A Novel DWT Based Blind Watermarking for Image Authentication

S. S. Sujatha[1] and M. Mohamed Sathik[2]
(Corresponding author: S. S. Sujatha)
Department of Computer Science, South Travancore Hindu College[1]
Nagercoil, Tamil nadu, Pin. 629002, India
Departmrnt of Compute Science, Sadakathullah Appa College, Tirunelveli, India[2]
(Email: sujaajai@gmail.com)
(Received Nov. 9, 2010; revised and accepted Jan. 30, 2011)

Abstract

Digital Watermarking is a technique which embeds a watermark signal into the host image in order to authenticate it. In our previous work [6], a watermark pattern was constructed from the information content of the image in the form of a Hankel matrix, but which was not robust against rotation operation. This paper proposes an innovative watermarking scheme, in which low frequency subband of wavelet domain and the rescaled version of original image are utilized in the watermark generation process. A scrambled version of watermark is obtained with the help of Arnold Transform. The operation of embedding and extraction of watermark are done in high frequency domain of Discrete Wavelet Transform since small modifications in this domain are not perceived by human eyes. This watermarking scheme deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained. Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are computed to measure image quality. In addition, the competency of proposed method is verified under common image processing operations and a comparative study is made against the technique proposed in [6].

Keywords: Content based watermarking, discrete wavelet transform, Hankel matrix, image authentication, robust watermarking

1 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.

The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little trade off between the embedding strength (the watermark robustness) and quality (the watermark invisibility). Increased robustness requires a stronger embedding, which in turn increases the visual degradation of the images. For a watermark to be effective, it should satisfy the following features. They are:

- **Imperceptibility -** It should be perceptually invisible so that data quality is not degraded and attackers are prevented from finding and deleting it.
- **Readily Extractable -** The data owner or an independent control authority should easily extract it.
- **Unambiguous -** The watermark retrieval should unambiguously identify the data owner.
- **Robustness -** It should tolerate some of the common image processing attacks.

The commonly used watermarking applications include copyright protection, authentication, and ownership identification. The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. Furthermore the invisible watermarks are categorized into watermarking techniques as fragile and robust. Generally, a robust mark is designed to resist attacks that attempt to remove or destroy the mark. These algorithms ensure that the image processing operations do not erase

the embedded watermark signal. On the other hand a fragile mark is designed to detect slight changes to the watermarked image with high probability.

Several methods have been proposed in literature. A survey is in [5]. 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 [4] which directly modifies the intensities of some selected pixels. The frequency domain technique transforms an image into a set of frequency domain coefficients [7]. 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 performing 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. 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 [8]. A detail survey on wavelet based watermarking techniques can be found in [13].

To improve the security, Wang *et al.* [10] adopted a key dependent wavelet transform. To take the advantage of localization and multiresolution property of the wavelet transform, Wang and Lin [11] proposed wavelet tree based watermarking algorithm. Tao et al. [9] put forward a discrete-wavelet transform based multiple watermarking algorithm. The watermark is embedded into LL and HH subbands to improve the robustness. Luo *et al.* [3] introduced an integer wavelets based watermarking technique to protect the copyright of digital elevation mode data by utilizing encryption technique to lift the security.

Yuan *et al.* [14] 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.* [2] 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. First, a DWT is performed on the host image and values in LL1 subband forms the first matrix. The second matrix is formed by finding average values from every 2x2 blocks. Watermark construction process finds the disparity values between those two matrices which have been constructed from the content of original image. The resultant matrix is disordered with the help of Arnold Transform. The extraction is done without using original image. This method is robust against many common image attacks and experimental results verify this. The security of the proposed method lies on the multifaceted procedure used to construct watermark.

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.

2 Related Background

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

2.1 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 [12], which is shown in Figure 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.

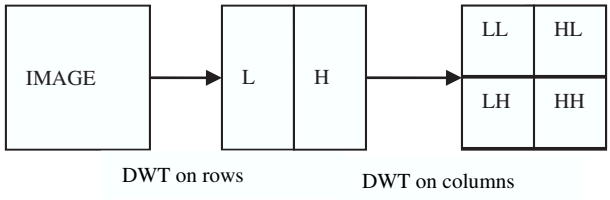

Figure 1: DWT decomposition of image

For a one level decomposition, the discrete two-dimensional wavelet transform of the image function $f(x, y)$ can be written as [1].

$$\begin{aligned} LL &= [(f(x,y) * \phi(-x)\phi(-y))(2n, 2m))]_{(n,m)\in Z^2} \\ LH &= [(f(x,y) * \phi(-x)\psi(-y)(2n, 2m))]_{(n,m)\in Z^2} \\ HL &= [(f(x,y) * \psi(-x)\phi(-y)(2n, 2m))]_{(n,m)\in Z^2} \\ HH &= [(f(x,y) * \psi(-x)\psi(-y)(2n, 2m))]_{(n,m)\in Z^2} \end{aligned}$$

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

2.2 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 $x,\ y \in \{0, 1, 2, 3, \ldots, N-1\}$ 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).

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

3 Proposed Method

In the proposed scheme, there are three significant phases: Watermark generation, Watermark embedding and Watermark Detection. The watermark is generated from pixel value 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 the 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 watermarks to decide authenticity.

3.1 Watermark Generation

The watermark pattern is generated from the spatial domain information. Watermark generation procedure includes the following steps:

- Consider the original image P of size $M \times M$.
- Perform 1-level DWT on the original image and acquire the LL1 component to find watermark pattern, which is of size $M/2 \times M/2$. Let this matrix be 'A'.
- A reduced size ($M/2 \times M/2$) image 'B' is obtained from original image by performing the following steps.
  - Partition the original image into non-overlapping blocks of size 2×2.
  - Compute one feature value from each block according to the following equation:

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

  where $0 \le x \le \frac{M}{2}$, and $0 \le y \le \frac{M}{2}$.
- Find the difference between A and B. Let it be C.
- A binary sequence 'W' can be obtained by applying the following constraint.

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

- Disorder the matrix 'W' with the help of Arnold Transform, which is the required watermark pattern to be embedded within the host image.

Example:
Consider the input matrix of size 8×8

$$\begin{pmatrix} 6 & 14 & 10 & 10 & 4 & 3 & 2 & 2 \\ 11 & 16 & 17 & 20 & 6 & 3 & 4 & 4 \\ 11 & 20 & 15 & 10 & 5 & 4 & 4 & 3 \\ 13 & 16 & 6 & 2 & 2 & 2 & 2 & 9 \\ 11 & 16 & 7 & 3 & 4 & 2 & 3 & 11 \\ 6 & 4 & 4 & 2 & 3 & 2 & 2 & 14 \\ 4 & 2 & 4 & 2 & 1 & 2 & 5 & 16 \\ 7 & 6 & 0 & 2 & 4 & 1 & 2 & 3 \end{pmatrix}$$

Applying 1-level DWT on the original matrix yields the LL1 component in integer form as

$$A = \begin{pmatrix} 24 & 29 & 8 & 6 \\ 30 & 17 & 7 & 9 \\ 19 & 8 & 6 & 15 \\ 10 & 4 & 4 & 13 \end{pmatrix}$$

Now the integer matrix B is obtained by taking average values of every blocks of size 2×2.

$$B = \begin{pmatrix} 12 & 14 & 4 & 3 \\ 15 & 8 & 4 & 4 \\ 9 & 4 & 3 & 7 \\ 5 & 2 & 2 & 6 \end{pmatrix}$$

Matrix 'C' is formed by calculating the difference between matrices A and B.

$$C = A - B = \begin{pmatrix} 12 & 15 & 4 & 3 \\ 15 & 9 & 3 & 5 \\ 10 & 4 & 3 & 8 \\ 5 & 2 & 2 & 7 \end{pmatrix}$$

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

$$W(x, y) = \begin{cases} 0, & \text{if } C(x, y) \bmod 2 = 0; \\ 1, & \text{otherwise.} \end{cases}$$

$$W = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

3.2 Watermark Embedding

The watermark is embedded in the high frequency subband of DWT as follows:

- Apply 1-level DWT to original image.

- It divides the host image into 4 sub bands namely LL1, LH1, HL1 and HH1.
- Insert the watermark in the high frequency component HH1 of DWT.
- Perform inverse wavelet transform (IDWT) to obtain the watermarked image.

3.3 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:

- Watermark is derived form the content of watermarked image using the steps described under watermark generation in Section 3.1.
- Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 subband.
- Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.
- Quality of watermarked image and the watermark is found out according to Equations (2) and (4).

4 Experimental Results

In this paper, we consider the images with number of rows and columns being of equal sizes since the embedded watermarks are square matrices. For testing, the size of the original image is taken as 512×512. Figure 2(a) shows original image. A 256×256 binary watermark signal is constructed from 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 2(b) shows watermarked image. The absolute difference of the pixel intensities of the watermarked image and the original image is shown in Figure 2(c). The difference image shows that the technique ensures high degree of fidelity.

(a) (b) (c)

Figure 2: (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 (2). The PSNR value of watermarked image is 59.1168, which indicates that there is very little deterioration in the quality of original image.

$$PSNR = 10 \log(\frac{255^2}{MSE}) \quad (2)$$

where MSE is Mean Squared Error between original and distorted images, which is defined in Equation (3).

$$MSE = \sum_{i=0j=0}^{M-1N-1} \frac{[OI(i,j) - DI(i,j)]^2}{M \times N} \quad (3)$$

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

The original constructed watermark and the extracted are shown in Figure 4. A comparison between extracted and original watermark can be done by computing Similarity Ratio (SR) between these two patterns as defined in Equation (4), which is the metric used for identifying robustness of the watermarking process.

$$SR = \frac{S}{S+D} \quad (4)$$

where S denotes number of matching pixel values and D denotes number of different pixel values.

(a) Original watermark

(b) Extracted watermark

In the proposed scheme, similarity ratio evaluated between extracted and calculated watermark is 0.8496 which indicates that the number of matching pixels are high and hence authenticity is preserved. The simulation results of previous Method [6] and the proposed one are exposed in Table 1.

Table 1: Quality evaluation of watermarking schemes

Metric used	Method [6]	Proposed
PSNR	56.2083	59.1168
SR	0.9933	0.8496

The proposed algorithm was tested using several attacks. The attacks chosen were adding noises such as Gaussian and salt & pepper noises, median filtering, linear filtering, intensity adjustment, blurring, histogram equalization, JPEG compression, Scaling and Rotation. Robustness of the proposed method under the common image processing operations was identified with the help of Similarity Ratio and is compared against our previous method [6]. Table 2 shows the experimental results.

Table 2: Assessment of watermarking schemes under attacks

Attacks		Similarity Ratio	
		Method [6]	Proposed
Adding Gaussian noise (mean, variance)	0.01, 0	0.9933	0.8371
	0, 0.001	0.3840	0.4243
Adding Salt & Pepper noise	0.002	0.9844	0.8370
Median filtering	3x3	0.5789	0.6629
Linear filtering	3x3	0.6010	0.6696
Image Adjustment	3x3	0.8988	0.8335
Blurring		0.7583	0.8083
Histogram Equalization		0.7040	0.7498
JPEG (Quality Factor)	90	0.5732	0.6488
	70	0.5917	0.6956
	50	0.6028	0.7418
	30	0.6149	0.7736
	10	0.7002	0.8158
Scaling (512-256-512)		0.6913	0.8463
Rotation	5	0.4641	0.7135
	10	0.4281	0.6957

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

Watermarked image is smoothed with a 3×3 median filter. Experimental results reveal that the proposed technique is more robust than the technique in [6]. Similar is the case with linear filtering. Experimental result against Image adjustment attack discloses that the robustness of watermark is high in both the methods.

For the rotation operation, the previous method gave up a less Similarity Ratio, while it is greater in the proposed technique, which reflects the robustness of the watermark.

5 Conclusion

This study has proposed a robust watermarking which provides a complete algorithm that embeds and extracts the watermark information effectively. In this method, a watermark pattern is constructed from host image itself. Watermark signal is disordered with the help of Arnold Transform. The designed method makes use of the low frequency component of Discrete Wavelet Transform for watermarking construction process and high frequency component for the embedding and extraction processes. Moreover the authentication process provides qualities like imperceptibility, robustness and security.

The performance of the watermarking scheme is evaluated with common image processing attacks such as adding noises, filtering, intensity adjustment, histogram equalization, JPEG compression, Scaling and rotation. Experimental results demonstrate that watermark is robust against those attacks. Moreover the simulation results of currently devised method are compared with that of our previous work [6], the results obtained show that the proposed technique is highly robust against attacks such as JPEG compression, scaling and rotation.

References

[1] S. Kumar, B. Raman, and M. Thakur, "Real coded genetic algorithm based stereo image watermarking," *JSDIA*, vol. 1, no. 1, pp. 23-33, 2009.

[2] Q. Lin, Z. Liu, and G. Feng, "DWT based on watermarking algorihthm and its implementing with DSP," *ASID'09 Proceedings of the 3rd international conference on Anti-Counterfeiting, security, and identification in communication*, pp. 131-134, 2009.

[3] Y. Luo, L. Z. Cheng, B. Chen, and Y. Wu, "Study on digital elevation mode data watermark via integer wavelets," *Journal of software*, vol. 16, no. 6., pp. 1096-1103, 2005

[4] C. I. Podilchuk, and E. J. Delp, "Digital watermarking: Algorithms and applications," *IEEE Signal Processing Magazine*, pp. 33-46, July 2001.

[5] C. Rey and J. Dugelay, "A survey of watermarking algorithm for image authentication," *Journal on Applied Signal Processing*, vol. 6, pp. 613-621, 2002.

[6] S. S. Sujatha, and M. M. Sathik, "Feature based blind approach for robust watermarking," *International Conference on Communication Control and Computing Technologies (ICCCCT10)*, pp. 182-185, Oct. 2010.

[7] A. K. Parthasarathy and S. Kak, "An improved method of content based image watermarking," *IEEE Transactions on broadcasting*, vol. 53, no. 2, pp. 468-479, June 2007.

[8] R. Reddy, M. V. N. Prasad, and D. S. Rao, "Robust digital watermarking of color images under noise attacks," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp. 334-338, May 2009.

[9] P. Tao, and A. M. Eskicioglu, "A robust multiple watermarking scheme in the discrete wavelet transform domain," *Proceedings of the SPIE*, vol. 5601, pp. 133-144, 2004.

[10] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Transactions on Image Process*, vol. 11, pp. 77-88,2002.

[11] S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection for watermarking," *IEEE Transactions on Image Process*, pp. 154-165, 2002.

[12] X. Xia, C. G. Boncelet, and Gonzalo, "Wavelet transform based watermark for digital images," *OPTICS EXPRESS* vol. 3, no.12, pp 497-511, 1998.

[13] 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.

[14] Y. Yuan, D. Huang, and D. Liu, "An integer wavelet based multiple logo-watermarking scheme," *Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences*, vol. 2 pp. 175-179, 2006.

S. S. Sujatha received the M.C.A degree from Alagappa University, Karaikudi, in 1993 and M.Phil degree from Manonmanium Sundaranar University, Tirunelveli in 2003. She is working as an Associate Professor in Department Computer Science at S.T.Hindu College, Nagercoil since 1994. She had presented and published thirteen papers in national and international conferences and Journals. Her current research interest focuses on digital watermarking and image authentication.

M. Mohamed Sathik received the M.Sc(Mathematics) degree from Bharathidhasan University in 1986, and the M.Phil and Ph.D. in Computer Science degrees from Manonmanium Sundaranar University in 1997 and 2006 respectively. He was also awarded the degrees M.Tech(CS&IT), MBA(Project Management) and M.S(Psycho Therapy). Currently he is an Associative professor in Computer Science department at Sadakathullah Appa College, Tirunelveli since 1988. His research interest is Virtual Reality Techniques. He had presented number of papers in National and International conferences and Journals.