Adaptive visible image watermarking based on Hadamard transform

Margarita Favorskaya*, Eugenia Savchina and Aleksei Popov
Reshetnev Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochy ave., Krasnoyarsk, 660037 Russian Federation
*E-mail: favorskaya@sibsau.ru

Abstract. One of the ways for implicit protection of rightful copyright information deals with application of visible watermark embedded in the host image. In this paper, we study behaviour of the proposed function, which makes the embedding of visible watermark smoother compared to the well-known sigmoid function, linear function, and Zernike moments. The Hadamard transform allows us to reduce the computational resources for watermarking processes. The proposed technique is especially useful in fragile watermarking as the additional level for protection.

1. Introduction
The open nature of Internet allows unscrupulous intruders to manipulate the transmitted data illegally or even steal them. Rapid distribution of multimedia resources enforces such illegal attempts. This causes a development of protection and authentication techniques regarding the data content. Numerous watermarking techniques are used to protect the ownership right, authentication, and integrity verification. This paper aims at developing image watermarking with tuning a watermark visibility from visible to invisible forms in a host image.

Algorithms of digital image watermarking are implemented in spatial domain [1] or frequency domain using different transforms such as Discrete Fourier Transform (DFT) [2], Discrete Cosine Transform (DCT) [3], Discrete Wavelet Transform (DWT) [4], Fourier-Mellin transform [5], etc. The Discrete Hadamard Transform (DHT) shows low standard deviation of noise at low quality compression [6]. This means that the DHT possesses higher embedding capacity relative to the DCT and DWT. Additionally the DHT has lower computational cost. These possibilities make the DHT attractive for usage in a watermarking.

Visible image watermarking is a technique that inserts copyright information into the host image noticeably in order to identify the ownership and prevent an unauthorized use. In conventional visible watermarking schemes, a visible watermark is usually irremovable [7], while in some applications, a visible watermark is required to be removable [8]. In general, a visible watermark should be visible but not significantly obscure the image details beneath it. These requirements contradict each other. If a visibility of a watermark is increased, then degradation of image quality becomes more significant, and vice versa. This motivates to consider the image content for embedding carefully [9].

The organization of the paper is as follows. Section 2 contains a review of some related watermarking methods. Mathematical model including the proposed function for adaptive control of a watermark visibility is given in section 3. Experimental results are discussed in section 4, while section 5 concludes the paper.
2. Related work
For visible watermarking, it is important to determine so called scaling factor (or scaling strength), from which a degree of a watermark visibility depends. Santhi and Arulmozhivarman published in 2013 a series of articles, where they used the sigmoid function [10], centralized and Zernike moments [11], Speeded Up Robust Features (SURF) technique [12], and luminance component [13] in embedding/extraction algorithms using DHT and DWT. All approaches in these three articles are similar and were directed on a watermark insertion into modified low frequency components of the corresponding transform of a host image. The close technique based on the Slant transform was developed in [14]. The Slant transform has been used extensively in image compression applications including a watermarking.

The sequency-ordered complex Hadamard transform (SCHT) was applied for robust phase watermarking scheme [15]. These authors claimed that their method is robust for geometric attacks and common image processing. The SCHT, which was based on the phase shift keying modulation, provided simpler implementation and lesser computational complexity respect the DFT.

A robust image-in-image watermarking algorithm based on the Fast Hadamard Transform (FHT) for the copyright protection of digital images was developed in [16]. A watermark was decomposed into Hadamard coefficients of a host image. The watermark scale factor was computed based on a visual model that included the edges and textures of a host image. All the AC Hadamard coefficients of watermark was scaled by the watermarking scale factor and then inserted into several middle and high frequency AC components of the Hadamard coefficients of a host image.

Note that some watermarking approaches are based on saliency paradigms. Thus, the integrated visual saliency-based watermarking method with a goal to synchronize the image authentication and copyright protection was proposed in [17]. First, all Regions of Interest (ROIs) with different sizes as the salient regions were extracted automatically using a visual attention model. Second, the copyright information was embedded into ROIs as the robust watermark. Third, the fragile watermark was additionally embedded into the edge map of the most salient ROI. Hence, this method is robust to attacks and also fragile to tampering. Such interpretation permitted to solve the image protection and authentication tasks simultaneously.

3. Proposed mathematical model
The 2D-Hadamard transform has been extensively used in image processing and compression. A distinctive feature of the DHT is in that the watermark information can be embedded into the low frequency AC components, increasing watermark reliability. Moreover, DHT has many useful middle and high frequency bands available for hiding a watermark at high noise environment. In this case, the watermark energy embedded into the equivalent low frequency components of DCT and DWT domain allows the DHT to survive to the compression. Finally, the DHT has a shorter processing time and simpler in hardware implementation respect to many commonly used orthogonal transforms.

A brief review of the Hadamard transform is considered in Section 3.1. The proposed control of scale factor is given in Section 3.2. Section 3.3 provides the embedding/extraction scheme of a watermark.

3.1. 2D-Hadamard transform
The Hadamard transform is an orthogonal transformation that decomposes a signal into a set of Walsh functions. The rows or columns of $N \times N$ Hadamard matrix $H_n$ are orthogonal, $N = 2^n$, $n = 1, 2, 3…$, with element values either $+1$ or $-1$.

Let $[HI]$ be the host image and $[HI']$ be the transformed image with sizes $K \times L$. Then, the 2D-Hadamard transform has a view:

$$[HI] = \frac{H_n[H'I']H_n}{N}$$

with the following property:
\[ H_n = H_n^* = H^T = H^{-1}. \]  

Since \( H_n \) has \( N \) orthogonal rows, \( H_n^*H_n = NI \), where \( I \) is the identity matrix, and \( H_n^*H_n^{-1} = I \), the inverse 2D DHT is defined by equation 3.

\[
[H'] = H_n^* [H] H_n = \frac{H_n^*[H] H_n}{N}.
\]

Usually the direct and reverse DHT is applied to the sub-blocks 8×8 elements of host and watermarked images, respectively. For \( N=2 \), the Hadamard matrix \( H_1 \) called as a core matrix is defined by equation 4.

\[
H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}
\]

The Hadamard matrix of the order \( n \) is generated through the Hadamard matrix of order \( n-1 \) using Kronecker product (symbol \( \otimes \)):

\[
H = H_{n-1} \otimes H_1 = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}.
\]

As it follows from equation 5, the third order Hadamard transform matrix \( H_3 \) is used for the 8×8 sub-blocks of an image.

Thus, according to the Hadamard matrix properties, we can embed a watermark into low frequency components that increases its reliability.

3.2. Watermark scale factor control

In literature, one can find different functions for adaptive control of a watermark visibility. The control parameter can be adjusted to provide either visible or invisible watermark. Among such functions, we can mention the sigmoid function, linear function, and Zernike moments. We suggest smoother function respect to sigmoid function, which tends to finite values for \( x \to \infty \) and \( x \to -\infty \). This function has a view of Equation 6.

\[
f(x) = \frac{1}{\pi} \left( \arctg x + \frac{\pi}{2} \right)
\]

The proposed function has real values, differentiable and, hence, continuous function. If \( x \to -\infty \), then \( f(x) = 0 \). If \( x \to \infty \), then \( f(x) = 1 \). If \( x = 0 \), then \( f(x) = 0.5 \). The scaling factor \( \alpha \) is obtained based on equation 6 and mean value of \( H'H' \):

\[
\alpha = \frac{1}{\pi} \left( \arctg(\mu(H'H')) + \frac{\pi}{2} \right) \frac{1}{10^m},
\]

where \( m \) is the controlling parameter, which defines a strength of watermark visibility, and mean value \( \mu(H'H') \) is defined as:

\[
\mu(H'H') = \frac{1}{K \cdot L} \sum_{k=1}^{K} \sum_{l=1}^{L} H'(k,l).
\]
is good without destroying the host image (visible watermarking scheme). If \( m = 2 \), then a watermark becomes invisible without degrading the quality of a host image (invisible watermarking scheme).

3.3. Embedding/extraction scheme

The embedding and extraction schemes are ordinary. First, the host image is converted from RGB color space into YUV color space. Second, the luminance component \( Y \) is transformed into frequency components using Hadamard transform. A watermark is also converted into frequency components using DHT. Third, a watermark is inserted by modulating the frequency components of the host image and watermark image using Equation 9, where \( Y' \) is the Hadamard transform of luminance component of a host image, \( Y'' \) is the DHT of luminance component of a watermarked image.

\[
Y'' = Y' + \alpha W . \tag{9}
\]

The embedding algorithm includes the following steps.

Input data: a host image and a watermark image.

Step 1. Convert a host image \( HI \) from RGB to YUV.

Step 2. Apply the Hadamard transform for luminance component \( Y \).

Step 3. Apply the Hadamard transform for watermark image.

Step 4. Calculate the scaling factor using Equations 7 and 8.

Step 5. Insert a watermark.

Step 6. Apply inverse Hadamard transform for recalculated \( Y' \).

Step 7. Convert YUV components into RGB components.

Output data: a watermarked image.

The extraction algorithm uses formulae 10, where \( W'_T \) is the extracted watermark, \( Y'_T \) is the Hadamard transform of luminance component of transmitted watermarked image.

\[
W'_T = \frac{Y'' - Y'}{\alpha} . \tag{10}
\]

The extraction algorithm involves the following steps.

Input data: a transmitted watermarked image.

Step 1. Convert a host image \( HI \) from RGB to YUV.

Step 2. Convert a transmitted watermarked image \( HI' \) from RGB to YUV.

Step 3. Apply the Hadamard transform for luminance components \( Y'_T \) and \( Y' \).

Step 4. Calculate the scaling factor using Equations 7 and 8.

Step 5. Extract a watermark.

Step 6. Apply inverse Hadamard transform for a watermark.

Output data: extracted watermark.

4. Experimental results

We study a behavior of the proposed function (equation 6), based on which a scale factor control is calculated. A view of this function is depicted in figure 1 as a dashed green curve. Also in figure 1, the sigmoid function (red curve) and linear function (black line) are placed. The disadvantage of a linear function is evident. Even for small values of argument \( x \), linear function oversteps from the defined boundaries \( f(x) \in [0…1] \). We can recommend to use it on the restricted interval, \( x \in [-2…2] \). Due to a symmetrical property of non-linear functions, let us consider a positive quarter of the graphs (figure 1b). The proposed function (Equation 6) is smoother and has more uniform lifting compared with a sigmoid function, which approximates sharply to its maximum already at \( x = 6 \).
Figure 1. Different scaling functions: a) general form of functions, b) positive quarter of the graphs.

A binary logotype with sizes 128×128 elements (figure 2a) was embedded into different color images. For this purpose, various values of scale factor were tested. Some examples are depicted in figure 2 with $m = 1$ and $m = 2$ (figures 2c and 2d, respectively).

Figure 2. Embedding binary logotype in images Baboon and House: a) watermark, b) original images, c) visible watermarking, $m = 1$, d) invisible watermarking, $m = 2$

The images with embedded watermark (figure 2d) have not visual difference with the corresponding original images (figure 2b). There were applied the following values of scale factors: for visible watermarking $\alpha = 0.0582$ for Baboon and $\alpha = 0.0831$ for House and for invisible watermarking $\alpha = 0.0058$ for Baboon and $\alpha = 0.0083$ for House.

5. Conclusions
Fragile watermarking is useful for evaluation of distortion degree of watermarked images after their transmission through unprotected communication channels. We provide more suitable tuning of the scale factor, which defines a visibility degree of fragile watermark in the host image. Experiments
show that we can embed the watermarks with a desirable degree of visibility with low computational cost.

References
[1] Chitra K and Prasanna Venkatesan V 2016 Spatial domain watermarking technique: An introspective study Proc. Int. Conf. Informatics and Analytics (ICIA-2016) 50
[2] Ganic E, Dexter SD and Eskicioglu AM 2005 Embedding multiple watermarks in the DFT domain using low- and high-frequency bands Proc. SPIE: Security, Steganography, and Watermarking of Multimedia Contents 5681 175-84
[3] Sahail MA and Obaidat MS 2003 Digital watermarking-based DCT and JPEG model IEEE Trans. Instrum. Meas. 52(5) 1640-7
[4] Makbol NM and Khoo BE 2012 Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition Int. J. Electron. Commun. (AEU) 67 102-12
[5] Zhao J 2015 Robust image watermarking algorithm based on Radon and analytic Fourier-Mellin transforms The Open Automation and Control Systems J. 7 1071-4
[6] Ramkumar M and Akansu AN 2001 Capacity estimates for data hiding in compressed images IEEE Trans. Image Proc. 10 1252-63
[7] Huang BB and Tang SX 2006 A contrast-sensitive visible watermarking scheme IEEE Multimedia 13(2) 60-7
[8] Yang Y, Sun X, Yang H and Li CT 2008 Removable visible image watermarking algorithm in the discrete cosine transform domain J. Electron. Imaging 17(3) 033008-1–033008-11
[9] Maiti S, Agarwal C, Bose A and Sarkar SK 2013 Robust data hiding technique in wavelet domain using saliency map Int. J. Advances in Engineering and Technology 6(4) 1674–86
[10] Santhi V and Arulmozhivarman P 2013 Hadamard transform based adaptive visible/invisible watermarking scheme for digital images J. Information Security and Applications 18(4) 167–79
[11] Santhi V and Arulmozhivarman P 2013 Visible watermarking for digital images in wavelet domain using centralized and Zernike moments Int. J. Applied Engineering Research 8(19) 2559–63
[12] Santhi V and Arulmozhivarman P 2013 Adaptive visible watermarking for digital images using SURF technique in wavelet domain Int. J. Tomography and Simulation 24(3) 70–85
[13] Santhi V, Thangavelu A and Arulmozhivarman P 2013 Adaptive visible watermarking in Hadamard domain for digital images Int. J. Information and Computer Security 5(3) 202–23
[14] Shanthakumari R and Malliga S 2017 Digital image-in-image watermarking for copyright protection of images using the Slant transform WSEAS Trans. Computers 16 326–34
[15] Aung A, Ng BP and Rahardja S 2011 A robust watermarking scheme using sequency-ordered complex Hadamard transform J. Signal Process. Systems 64(3) 319–33
[16] Ho ATS, Shen J and Tan SH 2003 A robust digital image-in-image watermarking algorithm using the fast Hadamard transform Mathematics of Data/Image Coding, Compression, and Encryption V, with Applications ed MS Schmalz Proc. SPIE vol 4793 pp 76–85
[17] Tian L, Zheng N, Xue J, Li C and Wang X 2011 An integrated visual saliency-based watermarking approach for synchronous image authentication and copyright protection Signal Process.: Image Commun. 26(8) 427–37