http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 9 (7): 1369-1375, 2010
ISSN 1812-5638

A Blind Image Watermarking Scheme Using Fast Hadamard Transform

[1]Yong Zhang, [2]Zhe-Ming Lu and [3]Dong-Ning Zhao
[1]Laboratory of ATR National Defense Technology Key, School of Information Engineering,
Shenzhen University, Shenzhen, 518060, China
[2]School of Aeronautics and Astronautics, Zhejiang University, Hangzhou, China
[3]Shenzhen Xitoy Science and Technology Co., Ltd, Shenzhen, 518060, China

Abstract: This study presents a Hadamard transform based blind digital watermarking scheme whose extraction process doesn't require the original image. In this scheme, we use a binary image as the original watermark. During the embedding process, the original cover image is first partitioned into non-overlapped 8×8 blocks and the Arnold transform is performed on the original watermark to make the scheme more robust. Secondly, the Hadamard transform is applied to the blocks. Thirdly, one bit information is embedded in each block by modifying the relationship of two coefficients in the transformed matrix. Finally, the inverse Hadamard transform is performed on the modified coefficient matrix to obtain the watermarked image. The experimental results show that the proposed watermarking method performs well in both security and robustness against general image processing operations and various kinds of attacks, while keeping the invisibility very well.

Key words: Image watermarking, blind watermarking, copyright protection, Hadamard transform

INTRODUCTION

With the development of information technologies and the growth of the Internet, vast amounts of multimedia data such as text and image have been digitized for easy storage, processing and transmission. However, the possibility of lossless and unlimited copies of digital contents is a major obstacle from the owner's viewpoint for entering the digital world. Copy protection, copyright protection and content authentication have therefore been the three most important issues in the digital world. To protect the ownership and prevent the multimedia from being tampered with, two main technologies have been proposed during the past decades. One is the encryption technology and the other is the information hiding technology that has two branches, i.e., digital watermarking and steganography. Conventional cryptographic systems permit only valid keyholders access to encrypted data, but once such data is decrypted there is no way to track its reproduction or retransmission. Over the last decade, digital watermarking has been presented to complement cryptographic processes. Digital watermarking (Khan *et al.*, 2008; Fiaidhi and Mohammed, 2003; Qureshi and Tao, 2006) describes the technologies to embed information, for example a number or a text or an image, into the digital media, such as images, video and audio, in order to protect the copyright, benefit of the investor and legal rights of owners.

Watermarking techniques can be classified into different categories according to the domain, visibility and permanence. In general, there are two types of digital watermarks addressed in the existing literature, visible and invisible watermarks. A visible watermark (Luo *et al.*, 2007) typically contains a visible message or a company logo indicating the ownership of the image. On the other hand, the invisibly watermarked digital content appears visually very similar to the original. The schemes, which are designed in the spatial domain, directly modify the multimedia data to hide information. The advantage of spatial domain-based techniques is the low computation complexity. However, spatial domain-based schemes are not robust enough to resist many attacks. Transform domain-based techniques (Choi, *et al.*, 2004; Chu, 2003; Gilani and Skodras, 2001; Ho *et al.*, 2002; Lu *et al.*, 2006; Li *et al.*, 2006; Qi and Qi, 2007; Saryazdi and Nezamabadi-Pour, 2005) have been found to offer several advantages over spatial domain-based methods, in terms of perceptibility and robustness. Several transforms, such as DCT (Discrete Cosine Transform) (Chu, 2003; Li *et al.*, 2006; Lu *et al.*, 2006), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform) are mainly used to hide watermarks in the coefficients of transform matrices. Recently, several Vector Quantization (VQ) based

Corresponding Author: Zhe-Ming Lu, Teaching Building 5, Yuquan Campus, Zhejiang University, 38 ZheDa Road, Hangzhou 310027, People's Republic of China

watermarking schemes (Lu *et al.*, 2003, 2009; Wang and Lu, 2009) have been proposed as a special branch, where the watermark information is embedded in codeword indices. Although traditional transform-domain watermarking schemes can resist various types of attacks, the computational cost and complexity are relatively high.

The Hadamard matrices possess many curious and useful properties that make the Hadamard transform useful in digital signal processing and image processing. For example, Hadamard transform has been successfully used in the fast codeword search area for image vector quantization (Chu *et al.*, 2007). Some Hadamard transform based watermarking schemes (Ho *et al.*, 2002; Gilani and Skodras, 2001; Saryazdi and Nezamabadi-Pour, 2005) have proved that the Hadamard transform is also useful in digital watermarking. However, they are either with high complexity or non-blind or with low transparency. Based on this state-of-the-art, we carry out the research project supported by the science and technology program of Shenzhen government to research the non-blind watermarking schemes.

THE HADAMARD TRANSFORM AND RELATED WORKS

2D-Hadamard transform: The 2D-Hadamard transform has been used extensively in image processing and compression. In this section, we give a brief overview of the Hadamard transform based representation of image data, which is used in the watermarking embedding and extracting process.

Let A represents the original image matrix and B is the transformed image matrix, then the 2D-Hadamard transform is given by:

$$B = \frac{H_n A H_n^T}{N} \qquad (1)$$

where, H_n represents the N×N Hadamard matrix ($N = 2^n$, $n = 1,2,3,...,$) with element values being either +1 or -1. The advantages of the Hadamard transform are that the elements of the Hadamard matrix H_n are binary and the rows or columns of H_n are orthogonal. Hence the Hadamard transform matrix has the following property:

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

H_n has N orthogonal rows, so, $H_n = NI$ (I is the identity matrix), $H_n H_n = NH_n H_n^{-1}$ and $H_n^{-1} = H_n / N$. The inverse 2D-fast Hadamard transform (IFHT) is given as:

$$A = H_n^{-1} B H_n^* = \frac{H_n B H_n}{N} \qquad (3)$$

In this proposed watermarking scheme, the forward and reverse Hadamard transforms are applied on the sub-blocks of the original or watermarked image. The two-dimensional FHT of an 8×8 block is performed by applying a one-dimensional FHT to the rows and columns, respectively. The Hadamard matrix of Order n can be generated in terms of the Hadamard matrix of Order n-1 using the Kronecker product ⊗ as follows:

$$H_n = H_{n-1} \otimes H_1 \qquad (4)$$

or

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix} \qquad (5)$$

Since, in this scheme, the watermarking process is performed on the 8×8 blocks of the cover image, the third order Hadamard matrix H_3 is adopted. By applying Eq. 4 or 5, we get H_3 as follows:

$$H_3 = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{bmatrix} \qquad (6)$$

For the H_3 matrix, the numbers of transitions for Row 1 to Row 8 are 0, 7, 3, 4, 1, 6, 2 and 5, respectively.

Related works: Although the Hadamard transform is widely used in image processing and image compression, it is seldom used in watermarking and there are just a few Hadamard transform based watermarking schemes. To present our proposed scheme, let's first review two Hadamard based watermarking schemes.

Let's first introduce Ho *et al.* (2002) watermarking scheme. The original cover image F(x, y) is decomposed into a set of non-overlapped 8×8 blocks. The algorithm pseudo-randomly selects the sub-blocks for embedding using an m-sequence random number generator. After that, a fast Hadamard transform (FHT) is performed on each selected sub-block of the original image. For each 8×8 sub-block, 64 Hadamard transform coefficients are obtained. The watermark W(x, y) is also transformed into FHT coefficients (they use a grayscale image of size 64×64 as the watermark). Therefore, the Hadamard transform based on the matrix H_6 is used. After transformation, we can obtain 64×64 Hadamard transformed coefficients denoted as m_i. The AC components of FHT coefficients of the sub-blocks of the original image, before and after embedding are denoted by x_i and x_i^*, respectively. In each 8×8 sub-block, only some AC components are modified and the remainders are kept unchanged, i.e., $i\epsilon(0, n)$ with n being the number of the watermarked coefficients (n = 16 in this scheme). The watermark strength factor is α and the embedding formula is x_i^*. After embedding, the IFHT is then applied to the 8×8 modified FHT coefficient matrix.

Another typical scheme is Saryazdi and Nezamabadi-Pours Hadamard transform based algorithm (Saryazdi and Nezamabadi-Pour, 2005). In their scheme, the cover image is first divided into 4×4 non-overlapping blocks. The embedding procedure has two steps. The first step is to estimate the first two low-frequency AC Hadamard coefficients in each block, according to its neighboring blocks. The second step is to embed a gray-level value of the watermark by replacing each low-frequency AC value in the central block with its estimated modified value. In their scheme, embedding the watermark will not change the DC component of the block, so all blocks could be chosen for watermark embedding (except for the blocks in the margins of the image).

THE PROPOSED SCHEME

Chaotic permutation: In this scheme, we use a binary image as the original watermark, which is shown in Fig. 1a. The original watermark is not suitable for embedding since it is usually meaningful and easy to be obtained. To construct a good watermark for embedding, the original watermark could be permuted to get a pseudo random sequence which is uncorrelated to the original watermark and also the cover image to be protected. Figure 1b shows the permuted result after 1 iteration and Fig. 1c shows the permuted result after 10 iterations.

Watermark embedding: Let A(n,n) be the original cover image and w(m,m) be the permuted binary watermark, where m = n/8. The embedding procedure can be detailed as follows:

- Partition the original image A(n,n) into non-overlapped blocks of size 8×8, denoted as $A_i(i = 1,2....,m\times m)$
- Apply the Hadamard transform to A_i and obtain the transformed matrix B_i
- Two coefficients $B_i(3,3)$ and $B_i(3,5)$ of B_i are selected such that we can embed one bit into this block by modifying the relationship between them
- Let Δ_1, modify the two coefficients by the following rule:

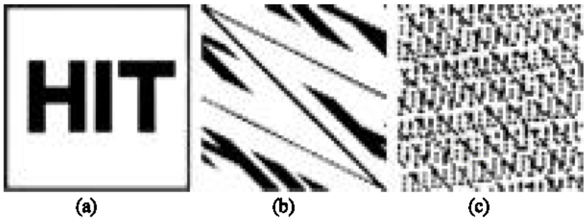


Fig. 1: (a) Original watermark, (b) the permuted result after 1 iteration and (c) the permuted result after 10 iterations

If $W(i, j) = 0$ and $\Delta_1<\Delta$, then
$$B_i(3,5) = B_i(3,5) + (\Delta - \Delta_1)/2 \text{ and } B_i(3,3) = B_i(3,3) + (\Delta - \Delta_1)/2$$
If $W(i, j) = 1$ and $\Delta_1>\Delta$, then
$$B_i(3,5) = B_i(3,5) - (\Delta + \Delta_1)/2 \text{ and } B_i(3,3) = B_i(3,3) + (\Delta + \Delta_1)/2$$

Here, Δ is set to be 20, it is selected according to the trade-off between invisibility and robustness. If Δ is too large, the distortion of the watermarked image will be terrible. While if Δ is too small, the robustness of extracted watermarks will decrease.

Equation 5 the inverse Hadamard transform is applied to B_i^*, obtaining the watermarked block A_i^w. And thus the watermarked image A^w can be obtained.

Watermark extraction: The extraction procedure is just the inverse procedure of embedding, let A^w be the watermarked or attacked image, the watermark extraction can be described in detail as follows:

- Partition A^w into non-overlapped blocks of size 8×8, denoted as A_i^w
- Apply the Hadamard transform to A_i^w and obtain the ransformed matrix B_i^w
- Let $\Delta_2 = B_i^w(3, 5)\text{-}B_i^w(3,3)$, extract one bit from each block as follows:

$$\text{If } \Delta_2>0,\ B_i^E = 0\text{; Otherwise, if } \Delta_2<0, B_i^E = 1$$

EXPERIMENTAL RESULTS AND DISCUSSION

The 512×512 grayscale Lena image and the binary watermark (the logo of Harbin Institute of Technology, HIT) of size 64×64 are served as the test image and the original watermark, respectively, as shown in Fig. 2a and c. The Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) are used to test the invisibility and robustness of the proposed method. For the unattacked watermarked image as given in Fig. 2b, the PSNR is 41.217 dB and the NC of the extracted watermark as given in Fig. 2d is 1. From these results, we can see that

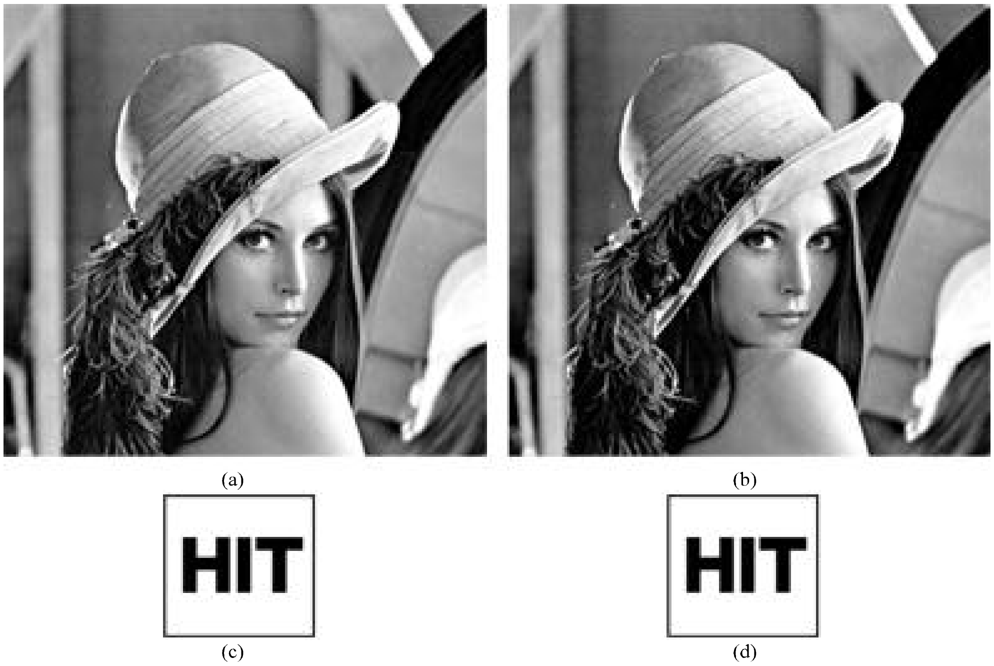


Fig. 2: The cover and watermarked images and the original and extracted watermarks without any attack, (a) Original cover image, (b) Watermarked image, (c) Original watermark and (d) Extracted watermark

our proposed method is with high transparency and we can the exact watermark without any loss from the unattacked watermarked image. Compared with the method (Gilani and Skodras, 2001) which can only get PSNRs less than 38.6 dB, our method is with higher transparency.

Table 1 shows the PSNR and NC values under JPEG compression with different quality factors. After several tests, we find that the PSNR value is generally higher than 35 dB, it means that the proposed algorithm can keep the invisibility very well. When the Quality Factor (QF) is larger than 60, the NC value decreases gradually. But if QF equals 60, the NC value decreases rapidly. It shows that this scheme is not robust enough to JPEG compression if the QF is low, this may be caused by the coefficients which are selected to embed the information.

Table 2 shows the PSNR and NC values of extracted watermarks when the watermarked image is attacked by adding Gaussian noises, adding saltandpepper noises and adding speckle noises, respectively. The Gaussian noise is of mean 0 and variance 0.001, the noise density of the saltandpepper noise is 0.01 and the speckle noise is added to the image I by using the equation J = I + n*I, where n is uniformly distributed random noise with mean 0 and variance 0.01. The above results show that the proposed method is robust enough to several kinds of noises for the extracted watermarks have NC values that are larger than 0.9. Compared with the extracted watermarks shown in the reference (Saryazdi and Nezamabadi-Pour, 2005), our method can extract watermarks with much better quality from the attacked watermarked image.

Table 1: The PSNR and NC values under JPEG compression

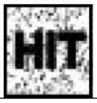
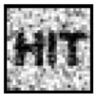
QF	90	80	70	60
PSNR (dB)	37.9460	36.7700	35.9440	35.5580
NC	1.00000	0.99614	0.96577	0.83807
Extracted watermark				

Table 2: The PSNR and NC values under noise attacks

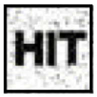
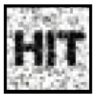
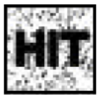
Noise	Gaussian	Salt and pepper	Speckle
PSNR (dB)	29.6840	25.2720	25.2380
NC	0.97782	0.92929	0.91414
Extracted watermark			

Figure 3a-i show some other attacks including the histogram equalization, median filtering, image adjustment, brightening, darkening and various kinds of cropping. The median filter adopts a 3×3 neighborhood, the image adjustment maps the values in the intensity image to new

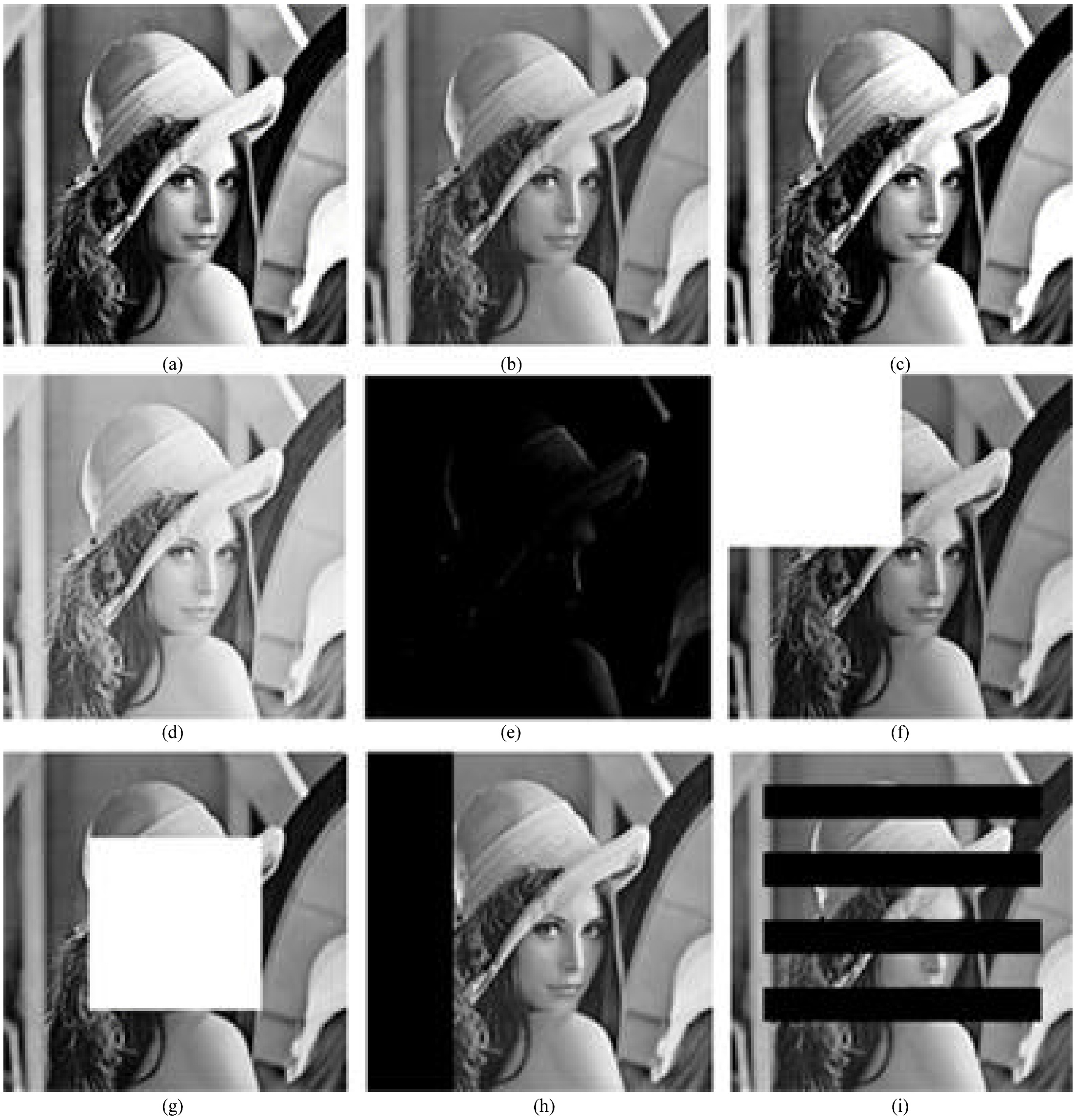


Fig. 3: The watermarked images under other attacks including the histogram equalization, media filtering, image adjustment, brightening, darkening and cropping, (a) Histogram equalization, (b) 3×3 media filtering, (c) image adjustment, (d) cropping 2, (e) cropping 3, (f) cropping 4, (g) brightening, (h) darkening and (i) cropping 1

values, the brightening and darkening will give a brighter and darker version of the original image, cropping1 crops a quarter of the original image on the top-left corner, cropping 2 crops a quarter of the original image in the center part, cropping 3 crops 128 columns on the left and cropping 4 crops four randomly selected regions of the original image. From these results, we can easily see that although the watermarked image has been severely attacked, our method can still extract watermarks with relatively high quality.

Figure 4a-i show the extracted watermarks when the watermarked image is under the corresponding image processing shown in Fig. 3a-i. We can easily recognize the extracted watermark is the logo of HIT for each case. And Table 3 shows the PSNR and NC values corresponding to the extracted watermarks in Fig. 4a-i. The PSNR value is very small under all the attacks except for the median filtering, because the watermarked image is distorted terribly, however, the NC values are still higher than 0.80000. The two tables give us a conclusion that our

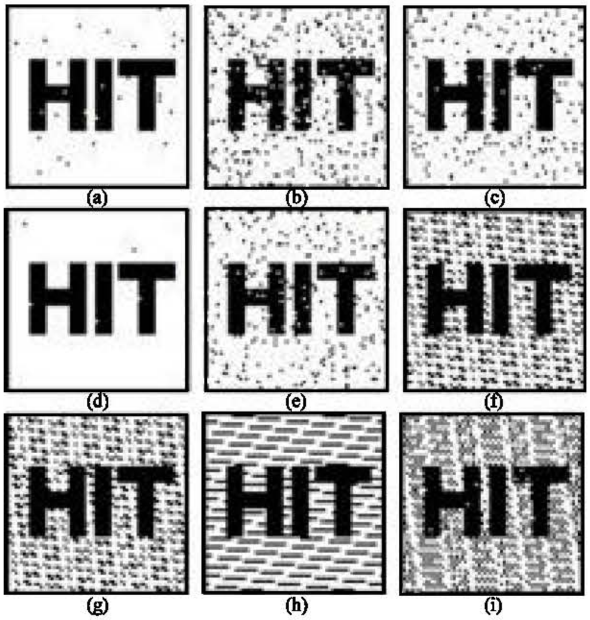


Fig. 4: The extracted watermark under the attacks including the histogram equalization, media filtering, image adjustment, brightening, darkening and cropping (a) histogram equalization, (b) median filter, (c) adjusting, (d) brightening, (e) darkening, (f) cropping 1, (g) cropping 2, (h) cropping 3 and (i) cropping 4

Table 3: The NC values under the attacks including the histogram equalization, media filtering, image adjustment, brightening, darkening and cropping

Operation	PSNR(dB)	NC
Histogram equalization	19.689	0.99549
Median filtering	34.746	0.94253
Image adjusting	18.687	0.96735
Image brightening	6.9424	0.99920
Image darkening	5.8360	0.96126
Cropping 1	5.3515	0.86584
Cropping 2	5.3507	0.86621
Cropping 3	12.244	0.86621
Cropping 4	5.3337	0.84176

new scheme is robust to various kinds of attacks. Before the embedding procedure, because we first apply the Arnold transform on the original watermark, thus our method can resist the cropping attacks well.

CONCLUSIONS

In this study, we present a blind Hadamard transform based digital watermarking scheme. The cover image is divided into 8×8 non-overlapped blocks and the original watermark is permuted using the Arnold transform. Then the fast Hadamard transform is applied to all blocks. For each block, one bit will be embedded by modifying the relationship between two coefficients in the transformed matrix. The results show that it is robust to various kinds of attacks. The future work is concentrated on how to obtain the reasonable embedding factor, which is a constant in our scheme. More coefficients also should be considered, since in this paper we just use two of them without considering how to determine the positions of these two coefficients using a certain method.

ACKNOWLEDGMENTS

This research was supported by the Science and Technology Program of Shenzhen Government (Project Number: JC200903120097A), the Scientific Research Foundation of Harbin Institute of Technology (Project Number: HIT.2003.52).

REFERENCES

Choi, W.H., H.J. Shim and J.S. Kim, 2004. Effective digital watermarking algorithm by contour detection. Lecture Notes Comput. Sci., 3064: 321-328.

Chu, W.C., 2003. DCT-Based image watermarking using sub sampling. IEEE Trans. Multimedia, 5: 34-38.

Chu, S.C., Z.M. Lu and J.S. Pan, 2007. Hadamard transform based fast codeword search algorithm for high-dimensional VQ encoding. Inform. Sci., 177: 734-746.

Fiaidhi, J.A.W. and S.M.A. Mohammed, 2003. Towards developing watermarking standards for collaborative e-learning systems. Inform. Technol. J., 2: 30-34.

Gilani, S.A.M. and A.N. Skodras, 2001. Watermarking by multi-resolution Hadamard transform. Proceedings of the European Conference on Electronic Imaging and Visual Arts, March 26-30, Florence, Italy, pp: 73-77.

Ho, A.T.S., J. Shen, S.H. Tan and A.C. Kot, 2002. Digital image-in-image watermarking for copyright protection of satellite images using the fast Hadamard transform. Proceedings of the 24th IEEE International Geoscience and Remote Sensing Symposium, June 24-28, Toronto, Canada, pp: 3311-3313.

Khan, A., X. Niu and Z. Yong, 2008. A robust framework for protecting computation results of mobile agents. Inform. Technol. J., 7: 24-31.

Li, H.F., W.W. Song and S.X. Wang, 2006. Robust image watermarking algorithm based on contourlet transform. J. Commun., 4: 87-94.

Lu, Z.M., W. Xing, D.G. Xu and S.H. Sun, 2003. Digital image watermarking method based on vector quantization with labeled codewords. IEICE Trans. Inform. Syst., 86: 2786-2789.

Lu, W., H. Lu and F.L. Chung, 2006. Robust digital image watermarking based on sub-sampling. Applied Math. Comput., 181: 886-893.

Lu, Z.M., J.X. Wang and B.B. Liu, 2009. An improved lossless data hiding scheme based on image VQ-index residual value coding. J. Syst. Software, 82: 1016-1024.

Luo, H., J.S. Pan and Z.M. Lu, 2007. Content adaptive visible watermarking during ordered dithering. IEICE Trans. Inform. Syst., 90: 1113-1116.

Qi, X.J. and J. Qi, 2007. A robust content-based digital image watermarking scheme. Signal Process., 87: 1264-1280.

Qureshi, M.A. and R. Tao, 2006. A comprehensive analysis of digital watermarking. Inform. Technol. J., 5: 471-475.

Saryazdi, S. and H. Nezamabadi-Pour, 2005. A blind digital watermark in Hadamard domain. Proc. World Acad. Sci. Eng. Technol., 3: 126-129.

Wang, J.X. and Z.M. Lu, 2009. A path optional lossless data hiding scheme based on VQ index table joint neighboring coding. Inform. Sci., 179: 3332-3348.