Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Exploitation of Toeplitz Matrix in attaining Semi-Fragile Watermarking Technique

**S. S. Sujatha**
Associate Professor in Computer Science
South Travancore Hindu College, Nagercoil, India

***Abstract— Digital Watermarking is known as a good solution for achieving copyright protection and content integrity protection by embedding the secret data into the content. The watermark can later be detected to verify the ownership when dispute over the copyright or integrity of the digital content arises. Semi-fragile methods are robust to incidental modifications but fagile to malicious attacks. The aim of this paper is to propose a semi-fragile techniqe which is able to discriminate intentional manipulations from admissible manipulations.The binary watermark is designed in the form of Toeplitz matrix and is embedded in the high frequency sub-band of Discrete Wavelet Transform. The robustness of the algorithm was addressed in [22]. The fragility of the method is identified under malicious attacks and is measured with a metric Similarity Ratio.Experimental results show that the technique preserves imperceptability and indicates the malicious attacks.***

***Keywords— Semi-Fragile, Digital watermarking, Toeplitz matrix, Image Authentication, Content based watermarking.***

## I. INTRODUCTION

Information security plays a very important role in modern computing information systems. The need for securing information arises from the use of computers in sensitive fields such as government, military, banking and industries. With the global acceptance of Internet, virtually every computer in the world is connected to every other. Nowadays, millions of people use Internet for immediate communication and transformation of vast information. Apart from these opportunities, Internet has created new risks for the users. Since copying and editing an image is carried out easily with powerful image editing software, authentication and copyright protection from unauthorized manipulation of a digital image becomes an important issue in the field of digital media.

Authentication of digital document assures the recipient that the document has been received from the right person. The aim of authentication is to provide a method to authenticate the image and assure the integrity of that image but not to protect the contents from being copied or stolen. Image authentication is achieved by a technique called Digital Watermarking. Watermarking for image authentication has four types [23] as mentioned below:

- ***Exact authentication*** - verifies that an image has not been altered at all since it has left a trusted party. Even if a single bit changes, the image is regarded as inauthentic.
- ***Selective authentication*** - verifies that an image has not been altered significantly. Therefore, if a single or even a small group of bits have been changed, the image is regarded as authentic. However, distortions leading to change in the perceptual quality of the image are regarded as inauthentic.
- ***Localization*** - identifies the regions of the image that have been corrupted, and identifies the remaining regions that are unaltered.
- ***Restoration*** - identifies the regions of the image that have been corrupted, and restores the altered image.

Visible digital image watermarking and Invisible image watermarking techniques are the tw categories of digital image watermarking scheme. 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[21]. Further, the invisible watermarks are categorized into watermarking techniques as robust, fragile and semi-fragile.

- *Robust* – Robust techniques are insensitive to incidental distortions and accept an image that has undergone such manipulations. 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] 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

A detailed survey on several watermarking methods have been provided in [4][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. A detail survey on wavelet based watermarking techniques and semi-fragile watermarking algorithms. can be found in [8] and [11] respectively.

Tsai and Chein [10] designed a semi-fragile watermark from low frequency band and embedding the watermark into the high frequency band by the help of HVS. The robustness of the algorithm is analyzed for mild modifications like JPEG compression and fragility to malicious attacks. 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 semi-fragile watermarking technique presented by Zhou X. et al. [13] constructs a watermark from the original image and inserts this watermark back into the image. Thus, it avoids additional signature files. This scheme is tolerant of lossy compression such as JPEG, but malicious changes of the image will result in the violation of the watermark detection. A survey on 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. Hung et al. [15] uses the block vector quantization indices for authentication data.

The shortcomings of the reported watermarking schemes are insecurity and low robustness to incidental operations. This paper proposes a novel DWT based blind semi-fragile watermarking scheme which assures security by designing a binary watermark pattern in the form of Toeplitz matrix. The rest of this paper is organized as follows: Section 2 gives an overview of Discrete Wavelet Transform, and Toeplitz 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

### *A. Discrete Wavelet Transform*

The DWT use wavelet filters like Haar, Daubechies Orthogonal and Daubechies Bi-Orthogonal and decomposes input image into four components namely LL, HL, LH and HH. 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. Toeplitz Matrix*

In mathematical discipline of linear algebra, a Toeplitz matrix or diagonal constant matrix is a matrix in which each descending diagonal from left to right is constant. It was named after Otto Toeplitz and is frequently encountered in applications where matrix computation is exploited in order to devise very effective numerical solution algorithm. For instance, a Toeplitz matrix is a square matrix with constant diagonals and for constructing a Toeplitz matrix of order NxN, we need 2N-1 elements.

Let P= {a, b, c, d, e, f, g, h, i}. Since there are 9 elements in this vector, a Toeplitz matrix of size 5x5 may be constructed so that its first row is first 5 elements and first column except the first element is last 4 elements, which is given in equation (1). The remaining elements are calculated according to equation (2).

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

$$A(i,\ j) = A(i-1,\ j-1) \qquad (2)$$

## III. PROPOSED METHOD

The successive stages of the proposed semi-fragile watermarking algorithm are provided in figure 1.

### *A. Watermark generation*

The watermark generation algorithm makes use of the Toeplitz matrix to design a watermark in the binary form. The procedure is described in detail as follows:

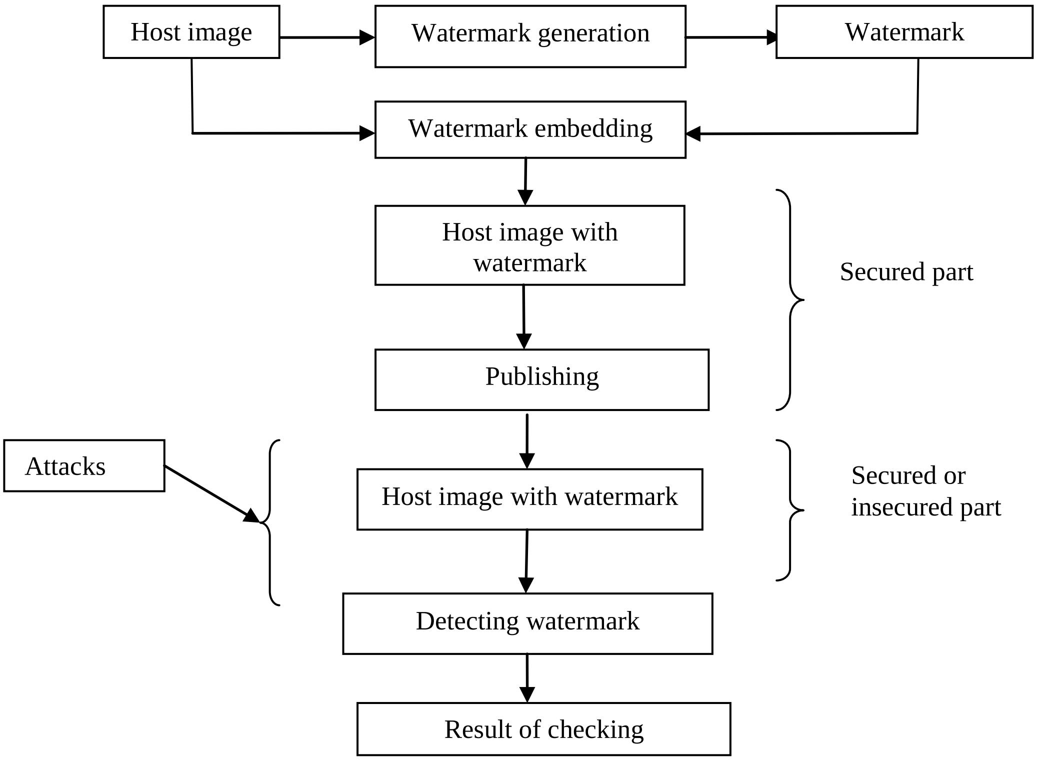

Fig. 1 Framework of proposed watermarking process

**Input:** The host image P of size M x M
**Output:** The watermark W of size M/2 x M/2

a) Consider the original image P of size MxM.
b) Randomly select M-1 elements from P so that all the pixels have valid 3x3 neighborhoods.
c) Let the neighborhoods of the selected pixel P(x, y) are P(x-1, y-1), P(x-1, y), P(x-, y+1), P(x,y+1), P(x+1,y+1), P(x+1,y),P(x+1,y-1), and P(x, y-1)
d) Find average value of those neighborhoods. Let it be $_{Pa}$(x, y).
e) 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.

f) A Toeplitz matrix of size M/2 x M/2 is constructed from the binary sequence B using the following procedure. First row elements are calculated according to equation (3), first column elements except the first are calculated according to equation (4) and remaining elements are computed by using equation (2).

$$T(1, j) = B(i + j - 1) \qquad (3)$$

$$T(i,1) = B(i + M/2 - 1) \qquad (4)$$

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

Now T is the watermark pattern to be embedded within 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

a) Use 'haar' wavelet and apply 1-level DWT on original image.
b) It decomposes the image into four sub-bands namely LL1, HL1, LH1 and HH1.
c) The watermark is embedded in the high frequency component HH1 of DWT by replacing it with the watermark.
d) Perform 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 watermark

a) Watermark is derived form the content of watermarked image using the steps described under watermark generation in section III.A.
b) Apply 1-level DWT to the watermarked image and extract the embedded watermark from HH1 subband.
c) Compare the two watermarks (derived and extracted). If two values match, authenticity is preserved. Otherwise the authenticity is suspected.
d) Quality of watermarked image and the watermark is found out according to equation (5) and (7).

## IV. EXPERIMENTAL RESULTS

The validity of the proposed algorithm is studied in this section by conducting many experiments under different cover images and watermarks. For testing, the size of the original image is taken as 512x512. Subsequently, the watermark is constructed from the perceptual information of original image in the form of a binary Toeplitz matrix pattern. In the experiment, the peak signal to noise ratio (PSNR) as defined in (5) is used to measure the embedding distortion, and Similarity Ratio (SR) as defined in (7) is used to measure the robustness and fragility.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (5)$$

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

$$MSE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\frac{[OI(i,j) - DI(i,j)]^2}{MxN} \qquad (6)$$

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

$$SR = \frac{S}{S+D} \qquad (7)$$

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

(a) (b)

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

The watermarked image is shown in Fig.2, and its PSNR is 54.1428 dB which indicates that the proposed algorithm is highly impercetible. Also, the high value (0.9801) obtained for SR between extracted and calculated watermarks shows that the number of matching pixels is high and hence authenticity is preserved.

To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on the cover image under some common image processing attacks which preserve the content of the image and the results are tabulated in Table 1. The attacks chosen were median filtering, linear filtering, blurring, JPEG compression, intensity adjustment and histogram equalization. The Similarity Ratio obtained reveals that the proposed method is able to withstand against incidental attacks and hence prove the robustness of the algorithm.

Table 1 sr against common attacks

| **Attacks** | | **SR** |
|---|---|---|
| No | | 0.9801 |
| Median filtering | 3x3 | 0.7227 |
| Linear filtering | 3x3 | 0.6539 |
| Blurring | | 0.7667 |
| JPEG compression | 50% | 0.7990 |
| Image adjustment | | 0.7509 |
| Histogram Equalization | | 0.8913 |

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 | 0.4983 |
| 0.02 | 0.3065 |
| 0.03 | 0.2971 |
| 0.1 | 0.2764 |
| 0.2 | 0.2590 |
| 0.3 | 0.2451 |

Table 3 sr under salt&pepper noise

| Density | SR |
|---|---|
| 0.02 | 0.4978 |
| 0.03 | 0.4904 |
| 0.04 | 0.4875 |
| 0.1 | 0.4712 |
| 0.2 | 0.4637 |
| 0.3 | 0.3948 |

An observation on the Similarity Ratio provided in Table 2 reveals that the proposed algorithm is fragile to additive Gaussian noises at various values for variance. Similarly, experimental results provided in Table 3 show that the proposed algorithm is able to identify salt&pepper noisy attacks for higher values of density.

## V. CONCLUSION

Apart from robust and fragile watermarking, the aim of semi-fragile watermarking is to tolerate the incidental attacks while indicating the intentional attacks if the image is heavily processed. This study has proposed a semi-fragile watermarking which designs a binary watermark from the host image in the form of a Toeplitz matrix and hides the watermark imperceptibly in the digital image inorder to secure it. Watermak is embedded in the high frequency sub-band of DWT and is extracted in the absence of original image, which results in a blind watermarking scheme.

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, Image adjustment and histogram equalization. Hence the proposed technique is effective for image authentication.

## REFERENCES

[1] Tamane S.C., Manza R. and Deshmukh R.R., “Digital Watermarking using Image Fusion Method”, International Journal of Recent Trends in Engineering, Vol.1, No.2, pp.113-116, 2009.

[2] Megha Kansal, Sukhjeet K. Ranade and Amandeep Kaur, “Fragile Watermarking For Image Authentication Using a Hierarchical Mechanism”, International Journal of Engineering Research and Applications, Vol. 2, No.4, pp.1759-1763, 2012.

[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] Liu T. and Qiu Z.D., “The Survey of Digital Watermarking based Image Authentication Techniques”, 6th International Conference, pp.1566-1559, 2002.

[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] 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.

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

[10] Tsai M.J. and Chein C.C., “A Wavelet based Fragile Watermarking with Recovery Mechanism”, Proceedings of IEEE, pp.3033-3036, 2008.

[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] 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.

[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) .

[21] Mohamed Sathik M., Sujatha S. S., “Authentication of Digital Images by using a Semi-fragile Watermarking Technique”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, No.11,pp.39-44, Nov 2012.

[22] Dr. M. Mohamed Sathik and S.S.Sujatha, “Application of Toeplitz Matrix in Watermarking for Image Authentication”, Proceedings of the IEEE International Conference on Computer, Communication and Electrical Technology (ICCCET-2011), Tirunelveli, March 2011.

[23] Cox I.J., Miller M. and Bloom J., “Digital Watermarking Principles and Practice”, Morgan Kaufmann Publishers, 2002.