0.50
Row/Col Removal 1 1	100	0.72	99	0.57	100	0.62
Row/Col Removal 1 5	99	0.63	99	0.54	100	0.55
Row/Col Removal 5 17	96	0.40	97	0.47	98	0.45
Shearing x 0 y 5	98	0.51	99	0.51	100	0.52
Shearing x 5 y 0	97	0.53	99	0.52	99	0.54
Shearing x 1 y 1	99	0.57	100	0.51	100	0.51
Shearing x 5 y 5	90	0.32	96	0.44	95	0.38
Rotation 1.0°+Crop	100	0.63	99	0.48	99	0.51
Rotation 5.0°+Crop	98	0.58	98	0.47	98	0.48
Rotation 10.0°+Crop	95	0.54	99	0.46	97	0.46
Rotation 15.0°+Crop	97	0.50	95	0.46	99	0.43
Scaling 0.8×	0	0.00	74	0.34	61	0.24
Scaling 0.9×	13	0.19	96	0.41	95	0.31
Scaling 1.1×+Crop	32	0.22	97	0.47	94	0.38
Scaling 1.2×+Crop	2	0.15	93	0.41	84	0.28

Acknowledgment

This work is financially supported by the Ministry of Labor through the fostering project of the Lab of Excellency.

References

[1] D.G. Lowe, “Distinctive image features from scale-invariant keypoints,” *Int. J. Comput. Vision*, vol. 60, pp. 91-110, 2004.

[2] P. Bas, J-M. Chassery, and B. Macq, “Geometrically invariant watermarking using feature points,” *IEEE Trans. Image Process.*, vol. 11, pp. 1014-1028, 2002.

[3] M. Kutter, S.K. Bhattacharjee, and T. Ebrahimi, “Towards second generation watermarking schemes,” in *Proceedings of IEEE Conference on Image Processing*, pp. 320-323, 1999.

[4] C.W. Tang and H-M. Hang, “A feature-based robust digital image watermarking scheme,” *IEEE Trans. Signal Process.*, vol. 51, pp. 950-959, 2003.