ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Novel Technique for Digital Watermarking with Feature Based Disparity Values

S.S.Sujatha*
Associate Professor in Computer Science,
S.T.Hindu College,
Nagercoil, India,
sujaajai@gmail.com

Dr.M.Mohamed Sathik
Associate Professor in Computer Science,
Sadakathullah Appa College,
Tirunelveli, India
mmdsadiq@gmail.com

Abstract: This paper presents a blind wavelet based image watermarking technique which embeds watermark signal into the host image in order to authenticate it. The proposed technique utilizes the perceptual information of the image content to generate the watermark. The watermark is designed by taking account of the values in the low frequency band of wavelet domain and the rescaled version of original image. The disparity between them is calculated and is disordered using Arnold transform to improve security of watermarking process. The resultant matrix is the required watermark and is embedded in the high frequency band in the wavelet domain. The watermarked image still preserves high image quality after the embedding process. Simulation results show that this technique is robust against some of the incidental image processing operations.

Keywords - Digital watermarking, Discrete Wavelet Transform, Arnold transform, Image Authentication, Content based watermarking.

I. INTRODUCTION

The internet is an excellent distribution system for the digital media because of its inexpensiveness and efficiency. Also the images can be readily shared, easily used, processed and transmitted which causes serious problems such as unauthorized use and manipulation of digital content. As a result, there is the need for authentication techniques to secure digital images. Digital watermarking is a technique which embeds additional information called digital signature or watermark into the digital content in order to secure it. A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image.

Several methods have proposed in literature. A survey is in [1]. Two categories of Digital watermarking algorithms are spatial-domain techniques and frequency-domain techniques. Least Significant Bit (LSB) is the simplest technique in the spatial domain techniques [2] which directly modifies the intensities of some selected pixels. The frequency domain technique transforms an image into a set of frequency domain coefficients [3]. The transformation adopted may be discrete cosine transform (DCT), discrete Fourier transforms (DFT) and discrete wavelet transforms (DWT) etc. After applying transformation, watermark is embedded in the transformed coefficients of the image such that watermark is not visible. Finally, the watermarked image is obtained by acquiring inverse transformation of the coefficients.

In feature based watermarking scheme, watermark is generated by applying some operations on the pixel value of host image rather than taking from external source. Recent studies revealed the fact that the content of the images could be used to improve the invisibility and the robustness of a watermarking scheme. In the proposed watermarking scheme, discrete wavelet transform (DWT) is used for embedding watermarks, since it is an excellent time-frequency analysis method, which can be well adapted for extracting the information content of the image [4]. A detail survey on wavelet based watermarking techniques can be found in [5].

Yuan et al.[6] proposed an integer wavelet based Multiple logo watermarking scheme, the watermark is permuted using Arnold transform and is embedded by modifying the coefficients of the HH and LL subbands. Qiwei et al.[7] put forward a DWT based blind watermarking scheme by scrambling the watermark using chaos sequence. Many of the algorithms proposed meet the imperceptibility requirement quite easily but robustness to different image processing attacks is the key challenge and the algorithms in literature addressed only a subset of attacks.

This paper proposes a novel DWT based blind watermarking scheme, in which watermark is constructed from the spatial domain and is embedded in the high-frequency band. The watermark construction process finds the disparity values between the low frequency band of the wavelet domain and the rescaled version of original image. The proposed method assures security by utilizing Arnold transform which scrambles the watermark pattern. The extraction is done without using original image. This method is robust against many common image processing attacks and experimental results verify this.

The rest of this paper is organized as follows: Section 2 gives an overview of Discrete Wavelet Transform and Arnold Transform. The details of watermark generation, embedding and extraction processes are explained in Section 3. Section 4 shows experimental results and discussion. Finally section 5 provides concluding remarks.

II. RELATED BACKGROUND

This section briefly describes the techniques and methods that have been adopted by the proposed scheme, including DWT and Arnold Transform.

A. Discrete Wavelet Transform

The DWT decomposes input image into four components namely LL, HL, LH and HH where the first

letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns [8], which is shown in Fig.1.

The lowest resolution level LL consists of the approximation part of the original image. The remaining three resolution levels consist of the detail parts and give the vertical high (LH), horizontal high (HL) and high (HH) frequencies. In the proposed algorithm, watermark is embedded into the host image by modifying the coefficients of high-frequency bands i.e. HH subband.

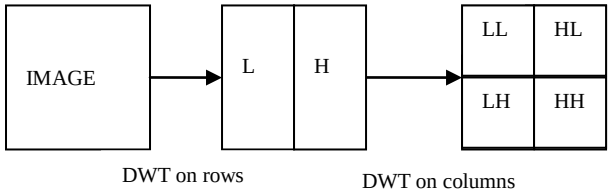

Figure. 1 DWT decomposition of image

For a one level decomposition, the discrete two-dimensional wavelet transform of the image function f(x, y) can be written as [9]

$$LL = [(f(x,y) * \phi(-x)\,\phi(-y))\,(2n, 2m)]_{(n,m)\in z^2}$$

$$LH = [(f(x,y) * \phi(-x)\,\psi(-y))\,(2n, 2m)]_{(n,m)\in z^2}$$

$$HL = [(f(x,y) * \psi(-x)\,\phi(-y))\,(2n, 2m)]_{(n,m)\in z^2}$$

$$HH = [(f(x,y) * \psi(-x)\,\psi(-y))\,(2n, 2m)]_{(n,m)\in z^2}$$

where $\phi(t)$ is a low pass scaling function and $\psi(t)$ is the associated band pass wavelet function.

B. Arnold Transform

A digital image can be considered as a two unit function f(x,y) in the plane Z. It can be represented as Z = f(x, y) where x, y $\in \{0,1,2,3....N-1\}$ and N represents order of digital image. The image matrix can be changed into a new matrix by the Arnold transform which results in a scrambled version to offer security. It is a mapping function which changes a point (x, y) to another point (x^1, y^1) by the equation (1)

$$\begin{aligned} x' &= (x+y) \bmod N \\ y' &= (x+2y) \bmod N \end{aligned} \qquad (1)$$

III. PROPOSED METHOD

In the proposed scheme, there are three significant phases. They are Watermark generation, Watermark embedding and Watermark Detection. The watermark is generated from the information content of original image and so there is no need of external image or logo. Hence it is necessary to devise a method to generate watermark. The resolution of watermark is assumed to be half of that of original image.

For embedding the watermark, a 1-level Discrete Wavelet Transform is performed. Watermark information is embedded in the high frequency bands (HH1) since it is robust against various normal image processing and malicious attacks. The resultant image is called watermarked image. In detection phase, watermark is once again generated from watermarked image and also extracted the embedded watermark from HH1 subband. Comparison is made between those two watermarks to decide authenticity.

A. Watermark Generation

The watermark pattern is generated from the spatial domain information. Figure 2 shows the steps involved in Watermark generation procedure.

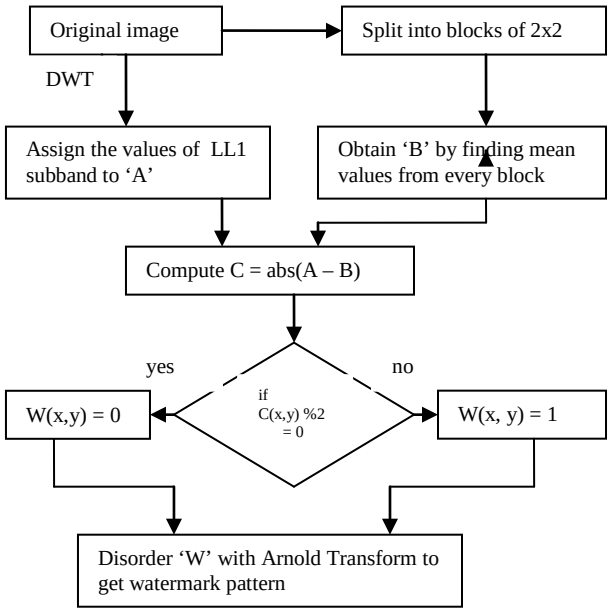

Figure. 2. Watermark Generation Procedure

The watermark is created according to the following steps:

[a] Consider the original image P of size M x M.

[b] Perform 1-level DWT on the original image and acquire the LL1 component to find watermark pattern, which is of size M/2 x M/2. Let this matrix be 'A'.

[c] A reduced size (M/2 x M/2) image 'B' is obtained from original image by performing the following steps.

(i) Partition the original image into non-overlapping blocks of size 2x2.

(ii) Compute one feature value from each block according to equation (2)

$$B(x,y) = \frac{\sum_{i=1}^{2}\sum_{j=1}^{2} P(x*2+i, y*2+j)}{4} \qquad (2)$$

where $0 \le x \le M/2$, *and* $0 \le y \le M/2$.

[d] Find the absolute difference between A and B. Let it be C.

[e] A binary sequence 'W' can be obtained by applying the following constraint.

$$W(x,y) = \begin{cases} 0 & \text{if } C(x,y) \text{ is even} \\ 1 & \text{otherwise} \end{cases}$$

[f] Disorder the matrix 'W' with the help of Arnold Transform, which is the required watermark pattern to be embedded in to the host image.

B. Watermark Embedding

The watermark is embedded in the high frequency subband of DWT as follows and is depicted in figure 3.

[a] Apply 1-level DWT to original image.
[b] The watermark is embedded in the high frequency component HH1 of DWT.
[c] Perform inverse wavelet transform to obtain the watermarked image.

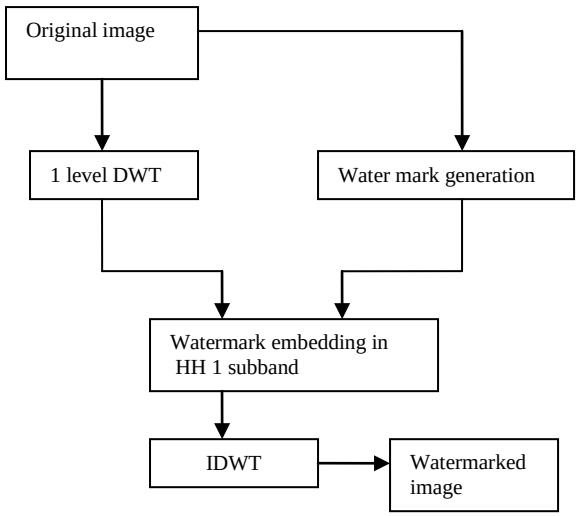

Figure. 3 Watermark Embedding Process

C. Watermark Detection

Proposed watermarking scheme extracts and generates watermark information from watermarked image and so original image is not essential. So it can be referred as blind watermarking.

The authentication process includes the following steps:

[a] Watermark is derived form the content of watermarked image using the steps described under watermark generation in section III.A.
[b] Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 subband.
[c] Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.
[d] Quality of watermarked image and the watermark is found out according to equation (3) and (5).

IV. EXPERIMENTAL RESULTS

In this paper, we consider the images with number of rows and columns are of equal size since the embedded watermark pattern is a square matrix. For testing, the size of the original image is taken as 512x512. Figure 4(a) shows original image. A 256x256 binary watermark signal is constructed from the perceptual information of original image and is embedded within itself. The proposed method is tested using MATLAB.

After embedding the watermark, there was no visual difference between the original and watermarked images. Figure 4(b) shows watermarked image. The absolute difference of the pixel intensities of the watermarked image and the original image is shown in figure 4(c). The difference image shows that the technique ensures high degree of fidelity.

(a) (b) (c)

Figure. 4(a) Original Image b) Watermarked Image (c) Difference Image

The visual quality of watermarked and attacked images is measured using the Peak Signal to Noise Ratio, which is defined in equation (3). The PSNR value of watermarked image is 59.1168, which indicates that there is very little deterioration in the quality of original image.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{3}$$

where MSE is Mean Squared Error between original and distorted images, which is defined in equation (4).

$$MSE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{[OI(i,j) - DI(i,j)]^2}{MxN} \tag{4}$$

where OI is original image and DI is the distorted image.

The metric used to test the robustness of the proposed algorithm is the Similarity Ratio, which is a comparison between extracted and original watermark as defined in equation (5).

$$SR = \frac{S}{S + D} \tag{5}$$

where S denotes number of matching pixel values and D denotes number of different pixel values. In the proposed scheme, similarity ratio evaluated between extracted and calculated watermark is 0.8406 which indicates that the number of matching pixels are high and hence authenticity is preserved.

Figure. 5. Sample Images

To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on various images with different textures under some common image processing attacks. Watermark invisibility and robustness is evaluated on images provided in Figure 5. The PSNR values and Similarity Ratios of these watermarked images are tabulated in Table 1. The calculated PSNR values for all images are greater than 35.00 db, which is the empirical value for the image without perceivable degradation. The proposed method shows better

authentication since the similarity ratios computed between extracted and original watermarks are having high values.

Table 1: Performance Of The Proposed Scheme

Picture	PSNR	SR
3.a	59.1168	0.8406
3.b	54.0368	0.8558
3.c	54.8213	0.8811
3.d	56.3542	0.8601
3.e	55.2045	0.8789
3.f	57.7054	0.8203

The proposed algorithm was tested using several incidental image processing operations. The attacks chosen were adding noises such as Gaussian and salt & pepper noises, median filtering, linear filtering, blurring, rescaling, JPEG compression, rotation, intensity adjustment and histogram equalization. Table 2 gives the performance of proposed watermarking scheme under various attacks.

The simulation results in the case of additive Gaussian noises show that increase in mean and variance affects the imperceptibility of watermarked image. But robustness of watermark in this attack is high with constant variance 0. An increase in variance affects the robustness. The watermarked image is attacked with salt & pepper noise with density 0.002, watermark is highly robust in this case.

Table 2: Quality Evaluation of Proposed Scheme

Attacks		PSNR(dB)	SR
No		59.1168	0.8406
Adding Guassian Noise (Mean and Variance)	0.01,0	38.3272	0.8371
	0, 0.001	30.0997	0.4243
Adding Salt & Pepper noise	0.002	32.1381	0.8370
Median filtering	3x3	29.5727	0.6629
Linear filtering	3x3	28.5485	0.6717
Blurring		37.8322	0.8083
Rescaling (512-256-512)		56.1065	0.8463
JPEG compression (QF)	90	43.1448	0.6488
	70	37.4799	0.6956
	50	35.2240	0.7418
	30	33.2002	0.7736
	10	29.1867	0.8158
Rotation with cropping	5^o	13.9492	0.7135
	10^o	12.0325	0.6957
Image adjustment		18.5312	0.8335
Histogram Equalization		19.0944	0.7498

Watermarked image is smoothed with a 3x3 median filter. Experimental results reveal that robustness and imperceptibility are in a moderate rate. Similar is the case with linear filtering.

A Gaussian lowpass filter of size 3x3 and a standard deviation sigma 0.5 is applied on the image. The quality of watermarked image is high in this case. The high value of Similarity Ratio indicates that the proposed method is able to withstand against blurring. In addition, the experimental result conveys that the proposed method is robust against scaling operation.

The watermarked image is compressed with lossy JPEG compression by applying the quality factor ranges from 0 to 100. Higher number means less degradation due to compression but the resulting file size is larger. Simulation results show that a decrease in quality factor decreases the imperceptibility of watermarked image but increases the robustness of watermark. Simulation results against rotation operation reveal the fact that the proposed algorithm is able to withstand such kind of attacks.

Experimental results against Image adjustment and Histogram equalization attacks disclose that the robustness of watermark is high but the quality of watermarked image is degraded.

V. CONCLUSION

This study has proposed a robust watermarking which provides a complete algorithm that embeds and extracts the watermark information effectively. In this method, the low frequency band of wavelet domain is used to construct the content dependent watermark and the watermark pattern is embedded in the high frequency coefficient in the wavelet domain. The designed method makes use of the Arnold Transform for scrambling the watermark and thereby offers better security. Moreover the authentication process provides qualities like imperceptibility, robustness and security. This watermarking scheme deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained.

The performance of the watermarking scheme is evaluated with common image processing attacks such as adding noises, filtering, blurring, scaling, rotation, JPEG compression, intensity adjustment and histogram equalization. Experimental results demonstrate that watermark is robust against those attacks.

VI. REFERENCES

[1] C.Rey, J.Dugelay: A survey of watermarking algorithm for Image authentication. In: Journal on Applied Signal Processing, Vol.6, pp.613-621, 2002.

[2] C.I.Podilchuk, E.J.Delp: Digital watermarking: algorithms and applications. In: IEEE Signal Processing Magazine, pp. 33-46, July 2001.

[3] Arvind kumar Parthasarathy, Subhash Kak: An Improved Method of Content Based Image Watermarking. In: IEEE Transaction on broadcasting, Vol.53, no.2, June 2007, pp.468 -479.

[4] Ramana Reddy, Munaga V.N.Prasad, D.Sreenivasa Rao: Robust Digital Watermarking of Color Images under Noise Attacks. In: International Journal of Recent Trends in Engineering, Vol.1, No. 1, May 2009.

[5] Q.Ying and W.Ying, "A survey of wavelet-domain based digital image watermarking algorithm", Computer Engineering and Applications, Vol.11, pp.46-49, 2004.

[6] Yuan Yuan, Decai Huang, and Duanyang Liu, "An Integer Wavelet Based Multiple Logo-watermarking Scheme," IEEE, Vol.2 pp.175-179, 2006.

[7] Qiwei Lin, Zhenhui Liu, and Gui Feng, "DWT based on watermarking algorihthm and its implementing with DSP," IEEE Xplore, pp. 131-134, 2009.

[8] Xiang-Gen Xia, Charles G.Boncelet, Gonzalo: Wavelet Transform based watermark for digital images. In: OPTICS EXPRESS, 1998 Vol.3, No.12, pp 497-511.

[9] Sanjeev Kumar, Balasubramanian Raman, Manoj Thakur: Real Coded Genetic Algorithm based Stereo image Watermarking. In: IJSDIA, 2009, Vol. 1 No.1 pp 23-33.

[10] Rafael C.Gonzalez, R.E.Woods, , Steven L. Eddins : Digital Image Processing Using MATLAB, India (2008)

[11] Hongmei Liu, Junhui Rao, Xinzhi Yao: Feature Based Watermarking Scheme for Image Authentication. In: IEEE, 2008, pp 229-232.

[12] J.Dittmann: Content-fragile Watermarking for Image Authentication. In: Proc. of SPIE, Security and Watermarking of Multimedia Contents III, vol.4314, pp.175-184, 2001.