Key Dependent Feature Point Based Image Watermaking Scheme

Ramesh Kumar Surapathi[1], Kamalika Datta[1], and I. Sengupta[2]

[1] School of Computer Engineering,
KIIT University,
Bhubaneswar PIN- 751024
[2] Dept. of Computer Science & Engineering,
Indian Institute of Technology Kharagpur,
Kharagpur PIN-721302

Abstract. An approach to a blind discrete Wavelet Transformation (DWT) domain feature point based image watermarking technique is proposed in this paper. The embedding of the watermark is performed into the image feature points defined by the Harris detector and the additional feature points are generated from the existing feature points using a key dependent algorithm. The proposed method is simple and secure. It is also experimentally found to be robust against various geometric and noise attacks.

Keywords: Image watermarking, DWT, Feature point extraction, Harris detector.

1 Introduction

With the rapid growth of Information Technology in particular, communication technology had pave the way for the usage of many multimedia data. These multimedia data includes images, audios and videos. As these data are very easily available, illegal copying and distribution are the two major issues of concern. To overcome from such issues, different copyright protection techniques are proposed in literature. One of the major forces to protect the multimedia data from illegal copying is Digital Watermarking. In this paper, we focus on Image Watermarking.

Digital Image Watermarking is a technique in which some additional information is embedded into the image file, which later helps to trace the authenticity of the particular image. Broadly, Image Watermarking techniques are divided into visible and invisible image watermarking. Visible image watermarking is a technique in which a logo is placed in the original image which identifies the owner of the image. On the other hand, invisible watermarking can again be divided into temporal domain and spatial domain techniques. Temporal domain techniques are those where the watermarks are directly embedded by changing the pixel values of the image, whereas in spatial domain techniques, the original image passes through some transformations before the watermark embedding. Spatial domain image watermarking techniques performs better as compared to simple temporal domain techniques. Again spatial

N. Meghanathan et al. (Eds.): CCSIT 2012, Part II, LNICST 85, pp. 498–507, 2012.

domain techniques can further be divided into DCT based image watermarking, FFT based image watermarking and DWT based image watermarking.

The following section two gives a brief survey of review works. In section three, the proposed technique is discussed, Section four discusses the experimental observations and finally Section five provides a brief conclusion.

2 Review Works

Spectral domain watermarking is heavily preferred over the spatial domain because of the robustness of the embedded watermark. The spectral domain image watermarking branches into DCT, DFT and DWT.

In [1] and [2], the combination of DCT and DWT has been joined together to give rise to a better and robust embedding scheme. In [5], the original image is transformed by DWT into four bands of frequencies (LL, LH, HL, and HH) using haar wavelet and then, DCT is performed in each of the four bands where the watermark image is embedded directly into the four bands. The coefficient of embedding in the LL band is 0.1 and the coefficient of embedding in the higher frequency bands is 0.2.

In [2], DCT or DWT is carried out on the original image to decompose the original image into various frequency components and then additive or multiplicative embedding of the one level DCT or DWT decomposed watermark is done in the mid frequency components of the decomposed original image. The linear relation between the transform coefficients of the watermark and a security key makes the watermark visually imperceptible. This is a semi blind watermarking scheme.

In [3], a DCT-SVD non blind based image watermarking scheme has been proposed .DCT is carried out on the original image which is haphazardly arranged into four different frequency bands on which SVD (Singular Value Decomposition) is carried out .The watermark undergoes Discrete Cosine Transform and SVD to form singular watermark values. The singular values of the original image are modified using the singular values of the watermark. This embeds the watermark into the image. The extraction of the watermark needs the original image.

In [5], a semi-blind DWT based image watermarking scheme has been illustrated. The original image is first decomposed using the ‘haar’ wavelet into three hierarchical levels using Discrete Wavelet Transform. The watermark is scrambled through a PN sequence and is embedded in the selected coefficients of the transformed image in HL, LH and HH bands at all levels and in the LL band of the third level. The watermark detection requires the original image.

In [6] Hu et al proposed a method of DWT domain feature point based image watermarking technique where he generated four image feature points using an intersection based feature point detector. Further using these feature points, some additional points are generated and then triangulation is performed in a key dependent manner, thereafter embedding is performed in the resulting triangles. In [7] Priya et al proposed a DWT domain image watermarking scheme which is geometric invariant. This scheme is found to be robust against some of the geometric attacks.

A feature point based image watermarking [8], [9] is a method of recovering the image from the distortions using the feature points as a content descriptor. Feature

points are often the corners or edges of the image. The identification of feature points robust to distortions are detected is the key landmark. Using these feature points, this paper enhances the embedding technique. Harris detector [10] is the required algorithm for the detection of the feature point within an image. Harries detector relies on both the Harris measure and the Gaussian scale representation. Therefore, a combination of both follows in the extraction of the feature points.

In this paper, we propose an feature point based image watermarking technique in DWT domain which is found to be robust against various geometric and other noise attacks. Our technique is found to be secure and imperceptible. Experiments have been carried out, which shows that the watermark image retains its quality.

3 Proposed Approach

The approach used here is a blind watermarking scheme of embedding the watermark in the wavelet domain. In our proposed approach, we perform a 3 level decomposition on the blue component of an original image in DWT domain using Haar wavelet. From the level 3 diagonal coefficient of image, the feature points are generated by Harris detector. Using the key dependent property, additional numbers of feature points are generated from the existing feature points and the watermark is finally embedded into the extracted feature points. The key used in the extraction of additional feature points acts as a secret key for security.

3.1 Embedding Technique

The embedding technique is a feature point based image watermarking scheme wherein watermark is embedded in the feature points of the third level diagonal coefficients. The Major postulates of the embedding technique are underlined herein:

1) Perform a 3 level DWT decomposition.
2) Extraction of feature points using a Harris Detector.
3) Generation of new feature points using a Key Dependent Algorithm.
4) Watermark Embedding.

3.1.1 Third Level DWT Decomposition

The blue component of an original image is first decomposed using the Haar wavelet into three hierarchical levels using DWT. Experiments have shown that the embedding of watermark on the diagonal coefficient of the blue component of an image results in high PSNR value. So, in our proposed technique the feature point's extraction is performed on the level 3 diagonal coefficient using a Harris detector.

3.1.2 Extraction of the Feature Points

Extraction of the feature points from the diagonal coefficient using a Harris detector algorithm involves the following steps: 1) Compute x and y derivatives of original image I using a convolution kernel dx and dy. Let the derivatives be Ix and Iy.

2) Compute products of derivatives at each pixel.

$$I_x^2 = I_x * I_x;$$
$$I_y^2 = I_y * I_y;$$
$$I_{xy} = I_x * I_y;$$

3) compute the sum of products of derivatives at each pixel using a Gaussian filter.

$$S_x^2 = G * I_x^2;$$
$$S_y^2 = G * I_y^2;$$
$$S_{xy} = G * I_{xy};$$

4) Compute the response of the detector at each pixel.

$$R = (S_x^2 .* S_y^2 - S_{xy}^2) - k*(S_x^2 + S_y^2)^2;$$

5) Find out the points with large corner response function R (R> threshold).
6) Take the points of local maxima of R.
The points generated are the required feature points. The feature points generated from the diagonal coefficient are shown in fig. 1(a).

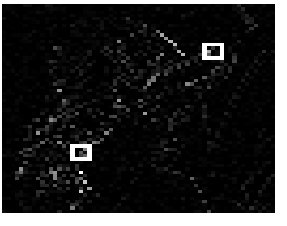


Fig. 1 (a).

3.1.3 Key Dependent Algorithm

From the existing feature points, the remaining numbers of required feature points are extracted depending upon the number of bits of the watermark. For the extraction of new feature points, we use a Key Dependent algorithm. This involves the generation of pseudo random numbers depending on a secret key, which is stored for the watermark extraction.

The steps involved in the key dependent algorithm are as follows:

1) Compute the bounding box of the existing feature points as follows.
X1 = Minimum x coordinate of the existing feature points
X2 = Maximum x coordinate of the existing feature points
Y1 = Minimum y coordinate of the existing feature points
Y2 = Maximum y coordinate of the existing feature points.

The Bounding Box is defined by {(X1, Y1), (X2, Y1), (X2, Y2), (X1, Y2)}.

2) Generate two uniform deviates h1 and h2 from the secret key. Then a new point is generated as

$$X = \lfloor (X1*(h1/200) + X2*(1-(h1/200))) \rfloor ;$$
$$Y = \lfloor (Y1*(h2/200) + Y2*(1-(h2/200))) \rfloor ;$$

3) Repeat step2, until the total number of feature points are equal to the number of bits of the watermark. All the feature points are shown in fig. 1(b).

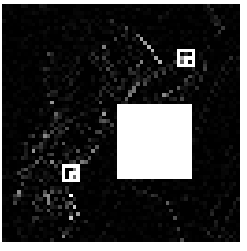


Fig. 1 (b).

3.1.4 Watermark Embedding

The watermark bits are embedded into the feature points by the formula,

$$D3(x, y) = D3(x, y) + 0.15*w(x1, y1);$$

x, y are the coordinates of the feature points
X1, y1 are the coordinates of the watermark
D3 is the level 3 diagonal coefficient
W is the watermark.

The original and the watermarked image is shown in fig 1(c) and fig 1(d) respectively.

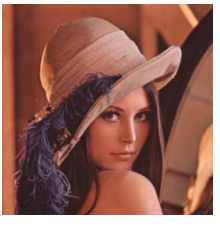


Fig. 1 (c).

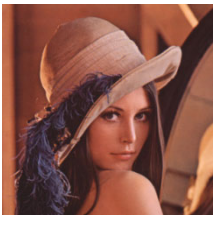


Fig. 1 (d).

3.2 Extraction Technique

The extraction of the watermark from the watermarked image requires the presence of the original image and the secret key.

1) Perform a 3 level DWT decomposition on original image and watermarked image.
2) Extraction of feature points using a Harris detector.
3) Generate new feature points using a Key Dependent Algorithm.
4) Watermark extraction is done.

Perform 3-level decomposition on the blue components of original image and watermarked image. Generate again all the feature points of the original image by repeating steps 3.1.2 and 3.1.3 using the secret key. Then the watermark is extracted from the feature points of original image and the watermarked image by using the formula,

$$W(x1, y1) = (Dw3(x, y) – D3(x, y))/0.15;$$

x, y are the coordinates of the feature points
Dw3 is the level 3 diagonal coefficient of watermarked image
D3 is the level 3 diagonal coefficient of watermarked image
W is the watermark.

The original and extracted watermark is shown in fig 1(e) and fig 1(f) respectively.

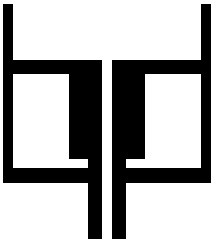


Fig. 1 (e).

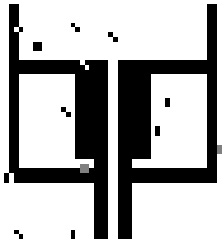


Fig. 1 (f).

4 Experimental Results

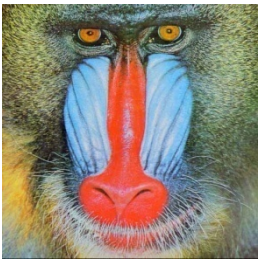
This section discusses the experimental results of our proposed watermarking scheme. The algorithm has been implemented using Matlab7. Rest of the section is characterized into:

1) Performance Evaluation without attacks
2) Watermark Extraction from various attacks
3) Performance Evaluation with attacks.

4.1 Performance Evaluation without Attacks

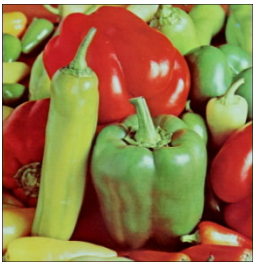
For this evaluation, we have taken the images Lena, Baboon, Airfield, and Peppers as shown below. On every image, the proposed watermarking technique is performed and then the respective PSNR value of the image is calculated by comparing the watermarked image with its original image. The results of the evaluation are shown in the table 1.

Lena



Baboon

Airfield



Peppers

Table 1. PSNR calculation of various watermarked images

Images	PSNR Values
Lena	38.9119
Baboon	36.8103
Airfield	38.3127
Peppers	38.1698

4.2 Watermark Extraction from Various Attacks

We have taken the Lena image to present the results of the watermark extraction. To evaluate the robustness of the proposed watermarking scheme, various attacks are tested.

Fig. 2 (a).

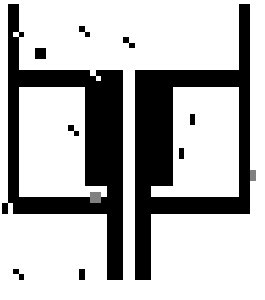
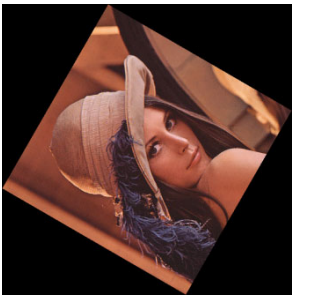


Fig. 2 (b).

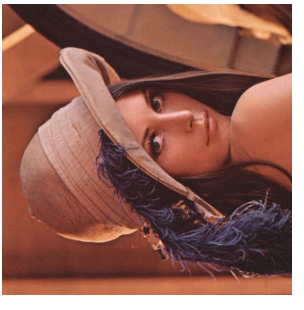
All these attacks are simulated using Matlab7. After each attack, the watermark is extracted by the proposed technique. The original Lena image of size 512*512 and the original watermark are shown in fig 2(a) and fig 2(b). The various attacks tested and their respective attacked images and the watermark retained are shown below.

Various Attacks Tested

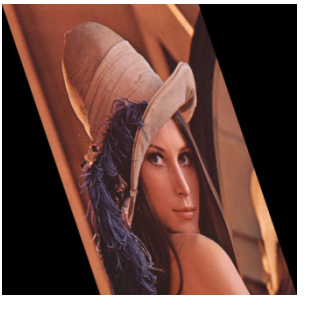
Scaling at 2:1



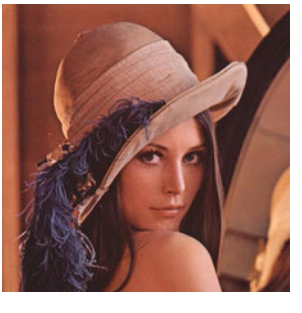
Rotation by 60º



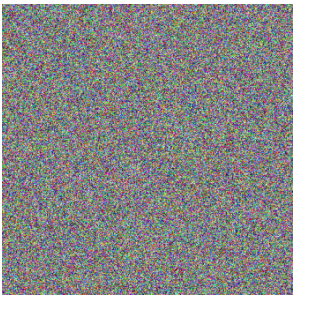
Combination of scaling at 2:1
And rotation by 90º



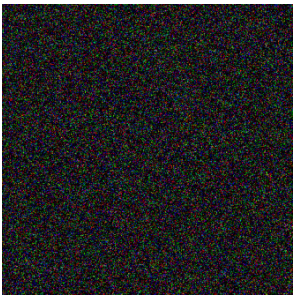
Transform



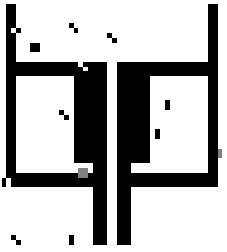
JPEG Compression by 1:19



Gaussian noise of mean and
Variance 0.5



Salt & Pepper Noise of noise Density 0.2



Extracted Watermark

4.3 Performance Evaluation with Attacks

To evaluate the imperceptibility of the proposed technique, few common attacks are tested on the watermarked Lena image and their respective PSNR values are shown in Table 2. All these attacks are performed using Adobe Photoshop CS3.

Table 2. Attacks on Images and the PSNR values

Lena Attacks	PSNR Values
JPEG Compression 1:19	32.4393
Gaussian Noise (2%)	32.9937
Sharpen Edges	35.1832
Uniform Noise (2%)	35.5392
Salt & Pepper Noise (0.001)	33.5771
Poisson Noise	28.0450
Speckle Noise(0.001)	35.0616

5 Conclusion

A feature point based image watermarking scheme in DWT domain is proposed in this paper. DWT is performed on the blue component of the image up to third level and the diagonal coefficients of the third level are chosen for embedding the watermark. Use of the secret key in embedding entails the presence of the secret key at the receiving side for watermark extraction, which is the feature which protects the watermark from being tampered by attackers. All the experimental results are found to be resistant against various signal processing attacks, geometrical and noise attacks.

References

1. Fotopoulos, V., Skodras, A.N.: A Subband DCT Approach to Image Watermarking. Electronics Laboratory Computer Technology Institute (CTI) University of Patras (July 1999)
2. Tripathi, S., Jain, R.C.: Novel DCT and DWT based Watermarking Techniques for Digital Images. Birla Institute of Technology & Science, Pilani. V. Gayatri, HP LABS
3. Sverdlov, A., Dexter, S., Eskicioglu, A.M.: Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies. Department of CIS, Brooklyn College, the Graduate Center the City University of New York (2004)
4. Huang, X., Chen, Z.: A Wavelet Based Scene Image Fusion Algorithm. School of Automation Science and Electrical Engineering, Beijing Institute of Aeronautics and Astronautics. In: Proceedings of IEEE Tencon 2002 (2002)
5. Safabaksh, R., Zaboli, S., Tabibiazar, A.: Digital Watermarking on Still Images Using Wavelet Transform. Computer Engineering Department, Amirkabir University of Technology (2002)
6. Hu, S.: Key-dependant decomposition based image watermarking Published by ACM 2004 Article. In: Proceeding MULTIMEDIA 2004 Proceedings of the 12th Annual ACM International Conference on Multimedia ©2004 table of contents (2004) ISBN: 1-58113-893-8
7. Nantha Priya, N.R., Lenty Stuwart, S.: Robust Feature Based Image Watermarking Process. International Journal of Computer Applications © 2010 by IJCA Journal (5) - Article 3 (2010)
8. Tang, C.W., Hang, H.M.: A feature-based robust digital image watermarking scheme. IEEE Transaction. Signal Process. 51(4), 950–959 (2003)
9. Alghoniemy, M., Tewfik, A.H.: Geometric invariance in image watermarking. IEEE Transaction. Image Process. 13(2), 145–153 (2004)
10. Harris, C., Stephens, M.: A combined corner and edge detector. In: Proceedings of 4th Alvey Vision Conference, pp. 147–151 (1988)