Volume 2, Issue 11, November 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Authentication of Digital Images by using a semi-Fragile Watermarking Technique

Dr.M.Mohamed Sathik
Principal,
Sadakathullah Appa College,
Tirunelveli, India

S.S.Sujatha
Associate Professor in Computer Science
S.T.Hindu College
Nagercoil, India

Abstract*— *Watermarking techniques which are fragile to intentional modifications while robust to incidental or unintentional manipulations are referred to as Semi-fragile. This paper proposes a semi-fragile watermarking technique which embeds watermark signal into the host image in order to authenticate it. 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. The watermark is generated as a binary pattern from the feature of the host image and is embedded in the high frequency sub band in the wavelet domain. 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, Arnold transform, 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.

Authentication of digital documents has aroused great interest due to their wide application areas such as legal documents, certificates, digital books and engineering drawings. In addition, more important documents such as fax, insurance and personal documents are digitized and stored. It is becoming important on how to ensure the authenticity and integrity of digital documents. 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. 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. A watermark is called imperceptible if the watermarked content is perceptually equivalent to the original, un watermarked content
- *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. A watermark is called robust if it resists a designated class of transformations. Robust watermarks may be used in copyright protection applications to carry copy and access control information

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.

- *Robust* - Generally, a robust mark [1] 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.
- *Fragile* – In fragile techniques [2], 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.
- *Semi-fragile* – Semi-fragile methods [3] [4] 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 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 [6] 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 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 [8]. A detail survey on wavelet based watermarking techniques can be found in [9].

Yuan et al.[10] 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.[11] 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 [12]. 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. [13] 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 [14] proposed an algorithm which is tolerate to JPEG compression. Hung et al. [15] 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 Geometric distortions. 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 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 Arnold Transform. 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 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 [16], 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.

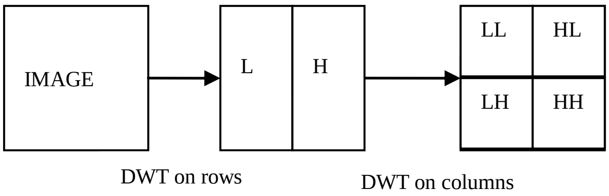

Fig. 1 DWT decomposition of image

For a one level decomposition, the discrete two-dimensional wavelet transform of the image function f(x, y) can be written as [17]

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

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

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

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

where ϕ (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 $\in \{0,1,2,3\ldots N-1\}$ 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)

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

III. PROPOSED METHOD

In the proposed scheme, there are three significant phases. They are Watermark generation, Watermark embedding and Watermark Detection. The algorithm first generates 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 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

- Perform 1-level DWT on the host image and acquire the LL1 component. Let this matrix be ‘A’ with size M/2 x M/2.
- 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* $0 \le y \le M/2.$

- Find the absolute difference between A and B. Let it be C.
- A binary sequence ‘W’ can be obtained by applying the following constraint.

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

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

Input : The host image of size and a watermark.
Output: The watermarked image

- Perform one-level DWT to original image.
- Replace the HH1 component of DWT with the watermark.
- 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

- Watermark is derived form the content of watermarked image using the steps described under watermark generation in section III.A.
- Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 sub band.
- 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 equation (3) and (5).

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, we only give the experimental results when using Fig.2 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.

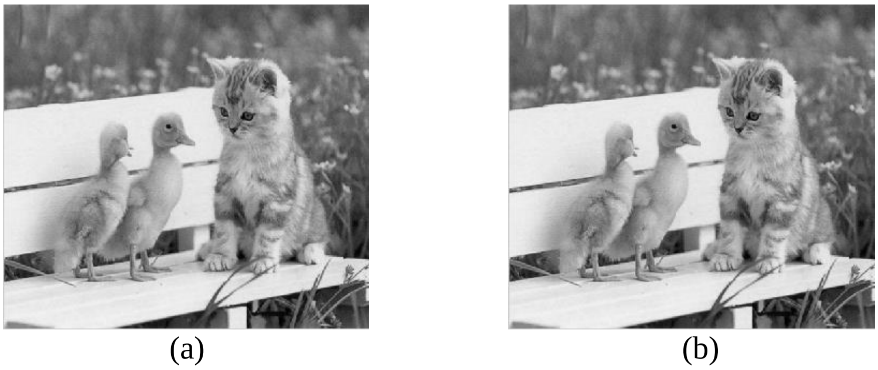

Fig 2. Input and Processed Images
(a) Original image (b) Watermarked image

In the experiment, the peak signal to noise ratio (PSNR) as defined in (3) is used to measure the embedding distortion, and Similarity Ratio (SR) as defined in (5) is used to measure the robustness and fragility.

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

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

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

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

$$SR = \frac{S}{S+D} \qquad (5)$$

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

The watermarked image is shown in Fig.5, and its PSNR is 59.1168 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 0.8496 which indicates that the number of matching pixels are high and hence authenticity is preserved.

Fig. 2(a) & Fig. 2(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.

TABLE 1
SR AGAINST COMMON ATTACKS

Attacks		**SR**
No		0.8496
Median filtering	3x3	0.6629
Linear filtering	3x3	0.6696
Blurring		0.8083
JPEG compression (QF)	90	0.6488
	70	0.6956
	50	0.7418
	30	0.7736
	10	0.8158
Rotation with cropping	5^o	0.7135
	10^o	0.6957
Scaling		0.8463
Translation		0.7894
Image adjustment		0.8435
Histogram Equalization		0.7598

The proposed algorithm has been tested using several incidental image processing operations. These operations preserve the content of the image. The attacks chosen were median filtering, linear filtering, blurring, JPEG compression, geometric distortions such as rotation, scaling& translation, intensity adjustment and histogram equalization. Table 2 gives the performance of proposed watermarking scheme under various attacks.

Experimental results against those operations disclose the fact that the robustness of watermark is high. The proposed method shows better authentication since the similarity ratios computed between extracted and original watermarks are having high values.

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 and the results are tabulated in Table 2 and Table 3.

TABLE 2
SR UNDER GAUSSIAN NOISE

Variance	**SR**
0.01	0.4089
0.02	0.4064
0.03	0.4058
0.04	0.4045
0.05	0.4039
0.06	0.4031
0.07	0.4023
0.08	0.4018
0.09	0.4009
0.1	0.3997
0.2	0.3982
0.3	0.3971

TABLE 3
SR UNDER SALT&PEPPER NOISE

Density	**SR**
0.02	0.7010
0.03	0.6904
0.04	0.6781
0.05	0.6667
0.06	0.6586
0.07	0.6483
0.08	0.6340
0.09	0.6244
0.1	0.6169
0.2	0.4882
0.3	0.4213

From table 2, it is concluded that the proposed algorithm is fragile to additive Gaussian noises at various values for variance. Experimental results provided in Table 3 show that the proposed algorithm identifies malicious attacks when the salt&pepper noise density is greater than 0.1, while tolerating the additive noises with low density i.e less than or equal 0.1.

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 preserves robustness with respect to Gaussian noise with a variance 0 while it is fragile for increased values for variance. The values in the SR column of Table 2 indicate this fact. In the case of salt & pepper noise an increase in density manipulate the digital image content. The proposed scheme is robust for a little additive noise but it is sensitive to other cases.

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 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. 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 content preserving common image processing attacks and content altering intentional attacks. Experimental results demonstrate that the proposed scheme guarantee the safety of the watermark, and identifies malicious attacks while tolerating Filtering operations, JPEG compression, Geometric distortions, Image adjustment and histogram equalization. Hence the proposed technique is effective for image authentication.

REFERENCES

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

[2] 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).

[3] 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).

[4] 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).

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

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

[7] 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.

[8] 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.

[9] 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.

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

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

[12] 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)

[13] 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).

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

[15] 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).

[16] 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.

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

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

[19] 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.

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