A Novel Watermark Recovery Technique in Various Attack Conditions

Madhusudhan.K.N.
Asst.Professor, Dept of E&C, BMSCE, Bangalore- 19

Lalitha.S.
Asst.Professor, Dept of E&C, BMSCE, Bangalore- 19

Ashwini.V
Asst.Professor, Dept of E&C, BMSCE, Bangalore- 19

Manjula.R
Student, Dept of E&C, BMSCE, Bangalore- 19

Abstract-In this paper a novel digital image watermarking scheme which is robust to both signal processing and geometric attacks is proposed. Watermark is embedded in the codebook of the imageby Discrete Cosine Transform technique in a spread-spectrum format. Codebook is generated by LBG algorithm and Vector Quantization is used to compress the image. Harris corner detector obtains the feature points of the watermarked image which is undergone rotation scaling and translation attacks. Delaunay triangulation of the feature points of the image is used to resynchronize the image to the position of the original image. After resynchronization, the watermark is recovered from the codebook of the image. In some situations the recovered watermark is poor or entirely lost.This is due to some reference feature points being lostas a result of the RST attacks. In our proposed scheme, RST attacks are estimated by comparing the Delaunay tessellation of the original image and the attacked watermarked image. Computer simulation results obtained using MATLAB confirms the accuracy of our proposed scheme.

Keywords: Spread-spectrum, LBG algorithm, Vector Quantization and Delaunay triangulation.

I. INTRODUCTION

Nowadays images appear in web pages and in storage media such as CD-ROM and DVD routinely. It is often desirable to embed watermark into the images as value added content, or for copyright control and authentication purposes. However, watermarking is removed or rendered useless by various attacks such as signal processing attacks or geometric attacks. Geometric attacks induce synchronization errors between the original and extracted watermarks during detection process. Therefore they are difficult to deal with as they involve displacement of pixels.

The watermark can be embedded in the Discrete Cosine Transform(DCT) domain, using the mid-band frequencies. Since the mid-band frequencies do not contain visually important features of the image, watermark embedded in this region is largely unaffected by filtering and noise attacks. There are a few Geometric-distortion focused watermarking schemes such as moment-based, template-based, invariant domain-based and feature-point-based. Among all these feature-point-based techniques offers high resistance to geometric attacks. The feature-point based techniques include Harris corner detector and Mexican hat wavelet. The Mexican hat wavelet generates synchronization errors when the geometric attacks are local and therefore Harris corner detector is preferred. The feature-points obtained using Harris corner detector are then used for Delaunay triangulation which are used for resynchronization. For the images to be efficiently stored and transmitted Vector Quantization (VQ) is often used to compress the image.

In some situations some of the feature points are lost due to, the attacks leading to the formation of substantial dark regions around the image and hence giving a different Delaunay tessellation. The difference in the tessellation leads to synchronization errors, so it is more difficult to estimate the rotation, scaling and translation (RST) attacks. Our proposed scheme uses comparison of the Delaunay tessellations to estimate the attacks on the image in order to restore it to the position of the original image. This ensures that the watermark can still be extracted even after losing a number of reference points.

This paper is organized as follows.

(II) Harris corner detector.
(III) Delaunay triangulation.
(IV) DCT domain watermarking
(V) Proposed scheme which includes
A. Watermark embedding algorithm.
B. Watermark extraction algorithm.
(VI) Experimental results.
(VII) Conclusion.

II. HARRIS CORNER DETECTOR

Harris corner detector is a popular interest point detector due to its strong invariance to rotation, scale, illumination variation and image noise. Robust feature-points of the watermarked image are obtained using Harris corner detector. This is done by obtaining feature-points and then rotating the image by various angles and repeating the above process, the features which are extracted for all the angles are then taken as the robust feature-points.
Harris corner detector is based on local auto-correlation function of a signal. Local auto-correlation functions measure the local changes of the signal with patches shifted by a small amount in different directions.
Given a shift (Δx, Δy) and a point (x,y), the auto-correlation function is defined as

$$c(x,y) = [\Delta x \ \ \Delta y] C(x,y) \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} \qquad (1)$$

Where matrix C(x, y) is given by

$$c(x,y) = \begin{bmatrix} \sum_{w} (I_x(x_i,y_i))^2 & \sum_{w} I_x(x_i,y_i) I_y(x_i,y_i) \\ \sum_{w} I_x(x_i,y_i) I_y(x_i,y_i) & \sum_{w} (I_y(x_i,y_i))^2 \end{bmatrix} \qquad (2)$$

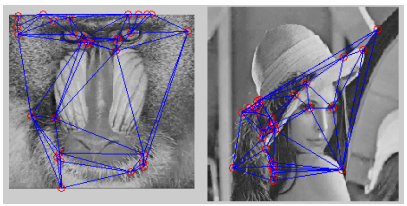
where I(·, ·) denotes the image function and (xi, yi) are the points in the Gaussian window of say 3-by-3 or 5-by-5 pixels centered at (x,y)and Ix(x,y)and Iy(x,y) are partial derivatives of the image function I(x,y) with respect to x and y respectively.

The matrix C(x,y)captures the intensity structure of the local neighborhood. Let λ1, λ2 be the eigen values of matrix C(x, y).From the eigen values of the matrix we get the following three cases:
1. If both λ1, λ2 are small, so that the local auto-correlation function is flat (i.e., little change in c(x, y) in any direction), this indicates a flat region.
2. If one eigenvalue is high and the other low, so that the local auto-correlation function is ridge shaped, this indicates an edge.
3. If both eigenvalues are high, so the local auto-correlation function is sharply peaked, this indicates a corner.

The feature-points are then used to obtain the Delaunay triangulation. The triangles are employed in synchronizing the image during watermark extraction.

III. DELAUNAY TRIANGULATION

In order to get the Delaunay tessellation of the feature points extracted from an image a Voronoi diagram of the image is obtained first.
Voronoi tessellation is constructed by defining the area Ai closest to a point pi than to any other point on the image. The perpendicular bisector of the two points is the boundary separating the two adjacent Voronoi regions Ai and Aj containing the two points pi and pj.
To construct the Delaunay tessellation nearest neighboring points, whose cells in the Voronoi tessellation share an edge are joined. The Delaunay tessellation of a set of feature points of images are shown in fig1.



(a) (b)

Fig1 Delaunay triangulation of the feature points for (a) Baboon (b) Lena test images.

IV. DCT DOMAIN WATERMARKING

Discrete-Cosine-Transform or DCT is a popular transform domain watermarking technique. The DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands. The literature survey reveals that mostly the middle frequency bands are chosen to embed the watermark because it does not contain visually important parts of the image. The low frequencies contain visually important parts of the image. By embedded the watermark in the mid-band frequency the compression and noise attacks are prevented which usually targets the high frequency components. The mid-band frequencies (FM) of an 8*8 DCT block is shown in fig2.

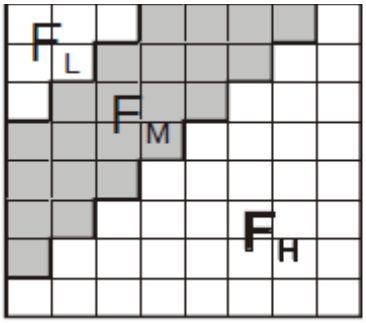


Fig2. Mid-band region of an 8*8 DCT block

V. PROPOSED METHOD

In this paper watermark embedding algorithm combines VQ, DCT and Spread-spectrum and watermark recovery algorithm incorporates Delaunay triangulation.

A. Watermark Embedding Procedure

The LBG algorithm is used to obtain the codebook of the cover image, the codebook is again decomposed into 8-by-8 pixel blocks and the DCT coefficients of each blockobtained. TheDCT coefficients of the watermark are then embedded additively into the coefficients of the codebook in a spread-spectrum format as given in the following equation.

$$I^*(u, v) = I(u, v) + \beta W(u, v) \quad (3)$$

where I(u, v), I*(u, v) and W(u, v) are the DCT coefficients of the cover image, watermarked codebook of the image and the watermark respectively. The value of β between 0.1 and 0.5 gives a trade of between robustness and visual quality depending on the pixel texture of the image.

Compute the IDCT of the watermarked codebook and then perform VQ decoding to obtain the watermarked image. The watermark embedding procedure is shown in fig3.

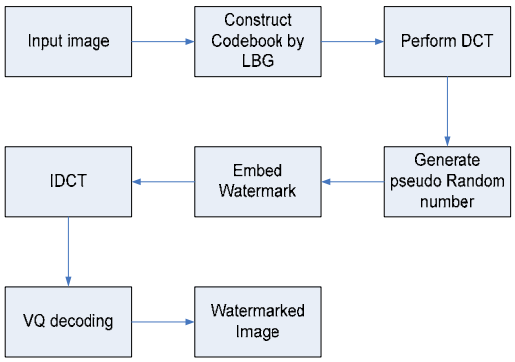


Fig3. Watermark embedding algorithm

B. Watermark Recovery Procedure

First the Delaunay tessellation of the feature points of the original and attacked image is obtained. The tessellation of the attacked image is rotated from 00 to 3600 and compared with the original image for every angle of rotation to estimate the amount of rotation attack. To estimate the amount of scaling attack, first the attacked image is reverse scaled that is for example if the attacked image is found to be higher scaled, then it is first lower scaled, and compared with the original image. To estimate the amount of translation attack sizes of the original image and attacked image is compared. To estimate the amount of combination of the attacks, combination of the above said procedure is used. Using the estimated rotation factor (RF), scaling factor (SF) and translation factor (TF) the image is restored to the position of the original image. After restoration the codebook of the resynchronized image is obtained, then its DCT coefficients is obtained. Finally the watermark is extracted from the embedded positions as given in the following equation.

$$W(u, v) = (I^*(u, v) - I(u, v)) / \beta \qquad (4)$$

Watermarkextraction procedure is shown in fig4.

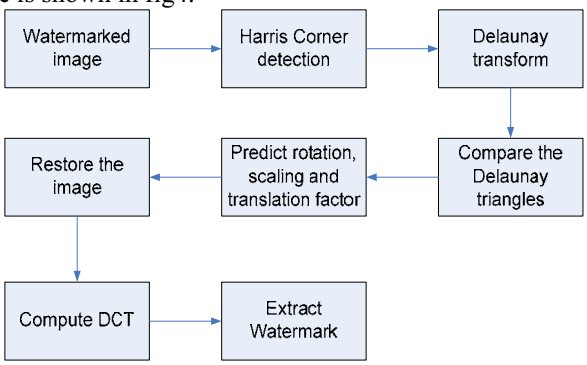


Fig4. Watermark recovery algorithm

VI. EXPERIMENTAL RESULTS

Performance of our proposed scheme is evaluated by determining the visual perceptibility and robustness of the embedded watermark.

A. Visual Perceptibility

Peak Signal-to-Noise Ratio (PSNR) is used to determine visual distortion as a result of the embedded watermark. Table1 shows the PSNR(dB) values for various test images at which there is no visible visual distortion.

	PSNR(dB)
Cameraman	31.3049
Lena	33.9739
Baboon	31.0482

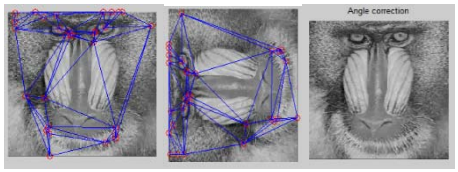
Tabel1. PSNR (dB) values of different test images

B. Robustness to Attacks

The robustness of a watermarked image can be evaluated by performing signal processing attacks and geometric attacks on the watermarked image and the quality of the extracted watermark evaluated using cross-correlation (CC) factor. Following are the types of attacks simulated.

1. Rotation attack

Several rotation attack angles were simulated and then a reversal was done for each angle and the watermark recovered. Fig5 illustrates the Delaunay tessellation of the watermarked image, rotatedwatermarked image and image after angle correction at RF 900.Fig6 illustrates original watermark embedded in baboon image,recovered watermark after restoring rotation attack



(a) (b) (c)

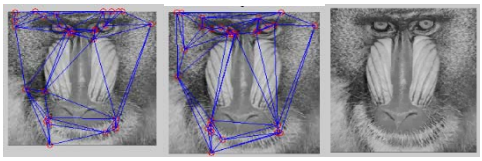
Fig5 (a) Watermarked image (b)Rotated watermarked image (c)Image after angle correction at RF 90^0

(a) (b)

Fig6 (a) Original watermark embedded in baboon image (b) Recovered watermark after restoring rotation attack

2. Scaling attack

The image was scaled from 10% to 500% of the original image size. From 10% to 89% the recovered watermark was unsatisfactory, while scaling levels above 90% the watermark is recovered successfully after restoration. Fig7 shows theDelaunay tessellation of the watermarked image, scaled watermarked image and image after scale correction at an SF 2. Fig8 shows the original watermark embedded and recovered watermark.



(a) (b) (c)

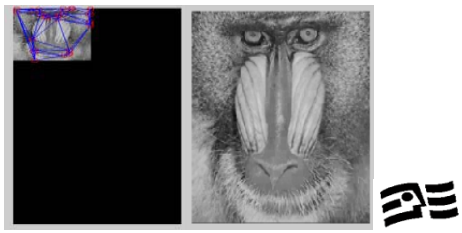
Fig7 (a) Watermarked image (b) Scaled watermarked image (c) Image after scale correction at SF 2.

(a) (b)

Fig8 (a) Original watermark embedded in baboon image (b) Recovered watermark at SF 2

3. Translation attack

Translation attacks for various TF were simulated and the watermark was recovered satisfactorily. Fig9 illustrates the Delaunay tessellation of the translated image, image after translation correction and the recovered watermark for a TF (800,300)

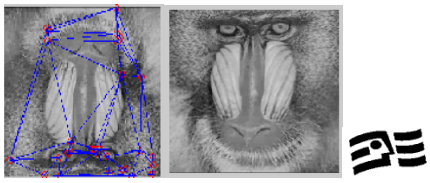


(a) (b) (c)

Figure9 (a) Translated image at a TF (800,300) (b) Image after translation correction (c) Recovered watermark

4. Scaling and rotation attack

A combination of scaling and rotation attack is simulated and the watermark recovered satisfactorily. Fig10 illustrates Delaunay tessellation of the scaled and rotated image, image after the corrections and the recovered watermark at a SF 1.2, RF 180^0



(a) (b) (c)

Fig10 (a) Rotated and translated image at SF of 1.2, RF 1800, (b) Corrected image (c) Recovered watermark

5. Rotation and Translation attack

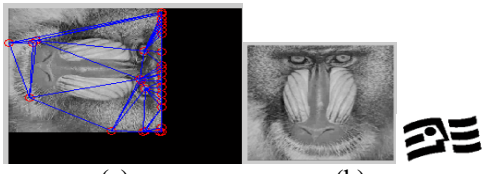
A combination of rotation and translation attack is simulated and the watermark recovered satisfactorily. Fig11 illustrates Delaunay tessellation of the rotated and translated image, image after the corrections and the recovered watermark at a RF 270^0, TF (0,200)

(a) (b) (c)

Fig11 (a) Rotated and translated image at RF 2700, TF (0,200) (b) Corrected image (c) Recovered watermark

6. Scaling, Rotation and Translation attack

A combination of scaling, rotation and translation attack is simulated and the watermark recovered satisfactorily. Fig12 illustrates Delaunay tessellation of the RST attacked image, image after the corrections and the recovered watermark for a SF of 1.5 RF of 270^0, TF of (100,200)



(a) (b) (c)

Fig12 (a) Scaled, Rotated and translated image at SF 1.5 RF 2700, TF (100,200) (b) Corrected image (c) Recovered watermark

Computer simulation experiments were conducted on other test images such as Cameraman, Lena. These experiments tested the robustness of the watermark to signal processing attacks JPEG compression and geometric processing attacks such as rotation, scaling, translation and a combination of these. In all situations watermark was successfully recovered with a high CC factor and the numerical results are shown in table 2.

	Cameraman	Lena	Baboon
JPEG (30%)	1.0000	1.0000	1.0000
Rotation 90^0	1.0000	1.0000	1.0000
Scaling 2	1.0000	1.0000	1.0000
Translation (800,300)	1.0000	1.0000	1.0000
Scaling, Rotation 1.3, 180^0	1.0000	1.0000	1.0000
Rotation, Translation 270^0, (0,200)	1.0000	1.0000	1.0000
RST 270^0,1.5,(100 ,200)	1.0000	1.0000	1.0000

Table 2.CC of various attacks on various images

VII. CONCLUSION

In this paper we have demonstrated that a watermark can be recovered after RST attacks on an image by employing Delaunay tessellation techniques. The proposed method has been tested with success on various test images on a MATLAB simulation tool.

REFERENCES

[1] R. Gonzalez, R.E. Woods, S.L. Eddins, Digital Image Processing, 3rd Edition, New Delhi, India: Prentice Hall of India Learning Pvt. Ltd, 2008.

[2] C.-H. Tang and H.-M. Hang. "A Feature-Based Robust Image Digital Image Watermarking Scheme," IEEE Trans. Signal Process., Vol. 51, No. 4, pp. 950-959, 2003.

[3] C. Harris and M. Stephens. "A combined corner and edge detector," Proc. 4th Alvey Vision Conference, pp. 147-151, 1988.

[4] H.C. Huang, S.C. Chu and Y.H. Huang, "VQ-Based Watermarking Techniques," Journal o of Comput., Vol.17, No.2,pp.37-50, July 2006.

[5] S. Katzenbeisser, and F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, MA, USA: Artech House Inc. 2000.

[6] X. Qi and J. Qi "A feature-point-based RST resistant watermarking scheme," Proc.7th LASTED Int. Conf. Signal Process., vol.51, No. 4,pp.950-959,2003.

[7] DCT : Theory and Application – Syed Ali Khayam, Department of Electrical and Computer Engineering, Michigan State University.

[8] Attacks on Copyright Marking Systems - Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn