IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. I (May-Jun. 2016), PP 58-64
www.iosrjournals.org

An Improved Non-Blind Digital Image Watermarking on Hadamard Transform for Image Authentication

Sanjida Sharmin[1], Rahima Afrose[2,] Lutfur Nahar[3], Nargis Akter[4]
[1]*Chittagong University of Engineering and Technology, Bangladesh*
[2]*International Islamic University Chittagong, Bangladesh*
[3] *Chittagong University, Bangladesh*
[4]*International Islamic University Chittagong, Bangladesh*

Abstract : *With the advent of internet digital media has been improving with massive advancement in recent years. The distribution of unauthorized copies of media content has also been increasing day by day. Because of easy access to digital content, online purchasing and distribution becomes easier. Thus there is an urgent need to provide protection for digital content. One solution gaining popularity in protecting digital content is digital watermarking. In proposed scheme, a breadth-first search technique is used to find the efficient embedding point to embed the watermark. The proposed algorithm results show that the experiment offers better image quality and robustness under various attacks and alteration, such a, cropping, JPEG compression sharpening and filtering among others. The results have manifested the higher robustness and imperceptibility of this scheme when compared with other available watermarking techniques.*
Keywords - *Digital watermarking, Hadamard Transform, Breadth-first search technique*

I. INTRODUCTION

Digital watermarking is the technique of hiding a message related to a digital signal (i.e. an image, song and video) within the signal itself, which may be used to verify its authenticity or the identity of its owners. . The concept of watermarking closely related to steganography, in that those both hide a message inside a digital signal .Watermarking can be classified in different ways. In terms of the need of original image in watermark extraction process, watermarking techniques are classified as either blind or non-blind. The original image is needed when detecting the watermark in a non-blind technique whereas a blind watermarking technique does no need the original image for extraction or detection. Our proposed method follows the non-blind watermarking technique. According to application, watermarks are sub-divided into semi-fragile, fragile, and robust. Fragile watermarks are very sensitive. They can be destroyed easily with slight alteration in the watermarked signal. Semi-fragile watermarking are also broken if the modifications to the watermarked signal exceed a user pre-defined threshold. If the value of threshold is set to zero then it operates as a fragile watermark. On the other hand, a robust watermark withstands against various malicious attacks, such as scaling, rotation, filtering and compression. Our method manifests the robustness of watermarking.

Previous researchers like Ho et al. proposed a frequency domain watermarking system for digital image using the Fast Hadamard Transform [1]. Saryazdi and Nezamabadi-pour developed a new blind gray-level watermarking scheme in which the host image is first divided into 4×4 non-overlapping blocks [2]. For each block, two first AC coefficients of its Hadamard transform are then estimated using DC coefficients of its neighbor blocks. Deb et al. proposed a combined DWT and DCT-based watermarking technique with low frequency watermarking with weighted correction [3]. Al-Haj described an imperceptible and robust combined DWT-DCT digital image watermarking algorithm for copyright protection [4]. Husain presented a survey of various digital watermarking techniques for multimedia data such as text, audio, image and video for copyright protection [5].Rui-mei et al. proposed a blind watermarking algorithm based on DCT for digital image in which a two-bit image is embedded in an eight-bit gray image [6]. Kountchev et al. proposed a new method where a still digital image is transformed using the complex Hadamard transform [7]. Lee et al. proposed a survey of watermarking systems that are applied to multimedia [8]. Sathik and Sujatha described a watermark construction process where a scrambled version of the watermark is obtained with the help of the Arnold transform [9].

In this paper, we propose a robust digital image watermarking method based on Hadamard Transform. The mean reason to use this method is its simplicity, also it offers significant advantages (less processing time and better hardware implementation) compared to most orthogonal transform techniques, such as DWT and DCT.

The rest of the paper is organized as follows. In Section II, we have introduced the Hadamard transform. Section III describes the selection of positive Hadamard Coefficient and labeling Section IV describes our proposed method of watermarking system including the watermark embedding process and the watermark extraction process. Section V represents our experimental results and analysis finally, Section VI concludes this paper.

II. HADAMARD TRANSFORM

The Hadamard transformation is also known as the Walsh–Hadamard transformation, Hadamard–Rademacher–Walsh transformation, Walsh transformation, or Walsh–Fourier transformation. It is an example of a generalized class of Fourier transforms .The 2D-Hadamard transform has been used extensively in image processing and image compression [1]

Let [*U*] represents the original image and [*V*] the transformed image, the 2D-Hadamard transform is given by:

$$[V] = \frac{H_m[U]H_m}{M} \tag{1}$$

Where H_m represents an $N \times N$ Hadamard matrix, $N=2n$, $n=1,2,3\ldots\ldots$ with element values either +1 or –1.

The advantages of Hadamard transform are that the elements of the transform matrix H_m are simple: they are binary, real numbers and the rows or columns of H_m are orthogonal. The inverse 2D-Hadamard transform (IHT) is given as:

$$[U] = H^{-1}{}_m[V]H^{*}{}_m = \frac{H_m[V]H_m}{M} \tag{2}$$

In our algorithm, the transform process is carried out based on the 8×8 sub-blocks of the whole image. the third order Hadamard transform matrix H_m is used.

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} \quad (3)$$

III. SELECTION OF POSITIVE HADAMARD COEFFICIENT AND LABELING

Breadth First search is an extremely very useful searching technique. It differs from the depth-first search in that it uses a queue to perform the search, so the order in which the nodes are visited is quite different. It has the extremely useful property that if all of the edges in a graph are unweighted or the same weight then the first time a node is visited is the shortest path to that node from the source node. It is a way to find all the vertices reachable from the given source vertex. Like depth first search, Breadth First search traverse a connected component of a given graph and defines a spanning tree.

In our implementation use an order for BFS searching. The order is given following. Here, C is centre point or main point. 1, 2, 3, 4, 5, 6, 7, 8 is order of the BFS algorithm searching. Fig 1. Shows the order of searching the node.

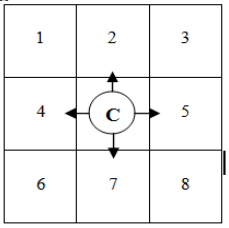

Figure 1. Order of searching

Now we apply BFS algorithm on the Hadamard co-efficient and finding positive connecting component. Then generate spanning tree from the Hadamard co-efficient. After applying breadth first search algorithm we get spanning tree of the co-efficient and also label of the spanning tree. Here, we using labeling technique we can count the number of trees. It will also help to find watermark embed point.

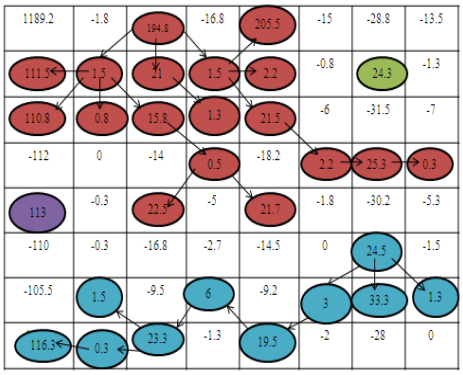

Figure 2. Labeling the Hadamard co-efficient.

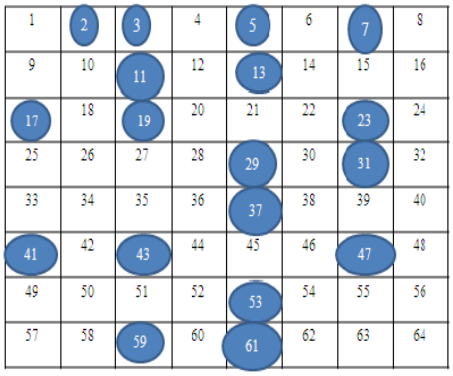

Figure 3. Mark the prime number for not embedding

By using BFS algorithm we get a matrix which represents the position of the Hadamard co-efficient, which is called visit matrix. The visit matrix is mainly use for watermark extraction process. Fig 2. Shows the labeling of the positive Hadamard Co-efficient. After that we will select the non prime block for embedding. Here block having Prime numbers are those Like as 2, 3, 5, 7, 11, 13 ……so on and non-prime numbers are 4, 6, 8, 9, 10, 12, 14, 15…… so on. Fig 3. Shows the prime number in each block. Prime number block are avoided here because after transformation if most of the value of prime block became totally zero then it is impossible for us to embed. It is not possible to select all point for watermarking. Because select all point of Hadamard Co-efficient may occur huge distortions of the watermarked image. That why we select the non prime block. In our embedded process we select only on 1st column. Because the rate of distortion of the watermarked image is very high in row wise because of matrix manipulation. Now in 1st column we will embed in two points 111.5 and 110.8 shown in figure fig 4.

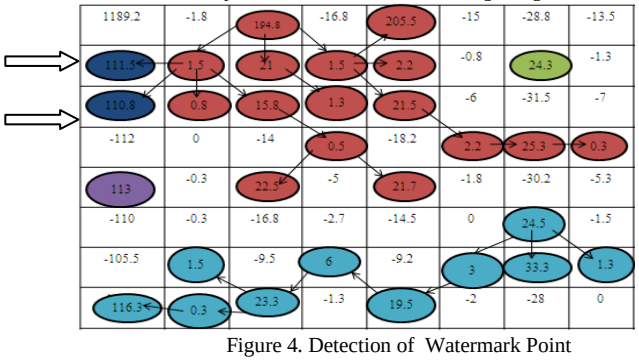

Figure 4. Detection of Watermark Point

IV. PROPOSED METHOD

In this section we will discuss about our proposed method of watermarking. This method consists of two processes; the watermark embedding process and the watermark extraction process.

4.1 Watermark embed process

For the embedding process we have the following steps. Fig 5.re presents the flow diagrams of the proposed embedding method.

Step 1: The host image is taken as input and divided into 8×8 non-overlapping blocks.

Step 2: Now Hadamard Transformation is applied on each block. Then we get Hadamard transform co-efficient for the block. Now we work on the Hadamard Transform co-efficient. Each block has a DC value which is avoid for any embedding. In an 8*8 block here has 64 co-efficient so one co-efficient is avoided and remaining 63 co-efficient is use for embed. The remaining 63 co-efficient are called AC value of the block.

Step 3: We apply BFS algorithm on the Hadamard co-efficient and finding positive connecting component. Then generate spanning tree from the Hadamard co-efficient.

Step 4: Next we use prime numbering system for selection of the block which is disused before. on prime block are selected for embedding.

Step 5: After selecting the Non-prime block we check the labeling component. Then select which labeling that positions on the 1st column and that .points is selected to embed watermarking. In this way we mark the watermark point. In our embedded process we select only on 1st column. Because the rate of the distortion of the watermarked image is very small.

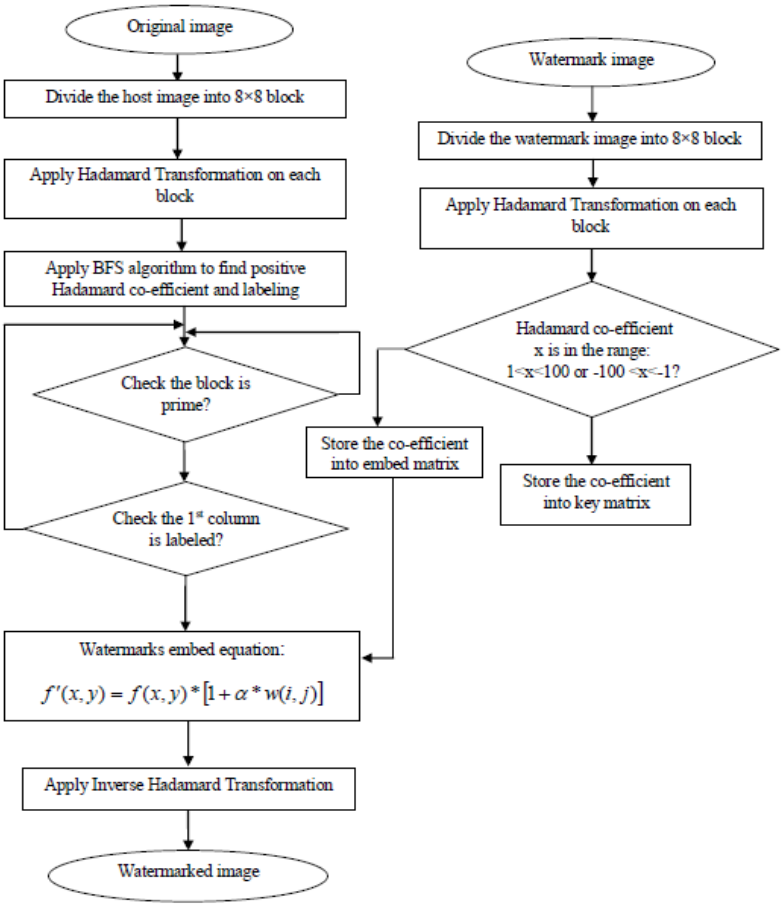

Figure 5. Flow Diagram of Watermark Embed Process

Step 6: Now take input the watermark image. Our watermark image size is 64× 64. Watermark image divide into 8×8 blocks and apply Hadamard Transformation on each block. From the coefficients of the watermark image after applying Hadamard transform, points within the range-: $0 < x < 1$ or $-1 < x < 0$ are selected and then stored in a visited matrix. The rest of the components are stored in a key matrix, which is used in the decoding process.

Step 7: We use Cox's equation for embed watermark Hadamard co-efficient into host Hadamard co-efficient.

$$f'(x,y) = f(x,y) * [1 + \alpha * w(i,j)] \quad (4)$$

where, $f'(x,y)$ = Watermarked Hadamard co-efficient, $f(x,y)$ = host Hadamard co-efficient, α = scaling factor and $w(i,j)$ = Watermark Hadamard co-efficient.

Step 8: After completing the embed process we again apply inverse Hadamard Transformation to produce watermarked image

4.2 Watermark Extraction process:

To extract the watermark image from watermarked image, the following steps are required. Fig 6. Presents the flow diagrams of the proposed extraction method.

Step 1: The watermarked image and host image divided in same manner of host image into 8×8 sub-blocks

Step 2: Hadamard transform is applied on each block of the both image.

Step 3: The visited matrix is used for watermark extraction. Here we use the inverse embed equation (4) for extract watermark image.

$$w'(x,y) = \frac{\left[\frac{f'(x,y)}{f(x,y)} - 1\right]}{\alpha} \quad (5)$$

Where, $w'(x,y)$ = watermark extract co-efficient, $f'(x,y)$ = Watermarked Hadamard co-efficient, $f(x,y)$ = Host Hadamard co-efficient

Step 4: Again we apply inverse Hadamard Transformation on extract Hadamard co-efficient. Then we get the extracted watermark image

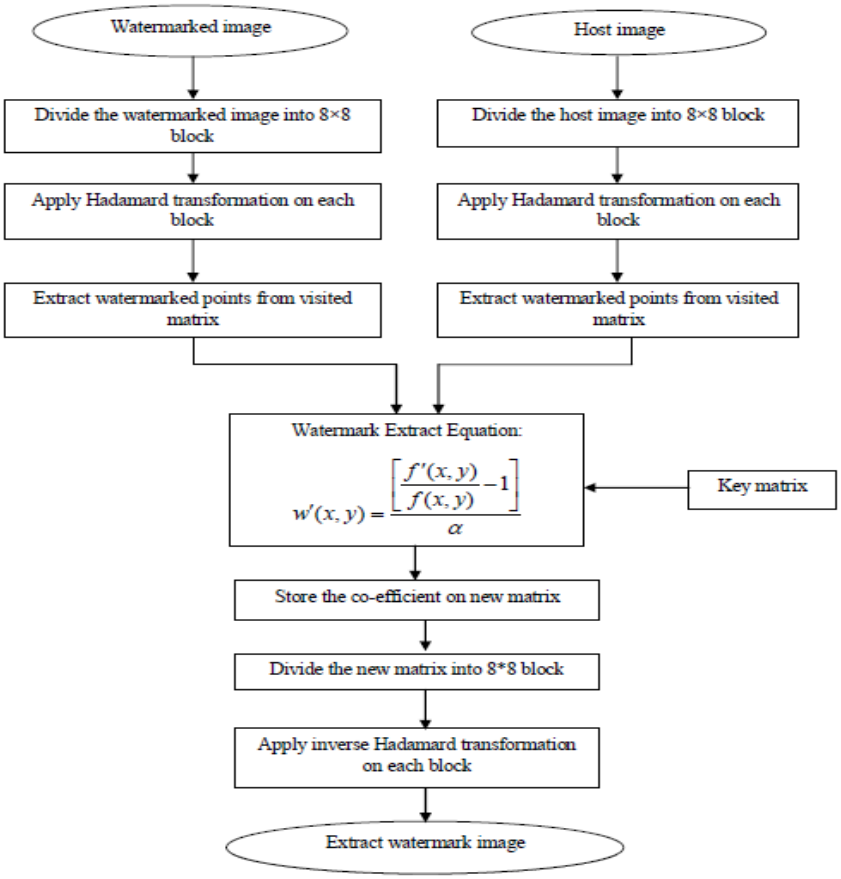

Figure 6. Flow Diagram of Watermark Extraction Process

V. EXPERIMENTAL RESULT AND ANALYSIS

To evaluate the quality of the watermarked image in comparison with host image we have used the peak signal to noise ratio (PSNR) .The Formula of PSNR is given below:

$$PSNR = 10\log_{10}\frac{255\times 255}{MSE} \quad (6)$$

Where $MSE = \frac{1}{M\times N}\sum_{N-1}^{M-1}\left[I(i,j) - K(i,j)\right]^2$

MSE (mean square error) will be computed first. The M and N are the height and width of the image, respectively. $I(i,j)$ And $K(i,j)$ are the values located at coordinates (i, j) of the host image and the watermarked image.

. The normalized correlation coefficient (NCC*)* is computed after extracting the watermark image. The original watermark and the extracted watermark is used to judge the existence of the watermark and to measure the correctness of an extracted watermark. It is defined as:

$$NCC = \frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j)\times w'(i,j) \quad (7)$$

Where, m and n are the height and width of the watermark, respectively. $w(i,j)$ And $w'(i,j)$ are the watermark bits located at coordinates (*i, j*) of the original watermark and extracted watermark.

We have taken two images figure 7. Lenna.. Figure 8. Pepper to test the experiment of watermarking.

(a) (b) (c)

Figure 7.Experiment of (Lenna) (a)Original image (b)Watermark image (c) Watermarked image

(a) (b) (c)

Figure 8.Experiment of (Pepper) (a) Original image (b) Watermark image (c) Watermarked image

Table 1.PSNR and NCC for no Alteration of Image

Name of Image	**PSNR**	**NCC**
Lenna	38.78	1
Pepper	40.59	1

(a) (b) (c)

(d) (e) (f)

Figure 9.Different attack applied on watermarked image (a) Original image (b) JPEG compression (c) Salt &Pepper (d) Cropping (e) Gaussian noise (f) Changing aspect ratio

Table 2. PSNR and NCC are after applying JPEG compression on both images

Attack	PSNR(Lenna)	NCC	PSNR(Pepper)	NCC
JPEG compression (QF=10)	32.7029	0.9742	30.0946	0.8956
JPEG compression (QF=30)	34.3765	0 .9809	34.6744	0.9034
JPEG compression (QF=50)	36.4525	0.9850	37.846	0.9345
JPEG compression (QF=70)	37.4557.	0.9926	38.545	0.9678
JPEG compression (QF=90)	38.125	0.9958	38.678	0.9889

Table 3. PSNR and NCC are after applying Different Noise attack

Attack	PSNR(Lenna)	NCC	PSNR(Pepper)	NCC
Gaussian Noise (Average=0,density=.002)	26.8266	0.9873	27.0004	0.9851
Speckle Noise (density=.01)	26.5200	0.9887	26.7301	0.9920
Salt & pepper noise (Strength=.01)	24.7564	0.9856	24.6497	0.9838

Table 4. PSNR and NCC are after applying Cropping attack

Attack	PSNR(Lenna)	NCC	PSNR(Pepper)	NCC
Cropping[32×32]	30.1313	0.9982	28.4461	0.9994
Cropping[64×64]	25.4391	0.9894	20.9221	0.9877
Cropping[128×128]	16.3047	0 .9595	14.6024	0.9611

Table 5. PSNR and NCC are after applying Different filtering attack

Attack	PSNR(Lenna)	NCC	PSNR(Pepper)	NCC
Linear filtering	32.456	0.9456	31.234	0.9876
Median filtering 3×3	34.4961	0.9873	24.9691	0.9883
Weiner filtering	36.2677	0.9711	31.4831	0.9854

Table 6. PSNR and NCC are after applying rotation attack

Attack	PSNR(Lenna)	NCC	PSNR(Pepper)	NCC
Rotation 5^0	30.1313	0.9983	28.4461	0.9984
Rotation 10^0	25.4691	0.9892	20.9262	0.9875

Table 7.Comparision of NCC with **Anthony's method** [1] with Proposed Method

Different Attack	Anthony's method[1]	Proposed method
Sharpening 3×3	0.9573	0.9933
1 row 1 column removed	0.9866	0.9883
Frequency mode Laplacian removal	0.9580	0.9754
Scaling.75	0.9354	0.9554
JPEG compression of factor 30	0.8688	0.9042
Changing aspect ratio	0.8199	0.8558

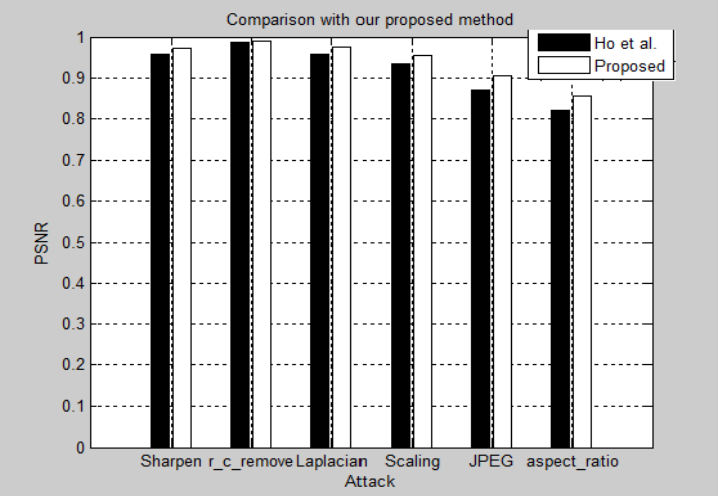

Figure 10. Bar chart of Comparison of NCC with Ho et al. Method with Proposed Method

VI. Conclusion

An In this paper, we proposed an improved digital image watermarking scheme based on the Hadamard transform which provides a complete method that embeds and extracts the watermark information very effectively. Our watermark embedding process persist the visual quality of the image. The performance of the watermarking scheme is evaluated with common image processing attacks and alteration.

Moreover this authentication process provides qualities such as robustness, imperceptibility and security. The experimental results show that our proposed method is efficient and manifest more robustness against those disruptive alterations.

REFERENCES

[1] Anthony T.S. Ho, J. Shen, Andrew K.K. Chow, J. Woon, Robust Digital Image-in-Image Watermarking Algorithm Using the Fast Hadamard Transform, *Proc. of IEEE International Symposium on Circuit and system* (*ISCAS '03*), vol. 3, pp. 826-829, 2003.

[2] S. Saryazdi, H. Nezamabadi-pour, A Blind Digital Watermark in Hadamard Domain, *Proc. of World Academy of Science, Engineering and Technology*, vol. 3, 2005.

[3] K. Deb, M.S. Al-Seraj, M.M. Hoque, M.I.H. Sarker, Combined DWT DCT Based Digital Image Watermarking Technique for Copyright Protection, *Proc. of IEEE International Conference on Electrical & Computer Engineering* (*ICECE*), 2012.

[4] A. Al-Haj, Combined DWT-DCT Digital Image Watermarking,*Journal of Computer Science*, vol. 3, no. 9, pp. 740-746, 2007.

[5] F. Husain ,A Survey of Digital Watermarking Techniques for Multimedia Data,*MIT International Journal of Electronics and Communication Engineering*, vol. 2, no. 1, pp. 37-43, 2012.

[6] R. Zhao, L. Hua, H. Pang, B. Hu, A Watermarking Algorithm by Modifying AC Coefficies in DCT Domain, *Proc. of IEEE International Symposium on Information Science and Engineering* (*ISISE*), 2008. Article (CrossRef Link)

[7] R. Kountchev, S. Rubin, M. Milanova, V. Todorov, Resistant Image Watermarking in the Phases of the Complex Hadamard Transform Coefficients,in *Proc. of IEEE International Conferecne on Information Reuse and Integration* (*IRI*), pp. 159-164, 2010.

[8] S.J. Lee, S.H. Jung, A Survey of Watermarking Techniques Applied to Multimedia, Proc. of *IEEE International Symposium on Industrial Electronics*, vol. 1, pp. 272-277, 2001.

[9] M. Sathik, S.S. Sujatha, An Improved Invisible Watermarking Technique for Image Authentication, *International Journal of Advanced Science and Technology* (*IJAST*), vol. 24, 2010.

[10] Liu Ping Feng, Liang Bin Zheng, Peng Cao, A DWT-DCT Based Blind Watermarking Algorithm for Copyright Protection, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 2010.

[11] Qingtang Su, Yugang Niu, Hailin Zou, Xianxi Liu, A blind dual color images watermarking based on singular value decomposition , Applied Mathematics and Computation, vol. 219, pp.8455–8466, 2013.

[12] Chih-Chin Lai and Cheng-Chih Tsai, Digital Image Watermarking Using Descrete Wavelet Transform and Singular Value Decomposition, IEEE transactions on instrumentation and measurement, vol. 59, no. 11, November 2010

[13] Athanasios Nikolaidis and Ioannis Pitas, Asymptotically Optimal Detection for Additive Watermarking in the DCT and DWT Domains, IEEE Transaction on Image Processing, vol. 12, no. 5, May 2003.

[14] Xiaotian Wu, Wei Sun, Robust copyright protection scheme for digital images using overlapping DCT and SVD, *Applied Soft Computing* , vol. 13, pp. 1170-1182, 2013