<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>A robust phase watermarking algorithm using conjugate symmetric sequency-ordered complex Hadamard transform</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Author(s)</strong></td>
<td>Aung, Aye; Ng, Boon Poh; Rahardja, Susanto</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>2010</td>
</tr>
<tr>
<td><strong>URL</strong></td>
<td><a href="http://hdl.handle.net/10220/7203">http://hdl.handle.net/10220/7203</a></td>
</tr>
<tr>
<td><strong>Rights</strong></td>
<td>© 2010 APSIPA. This paper was published in Proceedings of the Second APSIPA Annual Summit and Conference and is made available as an electronic reprint (preprint) with permission of APSIPA. The published version is available at: <a href="http://www.apsipa.org/proceedings_2010/AuthorIndex.htm">http://www.apsipa.org/proceedings_2010/AuthorIndex.htm</a>. One print or electronic copy may be made for personal use only. Systematic or multiple reproduction, distribution to multiple locations via electronic or other means, duplication of any material in this paper for a fee or for commercial purposes, or modification of the content of the paper is prohibited and is subject to penalties under law.</td>
</tr>
</tbody>
</table>
A Robust Phase Watermarking Algorithm Using Conjugate Symmetric Sequence-Ordered Complex Hadamard Transform

Aye Aung*, Boon Poh Ng* and Susanto Rahardja†

* School of Electrical & Electronic Engineering, NTU, Singapore 639798
E-mails: aye_aung@pmail.ntu.edu.sg, ebpng@ntu.edu.sg
† Institute for Infocomm Research, A*STAR, Singapore 138632
E-mail: rsusanto@i2r.a-star.edu.sg

Abstract—This paper presents a novel watermarking algorithm based on a newly developed transform known as conjugate symmetric sequency-ordered complex Hadamard transform (CS-SCHT). The algorithm is performed in the sequency domain where the phases of the CS-SCHT coefficients are altered to convey the watermark information using the phase-shift-keying (PSK) modulation. The amplitude boost (AB) method is employed to improve the robustness of the watermarking scheme and the spread spectrum (SS) technique is adopted to increase the security of the watermark against various attacks. The robustness of the proposed scheme is investigated by various types of image attacking operations such as JPEG compression, resizing, cropping and low-pass filtering.

I. INTRODUCTION

The proliferation of mobile multimedia devices and social networks coupled with exponential increase in capabilities of high-speed internet and communication technologies have led to an explosion in the amount of digital media content that are readily available. Such ease of distribution has caused violation of copyright and intellectual property rights. Owing to this, there is an increasing need for protection of intellectual properties through digital watermarking and other techniques that could allow tracking of usage of the digital multimedia works. Such a method is popular as in general it’s able to prevent or discourage unauthorized copying of multimedia content. By and large, a digital watermark is embedded in the digital data permanently to identify the source or ownership of the information.

In the literature, several methods have been developed for image watermarking. In general, they can be classified into two categories, one is processed in the spatial domain and the other in the transform domain. The watermarks embedded in the spatial domain are not robust to tampering as compared to that concealed in the transform domain [1]. One obvious disadvantage of the spatial domain watermarking is that a common picture cropping operation may deteriorate the watermark easily [2]. On the other hand, the transform domain watermarking schemes have several desirable features. For example, one can insert the watermarks into the host image based on the least perceptual significance of different transform coefficients. This will enhance the imperceptibility of the marks and lead to less visual degradation of the watermarked image. Besides, since the watermark is distributed over the transform coefficients irregularly, it is difficult for the attackers to remove the watermark. Various discrete transforms such as the discrete cosine transform (DCT) [2], [3], the discrete Fourier transform (DFT) [4], [5], [6], the discrete wavelet transform (DWT) [6], and the discrete fractional random transform (DFRNT) [1] have been used to transform the host image into an alternative domain. After transforming, the watermark is embedded using some robust algorithms. Finally, inverse transformation is performed to convert back to the spatial domain to obtain the watermarked images.

In this paper, we propose a novel robust image watermarking algorithm based on a newly introduced transform known as conjugate symmetric sequence-ordered complex Hadamard transform (CS-SCHT) [7]. The algorithm is processed in the sequency domain. The CS-SCHT is a complex Hadamard transform whose row vectors are arranged in an ascending order of sequencies (sequency is analogous to frequency in the DFT). Hence, sequency-based image analysis could be performed for watermarking (like frequency-based analysis for the DFT) with simpler implementation. The CS-SCHT matrix consists of four complex elements \((\pm 1, \pm j)\), hence, its transformation is very simple as compared to the DFT. Only additions or subtractions are needed to compute the transform. Besides, the CS-SCHT coefficients are complex numbers comprised of both amplitudes and phases so they are well suited to adopt phase modulation techniques [4], [5] to encode the watermark information. The complex Hadamard transform with sequency ordering (known as the SCHT) has been shown to be useful in image watermarking [8]. In fact, both SCHT and CS-SCHT show sequency ordering but the spectrum obtained by the CS-SCHT is conjugate symmetric (whereas the SCHT spectrum is not) so only half of the coefficients are needed for analysis.

In our proposed scheme, two dimensional binary pattern watermark is used since such kinds of visually recognized pattern are more intuitive to represent one’s identity than a sequence of random numbers is. First, the watermark is permuted into noises using the chaotic sequence to disperse the
spatial relationship. Then, each watermark bit is expanded by spread spectrum and embedded by PSK modulation. The paper is organized as follows. In Section 2, we provide the basic definition of the CS-SCHT. Section 3 presents the proposed embedding algorithm. Section 4 describes the watermark extraction process. The simulation results are discussed in Section 5. Finally, this paper is concluded in Section 6.

II. DEFINITION OF THE CS-SCHT

In this section, we shall provide a brief introduction to the CS-SCHT. The row vectors of this transform matrix are orthogonal to each other in the complex domain (unitary transform). The construction of the CS-SCHT matrix is described in the following [7]. Firstly, we define conjugate symmetric natural-ordered complex Hadamard transform (CS-NCHT). Let $\mathcal{H}_N$ be any CS-NCHT matrix of dimension $N \times N$. Then it is defined as

$$\mathcal{H}_N = W_N \circ A'_{n-1,n-1} \circ \cdots \circ A'_{2,2} \circ A_{1,1} \quad (1)$$

where $N = 2^n$, $\circ$ denotes the direct block matrix operator [7], $W_N$ is the $N \times N$ WHT matrix, and

$$A_{1,1} = [I_{2^n-1}, S_{2^n-1}]^T$$
$$A_{2,2} = [I_{2^n-2}, S_{2^n-2}, I_{2^n-2}, I'_{2^n-2}]^T$$
$$\vdots$$
$$A'_{n-1,n-1} = [I_{2^n-n-1}, S_{2^n-n-1}, I_{2^n-n-1}, I'_{2^n-n-1}]^T \quad (2)$$

where $S_{2^n-r} = \begin{bmatrix} I_{2^n-r-1} & 0 \\ 0 & 0 \end{bmatrix}$, $1 \leq r \leq n-1$, $I'_{2^n-k} = \begin{bmatrix} I_{2^n-k-1} & 0 \\ 0 & -I_{2^n-k-1} \end{bmatrix}$, $2 \leq k \leq n-1$ and $(\cdot)^T$ represents the transpose. As such any CS-NCHT matrix of dimension $N \times N$ where $N = 2^n$ can be obtained. Since the CS-SCHT is a bit-reversed version of the CS-NCHT, it can be constructed as follows. Let $\mathcal{H}_N$ be any CS-SCHT matrix of size $N \times N$. Then it is defined as $\mathcal{H}_N(p, k) = \mathcal{H}_N(b(p), k)$ where $0 \leq p, k \leq N-1$ and $b(p)$ is the decimal number obtained by the bit-reversed operation of the decimal $p$. The CS-SCHT of an $N$-point complex signal vector $x_N = [x(0), x(1), \ldots, x(N-1)]^T$ is defined as

$$X_N = \frac{1}{N} \mathbf{H}_N x_N \quad (3)$$

where $X_N = [X(0), X(1), \cdots, X(N-1)]^T$ is the transformed complex column vector and $(\cdot)$ denotes the complex conjugate. The data sequence can be uniquely recovered from the inverse transform, that is, $X_N = \mathbf{H}_N^T X_N$. The two dimensional (2-D) transform for an $N \times N$ image matrix can be obtained by applying 1-D transform on the rows followed by the columns of the image matrix.

III. WATERMARK EMBEDDING ALGORITHM

A novel transform domain based watermark embedding algorithm for grey-scaled images is presented in this section. A robust watermarking scheme must withstand several kinds of attacks, plus it should preserve the visual quality of the original image after embedding the watermark. Besides, it must be secure enough in order to protect the watermark from being stolen. Fig. 1 summarizes the steps for watermark embedding process. The details of some steps are presented further in the following.

A. Permutation of Watermark

In our approach, the watermark is pre-permuted into noises using a chaotic sequence obtained from the Logistic map in order to increase the security of the watermark. Logistic map is one of the simplest maps, defined by $x_{k+1} = \mu x_k (1-x_k)$ [9] where $0 \leq \mu \leq 4$ and $x_{k+1} \in (0, 1)$. When $\mu \in (3.5699, 4)$, the map is in the chaotic state. The sequences generated by the Logistic map are non-periodic, non-convergent and very sensitive to the initial conditions. First, the 2-D binary watermark is converted into 1-D sequence according to the row scanning method. Then, the chaotic sequence is obtained using $K_1$ as the initial value and $K_2$ as the value for $\mu$ ($K_1$ and $K_2$ are saved as $Ke$ for future detection purpose as shown in Fig. 1). The generated sequence is sorted according to a descending order, which gives rise to the stochastic index (label) sequence. The 1-D binary watermark sequence is permuted according to this label sequence to obtain the corresponding 2-D scrambled watermark $W_p$ which becomes chaotic as shown in Fig. 2. Hence, it will disperse the spatial relationship of the watermark as well as enhance its security against the attackers.

![Fig. 1. The flow chart of watermark embedding process.](image)

![Fig. 2. The watermark permuted by a chaotic sequence, (a) the original watermark, and (b) the permuted watermark.](image)

B. Spread Spectrum

The pseudo-noise (PN) sequence based spread spectrum (SS) method [3] is used in our system. SS ensures a large measure of security against various attacks as well as enhances the robustness of the system. In the PN-based SS system, each information bit is expanded into several bits using the PN
sequence. To accomplish the job, first $W_p$ is converted into a polar bit sequence, $d(i)$, where $i = 1, 2, \ldots, n$ by mapping $0$ to $1$ and $1$ to $-1$. Second, we generate a total of $n$ different PN sequences, $p_i(j) \in \{\pm 1\}$, with the same length of $l$ where $j = 1, 2, \ldots, l$ using a user’s secret key (which is $PN_1$). By multiplying $d(i)$ with $p_i(j)$, each information-bearing bit is spread into $l$ bits and the whole expanded polar bit sequence $m$ is expressed as $m_i(j) = d(i) \cdot p_i(j)$ where $j = 1, 2, \ldots, l$ and $i = 1, 2, \ldots, n$.

C. Random Block Selection

The image is transformed into the sequency domain using the CS-SCHT based on the $8 \times 8$ blocks. We embed one watermark bit into each $8 \times 8$ transformed block. Since the number of transformed blocks is more than the size of spread watermark bit sequence, the random block selection (RBS) is used to select the required number of blocks based on the PN sequence (which is expressed as $PN_2$ in Fig. 1). To make the watermarking scheme robust, the watermark bits should be inserted in the most significant components of an image because this portion of the host data is robust to the attacks and also highly sensitive to alteration. By doing so, it will increase the robustness of the watermarking scheme. We select $B(1, 1)$ as the location to embed the secret bit where $B$ is the selected block. The amplitude and phase of $B(1, 1)$ are denoted as $A$ and $\phi$ respectively as mentioned in Fig. 1.

D. Amplitude Boost

The purpose of amplitude boost (AB) strategy is to enhance the robustness. As mentioned earlier, the watermark information is inserted into the phases of the selected CS-SCHT coefficients. It has been known that the phase distortion due to an additive Gaussian noise is inversely proportional to the amplitude of the coefficient $[1], [4], [5]$. In order to keep the phase distortion below a certain level, the amplitude should be maintained at one defined level. Hence, the amplitude of a selected CS-SCHT coefficient is boosted to a fixed threshold value $th$ if its value is below $th$. That is,

$$A' = \begin{cases} th, & \text{if } A \leq th \\ A, & \text{if } A > th. \end{cases}$$

(4)

E. PSK Modulation

In the PSK modulation, the phase $\phi$ is modified into $\phi'$ according to the following rule:

$$\phi' = \begin{cases} \pi/2, & \text{if } m(r) = 1 \\ 3\pi/2, & \text{if } m(r) = -1 \end{cases}$$

(5)

where $m(r)$ is the spread polar watermark bit sequence and $r = 1, 2, \ldots, l \times n$.

IV. WATERMARK EXTRACTION ALGORITHM

Fig. 3 shows the steps for the watermark extraction process. It should be noted that the original host image is not needed during the recovering process. But it is important that the watermark bits are decoded from the same positions where they have been embedded previously. Therefore, the set of user’s keys $(Key_1, PN_1, PN_2)$ is reused in the extraction process as well. The PSK demodulation, inverse SS and reversed permutation are performed in the extracting process in order to inverse the operations of PSK modulation, SS and watermark permutation during the embedding process, respectively. As such the recovered watermark $W_R$ is obtained.

V. SIMULATION RESULTS

In this paper, peak signal-to-noise (PSNR) $[1], [4]$ is used to measure the degree of transparency of the watermarked image. In order to avoid the influence of subjective measurement (since the watermark is visually recognizable pattern), an objective judgement for the extracted fidelity is provided. In this paper, we use the bit-error-rate (BER) to measure the similarity between the extracted and referenced watermarks, which is defined as $BER = (e/T) \times 100\%$ where $e$ is the number of error bits detected and $T$ represents the total number of watermark bits inserted. In order to evaluate our proposed scheme, we use the grey-scaled Lena image of $512 \times 512$ pixels shown in Fig. 4, and a watermark image (pattern of NTU) of $32 \times 32$ pixels as shown in Fig. 2. We have tested on other standard images (Peppers, Barbara, Goldhill, etc) as well as a randomly generated bit string as a watermark. It is found that the results are consistent. The values of parameters used in the simulation are: $K_1 = 0.9$ and $K_2 = 3.8$ for the Logistic map, and $l = 3$, $th = 12$. The threshold for the BER value is set as 20% in order to decide the extracted fidelity of the watermark. The block size used is $8 \times 8$. The length of watermark bit sequence is $32 \times 32 = 1024$ and after spreading, it becomes $1024 \times 3 = 3072$. Therefore, RBS selects 3072 blocks from a total of available blocks, which is $(512 \times 512) / (8 \times 8) = 4096$ blocks as one secret bit is inserted into each $8 \times 8$ transformed block. Fig. 4 shows the original Lena image, and its watermarked versions using the proposed scheme based on the CS-SCHT and the DFT. Their PSNRs are 38.16 dB and 37.67 dB, respectively. Both watermarked images do not contain any visible artifacts as shown in the figure and the watermark is invisible.

Various attacks are considered in order to demonstrate the robustness of the proposed watermarking scheme where the Lena image is used as the test image again. Attacks include JPEG compression, resizing, cropping and filtering. For the JPEG compression attack, the watermarked image is compressed using the standard JPEG encoding at various
quality levels. For the image resizing, the watermarked copy is scaled down to $192 \times 192$ pixels (7.11 times reduced). The reduced image is re-scaled back to the original dimension before the extraction process. For the cropping attack, the watermarked image is cropped $(1/4)$ at the top-left corner. For the low-pass filtering, the watermarked image is filtered by using the rotationally symmetric Gaussian low-pass filter with the standard deviation $\sigma$ of 0.5. Table I shows the comparison of the BER values of the extracted watermarks from various attacked watermarked images between the proposed methods using the CS-SCHT and the DFT. It can be seen from the table that both schemes are able to recover the watermark from the resizing, cropping and filtering attacks as the extracted watermarks are clearly identified by human vision as shown in Fig. 5-a, b, c, d, f, g and h. The corresponding BER values are under the threshold as shown in the table. For the JPEG compression, the scheme using the CS-SCHT provides lower BER values than that using the DFT. Particularly, at 24% quality level, the BER value for the CS-SCHT based scheme is 18.46% (under the threshold) whereas it is 26.27% (above the threshold) for the DFT based scheme. As a result, the extracted watermark is more visually recognizable for the CS-SCHT based scheme as compared to that of the DFT (see Fig. 5-a and e). Besides, the PSNR value of the CS-SCHT watermarked image is even higher than the corresponding value of the DFT watermarked image as mentioned earlier.

Another additional advantage of the CS-SCHT based scheme over the DFT based scheme is the reduced computational complexity. Only addition/subtractions are required to perform the CS-SCHT computation. For example, in order to compute an 8-point CS-SCHT, it requires 24 complex addition/subtractions using the fast algorithm [7]. This is equal to the number of complex addition/subtractions required to compute an 8-point DFT using the radix-2 FFT algorithm. But 2 additional complex multiplications with the twiddle factors (i.e., $W_k^1$ and $W_k^2$ where $W_k^N = \exp(-j\frac{2\pi nk}{N})$) are required to perform the 8-point DFT operation, which is not needed in the CS-SCHT computation. Hence, if an image of $512 \times 512$ pixels is considered for image watermarking, an additional saving of $2 \times 16 \times 4096 = 131072$ complex multiplications can be obtained in the operation of watermark embedding. This will reduce the hardware requirement (the multipliers) when we actually implement the algorithm in hardware. The same is applied to the operation of watermark extraction as well. In fact, this is really significant in real-time implementation.

![Fig. 4. (a) The original image of Lena, the watermarked images of Lena using (b) the CS-SCHT with PSNR=38.16 dB, and (c) the DFT with PSNR=37.67 dB.](image)

![Fig. 5. The extracted watermarks: (a) the JPEG encoded at 24% quality level, (b) the resized, (c) the cropped, (d) the filtered for the CS-SCHT and the corresponding (e), (f), (g), (h) for the DFT.](image)

VI. CONCLUSION

A robust phase domain watermarking scheme for grey-scaled images based on the CS-SCHT is presented in this paper. The AB method and PSK modulation are adopted in order to enhance the robustness of the proposed scheme. In addition, the spread spectrum (SS) modulation and watermark permutation based on the chaotic sequence are incorporated into the scheme to provide an enhanced security for the watermark. The simulation results reveal that the proposed scheme is robust to various kinds of attacks such as JPEG lossy compression, resizing, cropping and low-pass filtering. Moreover, comparison between the proposed schemes using the CS-SCHT and the DFT shows that the CS-SCHT can be considered as a suitable candidate for such applications to replace the DFT with simpler implementation and less computational cost.

REFERENCES