# Digital Image-in-Image Watermarking For Copyright Protection Of Satellite Images Using the Fast Hadamard Transform

Anthony T.S. Ho, Jun Shen, Soon Hie Tan, Alex C. Kot

School of Electrical and Electronic Engineering
Nanyang Technological University
Nanyang Avenue
Singapore 639798
Email: etsho@ntu.edu.sg

***Abstract*-In this paper, a robust and efficient digital image watermarking algorithm using the fast Hadamard transform (FHT) is proposed for the copyright protection of satellite images. This algorithm can embed or hide an entire image or pattern as a watermark such as a company's logo or trademark directly into the original satellite image.**

**The performance of the proposed algorithm is evaluated using a benchmarking tool called Stirmark. Results show that this algorithm is very robust and can survive up to 60% of all Stirmark attacks. These attacks were tested on a number of satellite test images of size 512×512×8bit, embedded with a watermark image of size 64×64×8 bits. The simplicity of the fast Hadamard transform also offers a significant advantage in shorter processing time and ease of hardware implementation.**

**Index Terms: Fast Hadamard Transform, Satellite Images, Copyright Protection, Digital Watermarking**

## I INTRODUCTION

With the advent of the Internet, the online purchasing and distribution of satellite images can now be performed relatively easily. Over the past few years, the technology of digital watermarking has emerged as a leading candidate that could solve the problems of legal ownership and content authentications for digital multimedia data.

A great deal of research efforts has been focused on digital image watermarking in recent years. The techniques proposed so far can be divided into two main groups. One is the spatial domain approach. The simplest example is to embed a watermark into the least significant bits (LSBs) of the image pixels [1]. The other is the frequency domain approach. Cox et al. [2] used the spread spectrum communication for digital multimedia watermarking. They embedded a Gaussian distributed sequence into the perceptually most significant frequency components of container image. Hsu and Wu [3] embedded an image watermark into the selectively modified middle frequency of discrete cosine transform (DCT) coefficients of the container image.

The major problem with many watermarking schemes is that they are not very robust against different types of image manipulations or attacks such as the ones found in Stirmark. Moreover, some of these techniques are quite complicated to implement in real-time. In this paper, we propose a fast Hadamard transform (FHT) based watermarking approach. Grayscale image can be used as watermark, which is inserted into Hadamard coefficients of sub-blocks of the original container image.

This paper is organized as follows: the forward and reverse transformation of FHT and the choice of FHT domain is described in Section II. In Section III, image embedded watermarking algorithms are discussed. Experiment results under Stirmark attacks on a satellite image and the relevant discussions are presented in Section IV. Finally, the conclusion is given in Section V.

## II 2D-HADAMARD TRANSFROM OF IMAGE

The 2D-Hadamard transform has been used extensively in image processing and image compression [4].

Let $[U]$ represents the original image and $[V]$ the transformed image, the 2D-Hadamard transform is given by:

$$[V] = \frac{H_n [U] H_n}{N} \qquad (1)$$

where $H_n$ represents an $N \times N$ Hadamard matrix, $N=2^n$, $n=1,2,3\ldots$, with element values either +1 or −1. The advantages of Hadamard transform are that the elements of the transform matrix $H_n$ are simple: they are binary, real numbers and the rows or columns of $H_n$ are orthogonal.

The inverse 2D-Hadamard transform (IHT) is given as:

$$[U] = H_n^{-1} [V] H_n^{*} = \frac{H_n [V] H_n}{N} \qquad (2)$$

In our algorithm, the transform process is carried out based on the 8×8 sub-blocks of the whole image, the third order Hadamard transform matrix $H_3$ is used.

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \qquad (3)$$

In $H_3$, the number of sign transitions for row 1 to row 8 is 0, 7, 3, 4, 1, 6, 2 and 5 according to equation (3). The number of sign changes is referred to as sequency [4]. Zero sign transitions correspond to DC and a large number of sign transitions correspond to high frequency. In Hadamard matrix $H_3$, the elements are not arranged in increasing sequency, but in Hadamard order. It is possible that in the watermarking process, some of the watermark information can be embedded into the low frequency AC components. This increases the mark reliability and makes it more difficult to attack and remove.

Moreover, Hadamard transform has more useful middle and high frequency bands available, for hiding the watermark, as compared to other high coding gain transforms like DCT, at high noise environment. It has been shown that transforms including DCT are suitable for watermarking when the channel noise is low [5]. But low channel noise is not always the case. For low quality JPEG as well as some linear or nonlinear filtering, the processing noise is high. In these cases, the high gain transform watermarking methods are not very robust. But middle and high frequency Hadamard transform coefficients have components equivalent to where many DCT low-frequency AC coefficients are located. So it is more likely that in high noise environment the Hadamard transform bands would remain and unscathed. Another advantage of using the FHT is that it has a shorter processing time and its ease of hardware implementation.

## III WATERMARKING IN FHT DOMAIN

The block diagram of the proposed watermarking system is shown in Figure 1:

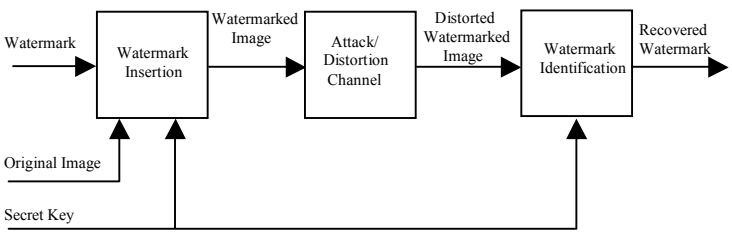


Figure 1: Block diagram of "blind" watermarking system

The proposed watermarking algorithm can hide visually recognizable patterns in the container image. In the watermarking embedding process, the watermark image, w(x,$y$), is first transformed into FHT coefficients by equation (1). We use a grayscale image of size 64×64 as a watermark for testing. After transformation, 64×64 Hadamard transform coefficients are obtained. The DC component is stored in the key file and the AC components are used for embedding.

The original satellite image, $f(x,y)$, is also decomposed into a set of non-overlapped blocks of $h \times h$, denoted by $f_k(x',y')$, $k$=0, 1, ···, K-1, where the subscript $k$ denotes the index of blocks and K denotes the total number of blocks. In our experiment, the sub-block size of 8×8 is used. The algorithm pseudorandomly selects the sub-blocks for watermark insertion using an m-sequence random number generator. The seed of m-sequence and initial state are stored in the key file. After that, FHT is performed on each selected sub-blocks of original image by equation (1). Thus for each sub-block, an 8×8 matrix of Hadamard transform coefficients is obtained. Sixteen middle and high frequency components are used for embedding. If the watermark FHT coefficients are denoted by $m_i$, the AC components of FHT coefficients of original image sub-blocks before and after inserting watermark are denoted by $x_i$ and $x_i^*$ respectively, and $i \in (0, n]$, with $n$ the number of the watermarked coefficients which is 16 in our experiment. The watermark strength factor is denoted by $\alpha$. The embedding formula is

$$x_i^* = \alpha m_i \qquad (4)$$

We choose $\alpha$ to be 0.8, an average value derived from the image sub-block statistics. The original coefficient $x_i$ is replaced by $x_i^*$. After the watermark insertion, a new 8×8 matrix of FHT coefficients of image sub-block is obtained. The IFHT is then applied on the 8×8 matrix using equation (2) to obtain the luminance value matrix of the watermarked image sub-block, $f_k'(x',y')$. After performing the watermark insertion for all the relevant sub-blocks of the original image, the watermarked image, $f'(x,y)$, is obtained and the hash file is generated for decoding process. The image-in-image watermark embedding process is shown in Figure 2: (original image spot.bmp marked with watermark image dmt.bmp)

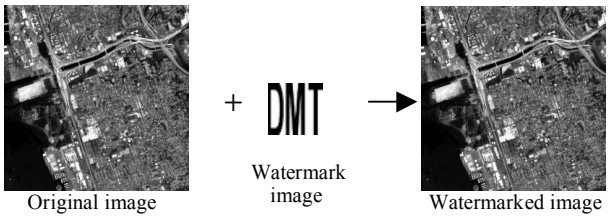


Figure 2: Image-in-image watermarking embedding process

The received watermarked image is denoted by $f''(x,y)$. By transforming all the relevant sub-blocks, $f_k''(x',y')$, into the FHT domain, we get all the Hadamard transform coefficients embedded with the watermark. Using one of the sub-block FHT coefficients as an example, the watermark is inserted into the bottom right sixteen middle and high frequency components. If these components are denoted by $x_i^{*'}$, the retrieved watermark FHT coefficients are denoted by $m_i'$, and $i \in (0, n]$, with $n$ the number of the watermarked coefficients selected is 16. The watermark extraction formula is given as:

$$m_i' = \frac{x_i^{*'}}{\alpha} \qquad (5)$$

All the watermark FHT coefficients are extracted from the sub-blocks of the watermarked image. The AC coefficients

together with the DC component stored in hash file are rearranged into a 64×64 FHT coefficients matrix. The extracted watermark image, $w'(x,y)$, is obtained by IFHT of the 64×64 Hadamard coefficients matrix using equation (2).

## IV EXPERIMENT RESULTS AND DISCUSSIONS

The experiment for the watermarking system is performed using the MATLAB 6. Two container test images consist of spot.bmp and landsat.bmp are used. These images are of sizes of 512×512×8bit. For the robustness test, we use the Stirmark that contains approximately 90 different types of image manipulations [6]. For our algorithm, a maximum image size of 256×256×8bit can be hidden into the container satellite image of size 512×512×8bit. In the experiment, a grayscale image dmt.bmp with size 64×64×8bit is used. The original and watermarked image examples are shown in figure 3: (spot.bmp marked with image dmt.bmp)

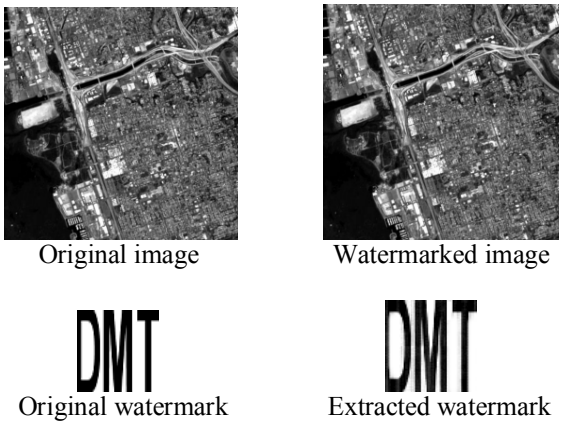


Figure 3: Container and watermark image

Results show that there were no perceptually visible degradations on the watermarked images. The extracted watermark is also highly correlated with the original watermark with correlation factor 0.989. Sample results using Stirmark are shown in Table 1: (spot.bmp is marked with image dmt.bmp)

| Image operations | Extracted watermark | Correlation |
|---|---|---|
| Sharpening 3×3 |  | 0.9573 |
| 1 rows 1 column removed |  | 0.9866 |
| FMLR |  | 0.9580 |
| Scaling 0.75 |  | 0.9354 |
| JPEG Compression of factor 30 |  | 0.8688 |
| Change aspect ratio x_1.00_y_1.20 |  | 0.8199 |

Table 1: Results of some Stirmark tests for image-in-image embedding algorithm

The image-embedding FHT domain watermarking algorithm was able to survive up to 60% against the Stirmark attacks. This algorithm was robust under jitter attacks. Cropping attacks up to 50% of the watermarked image could be resisted. The proposed algorithm was able to resist frequency mode Laplacian removal (FMLR) and 3×3 sharpening attacks. It survived some level of JPEG compression, up to a compression factor of 30. However, it performed relatively poorly against 3×3 Gaussian filtering, 2×2 median filtering and low factor JPEG compression (factor < 30). It was not so effective against random geometric transforms, such as shearing and general linear transforms. However the simplicity of the FHT offered a significant advantage over the commonly used DCT and DWT techniques, in terms of ease of hardware implementation.

## V CONCLUSION

This paper has presented a watermarking technique for embedding grayscale image watermark into a container satellite image based on the FHT. The experimental results showed that the proposed method is robust against the Stirmark attacks. Moreover, the Hadamard transform offers a significant advantage in shorter processing time and ease of hardware implementation. In future work, we plan to investigate the proposed algorithm against digital-analogue-digital conversion attack that has potential application of copyright protection for hardcopies and printed material of satellite images.

## REFERENCES


[1] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," Proc. IEEE Int. Conf. Image Processing, vol. 2, pp. 86–90, 1994.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol.6, pp. 1673–1687, Dec. 1997.

[3] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," IEEE Trans. Image Processing, vol. 8, pp. 58–68, Jan. 1999.

[4] E. H. Hall, Computer Image Processing and Recognition, New York: Academic Press, 1979.

[5] A. N. Akansu and R. A. Haddad, Multiresolution Signal Decomposition: Transforms, Subbands and Wavelets, Academic Press Inc., 1992.

[6] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on Copyright Marking Systems," in Proceedings of the Second International Workshop on Information Hiding, vol. 1525 of Lecture Notes in Computer Science, Springer,1998, pp 218-238.