ISSN 1512-1232

DUAL-LAYER DIGITAL IMAGE WATERMARKING FOR INTELLECTUAL PROPERTY RIGHT PROTECTION

H.E.Suyryavanshi[1], Amit Mishra[2] and Amit Sinhal[3]

[1] *Department of Information Technology, Technocrats Institute of Technology, Bhopal, India*
Email: hitendra.suryavanshi@gmail.com
[2] *Department of Information Technology, Technocrats Institute of Technology, Bhopal, India*
Email: amitmishra.mtech@gmail.com
[3] *Department of Information Technology, Technocrats Institute of Technology, Bhopal, India*
amit_sinhal@rediffmail.com

***Abstract**:*

In this paper, a wavelet based scheme for digital image watermarking is presented. This proposed scheme inserts two watermarks in an image which serves two different purposes. The first one is inserted using blind watermarking technique while second one acts as fragile watermark. As it is blind watermarking technique, there is no need of original image at the time of watermark extraction. The insertion of watermark is based on selection of suitable coefficients which are obtained after applying two-level wavelet decomposition. The result produced by this watermarking scheme is good as compared to conventional watermarking techniques.

***Index Term:** image watermarking, wavelet, blind watermarking, lsb*

I. Introduction

Digital image watermarking gains a lot of importance since last decade. The motivation behind this is to protect intellectual property rights, security, information hiding and fingerprinting. This section provides the formal introduction to the watermarking concept. Watermarking is a term which means hiding a message or some kind of data into an image. This message is called as watermark and an image is called as host image. Image watermarking imperceptibly embeds data into the host image. The general process of image watermarking is shown in Fig 1.

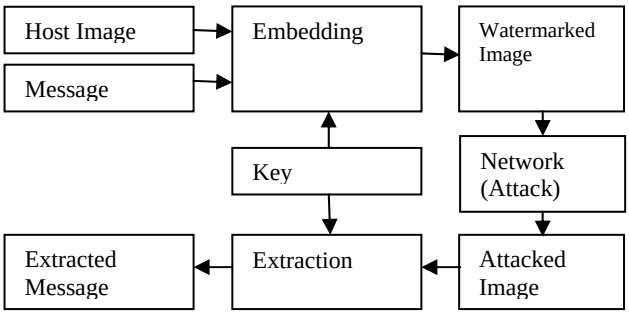


Fig. 1 General concept of watermarking

The original image is modified using the message to get the watermarked image. In this process some distortion may be introduced. But this distortion should be small. The watermarked image is then circulated over the internet from legal customer to illegal one.

ISSN 1512-1232

The watermark extraction process may or may not require the original host image to extract the message. Extracted message then compared with the original message and the difference between them should be low.

There are different types of watermark such as robust, fragile, public and private watermark. Each serves different purpose.

II. Discrete Wavelet Transform

Discrete wavelet transform is mathematical tool for hierarchically decomposing an image. Images are usually non-stationary two-dimensional signals and wavelet transform is effective in such case. Discrete wavelet transformation (DWT) when applied on image, it decompose image into four frequency sub-bands (LL, HL, LH, HH) where LL refers to low pass band and other three sub-bands corresponds to horizontal (HL), vertical (LH) and diagonal (HH) high pass bands [4].

Fig. 2 shows two-level DWT decomposition of image. In general, the watermark can be inserted into low frequency sub-bands (LL) because it increases the robustness of watermark but at the same time it may degrade the image significantly. High frequency bands (HH) contains edges and textures and changes that are caused due to watermark data inserted in such band cannot be noticed by human eye [5].

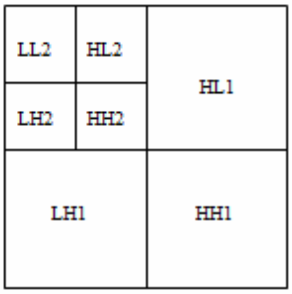


Fig. 2. Two-level DWT decomposition

II. Proposed Work

In this section we present our proposed watermark insertion and extraction method based on DWT.

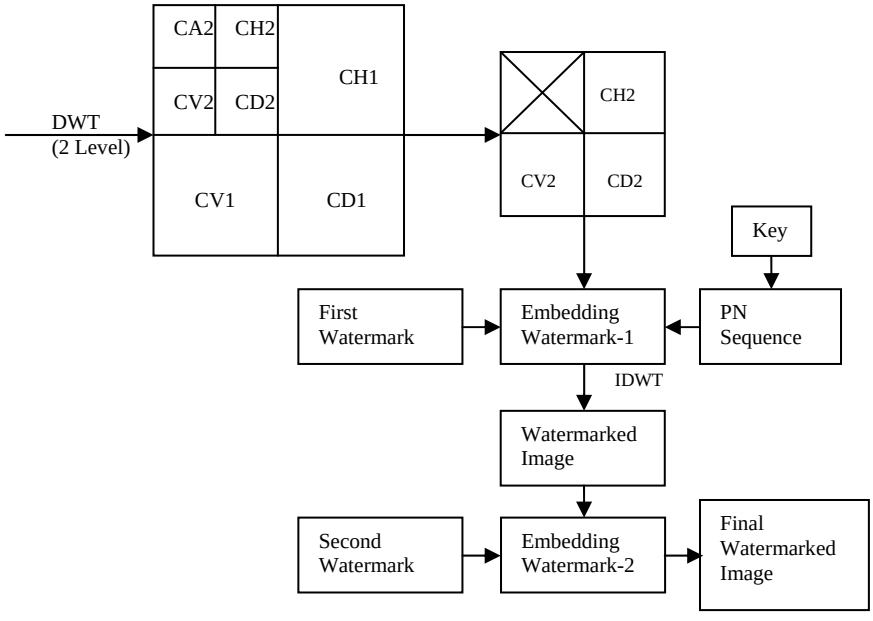


Fig. 3. Proposed Watermarking Scheme

ISSN 1512-1232

There are two watermarks to be inserted into cover image. The watermark insertion process is separated into two phases. The phase-1 inserts watermark, which is robust, by applying discrete wavelet transform on cover image. The phase-2 inserts the watermark using LSB substitution technique which is used for tamper detection. The phase-2 depends on phase-1. But, the extraction process is independent. Watermarks can be extracted in any order.

A. Watermark Insertion Method

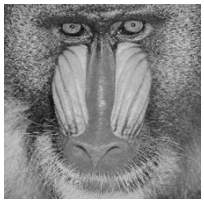
Step 1 Select the cover image C of MxN size. Also select two watermark images W1 (p, q) and W2(x, y).
Step 2 Decompose the cover image C by applying two-level DWT. Also create a binary matrix B of size (p, q) from W1.
Step 3 Set pseudo-random number (PN) generator and repeat step 4 to 5 for pxq times
Step 4 Generate PN sequence for selected components (i.e. CH2, CD2, and CV2).
Step 5 When B is zero, insert first watermark as Cx2=PN+K*Cx2. Where k is scaling factor and x is (CH2, CD2, and CV2)
Step 6 Apply inverses DWT to get watermarked image (I').
Step 7 Now, select second watermark W2(x, y) and resize it to (M, N) of cover image.
Step 8 Repeat the step 9 till (M, N)
Step 9 Add LSB of W2 (i, j) to LSB of I' (I, J)
Step 10 Results in new watermarked image (I")

B. Watermark Extraction Method

Step 1 Read the watermarked image I" (M, N)
Step 2 Decompose the watermarked image up to 2-levels using DWT
Step 3 Create image with all 1's called W1 (P, Q)
Where (P, Q) is size of original first watermark.
Step 4 Set pseudo-random number (PN) generator and repeat the step 5 to 6 (P x Q) times
Step 5 Generate PN sequence for selected components (i.e. CH2, CD2, and CV2)
Step 6 Find out correlation between PN and Cx2. Where x is (CH2, CD2, and CV2)
Step 7 Set W1 to zero based on correlation
Step 8 Results in first watermark W1 (P, Q)
Step 9 Apply Inverse DWT up to 2-levels on I" (M, N)
Step 10 Now create a matrix W2 of size (M, N)
Step 11 Repeat step 12 till (MxN) times
Step 12 Extract LSB from I" (I, J) and add to W2 (I, J)
Step 13 Results in Second watermark W2

III. Result Analysis

This section presents the experimental results of the proposed scheme for digital image watermarking. For the entire test in this paper MATLAB is used. The performance the proposed method is tested on 8-bit grayscale image of baboon and lena of size 512x512. The two watermark images which are to be embedded into cover images are copyright and cs as shown in fig 4.



(a) (b) (c)

Fig. 4. (a) Cover image of baboon, (b) first watermark image, (c) second watermark image

ISSN 1512-1232

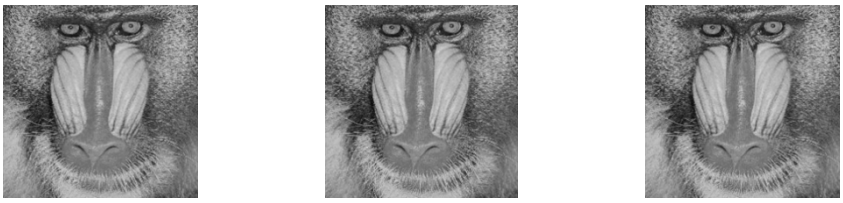
The performance of the proposed watermarking technique is evaluated in terms of the invisibility and robustness. The PSNR (Peak-Signal-to-Noise Ratio) and MSE (Mean Square Error) are used to measure the quality of the watermarked image and attacked image. The PSNR is defined as follows [1, 2]:

$$PSNR = 10 \log 10 \frac{I^2}{MSE}$$

Where,

$$MSE = \frac{1}{MN} \sum_{m,n} (I_{m,n} - I'_{m,n})2$$

Where, I and I' are cover image and watermarked image



(a) (b) (c)

Fig.5. (a) Original Image, (b) After inserting first watermark, (c) After inserting second watermark

Fig. 5 shows the original image of the baboon, the image after the insertion of first watermark and second watermark. The first watermark is inserted using blind watermarking technique. This is robust watermark. The second watermark is fragile watermark. This watermark is inserted using simple LSB substitution technique and it is mean for tamper detection.

(a) (b) (c)

Fig. 6. (a) Watermarked image, (b) Extracted first watermark, (c) Extracted second watermark

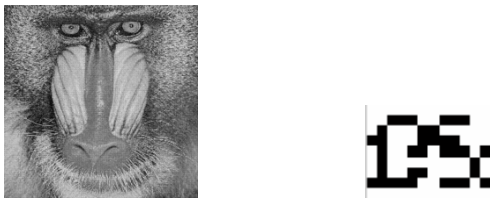
(a) (b) (c)

Fig. 7. (a) Attacked image (Tampering), (b) Extracted first watermark, (c) Extracted second watermark

ISSN 1512-1232

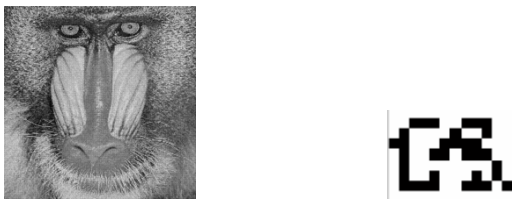
(a) (b) (c)

Fig. 8. (a) Attacked image (Salt & Pepper), (b) Extracted first watermark, (c) Extracted second watermark



(a) (b)

Fig. 9. (a) Attacked image (Gaussian), (b) Extracted first watermark



(a) (b)

Fig. 10. (a) Attacked image (Poisson), (b) Extracted first watermark

Table 1 Performance of proposed watermarking method

K	After Embedding first Watermark		After Embedding second watermark	
	MSE	PSNR	MSE	PSNR
0.1	0.2667	53.3803	0.4993	50.6566
0.2	1.4323	46.0440	0.5018	50.6346
0.3	2.6351	43.4324	0.5001	50.6496
0.4	4.5784	41.0691	0.4991	50.7299
0.5	7.1177	39.1529	0.4992	50.7294
0.6	10.1994	37.6264	0.4995	50.7269
0.7	13.7027	36.3797	0.5002	50.7921
0.8	18.0715	35.2134	0.4997	50.7959
0.9	22.7487	34.2491	0.4989	50.8734
1.0	28.2211	33.3482	0.4984	50.8780

ISSN 1512-1232

Conclusions

In this paper a novel digital image watermarking technique presented. This method is based on wavelet. Because using wavelet it is easy to extract the various features of images on the basis of time and frequency. The watermark is inserted using wavelet coefficient blocks. Watermark extraction process is independent on the original image. Watermarks can be extracted in any order. This scheme is tested against various attacks such as tampering, Gaussian noise. In the future research, we will try to enhance out algorithm to obtain watermarked images with less distortion and to recover the watermark with good accuracy.

Acknowledgment

The authors wish to thank Amit Mishra and Amit Sinhal for their valuable guidance.

References

1. Hanaa A. Abdallah et. Al. “Blind wavelet-based image watermarking”, in *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 4, No. 1, March 2011.
2. Salwa A. K. Mostafa et. Al., “Wavelet packets-based Blind watermarking for medical image management”, in *The Open Biomedical Engineering Journal*, Vol. 4, 2010, pp. 93-98.
3. Nikita Kashyap and Sinha G. R., “Image watermarking using two-level DWT”, in *Advances in Computational Research*, Vol. 4, No. 1, 2012, pp. 42-45.
4. Peining Tao and Ahmet M. Eskicioglu, “A robust multiple watermarking scheme in the descret wavelet transform domain”.
5. Ali Al-Haj, “Combined DWT-DCT digital image watermarking”, in *Journal of Computer Science* 3(9): 740-746, 2007, ISSN 1549-3636, © 2007 Science Publications.

Article received: 2013-01-03