International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:1, No:3, 2007

A Blind Digital Watermark in Hadamard Domain

Saeid Saryazdi, Hossein Nezamabadi-pour

Abstract**—** A new blind gray-level watermarking scheme is described. In the proposed method, the host image is first divided into 4×4 non-overlapping blocks. For each block, two first AC coefficients of its Hadamard transform are then estimated using DC coefficients of its neighbor blocks. A gray-level watermark is then added into estimated values. Since embedding watermark does not change the DC coefficients, watermark extracting could be done by estimating AC coefficients and comparing them with their actual values. Several experiments are made and results suggest the robustness of the proposed algorithm.

Keywords**—**Digital Watermarking, Image watermarking, Information Hiden, Steganography.

I. Introduction

Nowadays, there are many multimedia transmissions on the network. Because of the easy access to digital contents, copy control of digital data became an important issue.

In the recent years, there was a strong demand for secure copyright protection techniques for multimedia data. Copyright protection of digital images is defined as the process of proving the intellectual property rights.

Digital watermarking is a technique, which secretly embeds digital data into the material to identify the origin, owner, informal user, etc. Digital watermarks must be resilience against attempts to remove the hidden data.

There are three kinds of digital watermarking techniques according to their embedding purpose: robust, fragile, and, semi-fragile[1]. A robust watermark withstands malicious attacks, such as scaling, rotation, filtering, and compression. This kind of watermarking is usually used for copyright protection. Fragile watermarks can detect any unauthorized modification in an image, and therefore, they are quite suitable for an authentication purpose. However, a semi-fragile watermark is adopted to detect the unauthorized modifications, and, at the same time, it must survive some authorized image processing operations.

Depending on the application, the original host image is or is not available to the watermark recovery system. While most watermarking techniques require the original picture, there is a great interest in techniques that do not require the original data for recovering, i. e. blind watermarking techniques. That is because of the larger applications of such techniques [1].

Watermark embedding could be done in spatial or transform domain. Transform domain techniques are more robust and resistant to various attacks, and, most watermarking techniques use frequency domain to embed data.

In [2], Cox et al. Describe a method for embedding a binary watermark sequence in the highest magnitude DCT coefficients. Hsu and Wu [3,4] use the middle frequency coefficients of DCT/Wavelet transform to embed a binary watermark. These mentioned methods are robust against image processing. Their main drawback is requiring the original image to extract the watermark.

Wang et al. [5] describe a kind of blind watermarking based on relative modulation of the DCT coefficient value by referring to its estimated one. In their method, the DC values of a 3×3 neighborhood of 8×8 blocks are used to estimate the AC coefficients of central block. In each group of nine 8×8 blocks, five bits of watermark are embedded by modulating the first five DCT AC coefficients, in central block, with the following rule:

$$\text{Set } AC_i \leftarrow AC'_i + \Delta \text{ to embed bit “1”}$$

$$\text{Set } AC_i \leftarrow AC'_i - \Delta \text{ to embed bit “0”}$$

Where, AC_i and AC'_i are the real and estimated value of the AC coefficients, respectively. The watermark recovery is done by comparing AC_i and its estimated value. If $AC_i > AC'_i$, then the extracted bit is “1”, otherwise, it is “0”.

Several watermarking techniques in Hadamard domain have been proposed[6, 7, 8]. Gilani and Skodras[8], describe a watermarking scheme based on multi-resolution Hadamard transform. Their scheme is robust against most image processing and geometric operations. In[9], Fei et al. attempt to find a suitable transform domain to watermark images robust against JPEG compression attack. They show that the choice of the transform domain depends on the type of the embedded information. If the watermark is embedded by repetition coding, then the Hadamard transform gives the best results.

In this paper we propose a blind scheme for gray-level data embedding in Hadamard Domain. In the next section we review the Hadamard Transform. The proposed method will be described in section III. In section IV the experimental results are presented, and, finally, in section V a conclusion is given.

S. Saryazdi is with the Electrical Engineering Department of Shahid Bahonar University of Kerman, Kerman, Iran (phone: (98) 341-3335711, fax: (98) 341-3335711, e-mail: saryazdi@mail.uk.ac.ir).

H. Nezam Abadi pour is with the Electrical Engineering Department, Shahid Bahonar University of Kerman, Kerman, Iran (e-mail: nezam@mail.uk.ac.ir).

II. Hadamard Transform

Hadamard Transform (HT) is a non-sinusoidal transform, based on the Hadamard matrix [10]. A normalized $N \times N$ Hadamard Matrix, H, satisfies the following relation:

$$HH^T = I \quad (1)$$

Where, I is the unitary matrix. The $2N \times 2N$ Hadamard matrix is given by:

$$H_{2N} = \frac{1}{\sqrt{2}}\begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix} \quad (2)$$

Where H_N is the $N \times N$ Hadamard matrix. Furthermore, the 2×2 Hadamard matrix is given by:

$$H_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (3)$$

The Hadamard transform of a $N \times N$ two dimensional signal, I, is defined by:

$$\hat{I} = H.I.H^T \quad (4)$$

The transformed image could be considered as a linear combination of the Hadamard orthogonal basis functions. The number of sign changes in each row (column) of the Hadamard matrix is interpreted as the frequency of the row (column).

III. Proposed Method

In the proposed algorithm, the host image is first divided into 4×4 non-overlapping blocks. Our embedding procedure contains two parts. The first part is estimating the first two Hadamard low frequency AC coefficients (i.e. H(0,2) and H(2,0)) in each block, using its neighbor blocks. We use the following equations, to estimate the low frequency AC Hadamard coefficients of a block using the DC values of its 3×3 neighbor blocks [11, 12]:

$$\begin{aligned} H'(0,2) &= 1.13884 \times (DC_8 - DC_8)/8; \\ H'(2,0) &= 1.13884 \times (DC_8 - DC_8)/8; \end{aligned} \quad (5)$$

Where, DC_i presents the DC coefficient of i-th block in Fig.1.

The second part is embedding a gray-level value of watermark by replacing each low frequency AC value in the central block with its estimated modified value according to the following formulae:

$$AC_i \leftarrow AC'_i + \text{sign}(AC'_i) \times \alpha \times Iw(k,l) \quad (6)$$

Here $Iw(k,l)$ is the current pixel value in watermark image, α is a constant, and:

$$\text{sign}(x) = \begin{cases} 1 & if\ x > 0 \\ -1 & oth. \end{cases}. \quad (7)$$

Block1 DC_1	Block2 DC_2	Block3 DC_3
Block4 DC_4	Block5 DC_5	Block6 DC_6
Block7 DC_7	Block8 DC_8	Block9 DC_9

Fig.1: The central block and its neighbor blocks

If α is chosen small, the watermark will be very weak to attack. A large value of α, will degrade the quality of watermarked image. From our experiment, α can be chosen 0.1.

To recovery the watermark, one can simply calculate the difference between AC_i and its estimated value, so, the original image is not required.

Remark: embedding a watermark value will not change the DC component of the block, so, all blocks could be chosen for watermark embedding (excepted blocks in the margins of image).

IV. Experimental Results

In our experiment, we used two test images "Lena" and "Village" with a size of 512×512, and, a gray-level 128×128 watermarks, as shown in Fig.2. The watermarked images are presented in Fig.3. To demonstrate robustness of our algorithm, we performed different attacks by applying some typical image processing techniques:

- Adding "salt and pepper" noise
- JPEG compression with a compress factor of 50%
- Histogram equalization
- 3×3 Median filter

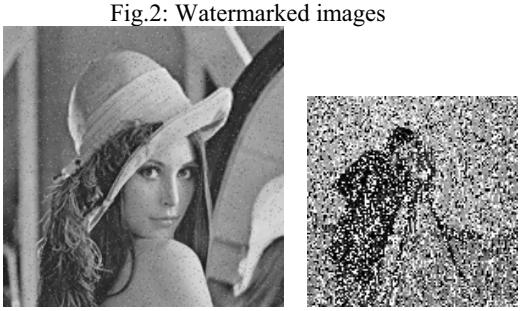
Our algorithm survives all attacks. The results for "Village" image are shown in Fig.4.

(a) (b)

(c)

Fig.2: Host images a) Lena, b) Village, c) Watermark image.

Fig.2: Watermarked images



a1 a2

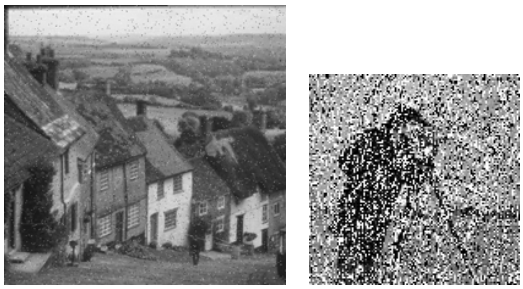
b1 b2

c1 c2

d1 d2

Fig.4: Different attacks to watermarked "Lena", a1) adding salt & pepper noise (0.02), a2) its corresponding extracted watermark, b1) JPEG Compression (50%), b2) its corresponding extracted watermark, c1) histogram equalization , c2) its corresponding extracted watermark, d1) median filtering (3*3), b2) its corresponding extracted watermark.

As these results suggest, the proposed algorithm has a good robustness and transparency.



a1 a2

b1 b2

c1 c2

d1 d2

Fig.5: Different attacks to watermarked "Village", a1)

adding salt & pepper noise (0.02), a2) its corresponding extracted watermark, b1) JPEG Compression (50%), b2) its corresponding extracted watermark, c1) histogram equalization , c2) its corresponding extracted watermark, d1) median filtering (3*3), b2) its corresponding extracted watermark.

V. Conclusion

For most watermark application, it is desired to recover the embedded data without using host image. In this paper, such a watermarking scheme for embedding gray-level watermarks is presented. In the proposed method, the two first Hadamard AC coefficients are estimated by their neighbor blocks. Then, a number proportional to the gray-level watermark value is added to each estimated AC coefficient. The recovery procedure consists of comparing the estimated values with actual ones.

Several attacks are performed, and, results suggest robustness of the proposed algorithm.

References

[1] Katzenbeisser, S., Petitcolas, F. A. P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House Editions, 2000.

[2] Cox, I. J., Kilian, J., Leighton, F. T., Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", IEEE Trans. On Image Processing, No. 6, Vol. 12,pp 1673-1687, 1997.

[3] Hsu, C. T., Wu, J. L., " Multi-resolution Watermarking for Digital Images", IEEE Trans. On Circuits & Systems: Analog & Digital Signal Processing, Vol. 45, No. 8, 1998.

[4] Hsu, C. T., Wu, J. L., " Hidden Digital Watermarks in Images", IEEE Trans. On Image Processing, Vol.8, No. 1, 1999.

[5] Wang, Y., Pearmain. A., "Blind Image Data Hiding Based on Self Reference", Pattern Recognition Letters, Vol. 25, Issue 15, pp. 1681-1689, November 2004.

[6] B.J. Falkowski, L. Lim, "Image watermarking using Hadamard transform", Electron. Lett. 36 (3), pp. 211–213, 2000.

[7] Ho, A., Shen, J., Soon, H. T., Kot, A. C., "Digital Image-in-image watermarking for Copyright Protection of Satellite Images using the Fast Hadamard Transform", IEEE Int. Geosciences and Remote Sensing Symp., pp. 3311-3313., 2002.

[8] Gilani, S. M., Skodras, A. N., "Watermarking by Multi-resolution Hadamard Transform", Proc. of European Conf. On Electronic Imaging and Visual Arts (EVA 2001), Florence, Italy, March 2001.

[9] Fei, C., Kundur, D., Kwong, R. H., "The Choice of Watermark Domain in the Presence of Compression", Proc. Of IEEE Int. Conf. On Information Technology: Coding & Computing, pp 79-84, Las Vegas, Nevada, April 2001.

[10] Prat, W. K., "Digital Image Processing", John Wiley Editions, 1991.

[11] Gonzales, C. A., Allman, L., Mccarthy, T., Wendt,P., "DCT Coding for Motion Video Storage Using Adaptive Arithmetic Coding ",Signal Processing: Image Communication,No.2,1990.

[12] Kim, C., Li, Q., Kuo, C., J., "Fast Intra-Prediction Model Selection for H-264 Codec", Proc. of ITCOM03, 2003.