Volume 3, No. 4, July- August 2012

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Secure Blind Semi-Fragile Watermarking Technique for Digital Image Authentication

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

Dr.M.Mohamed Sathik
Principal
Sadakathullah Appa College,
Tirunelveli, India
mmdsadiq@gmail.com

Abstract - In digital watermarking system, information carried by the watermark is embedded in an original image. The watermarked image is transmitted or stored, and then decoded so that it is resolved by the receiver. The aim of Semi-fragile Watermarking technique is to discriminate malicious manipulations from admissible manipulations. This paper proposes a semi-fragile watermarking technique which embeds watermark signal into the host image in order to authenticate it. Some pixels are randomly selected from original image, so that all of them have a valid 3x3 neighborhoods. A binary sequence is constructed from those pixels by comparing them against average values of neighborhoods. The binary sequence is then converted into a watermark pattern in the form of a Hankel matrix to improve security of watermarking process and is then embedded within the high frequency sub band in the wavelet domain. In our previous work[1], we addressed only the robustness of the algorithm. The central idea of this paper is to study about the fragile nature of the watermarking technique. Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are computed to measure image quality. Simulation results show that this technique still preserves high image quality after the embedding process and is robust against some of the incidental image processing operations while indicating the forgery if the image is heavily processed.

Keywords – Semi-Fragile, Digital watermarking, Hankel Matrix, Image Authentication, Content based watermarking.

I. INTRODUCTION

In recent years, the Internet and the explosion of digital technologies have enabled several applications in the area of multimedia communications in a cost and time efficient manner. The advantages are digital data can be readily shared, easily used, processed and transmitted, which in turn causes serious problems such as unauthorized use and manipulation of digital content. Thus, the authentication and copyright protection from unauthorized manipulation of a digital image becomes an important issue in the field of digital media.

On the other hand, the availability of the powerful image editing software has made copying and editing an image easier. Authentication and detection of tampering and forgery are thus primary concerns. Hence watermarking for image authentication has been a promising approach to improve these concerns. The commonly used watermarking applications include copyright related applications, content authentication applications, medical forensic and military applications.

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.

The digital image watermarking scheme can be divided into two categories. They are visible digital image watermarking and invisible image watermarking techniques. In visible watermarking, the information is visible in the picture or video. Typically, the information is text or a logo which identifies the owner of the original document. In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. Further, the invisible watermarks are categorized into watermarking techniques as robust, fragile and semi-fragile.

a. ***Robust*** - Generally, a robust mark [2] is generally used for copyright protection and ownership identification because they are designed to withstand nearly all attacks such as lossy compression, filtering operations and geometric distortions. These algorithms ensure that the image processing operations do not erase the embedded watermark signal.

b. ***Fragile*** – In fragile techniques [3], even one bit change in image is not allowable. They are mainly applied to content authentication and integrity attestation, because they are sensitive to almost all modifications. Here, the watermark is embedded so that any manipulation or modification of the image would alter or destroy the watermark.

c. ***Semi-fragile*** – Semi-fragile methods [4] [5] are robust to incidental modifications such as JPEG compression, but fragile to other modifications such as a high impact additive noises. That is, some incidental image manipulations have to be considered allowable during the process of media transmission and storage, while other malicious

modifications (e.g. alteration of content) from attackers should be rejected. – Intentional distortion

Several methods have been proposed in literature. A survey is in [6]. 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 [7] which directly modifies the intensities of some selected pixels. The frequency domain technique transforms an image into a set of frequency domain coefficients [8]. 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. 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 [9]. A detail survey on wavelet based watermarking techniques can be found in [10].

Yuan et al.[11] 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.[12] 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.

A survey on semi-fragile watermarking algorithms is in [13]. Lin et.al.[4] proposed an image authentication method that can differentiate the practical JPEG lossy baseline compression with a predefined LAJQ from malicious manipulation. Xiao et al. [14] presented a semi-fragile digital image watermarking method in which the LSB of the pixel is modified and is tolerant to Laplacian sharpening. Lin and Chang [15] proposed an algorithm which is tolerate to JPEG compression. Hung et al. [16] uses the block vector quantization indices for authentication data.

Most of the watermarking schemes reported in the literature have the shortcomings such as insecurity and low robustness to JPEG compression and failed to identify attacks such as additive noises. 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 forms a binary pattern in the form of a Hankel matrix and thereby increases the security of the proposed method. The extraction is done without using original image and hence a blind scheme is obtained. This method is robust against many common image processing attacks and is sensitive to malicious manipulation such as additive noises.

The rest of this paper is organized as follows: Section 2 gives an overview of Discrete Wavelet Transform and Hankel matrix. The details of watermark generation, embedding and extraction processes are explained in Section 3. Section 4 presents experimental results and discussion. The paper is concluded in section 5.

II. RELATED BACKGROUND

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

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 [17].

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.

B. Hankel Matrix:

Hankel matrices are frequently encountered in applications where matrix computation is exploited in order to devise very effective numerical solution algorithm. A Hankel matrix is defined as a matrix that is symmetric and constant across anti-diagonals, and has elements h(i, j) = p(i+j-1) where p is a vector represented as [col, row (2: end)] which completely determines the Hankel matrix[19]. It is a square matrix with constant positive slopping skew diagonals and for constructing a Hankel matrix of order NxN, we need 2N-1 elements.

$$H = \begin{pmatrix} a & b & c & d & e \\ b & c & d & e & f \\ c & d & e & f & g \\ d & e & f & g & h \\ e & f & g & h & i \end{pmatrix} \qquad (1)$$

Let P= {a, b, c, d, e, f, g, h, i}. Since there are 9 elements in this vector, a Hankel matrix of size 5x5 may be constructed so that its first column is first 5 elements and last row except the first element is last 4 elements, which is given in equation (1).

III. PROPOSED METHOD

In the proposed scheme, there are three significant phases. They are Watermark generation, Watermark embedding and Watermark Detection. The steps involved in the watermarking technique are described in this section.

A. Watermark generation:

The watermark pattern is generated by an algorithm, which is described in detail as follows:

Input: The host image P of size M x M

Output: The watermark W of size M/2 x M/2

Step 1. Randomly select M-1 elements from P so that all the pixels have valid 3x3 neighborhoods.

Step 2. Let P(x-1, y-1), P(x-1, y), P(x-1, y+1), P(x, y+1), P(x+1, y+1), P(x+1, y), P(x+1, y-1), P(x, y-1) are the neighborhoods of the selected pixel P(x, y).

Step 3. Find average value of those neighborhoods. Let it be $P_a(x, y)$.

Step 4. A binary sequence 'B' can be obtained by applying the following constraint.

$$B_i = \begin{cases} 0 & if \;\; P(x,y) > P_a(x,y) \\ 1 & otherwise \end{cases}$$

where i=1,2,3,…M-1

Step 4. A Hankel matrix of size M/2 x M/2 is constructed from the binary sequence B_i as

$$H(i, j) = B(i + j - 1)$$

where $1 \le i \le M/2, \quad and \quad 1 \le j \le N/2$

which is the watermark pattern to be embedded in to the host image.

B. Watermark embedding:

The algorithm embeds the watermark in the high frequency subband of host image. The detailed steps are listed as follows:

Input : The host image and a watermark.

Output: The watermarked image

Step 1. Perform one-level DWT to original image.

Step 2. Replace the HH1 component of DWT with the watermark.

Step 3. Apply one-level inverse wavelet transform to obtain the watermarked image.

C. Watermark Detection:

Proposed watermarking scheme extracts the embedded watermark and reconstructs watermark information from watermarked image. Thus the algorithm does not require the original image in the detection phase and hence it is referred as blind watermarking. The authentication process includes the following steps:

Input : The watermarked image.

Output : The extracted and reconstructed watermarks

Step 1. Watermark is derived form the content of watermarked image using the steps described under watermark generation in section 3.1.

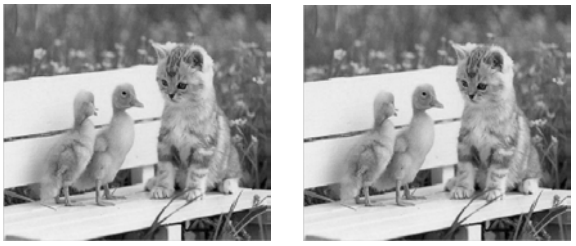
Step 2. Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 sub band.

Step 3. Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.

Step 4. Quality of watermarked image and the watermark is found out according to equation (2) and (4).

IV. EXPERIMENTAL RESULTS

Because the robustness and fragility to attacks is a crucial issue in the design of semi-fragile watermarking algorithms, the validity of the proposed algorithm is studied in this section. Many experiments are carried out under different cover images and watermarks. Due to limited space, the experimental results are provided when using Figure 1(a) with size 512x512 as the cover image. The watermark is a binary image with size of 256×256, which is constructed from the perceptual information of original image.



(a) (b)

Figure. 1 Images

(a) Original image (b) Watermarked Image

In the experiment, the peak signal to noise ratio (PSNR) as defined in (2) is used to measure the embedding distortion, and Similarity Ratio (SR) as defined in (4) is used to measure the robustness and fragility.

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

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

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

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

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

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

The watermarked image is shown in Figure 1(b), and its PSNR is 56.2083 dB which indicates that there is very little deterioration in the quality of original image. In addition to that, SR evaluated between extracted and calculated watermark is 0.9933 which indicates that the number of matching pixels are high and hence authenticity is preserved.

Table 1: SR Against Common Attacks

Attacks		**SR**
No		0.9933
Linear filtering	3x3	0.6010
Blurring		0.7583
JPEG Compression	70	0.5917
	50	0.6028
	30	0.6149
	10	0.7002
Rotation with cropping	5^o	0.4641
	10^o	0.4281
Rescaling (512-256-512)		0.6913
Translation		0.1725
Image adjustment		0.8988
Histogram Equalization		0.7040

Figure 1(a) and 1(b) indicate that the embedding distortion is very small, and it can't be sensed by human eyes. To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on the cover image under some common image processing attacks. A threshold is set on SR so that a value greater than

0.6 shows robustness and the rest indicate fragility or a failure to withstand the attacks.

The proposed algorithm has been tested using several incidental image processing operations. These operations preserve the content of the image. The attacks chosen are linear filtering, blurring, JPEG compression, geometric distortions such as rotation, scaling& translation, intensity adjustment and histogram equalization. Table 1 gives the performance of proposed watermarking scheme under various attacks.

Experimental results against those content preserving operations disclose the fact that the robustness of watermark is high in the case of Linear filtering, blurring, JPEG compression up to 50%, Scaling, Image adjustment and histogram equalization. At the same time, the proposed method fails to show robustness against rotation and translation operations.

To determine the fragile nature of the algorithm, the watermarked image has been subjected to intentional attacks such as Gaussian and Salt&pepper additive noises.

Typically Gaussian noise is added to the image with two parameters namely mean and variance. Here, the parameter 'variance' is very crucial in altering contents on the image. So experiments have been conducted with different values of 'variance' by preserving the mean value at 0 and the impacts are shown in Figure 2.

(a) (b) (c)

Figure 2. Impact of Guassian noise with zero mean

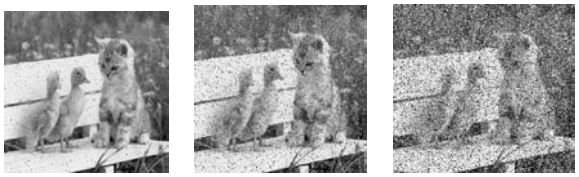
(a) Variance =0.04, (b) Variance=0.08, (c) Variance =0.2

The Similarity ratio calculated between original watermark and the extracted one is tabulated in table 2. The low values of SR indicate that the proposed algorithm is very sensitive to additive Gaussian noises for various values of variance.

Table 2: SR Under Gaussian Noise

Variance	SR
0.01	0.3482
0.02	0.3414
0.03	0.3307
0.04	0.3219
0.05	0.3178
0.06	0.3161
0.07	0.3096
0.08	0.3047
0.09	0.3013
0.1	0.2964
0.2	0.2930
0.3	0.2749

The image may also undergone salt&pepper noise during transmission. So salt&pepper noise is added to the image with a noise density 'd' and the resultant images are given in Figure 3, which indicates that a high value of 'd' manipulates the digital content of the image.



(a) (b) (c)

Figure 3. Impact of Salt&Pepper noise

(a) Density =0.02, (b) Density=0.1, (c) Density =0.3

The Similarity Ratio calculated are provided in Table 3. The similarity ratio calculated is high for noise densities less than or equal to 0.1. So it is considered that the proposed algorithm is able to withstand such kind of attacks and it is robust to salt&pepper noise for a less value of density. At the same time, the algorithm recognizes that the attack is malicious when the salt&pepper noise density is greater than 0.1.

Table 3: SR Under Salt&Pepper Noise

Density	SR
0.02	0.9063
0.03	0.8882
0.04	0.8306
0.05	0.8311
0.06	0.7853
0.07	0.7639
0.08	0.7319
0.09	0.6841
0.1	0.6792
0.2	0.5347
0.3	0.4599

V. CONCLUSION

This study has proposed a semi-fragile watermarking which provides a complete algorithm that embeds and extracts the watermark information effectively. In this method, the watermark pattern constructed in the form of Hankel matrix is embedded in the high frequency coefficient in the wavelet domain. The security of the proposed method lies on the multifaceted procedure used to construct watermark. The watermark is designed so that the integrity is proven if the content of the image has not been altered and under some mild processing on the image. 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. Experimental results demonstrate that the proposed scheme guarantee the safety of the watermark, and identifies malicious attacks while tolerating Filtering operations, JPEG compression to some extent, Scaling, Image adjustment and histogram equalization. Generally, as for as the additive noises are concerned, the greater parameter value affects the perceptual content of the image in a crucial manner. So these attacks are referred to as malicious manipulations. The proposed scheme is fragile with respect to Gaussian noise for increased values of variance. In the case of salt & pepper noise an increase in density manipulate the digital image content to a great extent. The proposed scheme is robust for a little additive noise but it is sensitive to other cases. Hence the proposed technique is effective for image authentication.

VI. REFERENCES

[1] Mohamed Sathik M. and Sujatha S. S., "Wavelet Based Blind Technique by Espousing Hankel Matrix for Robust Watermarking", International Journal of Advanced Science and Technology, Vol.26, pp.52-71 (2011).

[2] Ramkumar M and Akansu N, "A Robust Protocol for Providing Ownership of Multimedia content", IEEE trans on Multimedia, Vol.6, pp.469-478 (2004).

[3] Celik,M.U., Sharma, G., Saber E. and Tekalp, A.M., "Hierarchical Watermarking for Secure Image Authentication with Localization, "IEEE Trans on Image Processing, Vol.11, pp.585-595(2002).

[4] Lin.C, Su.T and Hsieh.W, "Semi-Fragile Watermarking Scheme for Authentication of JPEG Images", Tamkang Journal of Science and Engineering, Vol.10, No.1, pp.57-66 (2007).

[5] Zhou.X, Duan X., and Wang D., "A Semi-fragile Watermark Scheme for Image Authentication", IEEE International Conference on Multimedia modeling, pp.374-377 (2004).

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

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

[8] 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.

[9] 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.

[10] 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.

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

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

[13] Ekiei O., Sankur B., Coskun B., et. al, "Comparative evaluation of semifragile watermarking algorithms", Journal of Electronic Imaging, Vol.13(1), pp.209-216(2004).

[14] Jun Xiao, Ying Wang, "A Semi-Fragile Watermarking Tolerant to Laplacian Sharpening", IEEE International Conference on Computer Science and Software Engineering, pp.579-582 (2008)

[15] C. Y. Lin and S. F. Chang, ''Semifragile watermarking for authentication JPEG visual content,'' *Proc. SPIE* **3971**, 140–151 (2000).

[16] K.L.Hung,C.C.Cheng,and T.S.Chen, "Secure Discrete Cosine Transform Based Technique for Recovereable Tamper Proofing", Opt Eng. 40(9), pp.1950-1958(2001).

[17] 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.

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

[19] http://www.mathworks.com/access/helpdesk/help/techdoc/ref/hankel.html

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

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

Short Bio Data for the Authors

S.S.Sujatha received the M.C.A degree from Alagappa University in 1993 and M.Phil degree from Manonmanium Sundaranar University in 2003. She is working as an Associate Professor in Computer Science Department at S.T.Hindu College, Nagercoil since 1994. She has presented and published fifteen papers in national and international conferences and Journals. Her current research interest focuses on Digital watermarking and 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). He worked as an Associate Professor in Computer Science Department at Sadakathullah Appa College, Tirunelveli from 1988. Currently he is the Pricipal of Sadakathullah Appa College, Tirunelveli. His research area of interest is Virtual Reality. He had presented and published number of papers in national and international conferences and journals.