Journal of Information Hiding and Multimedia Signal Processing ©2011 ISSN 2073-4212
Ubiquitous International Volume **2**, Number **4**, October **2011**

A Watermarking Scheme Based on the Parametric Slant-Hadamard Transform

Alimohammad Latif

Electrical and Computer Engineering Department
Yazd University, Yazd, 89195-741, Iran
alatif@yazduni.ac.ir

Fahimeh Rashidi

Yazd, Iran
ffrashidi@gmail.com

Received February 2011; revised November 2011

Abstract. *In this paper, a watermarking scheme based on the parametric slant-Hadamard transform is presented. Our approach divides the image into separate blocks and applies the parametric slant-Hadamard transform on each block individually. Then based on a blind scheme, the watermark is inserted in the transform domain and the inverse transform is carried out. The advantage of the selected transform is contribution of parameters that can be used to change the requirements of watermarking such as fidelity and robustness. The changes of transform parameters can enhance the requirements of watermarking according to the applications. Experimental results show that the proposed technique has different fidelity and robustness based on different parameters in watermarking scheme.*
Keywords: Watermarking, Parametric slant-Hadamard, Robustness, Fidelity.

1. **Introduction.** The increasingly easy access to digital multimedia via the more and more popular Internet, and the increasingly powerful tools available for editing digital media have made authentication of digital multimedia a very important issue. One solution for this problem is digital watermarking. Digital watermarking is defined as a technique of embedding additional information called watermark into digital multimedia while preserving the perceptual quality of the watermarked data. The watermark can be detected or extracted for owner identification and integrity verification of the tested data[1].

According to the domain in which the watermark information is embedded, digital watermarking techniques can be classified as spatial and spectral domain techniques[2]. In general, spectral domain methods are more robust than spatial domain ones against many common attacks[3]. A fundamental advantage of transform-based techniques is that the image transforms have good energy compactness properties and the most of image energy can be captured within a relatively small region in the transform domain. In other words, the transform basis functions corresponding to these coefficients carry the most perceptually important information of the image[4].

The method proposed in this paper, consists of embedding a watermark in the Parametric Slant-Hadamard Transform (PSHT) domain which was introduced by Agaian mostly for signal processing[5]. The PSHT includes some parameters which are suitable for changing the requirements of watermarking such as fidelity and robustness. The motivation of the present work arises from the necessity of finding out the factors that are responsible

for adjusting the fidelity and robustness of watermarking scheme. The fidelity represents that the distortion between the original and watermarked image should remain imperceptible to a human observer. The robustness is that the ability of the detector to extract the hidden watermark from some altered watermarked image[6].

In the PSHT domain, changes of the parameters cause changes on the transform matrix and consequently changes on the requirements of watermarking. In addition, these parameters could be used as encryption keys for authorization process. Moreover, if these parameters are changed in the embedding process, the requirements of watermarking will be changed, and if these parameters are changed in the extracting process, the watermark cannot be extracted properly.

The rest of this article is organized as follows. In section 2, PSHT is reviewed. Next, in section 3, we discuss the embedding and extracting procedures of the proposed watermarking scheme. Section 4 is dedicated to the experimental results representation. Moreover, the performance of our algorithm against some common attacks is evaluated in this section too. Finally, the concluding remarks are presented in section 5.

2. **Parametric Slant-Hadamard Transform.** The 2D slant transform is used in digital image processing applications such as compression[7, 8, 9]. Ho et al. employed a classical slant transform for the first time for watermarking problem[10]. It should be noted that classical slant transform, which was used by Ho, is a kind of the PSHT where all the parameters are set one.

We are going to give a brief overview of PSHT representation of the image data that is employed in our watermarking scheme. Let f be the original and F be the transformed image, 2D PSHT is given by:

$$F = S_{2^n} f S_{2^n}^T \tag{1}$$

where S_{2^n} represents a $2^n \times 2^n$ parametric slant-Hadamard matrix with real elements. The inverse transform to recover f from the transform components matrix, F, is given by:

$$f = S_{2^n}^T F S_{2^n} \tag{2}$$

The parametric slant-Hadamard matrix of order 2^n is generated in terms of matrix of order 2^{n-1} using Kronecker product operator, $\bigotimes$, as:

$$S_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3}$$

$$S_{2^n} = \frac{1}{\sqrt{2}} Q_{2^n} (I_2 \bigotimes S_{2^{n-1}}) \quad , n > 1 \tag{4}$$

where I_2 denotes the identity matrix of order 2 and Q_{2^n} is the recursion kernel matrix defined as:

$$Q_{2^n} = \begin{pmatrix} 1 & 0 & \vdots & 0_{2^{n-1}-2} & \vdots & 1 & 0 & \vdots & 0_{2^{n-1}-2} \\ a_{2^n} & b_{2^n} & & & & -a_{2^n} & b_{2^n} & & \\ \cdots & & \cdots & \cdots & \cdots & \cdots & & \cdots & \cdots \\ 0_{2^{n-1}-2} & & \vdots & I_{2^{n-1}-2} & \vdots & 0_{2^{n-1}-2} & & \vdots & I_{2^{n-1}-2} \\ \cdots & & \cdots & \cdots & \cdots & \cdots & & \cdots & \cdots \\ 0 & 1 & \vdots & 0_{2^{n-1}-2} & \vdots & 0 & -1 & \vdots & 0_{2^{n-1}-2} \\ -b_{2^n} & a_{2^n} & & & & b_{2^n} & a_{2^n} & & \\ \cdots & & \cdots & \cdots & \cdots & \cdots & & \cdots & \cdots \\ 0_{2^{n-1}-2} & & \vdots & I_{2^{n-1}-2} & \vdots & 0_{2^{n-1}-2} & & \vdots & -I_{2^{n-1}-2} \end{pmatrix} \tag{5}$$

and the parameters a_{2^n} and b_{2^n} are obtained recursively by:

$$a_{2^n} = \sqrt{\frac{3(2^{2n-2})}{4(2^{2n-2}) - \beta_{2^n}}} \qquad b_{2^n} = \sqrt{\frac{2^{2n-2} - \beta_{2^n}}{4(2^{2n-2}) - \beta_{2^n}}} \tag{6}$$

for $-2^{2n-2} \leq \beta_{2^n} \leq 2^{2n-2}$ and $a_2 = 1$. It is verified that for $\beta_{2^n} > |2^{2n-2}|$ the parametric slant-Hadamard transform matrices lose their orthogonality and is not useful in some cases.

The matrix of PSHT has two elements such as a_{2^n} and b_{2^n}. These elements are related to the βs that can be set by user. Different βs gives different transform matrices and consequently, these matrices will outcome different robustness and fidelity to the watermarking scheme.

According to the β_{2^n} values, the PSHT falls into one of the below categories:

1. For $\beta_4 = \beta_8 = \ldots = \beta_{2^n} = \beta = 1$, It was obtained the classical slant transform.
2. For $\beta_{2^{2n}} = 2^{2n-2}$ for all β_2^n, $n \geq 2$, It was obtained the ordinary Walsh-Hadamard transform.
3. For $\beta_4 = \beta_8 = \ldots = \beta_{2^n} = \beta$, $|\beta| \leq 4$, It was refereed the constant-βs slant transform.
4. For $\beta_4 \neq \beta_8 \ldots \neq \beta_{2^n}$, $-2^{2n-2} \leq \beta_{2^n} \leq 2^{2n-2}, n = 2, 3, 4 \ldots$, It was refereed the multiple-βs slant transform[11].

In this paper, the building block of the transformed image is based on the 8×8 blocks, so PSHT matrices of order 8 is used and implemented. These matrices include β_4 and β_8 and we use the same value for each block. It is understood that these parameters can be changed for each block to improve the security of the algorithm.

Figure 1 shows the parametric slant-Hadamard basis patterns for the classical slant, the ordinary Walsh-Hadamard, the constant-βs slant, and the multiple-βs slant transform of size 8 using different random βs.

3. **Description of the Watermarking Procedure.** Watermarking in transform domain becomes very attractive since a concise frequency bands decomposition is materialized in typical transform domains. Transforms such as Discrete Fourier Transform (DFT)[12], Discrete Cosine Transform (DCT)[13], Discrete Wavelet Transform (DWT)[14], and Hadamard transform [15] have been used in transformed-based watermarking.

We have investigated the parametric slant-Hadamard transform for digital image watermarking because of the available parameters that can be used to set the requirements of watermarking. Besides, the size of the transform matrix in most transform-based algorithms is an integer power of two, however, the size of matrix in the proposed transform is power of an arbitrary number[16].

The most visually important parts of an image gathered in the lower frequency bands and any modification over there might be visually obvious. Whilst the higher frequency bands embedding, is more sensitive against the compression and noise attacks. Therefore, the Middle Frequency Bands (MFB) in transformed based scheme are more appropriate for embedding a watermark[17].

In the embedding process in this study, we firstly divide the host image into 8×8 non-overlapped blocks and the MFB of each block would be of interest. The MFB of block that is proposed by Ho is shown in figure 2 [18].

After transformation of each block, we modulate a given PSHT block using equation 7:

$$F_W(U,V) = \begin{cases} F(U,V) + k * W & U,V \in MFB \\ F(U,V) & U,V \notin MFB \end{cases} \tag{7}$$

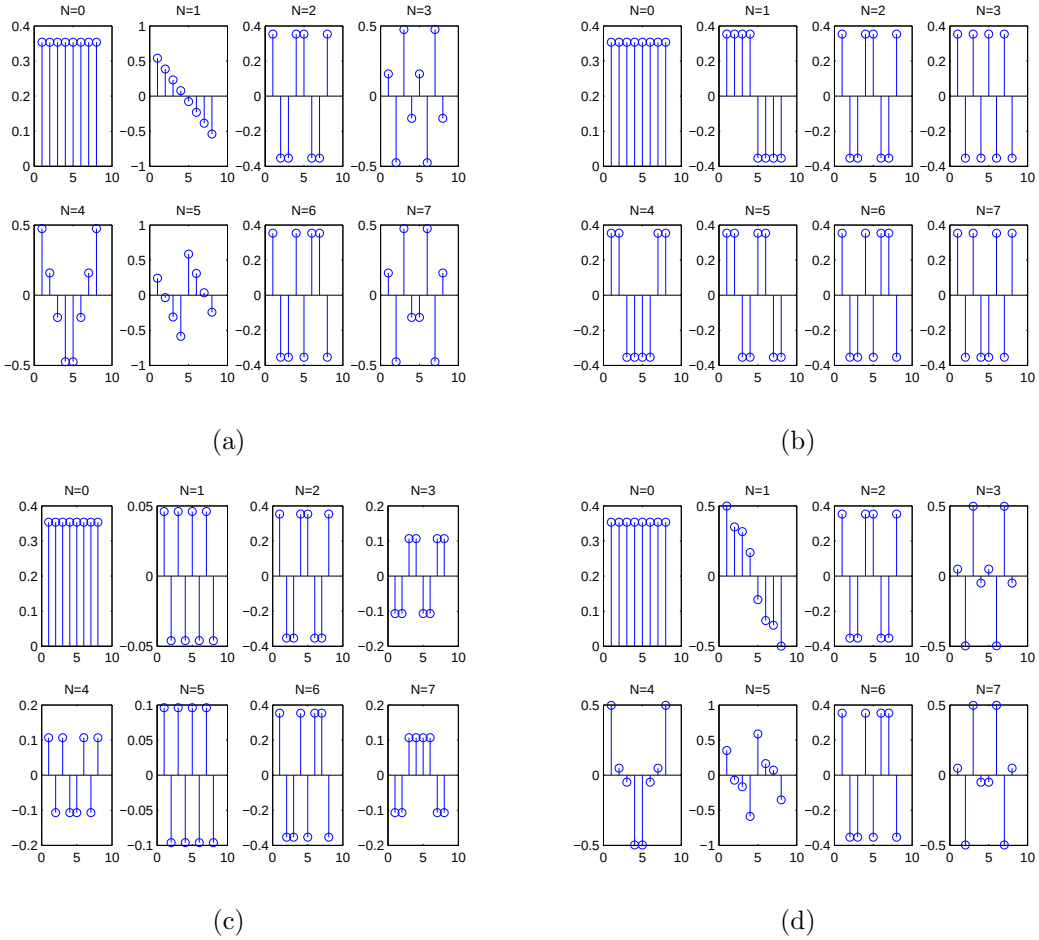

FIGURE 1. Basis patterns of (a) Classical slant with $\beta_4 = 1$, $\beta_8 = 1$ (b) Walsh-Hadamard with $\beta_4 = 4$, $\beta_8 = 16$ (c) Constant-βs with $\beta_4 = 2.2$, $\beta_8 = 2.2$ (d) Multiple-βs with $\beta_4 = -4$, $\beta_8 = 10$.

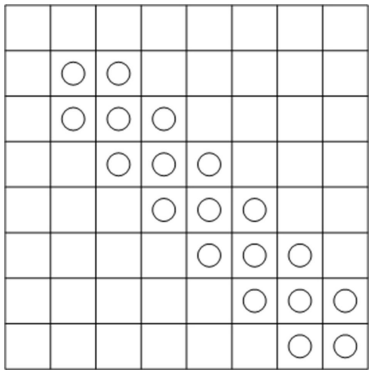

FIGURE 2. The middle frequency band of a 8×8 block that is proposed by Ho[18]

where F is the transformed image, k is the embedding strength, W is the watermark sequence which is defined based on binary watermark in equation 8, and F_W is the transformation of the watermarked image.

$$W = \begin{cases} W_0 & m = 0 \\ W_1 & m = 1 \end{cases} \tag{8}$$

In this formula, W_0 and W_1 are pseudo-random sequences with different keys and m is the watermark bit. After embedding the watermark, the inverse PSHT is performed to provide the watermarked image in the spatial domain.

The watermark extraction process does not need the transform coefficients of the original image and therefore this scheme is blind scheme. The watermark extraction procedure is correlation based and performs according to the following equation:

$$m^{'} = \begin{cases} 0 & corr(W_0, F_W^{'}) >= corr(W_1, F'_W) \\ 1 & corr(W_0, F_W^{'}) < corr(W_1, F_W^{'}) \end{cases} \tag{9}$$

where $corr(W_0, F_W)$ is the correlation between W_0 and F_W, pseudo-random and the middle coefficient of watermarked image. After extraction the pieces of watermark from each block, they are attached and the main watermark will be formed. The proposed embedding and extraction watermarking algorithm can be summarized as below:

Embedding

1. The host image, f, is divided into 8×8 non-overlapped blocks.
2. PSHT of each block is computed.
3. Concentrated on the MFB coefficient of each block at the PSHT domain, the watermark will be embedded using equation 7.
4. The inverse PSHT is computed and the host image is retrieved.

Extraction

1. The watermarked image, f_W, is divided into 8×8 non-overlapped blocks.
2. PSHT of each block is computed.
3. Concentrated on the MFB coefficient of each block at the PSHT domain, the watermark will be extracted using equation 9.
4. The extract watermark from each block attach to each other and make the original watermark.

4. **Experimental Results.** In order to evaluate the requirements of the proposed scheme, we employ the original 512×512 gray scale image of figure 3, and the 128×128 binary watermark of figure 4. The embedding strength, k, is set to 0.1 and the algorithm is repeated four times for different values of the parameters β_i $(i = 4, 8)$. The values of parameters that be used for classical slant, ordinary Walsh, constant-βs and, multiple-βs are $[1, 1], [4, 16], [2.2, 2.2], [-4, 10]$ respectively, for $[\beta_4, \beta_8]$ on each block.

FIGURE 3. The original host image

4.1. **Fidelity.** The results of watermarked image are shown in figure 5. This figure shows that the watermark has not imposed any obvious degradation to the host image and fidelity between the original image and watermarked image is high.

Figure 6 contains the result of the extraction process, where the visual quality of the extracted watermarks for all β_is are good and they are very similar to the original one.

FIGURE 4. The watermark

(a) (b) (c) (d)

FIGURE 5. Watermarked image (a) $\beta_4 = 1$, $\beta_8 = 1$ (b) $\beta_4 = 4$, $\beta_8 = 16$ (c) $\beta_4 = 2.2$, $\beta_8 = 2.2$ (d) $\beta_4 = -4$, $\beta_8 = 10$

(a) (b) (c) (d)

FIGURE 6. Extracted watermark (a)$\beta_4 = 1$, $\beta_8 = 1$ (b)$\beta_4 = 4$, $\beta_8 = 16$ (c)$\beta_4 = 2.2$, $\beta_8 = 2.2$ (d)$\beta_4 = -4$, $\beta_8 = 10$

We calculate Peak Signal to Noise Ratio(PSNR) to evaluate the fidelity of the proposed watermarking scheme more precisely[19]. The PSNR criteria is defined as:

$$PSNR = 10log_{10}(\frac{255^2}{E})_{db} \tag{10}$$

where E is the Mean Square Error (MSE) between the original and watermarked image as defined in 11:

$$E = MSE(I, I_W) = \frac{1}{M_1 N_1} \sum_{i=0}^{M_1-1} \sum_{j=0}^{N_1-1} (I(i,j) - I_W(i,j))^2 \tag{11}$$

where $I(i,j)$ and $I_W(i,j)$ denote the $(i,j)_{th}$ pixel values in the original image and watermarked image with size $M_1 \times N_1$, respectively.

4.2. **Robustness.** To demonstrate the robustness of our algorithm, we performed different attacks by applying some typical image processing techniques such as JPEG compression, median and average filtering, and histogram equalization[21].

We calculate Normalized Cross Correlation (NCC) to evaluate the robustness of the proposed scheme[20]. The NCC criteria is defined as:

$$NCC(W, W\prime) = \frac{\sum_{i=0}^{M_2-1} \sum_{j=0}^{N_2-1} (W(i,j) - \overline{W})(W\prime(i,j) - \overline{W\prime})}{\sqrt{\sum_{i=0}^{M_2-1} \sum_{j=0}^{N_2-1} (W(i,j) - \overline{W})^2} \sqrt{\sum_{i=0}^{M_2-1} \sum_{j=0}^{N_2-1} (W\prime(i,j) - \overline{W\prime})^2}} \tag{12}$$

where $\overline{W}$ and $\overline{W\prime}$ are the mean values of the original (W), and extracted watermark ($W\prime$) with size $M_2 \times N_2$, respectively.

Table 1 shows the results of calculating the PSNR and NCC for different set of βs using our scheme. The results suggest that the extracted watermark is highly correlated with the original one, so the method satisfies the basic requirements of a successful watermarking.

TABLE 1. PSNR and NCC for different categories of β_4 and β_8

Criteria	$\beta_4 = 1$ $\beta_8 = 1$	$\beta_4 = 4$ $\beta_8 = 16$	$\beta_4 = 2.2$ $\beta_8 = 2.2$	$\beta_4 = -4$ $\beta_8 = 10$
PSNR	33.762	33.956	33.132	33.634
NCC	0.997	0.987	0.996	0.995

To demonstrate the robustness of the scheme against attacks, the watermarked image is compressed using JPEG algorithm[22]. The reason of applying the JPEG compression as an attack is due to the popularity of transmitting JPEG images through the Internet. We applied a series of JPEG attacks with different quality factors ranging from 100 down to 10 and computed the NCC after each extraction.

Figure 7 illustrates the results of four different sets of βs. Compared to the results reported in[18], where a classical slant transform was used, the NCC of our algorithm is clearly higher and it suggests a higher robustness against the JPEG attack.

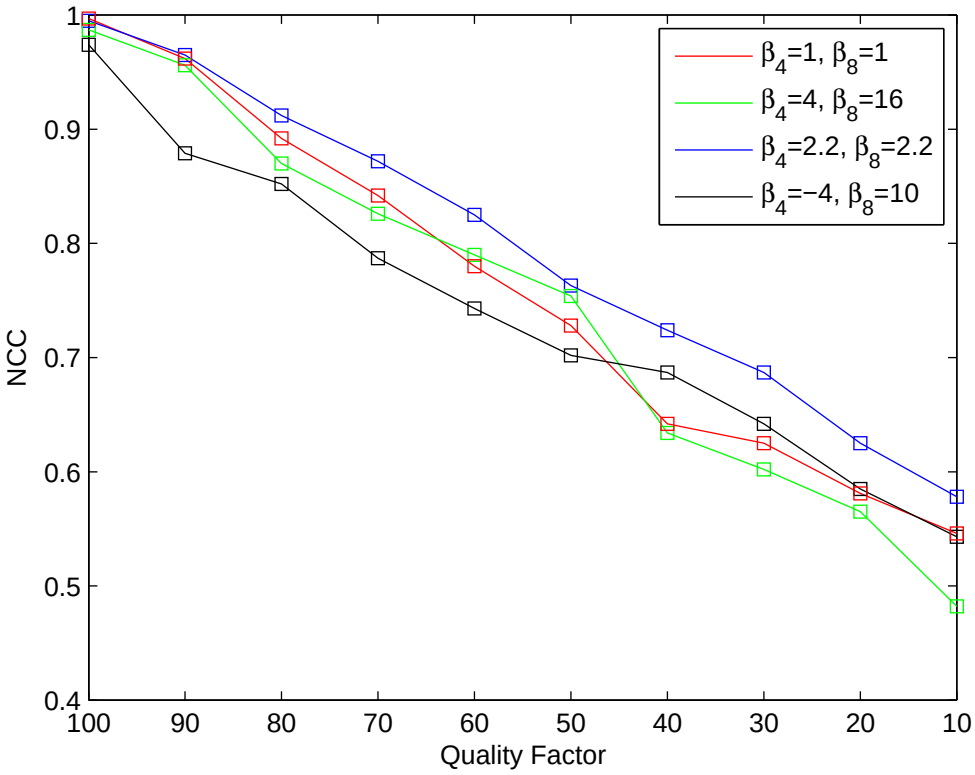

FIGURE 7. NCC versus JPEG attack

We are going to show that the PSHT watermarking is robust against the additive noise too. The Gaussian noise with zero mean and different standard deviations is added to

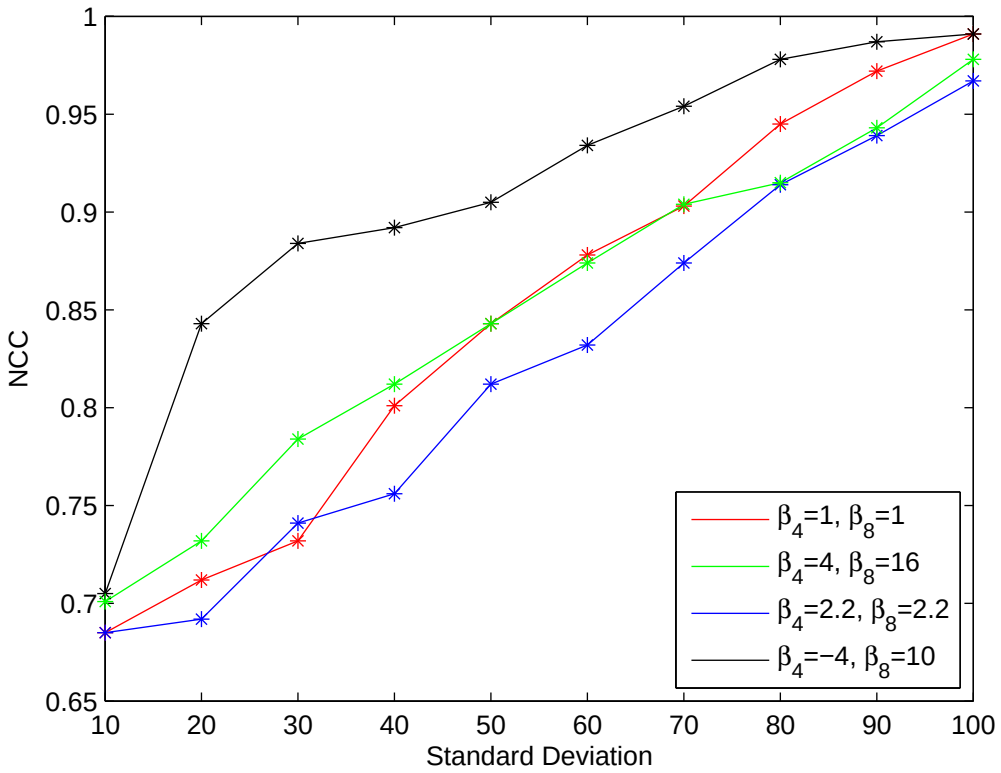

FIGURE 8. NCC versus additive noise attack

the watermarked image to test the robustness of algorithm against the additive noise. Figure 8 shows the results for different sets of βs, where it can be suggested that the multiple-β slant is the most robust ones to the additive noise attack.

Table 2 shows the outcomes of a series of further experiments where the NCC values of the extracted watermarks after various attacks are represented. It indicates that the proposed method is robust enough against different applied attacks. As results show, almost after all attacks the extracted watermark is recognizable. The worst case is when the image is applied to a high pass filter, however in this case the watermarked image itself is highly modified by the filter.

TABLE 2. NCC versus different attacks

Type of attacks	$\beta_4 = 1$ $\beta_8 = 1$	$\beta_4 = 4$ $\beta_8 = 16$	$\beta_4 = 2.2$ $\beta_8 = 2.2$	$\beta_4 = -4$ $\beta_8 = 10$
Histogram equalization	0.874	0.863	0.854	0.861
Median filter (3×3)	0.746	0.772	0.725	0.734
Adjust gray level (0.2, 0.8)	0.692	0.713	0.681	0.702
Gama correction (gamma = 1.5)	0.882	0.862	0.871	0.875
Average filter (3×3)	0.654	0.713	0.625	0.651
High pass filter ideal (Cut off fre. = 15)	0.424	0.412	0.416	0.421
JPEG (QF = 50)	0.792	0.791	0.789	0.805
Additive noise (STD = 50)	0.842	0.814	0.834	0.852

After the above experiments, we can summarize the advantage and disadvantage of PSHT scheme for watermarking:

1. The most traditional and famous transforms such as DCT in watermarking application have constant matrix and then, we do not have some explicit factors that are suitable for changing the requirements of watermarking. However, the parametric slant-Hadamard transform has some parameters that can be set by users and these parameters can affect the fidelity and robustness of the algorithm.
2. The applied PSHT can be used as a key-based transform, where the parameters of transform is used as encryption keys for authorize the process.
3. This transform has fast algorithm to compute[5].
4. In the most transform the size of image must be power of two, but in PSHT the size of image can be an arbitrary integer number.
5. The performance of our algorithm is highly correlated to the proper setting of the PSHT parameters. Therefore, a method for finding the proper parameter is needed. Also, the selected parameters have to be shared in protected way between embedding and extracting procedure.

5. **Conclusion.** In this paper, a new blind method for digital image watermarking based on the PSHT is presented and evaluated. The PSHT has some parameters that may be used for adjusting the requirements of watermarking such as fidelity and robustness. Based on different parameters, the proposed scheme has different fidelity and robustness. Different experiments using various sets of parameters are carried out and their outcomes are compared. The experimental results show that each setting of parameters may be more robust to a particular subset of attacks. Therefore in different application, it would be possible to have a more robust method against known attacks by choosing proper set of the PSHT parameters.

Acknowledgements. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] I. J. Cox, J. Kilian, F. T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia. *IEEE Trans. Image Processing*, vol. 6, no. 12, pp. 1673–1687, 1997.

[2] N. Liu, P. Amin, A. Ambalavanan, K. P. Subbalakshmi, W. Zeng, Y. Heather and L. Ching-Yung, Multimedia security technologies for digital rights management, *Academic Press*, 2006.

[3] J. Liu, D. Lou, M. Chang and H. Tso, A robust watermarking scheme using self-reference image, *Computer Standards and Interfaces*, vol. 28, no. 3, pp. 356–367, 2006.

[4] C. Fei, D. Kundur and R. Kwong, Analysis and design of watermarking algorithms for improved resistance to compression, *IEEE Trans. Image Processing*, vol. 13, no. 2, pp. 126–144, 2004.

[5] S. Agaian, K. Tourshan and J. Noonan, Parametric slant-hadamard transforms with applications, *IEEE Signal Processing Letters*, vol. 9, no. 11, pp. 375–377, 2002.

[6] G. Dorr and J. L Dugelay, A guide tour of video watermarking, *Signal Processing, Image Communication*, vol. 18, no. 4, pp. 263–282, 2003.

[7] W. Pratt and W. H. Chen, L. Welch, Slant transform image coding, *IEEE Trans. Communications*, vol. 22, no. 8, pp. 1075–1093, 1974.

[8] P. Mali, B. Chaudhuri and D. D. Majumder, Some properties and fast algorithms of slant transform in image processing, *Signal Processing*, vol. 9, no. 4, pp. 233–244, 1985.

[9] M. Anguh and R. Martin, A truncation method for computing slant transform with application to image processing, *IEEE Trans. Communications*, vol. 43, no. 6, pp. 2103–2110, 1995.

[10] A. T. S. Ho, X. Zhu, Y. L. Guan and P. Marziliano, Slant transform watermarking for textured images, *Proc. of Symposium on Circuit and Systems*, vol. 5, pp. 700–703, 2004.

[11] S. Agaian, K. Tourshan and J. Noonan, Partially signal dependent slant transforms for multi-spectral classification, *Integrated Computer-Aided Engineering*, vol. 10, no. 1, pp. 23–35, 2003.

[12] V. Viswanathan, Information hiding in wave files through frequency domain, *Applied Mathematics and Computation*, vol. 201, no. 1-2, pp. 121–127, 2008.
[13] M. Suhail, M. Obaidat, Digital watermarking-based DCT and JPEG model, *IEEE Trans. Instrumentation and Measurement*, vol. 52, no. 5, pp. 1640–1647, 2003.
[14] H. Victor, C. Clara, N. Mariko and P. Hector, Watermarking algorithm based on the DWT, *IEEE Trans. Latin America*, vol. 4, no. 4, pp. 257–267, 2006.
[15] B. Falkowski and L. Lip-San, Image watermarking using hadamard transforms, *Electronics Letters*, vol. 36, no. 3, pp. 211–213, 2000.
[16] S. Agaian, K. Tourshan and J. Noonan, Generalized parametric slant-hadamard transform, *Signal Processing*, vol. 84, no. 8 , pp. 1299–1306, 2004.
[17] C. De Vleeschouwer, J. F. Delaigle and B. Macq, Invisibility and application functionalities in perceptual watermarking an overview, *Proceedings of the IEEE*, vol. 90, no. 1, pp. 64–77, 2002.
[18] A. T. S. Ho, X. Zhu and J. Shen, Slant transform watermarking for digital images, *Proc. of Visual Communications and Image Processing*, pp. 1912–1920, 2003.
[19] C. Chang and P. Lin, Adaptive watermark mechanism for rightful ownership protection, *Journal of Systems and Software*, vol. 81, no. 7, pp. 1118–1129, 2008.
[20] D. Zheng, Y. Liu, J. Zhao and A. E. Saddik, A survey of RST invariant image watermarking algorithms, *ACM Computer Survey*, vol. 39, no. 2, pp. 5, 2007.
[21] F. Petitcolas, Watermarking schemes evaluation, *IEEE Signal Processing Magazine*, vol. 17, no. 5, pp. 58–64, 2000.
[22] G. Wallace, The JPEG still picture compression standard, *IEEE Trans. Consumer Electronics*, vol. 38, no. 1, pp. 30–44, 1992.