Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform

Anthony T.S. Ho, Jun Shen,
Andrew K.K. Chow*, Jerry Woon*

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

* DataMark Technologies Pte Ltd
Singapore Technologies Building
100 Jurong East Street 21
Singapore 609602
http://www.datamark-tech.com

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 digital 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 image. The performance of the proposed algorithm is evaluated using Stirmark 3.1 that consists of 90 different types of image attacks. Results show that this algorithm is very robust and can survive most of the Stirmark attacks.

These attacks were tested on a number of test images of size 512×512×8 bits, 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 than other orthogonal transforms, such as the discrete cosine transform and wavelet transform.

1 Introduction

With the advent of the Internet, the online purchasing and distribution of digital images can now be performed relatively easily. However, there exists one major problem associated with the distribution of any digital images is the important issue of copyright protection and the proof of rightful ownership. Over the past few years, the technology of digital watermarking has gained prominence and emerged as a leading candidate that could solve the fundamental problems of legal ownership and content authentications for digital multimedia data (e.g. audio, image, and video).

The earliest watermarking techniques are mainly focused in the spatial domain and the simplest example is to embed the watermark into least significant bits (LSBs) of the image pixels [1]. However, this technique has relatively low information hiding capacity and can be easily erased by lossy image compression. The other is the frequency domain approach. This approach can embed more information bits and is relatively robust to attacks. Cox et al. used the spread spectrum communication for digital multimedia watermarking [2]. They embedded a Gaussian distributed sequence into the perceptually most significant frequency components of container image.

Several methods used discrete wavelet transform (DWT) to hide the data to the frequency domain [3]. The major problem with many of these 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 that embeds a grayscale image as a watermark. The grayscale image is decomposed into Hadamard coefficients for embedding. To increase the invisibility of the watermark, a visual model based on original image characteristics, such as edges and textures are incorporated to determine the watermarking strength factor. This factor is used to scale the watermark coefficients to a similar range to the coefficients from the Hadamard coefficients of the sub-blocks of the container image. The FHT embedding algorithm was found to provide a robust and efficient approach to perform digital watermarking of digital image data for copyright protection and proof of ownership. The simplicity of FHT offers a significant advantage in shorter processing time and ease of hardware implementation than most orthogonal transform techniques such as DCT and DWT.

2 2D-Hadamard transform of signal

The 2D-Hadamard transform has been used widely in image processing and image compression. In this section, we give a brief overview of the Hadamard transform representation of image data, used in the watermarking embedding and extraction process. 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, $N = 2^n$, $n = 1,2,3...$ 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 Hadamard transform matrix has the following property:

$$H_n = H_n^* = H^T = H^{-1} \qquad (2)$$

Since H_n has N orthogonal rows $H_nH_n = NI$ (I is the identity matrix) and $H_nH_n = NH_nH_n^{-1}$, thus $H_n^{-1} = H_n/N$. The Hadamard matrix of the order n is generated in terms of Hadamard matrix of order n-1 using Kronecker product, $\otimes$, as

$$H_n = H_{n-1} \otimes H_1 \qquad (3)$$

or

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix} \qquad (4)$$

The processing is performed based on the 8×8 sub-blocks of the whole image, a Hadamard transform matrix H_3 is used. By applying equation (3) or (4), H_3 becomes:

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \qquad (5)$$

The Hadamard transform matrix H_3 has its AC components in random 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.

3 Image Watermarking in FHT Domain

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. Thus in the FHT, Hadamard transform matrix H_6 is used. 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 proposed watermarking 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. Since the sub-block size is 8×8, the Hadamard transform matrix used here is H_3.

Let the watermark FHT coefficients denote 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. Where $i \in (0, n]$, and the number of the watermarked coefficients, $n = 16$. The watermark strength factor is denoted by α. The embedding formula is

$$x_i^* = \alpha m_i \qquad (6)$$

The watermarked image is then passed through a channel and possibly distorted by channel noise and external attacks. The watermark is extracted by using the embedding position and the watermark strength factor α as follows. The received watermarked image is denoted by $f''(x,y)$. The information of watermark embedded sub-blocks' position is extracted from the seed of m-sequence and initial state number stored in the key file. 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. The watermark extraction formula is given as:

$$m_i' = \frac{x_i^{*'}}{\alpha} \qquad (7)$$

All the watermark FHT coefficients are extracted from the sub-blocks of the original image. The AC coefficients together with the DC component stored in the key 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.

4 Watermark Strength Factor

The determination of the watermark strength factor is based on the original image textures and edges characteristic. It is found that edge information of an image is the most important factor for our perception of the image, so it is essential to maintain edge integrity to preserve the image quality.

The classification of different areas is based on the Hadamard transformed space energy analysis and Canny edge detection algorithm [4]. The first visual mask model is determined by the Hadamard transformed space image energy distribution. For coarse texture and outstanding edge areas, the signal energy is mainly concentrated in the AC components. For smooth areas, most of the energy is concentrated in around the low AC components and DC component. We use a squared sum of AC components to generate this visual mask, $mask_1(j,k)$ to distinguish the smooth and coarse texture areas. The second mask model is based on a Canny edge detection algorithm.

The Canny edge algorithm was selected because of its ability in detecting weak edges by using two different thresholds. It is applied to each selected sub-blocks of the original image used for watermarking. Counting the number of edge points in each sub-block, we obtain another visual mask, $mask_2(j,k)$. Large values in this mask indicate that the corresponding block is highly textured. Smaller values indicate that the block contains outstanding edges [3]. The watermark strength factor α is calculated by multiplying the two mask values and scale them to the proper range, as follows:

$$\alpha = \beta * mask_1(j,k) * mask_2(j,k) \qquad (8)$$

Where β is the scaling factor, j and k indicate the positions of the sub-blocks.

The watermark strength factor α can be controlled according to the texture areas. High textured areas are watermarked with higher strength and outstanding edge areas and smooth areas are watermarked with less strength. In this way, the invisibility of watermarked image can be improved.

5 Experimental Results

Results showed that there were no perceptually visible degradations on the watermarked images. Test results using benchmarking software Stirmark are shown Table 1. Some sample attacks are illustrated in figure 1.

The image embedded FHT domain watermarking algorithm was able to survive up to 60% against the Stirmark attacks. It was robust against jitter attacks and cropping attacks up to 50%. By incorporating post-processing techniques, the algorithm correctly retrieved the watermark against upscaling to twice the image, downscaling to 75%, changing of aspect ratios either in the x-axis or y-axis and small angle rotation attacks. 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.

This algorithm was very efficient in term of processing time. It took approximately 2 seconds for the embedding process and approximately 1 second for extraction using a MATLAB 6 platform running on a Pentium III 400 MHz PC system. The simplicity of FHT also offered an advantage over the commonly used DCT and DWT techniques for ease of hardware implementation.

6 Conclusion

This paper has presented a robust hybrid watermarking technique for embedding a grayscale image watermark into a container image based on the FHT. The experimental results showed that the proposed method was robust against 60-70% of Stirmark. The Hadamard transform has more useful middle and high frequency bands than several high gain transforms, such as DCT. It also offers a significant advantage in shorter processing time and ease of hardware implementation than commonly used transform techniques.

References

1. Van Schyndel, R.J., Tirkel, A.Z., Osborne, A.F., "A digital watermark," Proc. IEEE Int. Conf. Image Processing, vol. 2, 86–90, 1994.
2. Cox, I.J., Kilian, J., Leighton, F.T., Shamoon, T., "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol.6, 1673–1687, Dec. 1997.

3. Taskovski, D., Bogdanova, S., Bogdanov, M., "A Low Resolution Content Based Watermarking of Image in Wavelet Domain," Image and Signal Processing and Analysis, 2001. ISPA 2001. Proceedings of the 2nd International Symposium on, 200,1 604-608
4. Canny, J., "A Computational Approach to Edge Detection," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 8, No. 6, Nov 1986
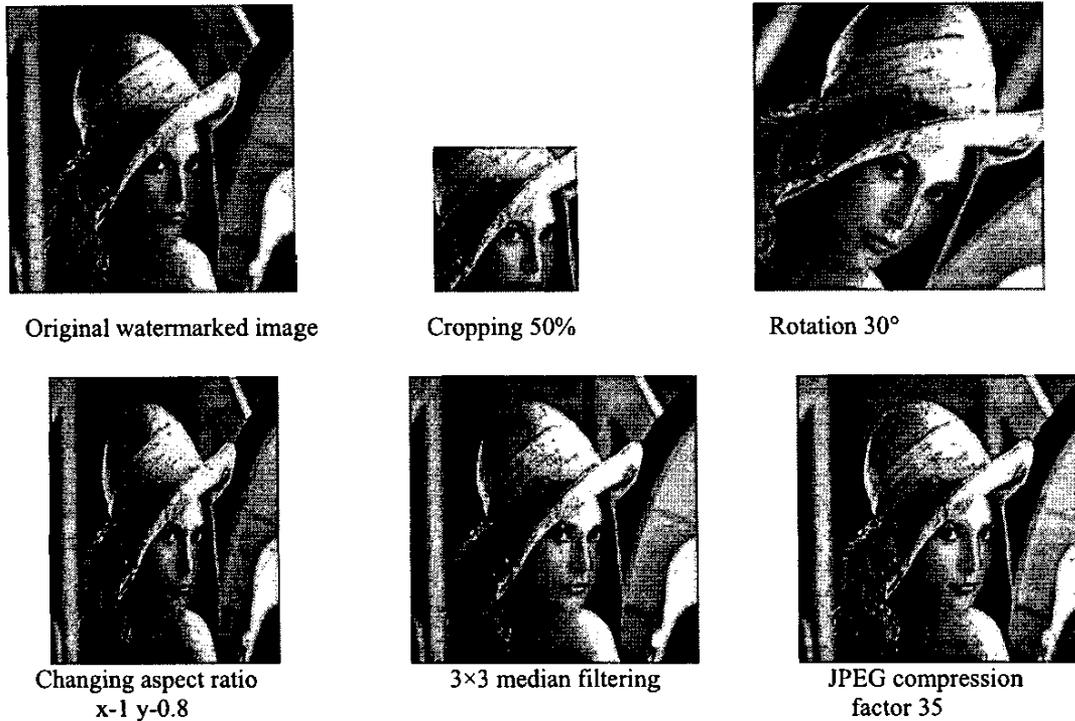
Original watermarked image	Cropping 50%	Rotation 30°
Changing aspect ratio x-1 y-0.8	3×3 median filtering	JPEG compression factor 35

Figure 1: Stirmark attack examples on watermarked image lenna.bmp

Image operations	Extracted watermark	Correlation
Sharpening 3×3		0.9573
1 rows 1 column removed		0.9866
Frequency Mode Laplacian removal		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