


Robust image watermarking scheme using bit-plane of hadamard coefficients

Elham Etemad¹ · Shadrokh Samavi^{2,4} ·
S. M. Reza Soroushmehr³  · Nader Karimi² ·
Mohammad Etemad¹ · Shahram Shirani⁴ ·
Kayvan Najarian³

Received: 20 December 2015 / Revised: 2 November 2016 / Accepted: 15 December 2016
© Springer Science+Business Media New York 2017

Abstract Nowadays, due to widespread usage of the Internet, digital contents are distributed quickly and inexpensively throughout the world. Watermarking techniques can help protect authenticity of digital contents by identifying their owners. In a watermarking procedure, owner information may be embedded in the spatial domain or transform domain of host images. Since watermarking algorithms must be tamper resistant and transparent, we present a watermarking method based on a transform domain. In this method, we employ Hadamard transform as it requires simpler operations compared to other transforms such as discrete cosine transform (DCT) and discrete wavelet transform (DWT) while it still attains robustness. We analyze each bit of the Hadamard's coefficients in terms of robustness and transparency for hiding the watermark information and find a bit-plane that maintains both robustness and transparency. After that, watermark information is hidden redundantly in the selected bit-plane. The proposed extraction algorithm is classified as a blind algorithm since it extracts all versions of the concealed watermark with no information from the host image. The output of the extraction algorithm is a logo obtained by an intelligent voting among all versions of the hidden logo. The experimental results show that the proposed method, while providing transparency, is robust against many image processing attacks such as compression, image cropping and Gaussian filtering.

✉ S. M. Reza Soroushmehr
ssoroush@umich.edu

Elham Etemad
eefami@dal.ca

¹ Department of Computer Science, Dalhousie University, Halifax, NS, Canada

² Department of Electrical and Computer Engineering, Isfahan University of Technology, Isfahan 84156-83111, Iran

³ University of Michigan Center for Integrative Research in Critical Care (MCIRCC), University of Michigan, Ann Arbor, MI, USA

⁴ ECE Department, McMaster University, Hamilton, ON, Canada

Keywords Image watermarking · Hadamard transform · Copyright · Robustness · Transparency

1 Introduction

In the current century, the Internet is approaching a ubiquitous tool for transforming information and distributing digital contents around the world in a short period of time. On the other hand, recent advances in the digital technology domain result in reproducing new versions of digital contents with no considerable degradation and hence create additive concerns for digital content producers. Also, the advent of various tools for manipulating digital data causes concerns about preserving the original nature of the data. These advances have persuaded researchers to seek new methods to conceal owner-related and content-related information on digital contents.

Since images account for a major share of digital contents, many attempts have been made to watermark them with information about the owner's identity. In the transmission channel, logo information might change unintentionally or intentionally. Therefore, watermarking methods must be robust and resistant against these changes to securely protect intellectual property.

There are several methods for embedding information such as coefficients quantization and aggressive embedding [8, 13, 17]. If a watermarking procedure alters intensities of an image's pixels, it is called spatial domain watermarking. Even though these methods provide a high payload for concealing a watermark logo, they are not robust against image processing attacks such as compression, filtering, and affine transforms [4, 20, 21]. On the other hand, to perform a robust watermarking, transform domains could be used in which a discrete transform is applied on an image first and then its coefficients are used for embedding information. Generally, watermarking in a transform domain provides more robustness as well as a high capacity for hiding information. There are several transforms that could be used for this purpose such as discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Hadamard transform (DHT) and Karhunen-Loeve transform (KLT) [3, 5, 24] that are computationally complex.

Besides robustness, transparency is another important feature measured by the amount of resemblance between the visual quality of watermarked and host images. This resemblance has to be in a way that the human visual system (HVS) cannot recognize differences between the two images. There is a trade-off between watermarking system robustness and its transparency. More concerns about the robustness of watermarking enforce watermarking algorithms to make more alteration in the host images which decreases the transparency of the images. On the other hand, higher focus on watermarked image transparency leads to less alteration in the images. Hence, the resulting watermark may be distorted by image processing attacks.

In this paper we propose a watermarking method with the following contributions.

- Defining a criterion that considers both robustness and transparency.
- Analyzing bit-planes of Hadamard coefficients in terms of robustness and transparency.
- Embedding a watermark logo in non-overlapping blocks of a host image redundantly.
- Developing a blind extracting method that doesn't require the host image or original watermark. Final extracted watermark is produced by voting among all extracted versions of the watermark.

- Proposing a method that has high capacity of embedding and transparency. It is also robust against some image processing attacks such as JPEG compression, image cropping and Gaussian filtering.

The rest of the paper is organized as follows. In Section 2, we review some related works and also give a brief description on Hadamard transform. The proposed method is explained in Section 3 where the proposed embedding and extraction algorithms are illustrated in different subsections. Implementation details and experimental results are demonstrated in Section 4. Finally, Section 5 gives some concluding remarks and possible future work.

2 Background

In this section we first review the state-of-the-art methods on image watermarking and then give a brief introduction to Hadamard transform and its features.

2.1 Related work

Several image watermarking methods have been presented in the last three decades. Each method usually has two stages: 1) embedding a watermark logo in an image and 2) extracting the watermarked logo from the image. Watermark extraction algorithms could be categorized into three classes based on the amount of information used from the host image. These classes are named informed, semi-informed and blind watermarking [14, 16]. Extractors of informed watermarking need the host image while extractors of semi-informed watermarking need some kind of information about the host image. Blind extractors, on the other hand, don't require information about host images.

In the category of informed watermarking we can refer to the method of [19] that uses Hadamard transform on non-overlapping blocks of host images and watermark logos. This method employs human visual system properties to hide watermark coefficients in host image coefficients. Its informed extractor produces an HVS mask of a host image and deduces the coefficients of host and watermarked images. Moreover, contrast masking, in addition to the Watson model for DHT, is used as an HVS masking to consider frequency, luminance and adjacent pixels correlation. They also utilized Spread transform which selects host signal coefficients randomly to embed the watermark. Although this method can improve robustness and maintain imperceptibility, the optimal local embedding strengths cannot be determined easily. In the method presented in [9], watermark bits are embedded additively in Hadamard transform coefficients of high entropy blocks. The extraction procedure calculates block entropies and extracts watermark bits from those blocks whose entropies are higher than a predefined threshold. The performance of this method depends on the threshold which is chosen as a fixed value while the entropy changes depending on the image and degradation level and hence this threshold needs to be selected adaptively. DCT coefficients of logos corresponding to low frequencies have been embedded into Hadamard coefficients of textured blocks of the host image in [6]. Its extractor algorithm is an informed algorithm as it extracts watermark coefficients by computing the difference between host and watermarked image coefficients. Moreover, the watermark logo is reconstructed by using extracted DCT coefficients of logo blocks. This method also uses a threshold for segmenting the textures and its performance might change by changing the threshold. One of the recent approaches towards informed digital image watermarking is

presented in [23]. In this method, the Best–First–Search approach is applied on Hadamard coefficients of host image blocks to obtain the increasing sequence of each block. In addition, the highest value of the longest sequence for watermark embedding is selected and the watermark is concealed by multiplying the watermark coefficient by the scale factor and replacing the host image coefficient. In the extraction algorithm, the reverse routine is implemented and the watermark is fetched by dividing each coefficient by the scale factor. In this method all the coefficients except for the DC coefficient are involved which might make this method fragile to different types of noise.

Blind watermarking methods are usually classified into complex–transform and non–complex–transform methods. In the non–complex category, we can refer to [27] where watermark embedding is performed by using Arnold transform on the watermark image to increase the robustness. In this method, the watermark is concealed by changing the relationship between two Hadamard coefficients in each block. Its extractor, by investigating the relationship among these coefficients, could determine watermark bits blindly. Compared to methods that conceal more copies of a logo in one block, this method could achieve lower transparency. The method presented in [18] divides image regions into three levels based on their level of information using an Entropy measure. These levels are low, mid and high informative blocks. Then, Hadamard transform is applied to low informative blocks and one of the low significant bit–planes of the low frequency Hadamard coefficient is replaced by the watermark. Also, the watermark is redundantly concealed in a bit–plane of coefficients with the highest magnitude of mid–informative blocks. In the extraction routine, watermarks of each block category are extracted independently and the final watermark is determined using both versions of the extracted watermark. In this method, the authors select the low informative blocks of an image, based on the entropy measure, which are mostly flat areas of the image where even a small degradation is recognizable. This results in lower transparency of the watermarking method. The authors of [10] embed a watermark in Hadamard coefficients of an image blocks. The main contribution of this method is in using the most significant bit–plane of the host image and all bit–planes of the watermark to form a match matrix used in the watermark extraction algorithm. They also hide the watermark using a spread spectrum technique and extract it by Bi–phase demodulation. The main issue with this method is setting the values of demodulation index experimentally which results in instability of the results on different images and logos.

In the complex category, authors of [15] hid the watermark in a gray scale image using complex Hadamard transform [15]. To perform watermarking, they altered phases of complex conjugate coefficients corresponding with the value of watermark bits. The amount of phase change is determined experimentally considering robustness and transparency. In their method, watermark extraction is performed by computing a linear correlation between original and extracted watermarks [15]. Although this method is a robust watermarking technique, its performance relies on the angle parameter which is determined experimentally. Another method based on complex Hadamard transform was presented in [28] where a sequence of zero and one values was concealed in the host image by applying XOR operation on the watermark sequence and the sequence of coefficients signs. In this method a Spread Spectrum technique is used to increase the length of the watermark sequence and gain more robustness. Suitable coefficients for watermarking are selected from normalized image blocks which are in a square around the invariant centroid of host images. To extract the watermark, the original watermark sequence was regenerated and altered coefficients of the image are obtained by applying a similar routine to the embedding algorithm. Finally, the presence or absence of the watermark was determined by calculating normalized correlation between the original and extracted watermark sequences. This method is a robust

watermarking method that its highest reported normalized cross correlation (NCC) is around 0.89 which is lower than the ideal NCC for watermark extraction, i.e. $NCC = 1$.

Considering sequency-ordered of complex Hadamard transform, another method presented in [2] in which the embedding algorithm exploits techniques such as Low Amplitude Block Selection to choose blocks that impose less distortion, Amplitude Boost method to increase the robustness of its scheme and Phase-shift keying (PSK) modulation technique to select suitable coefficients for watermarking. In this method, each bit is embedded by modifying the selected coefficients. Moreover, in order to extract the watermark, PSK demodulation is applied to watermarked blocks of the image and watermark bits are extracted. Although the focus of image watermarking methods is on obtaining a method to satisfy the trade-off between robustness and transparency, the robustness of this method is considerable. However, its transparency for watermark embedding is relatively low. Authors of [22] proposed a reversible image watermarking scheme using reversible Hadamard transform. In this method, low frequency AC components of each image block are estimated first and then the difference between original and estimated values is computed and each watermark bit is embedded into predicted error expansion of a block. The extraction method is similar to embedding algorithm in most steps and watermark bits are extracted by computing the difference between watermarked and estimated AC coefficients. The transparency of this method is considerable, while its robustness is not proved. Since they use the blocks with the size of 4×4 , this method might be fragile against JPEG compression attacks.

2.2 2D Hadamard transform

Contrary to other orthogonal transforms such as sine and Fourier transforms that use complex calculations, Hadamard transform is not computationally intensive. This transform is based on Walsh function that needs only binary operations on real numbers and performs simple calculations [1] that simplifies hardware implementation of forward and inverse Hadamard transform. Moreover, it has the same forward and inverse transform cores. These particular features make this transform suitable for many image processing applications and real-time watermarking. To perform Hadamard transform on a $2^n \times 2^n$ image, a $2^n \times 2^n$ matrix, H_n , consisting of only 1's and -1 's is employed. Hadamard transform matrix for $n = 3$ is shown in (1).

$$H_3 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \quad (1)$$

The transform matrix H_n is produced using Kronecker rule based on the assumption that $H_1 = 1$ and H_n can be calculated recursively using (2):

$$H_n = H_{n-1} \otimes H_1 \quad (2)$$

where \otimes denotes the Kronecker product of two matrices.

Since the rows and columns of H_n are orthogonal, this matrix has some sole characteristics such as the one shown in (3) that makes the calculation of forward and inverse Hadamard transform simple.

$$H_n = H_n^T = H_n^{-1} \quad (3)$$

In (3), H_n^{-1} is the inverse matrix of H_n and H_n^T is the transpose of H_n matrix. The Hadamard transform of an arbitrary matrix U can be calculated using the following equation:

$$V = (H_n \times U \times H_n)/N \quad (4)$$

where V is the transformed matrix and the size of Hadamard matrix, H_n , is $N \times N$ where $N = 2^n$. Using orthogonality feature and considering I as the identity matrix, the following equation is obtained.

$$H_n \times H_n = N \times I \quad (5)$$

Using the above equation we can obtain the inverse Hadamard transform formula (6).

$$U = (H_n \times V \times H_n)/N \quad (6)$$

Using Shannon law it has been proved that applying Hadamard transform in image watermarking imposes less changes on image information than applying other transforms with multi-variable kernels [19]. Hadamard transform also presents the "sequency" effect that is equivalent to frequency of Fourier transform and determines the number of sign changes in each row of the Hadamard matrix. It has been shown that the major part of the signal's energy could be packed in special bands called mid-sequency which are equivalent to mid-frequency [19]. The mid-sequency bands provide better perceptual transparency and hence increase the capacity of the watermarking scheme compared to some other transforms such as Fourier transform. Hadamard transform is also robust against compression with low quality factors [19]. Another feature of Hadamard transform that is suitable for image watermarking is the orthogonality feature between rows and columns of its kernel which provides a suitable degree of independency among Hadamard transform coefficients [19]. Considering these features, Hadamard transform is utilized in this paper.

3 Proposed method

In the proposed method a binary watermark logo is concealed in a gray scale image by decomposing Hadamard transform coefficients of each image's blocks into its bit-planes. Moreover, the watermark is embedded redundantly on one of these bit-planes. A detailed explanation of these steps is presented in Section 3.1. The proposed watermark extractor has no information about the host image, the image without watermark, and the final logo is produced by voting on the intensity resemblance among different versions of the extracted watermark. More detailed information about the steps of the watermark extraction is presented in Section 3.2.

3.1 Watermark embedding

In order to conceal a watermark logo in a host image, we first divide the host image into non-overlapping blocks. Then, the Hadamard transform is applied to each of these blocks and a watermark logo is embedded redundantly in some special coefficients of mid-sequency bands of the blocks obtained by Hadamard transform. Figure 1 shows the block diagram of the proposed watermark embedding method. The main contribution of this

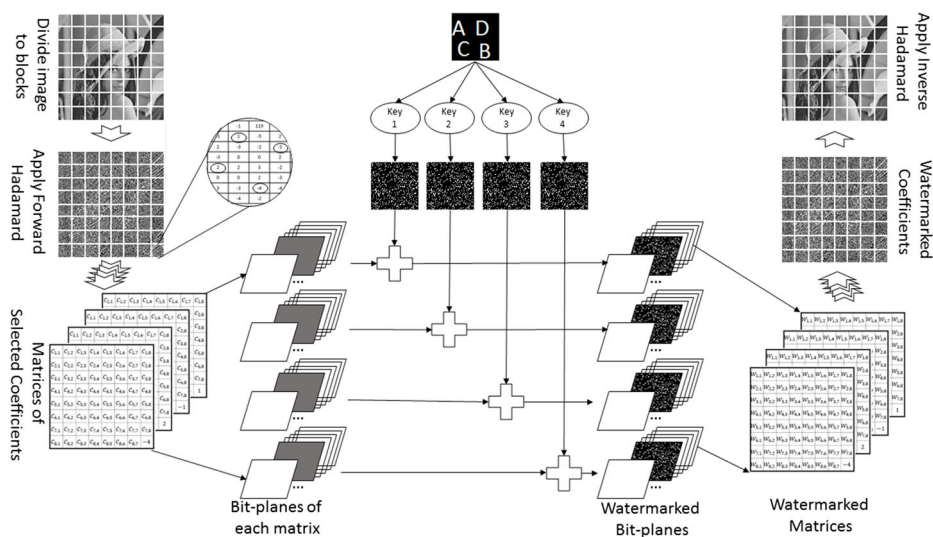


Fig. 1 Block diagram of the proposed embedding method

algorithm is in embedding the watermark logo into *bit-planes* of Hadamard transform of each block of the host image *redundantly*.

In the first step of the embedding algorithm, a host image with the dimension of $N \times N$ is divided into non-overlapping blocks with the dimension of $M \times M$. The main reason for choosing block-wise embedding is lowering the number of pixels affected by altering a Hadamard transform coefficient. Therefore, more coefficients can be used for watermarking and more information can be hidden while the same transparency is achieved. After dividing the host image into blocks, the Hadamard transform is applied to all of these blocks individually to provide the mid-sequence coefficients suitable for watermarking.

In addition to providing transparency, it is necessary to embed hashed versions of owner's logo in the host image to increase the security of the image watermarking method. Therefore, the logo is randomized using pseudo-random sequences whose keys are only known by the image holder. In this method, we conceal n different versions of a single logo in a host image redundantly to increase the robustness of the image watermarking. Since n different versions of the logo are demanded, we randomize it using n different keys and generate n different pseudo-random sequences. As a result, a single logo is hashed using different keys and hence each version of the logo would be different from the other versions for a single host image. This randomization method not only increases the system's immunity, but also results in scattering of attack's effects into different parts for each extracted version of the logo. This along with the voting algorithm in our watermark extraction routine result in improving the robustness of our watermarking method.

When Hadamard coefficients and randomized logo are obtained, n coefficients of each block are selected and modified where each coefficient is utilized for concealing one bit of a single version of the logo. In the proposed method, n is selected to be an even number to provide the opportunity of utilizing neighborhood pixels' information in the watermark extraction routine. n matrices are created from co-sequence coefficients of all the image's blocks. In the other word, coefficients with a similar sequence but in different image's

blocks are collected together to form a single matrix, where n different sequences are selected for hiding the logo.

Each of these matrices are decomposed into its bit-planes and one of these planes is replaced by one of the randomized versions of the logo. Selecting the suitable bit-plane requires an investigation on the trade-off between the robustness and transparency of the algorithm. In this method the suitable bit-plane is assumed to be the l^{th} bit-plane of these matrices. The selected bit-plane can be replaced with a version of the logo through (7) which provides three levels of quantization, $L, 0$, and $-L$, where $L = 2^{l-1}$. This three-level quantization makes the proposed algorithm more transparent and flexible, since there are coefficients that carry information without any alteration. In (7), W_i , C_i and \hat{C}_i are i^{th} watermark bit, Hadamard coefficient, and watermarked Hadamard coefficient respectively. Also, $B(C_i, L)$ shows L^{th} bit of C_i .

$$\hat{C}_i \leftarrow C_i + L \times (W_i - B(C_i, L)) \quad (7)$$

Finally, watermarked coefficients are rearranged and replaced on their corresponding positions in transformed blocks of the image. Then, by applying the inverse Hadamard transform to these blocks and merging them, the watermarked image is obtained.

3.2 Watermark extraction

In order to extract the logo from the watermarked image, we introduce an algorithm which is mostly reverse of the watermark embedding algorithm, following by a voting routine among different versions of the extracted logo. The schematic diagram of the proposed watermark extraction method is depicted in Fig. 2.

The first four steps of the proposed watermark extraction algorithm (i.e. blocking, Hadamard transform, Creating matrices and creating bit-planes) are similar to the corresponding ones of the embedding algorithm and the only difference is in the final steps. This means that at first we divide the image into non-overlapping blocks. We apply Hadamard

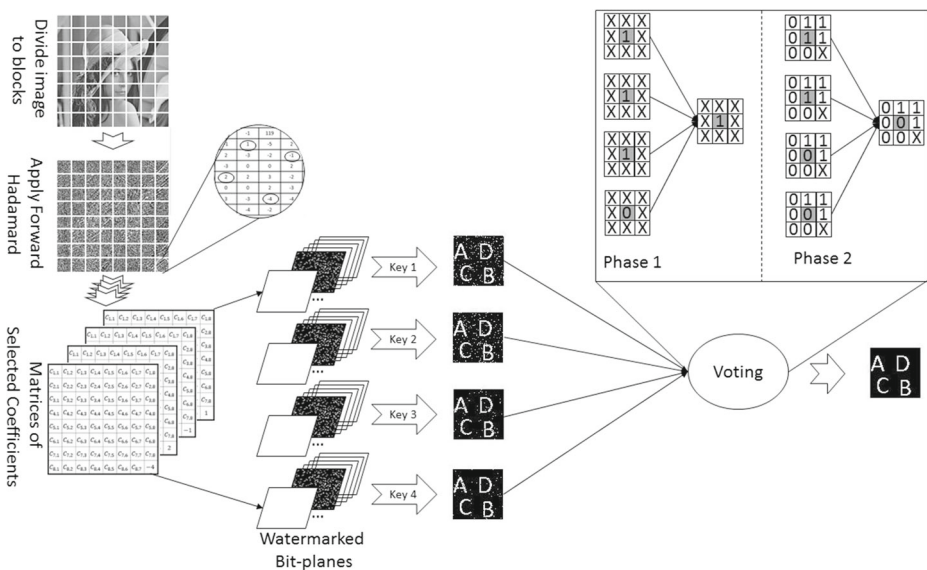


Fig. 2 Block diagram of the proposed extraction method

transform to each of those blocks and create matrices from the coefficients with the same sequence. Finally, we extract one bit-plane from each matrix which is the bit-plane used for the watermark embedding routine. The method to extract each bit-plane is formulated in (8). In this equation, \tilde{C}_i and \tilde{W}_i are the Hadamard coefficients of the i^{th} block of the watermarked image, and the i^{th} bit of the extracted watermark respectively. Each extracted bit-plane is one version of the watermark logo.

$$\tilde{W}_i \leftarrow \mathcal{B}(\tilde{C}_i, L) \quad (8)$$

The final watermark is calculated by voting between pixel's intensities of all the extracted versions of the logo. If n (i.e. the number of versions of the hidden logo) is odd, the number of extracted watermark bits with the value of zero is not equal to the number of bits with the value of one; resulting in an efficiency of a simple voting algorithm for determining the value of the extracted watermark bit. Otherwise, in order to determine the value of each bit of the extracted logo, the voting algorithm uses the information of its neighborhood bits when the number of 0 candidate values is equal to the number of 1 candidate values for that bit.

This voting algorithm consists of two phases: determining values for the bits with a dominant candidate value and determining values for all the remaining bits. First, the final intensity of all bits of the extracted logo with dominant intensity is determined (the gray bit in phase 1 of Fig. 2). In this algorithm, when the values of a special bit in most of the extracted versions of the logo are identical, its value in the final logo is equal to the dominant value. In the second phase, if the number of various values of a special bit in different versions is equal, there is no dominant value for that bit (gray bit in phase 2 of Fig. 2) and hence the algorithm votes among the neighboring bits values (obtained in the first phase) to determine the value of the current bit in the extracted watermark. The pseudo-code of the voting algorithm is presented in Algorithm 1. In this code, $\bar{G}_k(i, j)$ is the final value of a bit at location (i, j) in the k^{th} extracted logo.

Algorithm 1 Pseudo-code of voting among different versions of extracted watermark

```

input   :  $\bar{G}_k$ , Extracted Logos ( $k = 1, \dots, n$ )
output :  $\hat{G}$ , Extracted Watermark

1   $n_1 \leftarrow \sum_{k=1}^n \bar{G}_k(i, j)$ 
2  if  $2 \times n_1 < n$  then
3     $\hat{G}(i, j) \leftarrow 0$ 
4  end
5  else
6    if  $2 \times n_1 > n$  then
7       $\hat{G}(i, j) \leftarrow 1$ 
8    end
9    else
10      $n'_1 \leftarrow \#$  of ones in the  $3 \times 3$  window centered on  $\bar{G}_k(i, j)$ 
11      $n'_0 \leftarrow \#$  of zeros in the  $3 \times 3$  window centered on  $\bar{G}_k(i, j)$ 
12     if  $n'_1 > n'_0$  then
13        $\hat{G}(i, j) \leftarrow 1$ 
14     end
15     else
16        $\hat{G}(i, j) \leftarrow 0$ 
17     end
18   end
19 end

```

4 Experimental results

In order to evaluate our proposed method, we applied some experiments on a set of gray-scale host images with the size of 512×512 , and a set of binary logos with the size of 64×64 . In our experiments, the watermark logo was encrypted using four diverse keys to increase the robustness and immunity of our watermarking method. These keys are the only information the extractor has about the embedding procedure. Each key produces a different pseudo-random sequence and makes a different hashed logo for embedding in the image. These keys act as passwords for watermark embedding and the performance of our method is completely independent from this selection. In all of our experiments, we chose 100, 200, 300 and 500 as the security keys.

There are two parameters that should be determined for our image watermarking method: 1) the size of Hadamard blocks of the host image, and 2) the coefficients of the Hadamard transform. In our experiments, each host image is decomposed into 8×8 non-overlapping blocks to be consistent with the JPEG compression algorithm [19]. To determine a set of Hadamard coefficients, we should consider the fact that these coefficients are independent and except for the coefficient located in (1, 1), all of them are middle and high frequency components [12].

Finding the best set of coefficients to achieve the highest performance is challenging as the complexity of this problem is of the order of $O(2^{n_c})$ where n_c is the number of coefficients; for a block with size of 8×8 , $n_c = 64$. Here, we choose four Hadamard coefficients at locations (1, 3), (3, 1), (5, 7) and (7, 5) after experimenting with different sets of coefficients. We noticed that using more coefficients doesn't necessarily improve the performance of our proposed method.

We have tested our method on a Linux system with Core i7 CPU and 32 GB of Memory using Matlab R2016a. The required time for watermark embedding and extraction using this system are 1.23 and 0.12 seconds on average respectively.

4.1 Robustness-transparency trade-off measure

For measuring the performance of an image watermarking method, there are two metrics whose trade-off is important: robustness, and transparency. In this section, we define a measurement that its value is a representative of this trade-off based on a transparency and a robustness metric.

In order to measure the transparency of a watermarking method, we calculate the Mean Structural SIMilarity (MSSIM) index [26] between the host and the watermarked images. This metric measures the transparency by comparing the similarity between the host and the watermarked images. The defined range of MSSIM metric is $[0, 1]$ where values close to 1 represent higher transparency.

Moreover, we calculate the NCC between the original logo and the extracted logo from the watermarked image after performing an image processing attack. NCC measures the robustness of the proposed image watermarking method by investigating the correlation between the extracted logo and the original logo. The range of NCC is also defined as $NCC \in [0, 1]$ where the higher value represents the more correlation between the original and the extracted logos, and the more robustness of the watermarking method.

Using these two individual metrics, we defined $\rho = MSSIM \times NCC$ as a criterion to measure the robustness and transparency at the same time. The ρ takes its values from the range of $\rho \in [0, 1]$ and represents the trade-off between transparency and robustness.

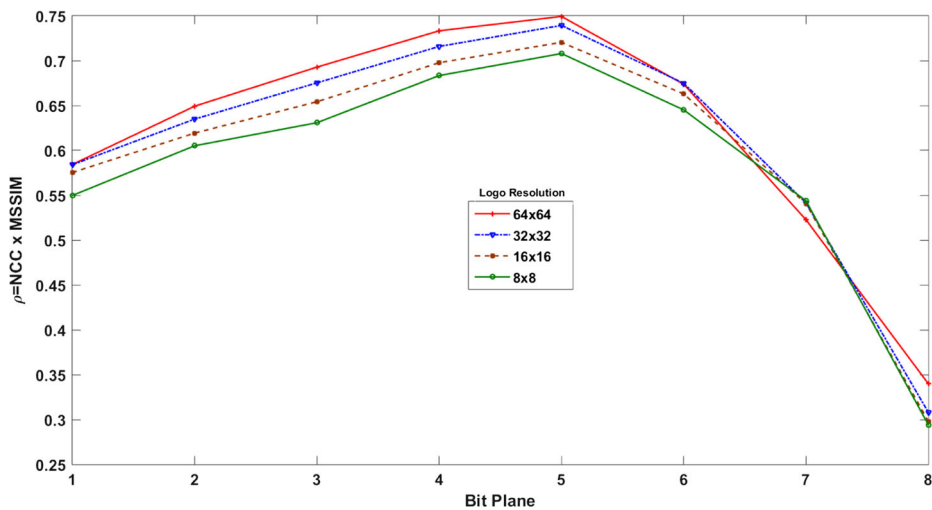


Fig. 3 Average of ρ using different attacks on 100 host images. Four scales of a random logo were used as watermark and concealed at each bit-plane

Values close to 1 satisfy both MSSIM and NCC measures while values close to 0 represent weakness in either or both of these aspects.

4.2 Parameter evaluation

Before continuing our experiments and comparing our method with the recent advances in this domain, there is a parameter in our method that needs to be determined that is the suitable bit-plane of the host image for concealing the watermark logo.

In order to figure out which bit-plane is better in terms of both transparency and robustness, we applied our method on 100 natural gray-scale images using four scales of a random binary logo and 18 different attacks. The resolution of each image is 512×512 and the resolutions of the logos are 64×64 , 32×32 , 16×16 and 8×8 . Since the goal of this experiment is to find the best bit-plane for watermark embedding, we avoid imposing any changes in other parameters of the method. This means that, even though for the logos with the smaller size, there is a possibility of concealing more redundant versions of the logo in the image, we choose four redundant versions in all the cases.

Considering 100 host images, four logos and 18 attacks, we performed $100 \times 4 \times 18 = 7200$ simulations. Figure 3 shows the average of ρ over 100 images. As can be seen, the 5th bit-plane has the highest ρ which means that in average, concealing the watermark in this plane gives a trade-off between the transparency and robustness of the scheme for four various watermark capacities.

4.3 Comparison

To represent the transparency of our proposed method, some host images and their corresponding watermarked images are shown in Fig. 4, utilizing the logo image of Fig. 5 as

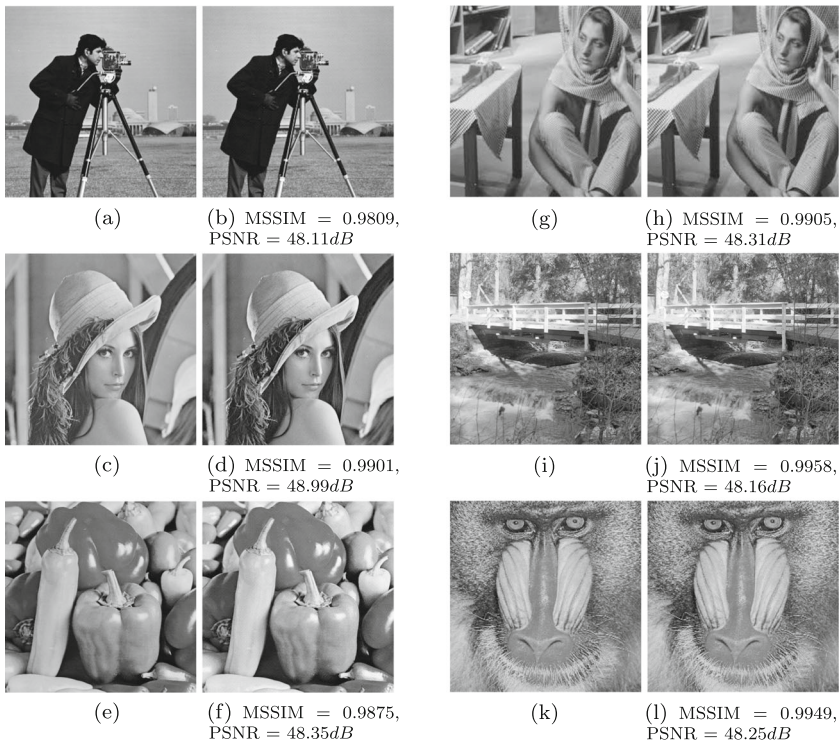


Fig. 4 5a, 5c, 5e, 5g, 5i and 5k are input images. 5b, 5d, 5f, 5h, 5j and 5l are watermarked images corresponding to input images. MSSIM and PSNR are calculated for each image

Fig. 5 The logo image with the size of 64×64



Table 1 Comparing the transparency of the proposed method with some recent image watermarking methods on different images based on PSNR values (db)

Image Method	Lena	Barbara	Baboon	Peppers	Bridge
Fazlali [7]	—	42.89	40.06	—	41.74
Tsougenis [25]	40.18	—	—	40.28	—
Hamghalam [11]	43.45	—	—	42.71	43.20
Proposed method	48.99	48.31	48.25	48.35	48.16

Table 2 Normalized cross correlation (NCC) values between original and extracted logos from the attacked watermarked images

Measure \ Attacks	Gamma Correction	Corner Crop (128 × 128)	Center Crop (128 × 128)	Salt & Pepper Noise (0.01)
NCC	0.791	0.997	0.999	0.760
Measure \ Attacks	Intensity Adjustment	Brightenning (0.02)	Scaling (0.5)	Gaussian Filter
NCC	0.679	0.895	0.664	0.941
Measure \ Attacks	Darkening	Jpeg (90)	Jpeg (85)	Jpeg (80)
NCC	0.995	0.989	0.973	0.957
Measure \ Attacks	Jpeg (70)	Jpeg (60)	Jpeg (50)	Jpeg (40)
NCC	0.899	0.816	0.836	0.836



Fig. 6 6a, 6c, 6e, 6g, 6i and 6k are attacked watermarked images. 6b, 6d, 6f, 6h, 6j and 6l are extracted logos from the corresponding attacked watermarked images. NCC values for all extracted logos are calculated

watermark logo. As can be observed, the watermarked images are visually similar to their corresponding input images which is proved by calculated PSNR and MSSIM similarity.

A comparison between the transparency of our proposed method and some recently presented image watermarking methods is provided in Table 1. The highest value for each image is marked as bold, which represents the superiority of our proposed method in terms of transparency.

In addition to transparency, the robustness of our algorithm was examined and the NCC between the extracted logo and the original logo was calculated. These results are presented in Table 2 that illustrate the robustness of the proposed method against attacks such as rotation, different image cropping attacks and Gaussian filtering. Although this method is somehow fragile against attacks such as image adjustment and brightening, Salt and Pepper noise, Gamma correction, and scaling, the extracted logo is still recognizable considering the recognition threshold of 0.65 for NCC [18]. The special robustness of the proposed method is observed in JPEG compression, based on the results showed in Table 2.




The extracted logos after some different image processing attacks are shown in Fig. 6. These results illustrate that the proposed method is robust against attacks such as different image cropping while its weakness against darkening/brightening attacks is negligible since the extracted logos after these attacks are still recognizable.

In order to prove that the proposed method's performance is independent from the content of host images, the robustness criterion is also investigated for different images where some of our findings are represented in Table 3. We also reported the average NCC among different images for each attack that illustrates the robustness of our method. The robustness of the proposed method against some attacks is also investigated on cases with different logos. These results along with the average robustness against some attacks are represented in Table 4.

Table 3 NCC values for various attacks on different images

	Lena	Bridge	Baboon	Peppers	Barbara	Average
Edge Crop 512×64	0.9946	0.9968	0.9957	0.9968	0.9968	0.9961
Edge Crop 512×128	0.9615	0.9829	0.9872	0.9936	0.9861	0.9822
Edge Crop 512×256	0.6348	0.9432	0.9274	0.9689	0.9518	0.8852
Brightening 0.2	0.7944	0.4321	0.4350	0.7689	0.6890	0.6238
Corner Crop 64×64	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Corner Crop 128×128	0.9989	0.9989	0.9989	1.0000	0.9989	0.9991
Corner Crop 256×256	0.9503	0.9936	0.9936	0.9936	0.9925	0.9847
Center Crop 64×64	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Center Crop 128×128	0.9989	0.9979	1.0000	0.9968	0.9989	0.9985
Center Crop 256×256	0.9377	0.9819	0.9851	0.9829	0.9851	0.9745
Salt & Pepper Noise 0.01	0.8104	0.7982	0.8444	0.8019	0.8025	0.8114
JPEG Comp. $Q = 70$	0.7594	0.4769	0.6030	0.6160	0.7764	0.6463
JPEG Comp. $Q = 80$	0.7933	0.6945	0.7897	0.7706	0.8388	0.7773
JPEG Comp. $Q = 90$	0.9520	0.9239	0.9534	0.9349	0.9637	0.9455
Rotation 90	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Gaussian Filter 0.5	0.8844	0.5906	0.6105	0.8727	0.9007	0.7717

Table 4 NCC values for various attacks when different logos are embedded

	IUT WL	A D C B				Average
Edge Crop 512×64	0.9906	0.9946	0.9959	0.9956	0.9940	0.9941
Edge Crop 512×128	0.9519	0.9616	0.9700	0.9727	0.9431	0.9599
Edge Crop 512×256	0.6202	0.6348	0.7090	0.7080	0.6205	0.6585
Brightening 0.2	0.8180	0.7944	0.9443	0.9403	0.7375	0.8469
Corner Crop 64×64	0.9981	1.0000	0.9998	0.9995	1.0000	0.9995
Corner Crop 128×128	0.9944	0.9989	0.9976	0.9976	0.9955	0.9968
Corner Crop 256×256	0.9578	0.9503	0.9638	0.9630	0.9400	0.9550
Center Crop 64×64	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Center Crop 128×128	0.9991	0.9989	0.9995	0.9990	1.0000	0.9993
Center Crop 256×256	0.9500	0.9377	0.9715	0.9751	0.9573	0.9583
Salt & Pepper Noise 0.01	0.8434	0.8104	0.9572	0.9514	0.7849	0.8695
JPEG Comp. $Q = 70$	0.7951	0.7594	0.9378	0.9283	0.7405	0.8322
JPEG Comp. $Q = 80$	0.8235	0.7594	0.9378	0.9283	0.7405	0.8322
JPEG Comp. $Q = 90$	0.9600	0.9520	0.9868	0.9909	0.9320	0.9643
Rotation 90	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000
Gaussian Filter 0.5	1.0000	1.0000	1.0000	1.0000	1.0000	1.0000

In order to compare the proposed method with some recent watermarking methods we presented the Bit Error Rate (BER) percentage between the extracted logo and the original logo for our method as well as a number of methods in Table 5 using a number of attacks. We also presented a comparison on NCC of our method with another recent watermarking method in Table 6. These results illustrate that the proposed method is more robust generally on geometric attacks such as rotation, scaling and image cropping. While it has weakness on some image processing attacks, it can not be proven that our method work worse than these watermarking methods considering the size of the logo which is concealed in the host image (Table 7).

In another simulation, the sensitivity and specificity of the proposed method for various thresholds on NCC were calculated using 100 different host images. The obtained ROC diagrams are depicted in Fig. 7. Also the sensitivity and specificity of our algorithm against 20 attacks with the threshold of 0.8 on NCC are listed in Table 8 which represent the considerable accuracy of the proposed method.

Table 5 BER(%) of the proposed method along with results claimed in two other image watermarking methods using Peppers as host image

	Crop 5 %	Crop 10 %	Scale 1.5	Rotate -5	Rotate 5	Gaussian Filter	JPEG 85
Tsougenis [25]	51	–	8	44	–	–	10
Hamghalam [11]	6.58	10.48	0	4.72	5.84	3.55	3.76
Proposed Method	0.02	0.02	0.05	0.06	0.08	0.00	6.2

Table 6 NCC of the proposed method along with results claimed in another image watermarking method for image cropping and Gaussian Filters with ($\sigma = 2$) using Barbara as host image

	Crop 5 %	Crop 10 %	Crop 15 %	Crop 20 %	Gaussian Filter 3 × 3	Gaussian Filter 5 × 5	Gaussian Filter 7 × 7
Fazlali [7]	1	0.9930	0.9574	0.9280	0.99	0.85	0.63
Proposed Method	1	0.9979	0.9946	0.9872	0.9007	0.8947	0.8955

Table 7 Comparing the proposed method with other methods in terms of the size of the watermark logo

	Fazlali [7]	Hamghalam [11]	Tsougenis [25]	Proposed Method
payload (bits)	128	128-1024	100-300	4096

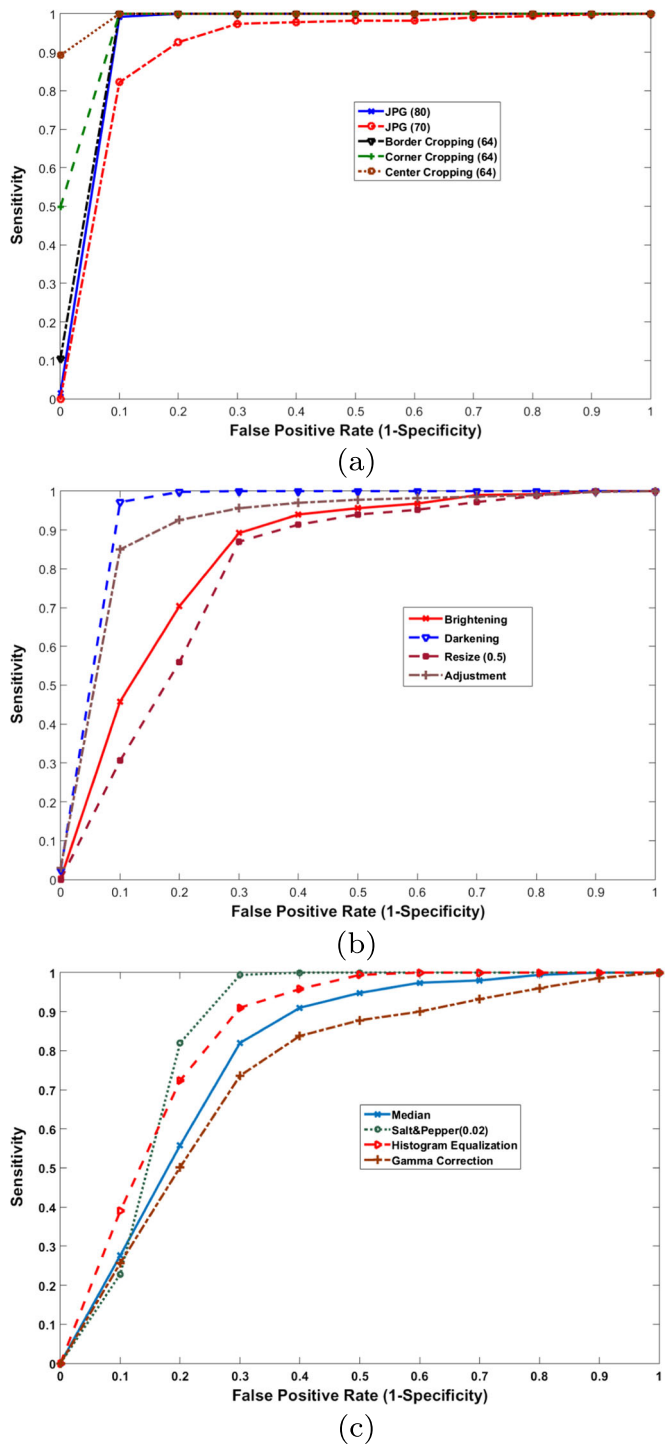


Fig. 7 ROC diagram of our method with different attacks

Table 8 The Specificity and Sensitivity of different attacks when the NCC threshold is 0.8

Measure \ Attacks	Edge Crop 512 × 64	Speckle Noise 0.04	Brightening 0.2	Darkening 0.2
Sensitivity	1	1	1	1
Specificity	0	0	0	0
Measure \ Attacks	Median Filter 3 × 3	Crop Cor- ner 64 × 64	Crop Cen- ter 64 × 64	Average Filter 3 × 3
Sensitivity	1	1	1	0.99
Specificity	0	0	0	0
Measure \ Attacks	Blurring	Gamma Correction	Salt & Pepper Noise 0.02	Gaussian Noise 0.05
Sensitivity	0.91	1	1	1
Specificity	0	0	0	0
Measure \ Attacks	Resize 0.5	Histogram Equalization	Flattening 0.1	JPEG Comp. 80
Sensitivity	1	1	1	1
Specificity	0	0	0	0
Measure \ Attacks	JPEG Comp 70	JPEG Comp 60	Sharpening 0.1	Intensity Adjustment
Sensitivity	1	1	1	1
Specificity	0	0	0	0

5 Conclusion

In this paper a new watermarking algorithm based on Hadamard transform was introduced. The watermark embedding procedure partitioned the host image into non-overlapping blocks and the watermark logo was concealed redundantly in special bit-planes of some coefficients of these blocks. The proposed watermark extractor is a blind algorithm that doesn't require information about the host image. The voting algorithm used in the extractor was a pseudo-intelligent algorithm which used the intensity values of adjacent pixels for determining the intensity of the current pixel. The proposed method proved to have high transparency in such a way that the human visual system could not detect degradation in watermarked images. Additionally this method was robust against many attacks such as JPEG compression and image cropping. Although this method was somehow fragile against a few attacks such as brightening and Gamma correction, the extracted logo was still recognizable. In our future work, the effect of hiding information in more than one bit-plane could be investigated to improve the robustness of the method.

References

1. Aung A, Ng BP, Rahardja S (2008) Sequency-ordered complex hadamard transform: Properties, computational complexity and applications. *IEEE Trans Signal Process* 56(8):3562–3571

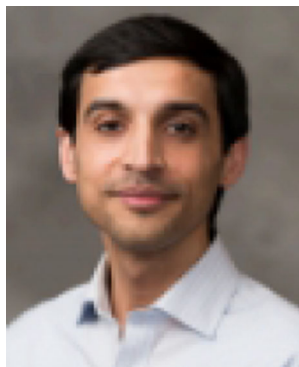
2. Aung A, Ng BP, Rahardja S (2011) A robust watermarking scheme using sequency-ordered complex hadamard transform. *Journal of Signal Processing Systems* 64(3):319–333
3. Botta M, Cavagnino D, Pomponiu V (2014) Fragile watermarking using Karhunen–Loève transform: the KLT-F approach. *Soft Comput*, 1–15
4. Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: Survey and analysis of current methods. *Signal Process* 90(3):727–752
5. Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2007) *Digital watermarking and steganography* Morgan Kaufmann
6. Fami ES, Samavi S, Kaviani HR, Radani ZM (2012) Adaptive watermarking in hadamard transform coefficients of textured image blocks, *International Symposium on Artificial Intelligence and Signal Processing (AISP)*, 503–507, IEEE
7. Fazlali H, Samavi S, Karimi N, Shirani S (2016) Adaptive blind image watermarking using edge pixel concentration, *Multimedia Tools and Applications*, 1–16
8. Feng B, Lu W, Sun W, Huang J, Shi YQ (2016) Robust image watermarking based on tucker decomposition and adaptive-lattice quantization index modulation. *Signal Process Image Commun* 41:1–14
9. Franklin RV, GRS M, Santhi V et al (2011) Entropy based robust watermarking scheme using hadamard transformation technique. *Int J Comput Appl* 12(9):14–21
10. Ghosh S, Talapatra S, Chakraborty S, Chatterjee N, Rahaman H, Maity SP (2012) Vlsi architecture for spread spectrum image watermarking in walsh-hadamard transform domain using binary watermark, *International Conference on Computer and Communication Technology (ICCT)*, 233–238, IEEE
11. Hamghalam M, Mirzakuchaki S, Akhaee MA (2014) Geometric modelling of the wavelet coefficients for image watermarking using optimum detector. *IET Image Process* 8(3):162–172
12. Ho AT, Shen J, Tan SH (2003) Robust digital image-in-image watermarking algorithm using the fast hadamard transform, *International symposium on optical science and technology*, pp. 76–85. *International Society for Optics and Photonics*
13. Hu HT, Hsu LY (2016) Collective blind image watermarking in dwt-dct domain with adaptive embedding strength governed by quality metrics, *Multimedia Tools and Applications*, 1–20
14. Hua G, Xiang Y, Bi G (2016) When compressive sensing meets data hiding. *IEEE Signal Process Lett* 23(4):473–477
15. Kountchev R, Rubin S, Milanova M, Todorov V, Kountcheva R (2010) Resistant image watermarking in the phases of the complex hadamard transform coefficients, *IEEE International Conference on Information Reuse and Integration (IRI)*, 159–164, IEEE
16. Liu S, Hennelly BM, Guo C, Sheridan JT (2015) Robustness of double random phase encoding spread-space spread-spectrum watermarking technique. *Signal Process* 109:345–361
17. Liu Y, Prabhakaran B, Guo X (2008) A robust spectral approach for blind watermarking of manifold surfaces, *Proceedings of the 10th ACM workshop on Multimedia and security*, 43–52, ACM
18. Maity SP, Kundu MK (2010) DHT domain digital watermarking with low loss in image informations. *AEU Int J Electron Commun* 64(3):243–257
19. Maity SP, Kundu MK (2011) Perceptually adaptive spread transform image watermarking scheme using hadamard transform. *Inf Sci* 181(3):450–465
20. Muhammad K, Sajjad M, Baik SW (2016) Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy. *J Med Syst* 40(5):1–16
21. Muhammad K, Sajjad M, Mehmood I, Rho S, Baik SW (2015) A novel magic lsb substitution method (m-lsb-sm) using multi-level encryption and achromatic component of an image, *Multimedia Tools and Applications*, 1–27
22. Pakdaman Z, Saryazdi S, Nezamabadi-pour H (2013) A reversible image watermarking in hadamard domain, *Information and Knowledge Technology (IKT) Conference*, 447–452, IEEE
23. Sarker MIH, Khan MI (2013) An efficient image watermarking scheme using BFS technique based on hadamard transform. *SmartCR* 3(5):298–308
24. Tsai MJ, Yin JS, Yuadi I (2014) Tree group based wavelet watermarking using energy modulation and consistency check (WW-EMCC) for digital images, *Multimedia Tools and Applications*, 1–23
25. Tsougenis E, Papakostas GA, Koulouriotis DE (2015) Image watermarking via separable moments. *Multimedia tools and applications* 74(11):3985–4012
26. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. *IEEE Trans Image Process* 13(4):600–612
27. Zhang Y, Lu ZM, Zhao DN (2010) A blind image watermarking scheme using fast hadamard transform. *Inf Technol J* 9(7):1369–1375
28. Zhang Y, Wu J, Shu H (2010) Robust watermarking using conjugate symmetric sequency-ordered complex hadamard transform and norMalization, *International Congress on Image and Signal Processing (CISP)*, 3, 1176–1180, IEEE



Elham Etemad earned her B.Sc in 2010 from Isfahan University of Technology and continued her education in the same university and obtained her MSc in 2012. She started her PhD education at Dalhousie University in 2014. Her main research interests are Computer Vision, Object Recognition, Deep Learning and Augmented Reality.



Shadrokh Samavi received the B.S. degree in industrial technology and another B.S. degree in electrical engineering from California State University, the M.S. degree in computer engineering from the University of Memphis, and the Ph.D. degree in electrical engineering from Mississippi State University, USA. He is a Professor of computer engineering, Isfahan University of Technology, Iran, and an Adjunct Professor with the ECE Department, McMaster University, Canada. His research interests include image processing and hardware implementation, optimization of image processing algorithms, and watermarking of images and related subjects. Prof. Samavi is a member of the IEEE and the Eta Kappa Nu and Tau Beta Pi societies. He is a Registered Professional Engineer (PE), USA.



S. M. Reza Soroushmehr is a postdoctoral fellow at University of Michigan, Ann Arbor, MI, USA. Prior to this position he was a postdoctoral fellow at Electrical and Computer Engineering (ECE) department of McMaster University, Hamilton, ON, Canada. He received his B.Sc, M.Sc. and Ph.D. (with honor) respectively in 2000, 2004 and 2013 from the ECE department of Isfahan University of Technology (IUT), Isfahan, Iran. His main research interests include image processing, video compression, algorithm design and optimization.



Nader Karimi received the B.S. degree (summa cum laude) in computer engineering from Azad University, Arak Branch, Iran, in 2002 and the M.Sc. and Ph.D. degrees (honor) in computer engineering and electrical engineering from Isfahan University of Technology (IUT), Iran, in 2004 and 2012, respectively. He is currently an Assistant Professor at the Department of Electrical and Computer Engineering, Isfahan University of Technology. His research interests are image compression, hardware implementation and optimization of image processing algorithms, and watermarking.



Mohammad Etemad received his BSc and MSc in Computer Engineering from Azad University of Arak respectively in 2007 and 2012. Currently he is an executive manager at Hooshmand Rayaneh Gostar Inc, Iran. His research interests are data mining, machine learning and big-data analysis.



Shahram Shirani (SM'04) received the B.Sc. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 1989, the M.Sc. degree in biomedical engineering from the Amirkabir University of Technology, Tehran, in 1994, and the Ph.D. degree in electrical and computer engineering from the University of British Columbia (UBC), Vancouver, BC, Canada, in 2000. Since July 2000, he has been with the department of Electrical and Computer Engineering, McMaster University, Hamilton, ON, Canada, where he is currently a full Professor. His research interests include image and video compression, multimedia communications, and ultrasonic imaging. Dr. Shirani is a registered Professional Engineer (P.Eng.).



Kayvan Najarian (SM'07) received the B.Sc. degree in electrical engineering from Sharif University, Tehran, Iran, the M.Sc. degree in biomedical engineering from Amirkabir University, Tehran, and the Ph.D. degree in electrical and computer engineering from the University of British Columbia, Vancouver, Canada. He is an Associate Professor in the Departments of Computational Medicine and Bioinformatics, and Emergency Medicine at the University of Michigan, Ann Arbor, MI, USA. He also serves as the Director of the Michigan Center for Integrative Research in Critical Care's Biosignal- Image and Computational Core program. His research interests include design of signal/image processing and machine learning methods to create computer assisted clinical decision support systems that improve patient care. Dr. Najarian serves as the Editor-in-Chief of a journal in the field of biomedical engineering as well as the Associate Editor of two journals in the field of biomedical informatics. He is also a Member of many editorial boards and has served as a Guest Editor of special issues for several journals.