World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:2, No:11, 2008

A Secure Semi-Fragile Watermarking Scheme for Authentication and Recovery of Images based on Wavelet Transform

Rafiullah Chamlawi, Asifullah Khan, Adnan Idris, and Zahid Munir

***Abstract*—**Authentication of multimedia contents has gained much attention in recent times. In this paper, we propose a secure semi-fragile watermarking, with a choice of two watermarks to be embedded. This technique operates in integer wavelet domain and makes use of semi fragile watermarks for achieving better robustness. A self-recovering algorithm is employed, that hides the image digest into some Wavelet subbands to detect possible malevolent object manipulation undergone by the image (object replacing and/or deletion). The Semi-fragility makes the scheme tolerant for JPEG lossy compression as low as quality of 70%, and locate the tempered area accurately. In addition, the system ensures more security because the embedded watermarks are protected with private keys. The computational complexity is reduced using parameterized integer wavelet transform. Experimental results show that the proposed scheme guarantees the safety of watermark, image recovery and location of the tempered area accurately.

***Keywords*—**Integer Wavelet Transform (IWT), Discrete Cosine Transform (DCT), JPEG Compression, Authentication and Self-Recovery.

I. Introduction

THE ease, by which digital multimedia data can be manipulated, has always raised many concerns about the possibility to reliably trust their content. Digital data authentication is thus one of the most important and investigated security applications.

In our proposed approach, the image authentication and recovery is based on a comprehensive technique that operates with the computing of two watermarks [1], an image digest and a binary image. The image digest is computed through a properly modified version of JPEG coding operating at very high compression ratio on original image [2]. Thus image digest is a compressed version of the image itself and it helps in obtaining an estimate of the original contents. The modification is introduced in the digest to make it insensitive to global, innocuous manipulations. The other watermark, binary signature (second watermark) is processed with a private key to ensure security [3]. The scheme is flexible enough with the choice of users, either to embed image digest, binary image or both. Embedding binary image can help in accurately detecting manipulations made in image, but it cannot ensure recovery of an estimated image. Similarly embedding image digest can retrieve the estimated image but leaves the users to judge the authenticity by themselves. Thus, embedding image digest as well as binary image can lead to both authentication and recovery. For the reason we use image digest as a compressed version of the original image, our technique can also be referred as a self-recovery technique.

The scheme use the parameterize integer wavelet transform which is the fast approach of Discrete Wavelet Transform. Based on the idea, [4] proposed for the first time to use the parameterized wavelet transform. However, his scheme is still based on conventional DWT. Lifting scheme is an effective method to improve the processing speed of DWT. Integer wavelet transform allows to construct lossless wavelet transforms. By lifting scheme, we can construct integer wavelet transform. In this paper, we will address the secure semi-fragile watermarking for image authentic-cation and recovery based on integer wavelet transform with parameters.

In current communication, we discuss the watermarks generation, embedding and extraction in section 2, section 3 explains the temper detection. We report experimental results in section 4 and conclusion are made in section 5.

Rafiullah Chamlawi, and Asifullah Khan are with Pakistan Institute of Engineering and Applied Sciences (PIEAS), Islamabad, Pakistan (e-mail: chamlawi@gmail.com, asif_jg@yahoo.com).

Adnan Idris is with AJK University, Rawalakot, Azad jamu and Kashmir, Pakistan (e-mail: adnaidris@gmail.com).

Zahid Munir is with Electronic Division PINSTECH, Nilore, Islamabad, Pakistan (e-mail: mzahid@pinstech.org.pk).

II. Watermark Generation

Our scheme is based on embedding of two watermarks. We proceed for the watermarks generation in this section.

A. Binary Image Preprocessing

A binary signature is preprocessed before embedding as a watermark. Let W be a binary signature of size $M \times N$ and PN be a pseudorandom matrix of same size generated by a secret key. The binary signature W and pseudorandom matrix PN are represented as;

$$W = w(i,j) \qquad (1 \le i \le M, 1 \le j \le N) \tag{1}$$

where $w(i,j) \in \{0,1\}$

$$RandomMatrix = p_n(i,j) \qquad (1 \le i \le M, 1 \le j \le N) \tag{2}$$

where $p_n(i,j) \in \{0,1\}$

We adopt the formula (3) to get the ultimate watermark W_1 :

$$W_1 = W \oplus RandomMatrix \quad (3)$$

where $\oplus$ denotes the exclusive OR.

B. Digest Generation

The image digest (second watermark) is a comp-ressed version of original image and it is generated using following steps:

- One level Integer Wavelet Transform is applied on the original image size $N \times N$.
- Full frame DCT on low pass version (LL1) is computed.
- DCT coefficients are quantized to decrease their obtrusiveness.
- The scaled DCT values are ordered through a zigzag scan and first M coefficients are likely to be selected and stored in vector v:

$$v = (v_1, v_2, v_3 \ldots v_M) \quad (4)$$

where $M = N^2/32$. DC component is discard-ed because of its too high energy.

- Coefficients are further scaled based on secret key (k_1), using equation (5):

$$v_{scaled}(i) = v(i).\alpha.\log(i + 2 + r(i)) \quad (5)$$

where α is a strength factor and r is ranging from -0.5 to 0.5.

- DCT coefficients are quadruplicated because we have $N^2/8$ available positions (shown in Fig. 1) which are four times M coefficients. Thus, we get a new vector Q as.

$$Q = (v_1, v_2 \ldots v_M, v_1, v_2 \ldots v_M, v_1, v_2 \ldots v_M, v_1, v_2 \ldots v_M)$$

- $P_{scrambled}$ is obtained by scrambling vector Q with the help of a secret key, in order to make it more secure. Thus, $Q_{permuted}$ is yielded image digest to be embedded in the highlighted subbands as shown in Figure 1. W_2 is our second watermark ready for embedding.

$$W_2 = Q_{permuted} \quad (6)$$

C. Watermark Embedding

Both the watermarks (image digest and binary signature) have been computed and now both are embedded into the original image with the following steps:

- Applying 1-level IWT on image, the two horizontal and vertical details subbands are further decomposed while approximation subband is two times decomposed. Embedding areas are highlighted in Fig. 1.
- We use the following formula, [5] to embed the watermark W_1 in the LL3 subband coefficients. Let $F(a)$ denote the five least significant bits of a, $F(a,b)$ represent the substitution of b for the five least significant bits of a.

When $W_1(i,j) = 0$, formula (7) is adopted

$$f^*(i,j) = \begin{cases} F(f(i,j) - 01000, 11000) & F(f(i,j)) \le 01000 \\ F(f(i,j), 11000) & otherwise \end{cases} \quad (7)$$

When $W_1(i,j) = 1$, formula (8) is adopted

$$f^*(i,j) = \begin{cases} F(f(i,j) + 10000, 01000) & F(f(i,j)) \le 11000 \\ F(f(i,j), 01000) & otherwise \end{cases} \quad (8)$$

where $f(i,j)$ is a IWT coefficient in LL3 subband before embedding, $f^*(i,j)$ is the IWT coefficient after embedding.

- HL2 and LH2 are replaced by generated digest W_2 as shown in Fig. 1.
- Performing the inverse IWT, we get a watermarked image.

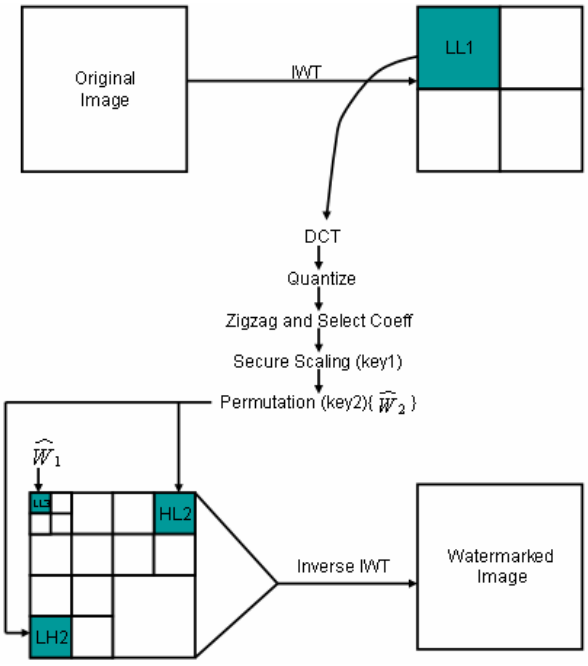


Fig. 1 Embedding Diagram

D. Integrity Verification

In this phase the watermarked image is undergone a procedure and embedded watermarks (W_1 and W_2) are extracted. The extraction procedure of W_1 includes the following step:

- Given an $N \times N$ watermarked image, after applying a One-level IWT, the approximation subband is two times decomposed and LL3 is selected as shown in Fig. 2.

- Let $\overline{W}_1^{*'}(i,j)$ denote the extracted watermark bit , LFB(a) denote the five least significant bits of a , we do the following:

$$\overline{W}_1^{*'}(i,j)=\begin{cases}1 & LFB(f^{*'}(i,j))=0\\ 0 & LFB(f^{*'}(i,j))=1\end{cases} \quad (1\le i\le M, 1\le j\le N) \qquad (9)$$

- To acquire the ultimate watermark $\overline{W}_1$ (a binary image), equation (10) is required.

$$\overline{W}_1^{'}(i,j)=\overline{W}_1^{**}(i,j)\oplus RandomMatrix(i,j) \quad (1\le i\le M, 1\le j\le N) \qquad (10)$$

- We express the difference mark as (11)

$$D(i,j)=\left|\overline{W}_1(i,j)-\overline{W}_1^{'}(i,j)\right| \quad (1\le i\le M, 1\le j\le N) \qquad (11)$$

If $D(i,j)=1$, then the pixel in the difference binary image is white and represents mark extraction error, contrarily, it is black and represents accurate mark extraction.

To get estimated image we move further to extract $\overline{W}_2$.Following steps are taken for the extraction of $\overline{W}_2$:

- Horizontal and Vertical details are further decomposed and HL2 and LH2 are selected.
- Here the data is reversed into a vector $Q^{'}_{permuted}$, which is inversely permuted by means of the same key, thus resulting in a sequence $Q^{'}$. An estimate of the hidden DCT coefficients is then obtained by averaging all four copies of each extracted coefficient. A unique set of authentication data $v_{extracted}$ (i.e. M coefficients) is obtained.
- Invert scaling operation is performed using the same key with the help of formula (12).

$$v_{reconstructed}(i)=v_{extracted}(i).\frac{1}{\alpha}.\frac{1}{\log(i+2+r(i))} \qquad (12)$$

- The $v_{reconstructed}$ then replaced in their correct positions, by means of an anti-zigzag scanning (missing elements are set to zero and a DC component with value 128 is reinserted).
- These obtained values are inversely quantizes and DCT is applied to finally obtain an approximation of the original image.(having size $N/2, N/2$)

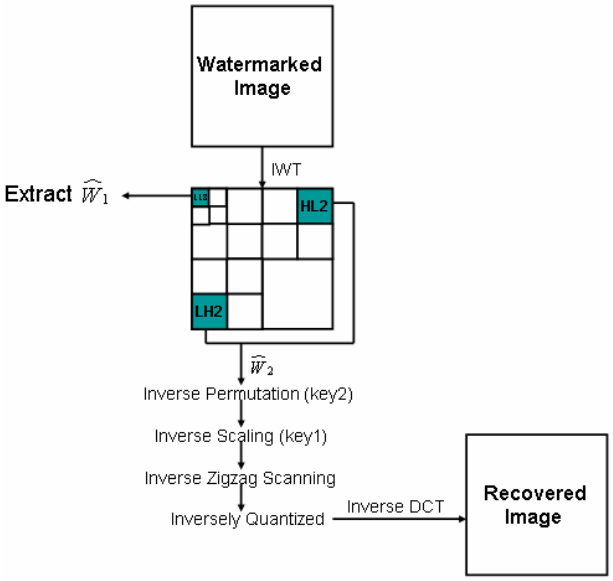


Fig. 2 Extraction Diagram

III. Temper Detection

We express the difference mark as (13):

$$Difference=\left|\overline{W}_1(i,j)-\overline{W}_1^{'}(i,j)\right| \qquad (13)$$

If *Difference* is '1', then pixel in Difference binary image is white and shows the error. It accurately locates the tampered area and distinguishes between malicious attack and incidental attack. A method is given as follows:

Dense pixel: For a mark error pixel in the difference image, it is a *dense pixel* if at least one of its eight neighbor pixels is a mark error pixel and a *sparse pixel* otherwise [3]. Thus, we have the following parameters.

DenseArea → The total of dense pixel of LL subband
SparseArea → *T*he total of sparse pixel of LL subband
Area → The total pixel of LL subband}
TotalArea → DenseArea + *SparseArea*

$\Delta = TotalArea / Area$

$\delta = Area_{Dense} / Area_{Sparse}$

- *if* $\Delta = 0$ Then the image is not tampered)
- *if* $\Delta > 0$ and $\zeta < \beta$ then tampering is incidental, where $\beta = [0.5,1]$
- *if* $\zeta \ge \beta$ then tampering is malicious

Following above parameters depict that if difference image has sparse pixels then the image is incidentally attacked otherwise in a case of dense pixels on the difference image, the image is maliciously attacked.

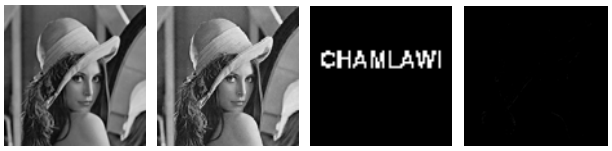
IV. Experimental Results

We have tested our scheme on Lena image. In our work, we apply two and three level IWT for embedding process. The PSNR of the watermarked image is 38dB, which is quite reasonable. The watermarks are perceptually invisible. Fig. 3 shows the original and watermarked images of Lena and a binary signature, which is embedded in LL3, subband of the Lena image.

(a) (b) (c)

Fig. 3 (a) The original Lena Image (b) The Binary signature (c) The watermarked Image (PSNR 38dB)

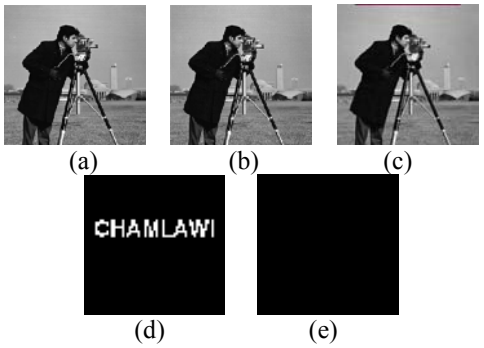
The extracted watermark (Binary Signature) and reference image (Recovered image) without any attack is shown in Fig. 4.



(a) (b) (c) (d)

Fig. 4 (a) The watermarked image (b) the recovered Image (c) The extracted binary signature (d) Difference in original and extracted binary signature

We have tested the scheme on the Cameraman image and get the following results, shown in Fig. 5.



(a) (b) (c)

(d) (e)

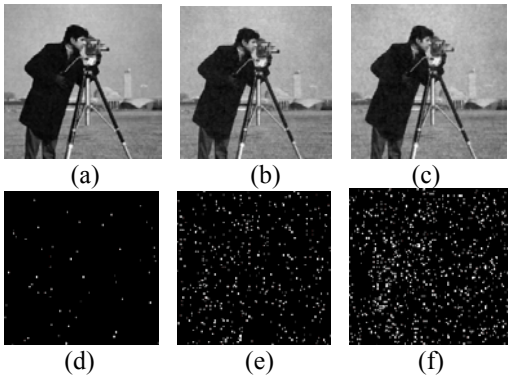
Fig. 5 (a) Original image of cameraman (b) the watermarked image, PSNR 38.2dB (c) Recovered image (d) extracted binary image (e) Difference in binary images

Results obtained after tampering which are not visible as shown in Fig. 6. The Lena image is tampered invisibly. The scheme recovers the approximated image and also locates the tampered area accurately.

(a) (b) (c)

Fig. 6 (a) Original image (b) Watermarked image (c) Difference which shows those areas which are tampered

Fig. 7 shows the estimated image recovered and extracted binary signatures from the watermarked image compressed by JPEG at different quality factors (QF). We can see that the proposed scheme can resist as low as 70% JPEG compression while in case the quality less than 70% should be considered malicious manipulation and also the recovered image will be degraded.



(a) (b) (c)

(d) (e) (f)

Fig. 7 (a), (b), (c) The recovered images in first row and (d), (e), (f) the difference in the second row after compressing the watermarked image with quality factors 90, 80, 70 respectively.

The dots on the difference images show the parse pixels that the image is incidentally tampered, not maliciously. Below 70, the dense pixels occur on the difference image.

V. Conclusion

The detailed experiments are conducted and it is found that the proposed scheme is able to distinguish the malicious and incidental attacks and also recovers a good estimate of original contents. The technique is highly secure because of inclusion of three private keys at various stages of watermark generation. The proposed scheme also shows efficient authentication for a smallest scale transformation on an image. Embedding of two watermarks in this scheme makes it more efficient in accurate detection of tampered area and recovery of estimated image. Invisible tamper detection is another authentication criteria achieved in this semi fragile secured watermarking method.

REFERENCES

[1] Ching-Yang Lin and Shi Fu-Chang, *Semi-Fragile Watermarking for authentication of JPEG visual contents.*

[2] Alessandro Piva, Franco Bartolini and Roberto Caldelliy, *Self recovery authentication of images in the DWT domain,* International Journal of Image and Graphics Vol. 5, No. 1 149-165 (2005)

[3] Xiaoyun Wu, Junquan Hu, Zhixiong Gu, Jiwu Huang (contacting author), *A Secure Semi-Fragile Watermarking for Image Authentication Based on Integer Wavelet Transform with Parameters,* Copyright © 2005 Australian Computer Society, Inc. This paper appeared at the Australasian Info: Security Workshop 2005,

[4] Meerward, P.and Uhl,A. *watermark security via wavelet filter parameterization.* Proc. IEEE Int. Conf. on image processing, (3): 1027-1030 (2001)

[5] Ingemar J Cox, Methiw L Miller and Jeffery A Bloom, *Digital Watermarking.* (2002).

[6] Liu, H.M., Liu, J.F, Huang, J.W, Huang, D.R. and Shi, Y.Q. (2002): *A robust DWT-based blind data hiding algorithm*. Proc. of IEEE on Circuits and Systems, (2):672 - II-675.

[7] Kurato Maeno, Qibin Sun, Shih-Fu Chang, Masayuki Suto, *New Semi-Fragile Image Authentication Watermarking Techniques, Using Random Bias and Non-Uniform Quantization,* IEEE Transactions on Multimedia, Vol 8, No 1, (2006).