A Robust Watermarking Scheme for Digital Video Sequence using Entropy and Hadamard Transformation Technique

Manekandan. GRS, Franklin Rajkumar. V
MS Software Engineering
School of Information Technology and Engineering
VIT University-Vellore

ABSTRACT
In this paper, a robust watermarking scheme for digital video sequence which is based on Entropy concept and Hadamard transformation technique is proposed. The proposed technique can hide an entire image or pattern as a watermark directly into the original video sequence. Hadamard transformation is used for converting cover video from spatial domain to transform domain in order to reduce the computational complexity of the proposed algorithm. Similarly for preserving the quality of the digital video, the entire video blocks are not altered for embedding. Instead only few blocks are selected and used based on the size of the watermark and information content of the video block. Entropy concept is used for selecting those video blocks. The proposed algorithm is tested with rugby video sequence containing 209 frames and watermark of size 64x64 using MATLAB software. The experimental results show that the proposed scheme is robust to random noise addition attacks such as Salt and Pepper, Gaussian, Poisson and Speckle.

General Terms
Image Processing, Multimedia Security, Digital Watermarking

Keywords
Digital Video Watermarking, Hadamard transform based watermarking, Entropy based watermarking, transform domain watermarking.

1. INTRODUCTION
With the Revolution of the Internet, in this modern digital world, copyright enhancement schemes that protect copyright ownership of digital media is highly required. Watermarking is one of the multimedia authentication techniques [1]. Watermarking is the process of embedding a piece of digital information into any multimedia data such as an image, audio or video file for the purpose of authentication. Watermarks can be embedded in the pixel/spatial domain or a transform domain [2]. In spatial domain, the watermark is embedded directly by modifying the intensity values of pixels. In frequency domain, the watermark is embedded by changing the frequency coefficients. To transform image into frequency domain, the transformation techniques such as discrete wavelet transformation (DWT), discrete cosine transformation (DCT), discrete Hadamard transformation and discrete Fourier transformation are used. Spatial domain watermarking technique is easier and its computing speed is high, than transform domain watermarking. But the disadvantage is that it is not robust against common image processing operations. Transform domain techniques are introduced to increase the robustness of the digital media.

An effective watermark should have the following characteristics:

a) It should be perceptually invisible or its presence should not interfere with the work being protected [3, 4].

b) It should be robust to common signal processing operations such as sharpening, dithering, resizing, compression, noise addition and so on [5, 6].

The most important uses of watermark include copyright protection, authentication and disabling unauthorized access to the contents [7].

In section 1 introduction about the necessity of watermarking is given. Section 2 discuss briefly about the review of related works. In section 3 and 4 discusses about preliminaries of transformation techniques and entropy. In Section 5 proposed algorithm is given in detail as step by step procedure discusses in detail. Section 6 tells about the performance evaluation of proposed technique. Proposed technique is concluded in section 7. Finally, in section 8 all the papers which are referred are mentioned.

2. REVIEW OF RELATED WORKS
Anthony T.S. Ho et al makes clear that that the simplicity of the fast Hadamard transformation not only offers a significant advantage in shorter processing time and ease of hardware implementation but also has more useful middle and high frequency bands available, for hiding the watermark [8]. This technique is robust to 60%of stir mark attacks. They described again how to embed a watermark in an image using fast Hadamard transformation [9]. To increase the invisibility of the watermark, a visual model based on original image characteristics, such as edges and textures are incorporated to determine the watermarking strength factor.

Yasunori Ishikawa, Kazutake Uehira and Kazuhisa Yanaka tells about how to embed an illumination (invisibly contains watermark) using discrete cosine transformation and fast Hadamard transformation [10]. This technique is robust to illegal use of images of objects which has not watermarked. The data is embedded by two methods. First is, block method in which 1 bit data is embedded on one block and next is, majority method where same 1 bit is embedded in first three blocks sufficiently form one another. Thus improves the accuracy of reading the data.

B. J. Fnlkowski et al embedded a watermark using multiresolution Hadamard and complex Hadamard transforms in a grey scale image [11].They segmented the multiresolution Hadamard transformed image into numerous 8*8 blocks and then applied forward complex Hadamard transformation. This technique is robust to JPEG compression up to 10% quality factor, successive watermarking effects, and common signal processing operations such as dithering distortion (25%), image resizing, cropping and scaling (56.25%). Bogdan J. et al embedded a watermark using multiresolution and two dimensional complex Hadamard transformation techniques [12]. The process is similar to their previous work [11] and it classified as non blind technique. In Tang Xianghong et al work watermark is embedded using singular value decomposition [13]. Cryptographic method can also be used to strengthen the secrecy of watermarking.

Aris Marjuni, Rajasvaran Logeswaran, and M. F. Ahmad Fauzi proposed a watermarking scheme in which fast Walsh Hadamard transformation (FWHT) is applied on the original watermark before it is embedded on the DC coefficients of the host image [14]. The digital cosine transformation is applied to each 8*8 block of original image to get the DC coefficient then embed the PN sequence and then apply the inverse discrete cosine transformation on DC component to reconstruct the watermarked image. It provides good visual perception and robust against common attacks.

Bogdan J. Falkowski reveals about how to embed a watermark on the grey scale image using multi-resolution modified multi-polarity Walsh-Hadamard transform and complex Hadamard transform [15]. The process is, the raw pixels are extracted from the bit map image and it is stored in two dimensional arrays. Then multi polarity Walsh-Hadamard transformation is applied to decompose the image into pyramid structure with various sub bands. The lowest frequency sub band is selected and segmented into 8*8 blocks and then apply one dimensional complex Hadamard transformation on the rows followed by columns. Then complex Hadamard transform coefficients are altered and watermark is embedded. Then inverse complex Hadamard transformation and modified multi resolution Walsh-Hadamard transformation is applied and low frequency sub band is kept in the original position to get the watermarked image. This technique is robust to jpeg encoding, image resizing, dithering noise distortions, sharpening, cropping and successive watermarking**.**

Gaurav Bhatnagarl and Balasubramanian Raman describes about how to decompose an image using MR-WHT (Multiresolution Walsh-Hadamard Transform) and then middle singular values of High frequency sub-band at the finest and the coarsest level are modified with singular values of watermark [16]. The process of watermark embedding involves, Performing L-level MR-WHT on the host image and Selecting HH sub-band from the coarsest and the finest level and then Apply SVD on both HH sub-band and watermark image. Modify the middle singular values of the HH sub-band Perform inverse SVD to construct the watermarked Map modified sub-band to its original position and L-level inverse MR-WHT is performed to get the watermarked image.

Roumen Kountchev et al discussed about how to embed a watermark based on decomposition with inverse difference pyramid and complex Hadamard transformation [17]. The features of this process are, it has no quantization values of transform coefficient, low computational complexity and different watermarking in every consecutive pyramid level. It deals about two types of watermarking. The technique proposed is robust against tampering, compression, affine transforms, filtration, dithering.

Yasunori Ishikawa, Kazutake Uehira, and Kazuhisa Yanaka proposed an "Illumination Watermarking" technology with which the images of objects without copyright protection can contain invisible digital watermarking [18]. The main attribute of this technology is watermarking can be added by light. The watermark is embedded by using fast Hadamard transformation and discrete cosine transformation. It has two methods to get a watermarked image. First is, by using two dimensional discrete cosine transformation and the next is, using two dimensional Hadamard transformation. It provides 100% accuracy and it is robust to jpeg compression.

Emad E. Abdallah et al describes how to make a transparent and high rate embedding of watermarks into digital images using fast Hadamard transform and singular value decomposition [19]. The three main attractive features of their work are: high rate of watermark embedding into the cover image, robustness to the most common attacks, and possible implementation in real time. Elijah Mwangi describes a technique that embeds a grey level binary image as a watermark at selected DWT coefficients by the use of a private key [20]. This is achieved by spreading the binary image bits into the elements of a Hadamard matrix row by using CDMA techniques. The depth of watermarking is adjusted to give an image of acceptable quality. A correlation process is used to detect and recover the watermark. Their algorithm is effective against common signal processing attacks such as additive Gaussian noise, cropping, low pass filtering, and JPEG compression.

From the above survey, it is observed that the complexity of the Hadamard transformation based watermarking work is greatly reduced as the transformation matrix has only +1 and -1. In addition to that, watermark which is embedded in Hadamard transform domain proved to be more robust to many attacks. As a result in the proposed algorithm Hadamard transformation technique is combined with entropy model. This entropy model measure the information content of each block which is used as criterion for selection of blocks where watermark to embedded.

3. OVERVIEW OF HADAMARD TRANSFORMATION

The Hadamard transform is a non-sinusoidal, orthogonal transformation that decomposes a signal into a set of orthogonal, rectangular waveforms called Walsh functions. The transformation has no multipliers and is real because the amplitude of Walsh (or Hadamard) functions has only two values +1 or -1

The Hadamard matrix is a square array of plus and minus ones whose rows (and columns) are orthogonal to one another. If H is an N x N Hadamard matrix then the product of H and its transpose is the identity matrix
Let $[U]$ represents the original image and $[V]$ the transformed image, the 2D-Hadamard transform is given by

$$[V]=(H_n [U] H_n)/N \qquad (1)$$

Where *H*, represents an *NXN* Hadamard matrix, $N=2^n$, n=1,2,3 ... with element values are either +1 or -1. The advantage of Hadamard transform is that the elements of the transform matrix H_n, are binary real numbers. The inverse 2D-Hadamard transform (IHT) is given as

$$[U]=H_n^{-1}[V]H_n^{*}=(H_n[V]\ H_n)/N \qquad (2)$$

In the proposed algorithm, the transformation process is carried out on 8×8 blocks using the third order Hadamard transform matrix H_3 which is given below.

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

4. PRELIMINARIES OF ENTROPY

Entropy is a statistical measure of randomness that can be used to characterize the texture of the input image.
Let P contains the histogram counts. The entropy is represented as

$$E = -\sum P\ log2(P) \qquad (3)$$

5. PROPOSED ALGORITHM

In our proposed algorithm, Hadamard transformation technique and entropy concepts are used for embedding watermark. The input video sequence is divided into many frames. Then each frame is divided into many blocks and entropy is calculated for each block. If the information content is very high, then those blocks are marked as primer blocks for embedding watermark. The embedding and extraction process of watermark is given in Fig.1 and Fig.2. The test video sequence of size 256*256 and watermark of size 64x64 is used to test the proposed system. The embedding and extraction algorithm is given below in detail.

5.1 Watermark Embedding Algorithm

1. Read the frames F from the video sequence A.
2. Select the red component R from each frame in which the watermark is to be embedded.
3. Divide the red component R into blocks B_{ij} of size 8 x 8.
4. Find entropy E_{ij} for each 8 x 8 blocks and find the threshold value T_{ij}.
5. Select the 8 x 8 blocks B_{ij}^{*} whose entropy value is greater than threshold value
6. Apply Hadamard Transformation to the selected 8 x 8 blocks $B_{ij}^{*}=(H_n[B_{ij}^{*}]H_n)/N$..
7. Divide the watermark W into blocks W_{ij} of size 8 x 8.Embed the watermarked block W_{ij} with the selected block B_{ij}^{*} using constant factor.
8. Apply IHT to the embedded 8 x 8 blocks
$B_{ij}^{*}=H_n^{-1}[B_{ij}^{*}]H_n^{*}= B_{ij}^{*}=(H_n[B_{ij}^{*}]H_n)/N$.
9. Rearrange the modified 8 x 8 blocks B_{ij}^{*} with the unmodified 8 x 8 blocks B_{ij}.
10. Integrate the 8 x 8 blocks B_{ij} to get the watermarked red component R^{*}.
11. Integrate modified red component R* with unmodified green and blue component.
12. Develop the watermarked video sequence A* using different watermarked frames.

5.2 Watermark Extraction Algorithm

1. Read the frames F* from the watermarked video sequence A*.
2. Select the red component R* from each frame in which the watermark is to be extracted.
3. Divide the red component R* into blocks B_{ij} of size 8 x 8.
4. Find entropy for each 8 x 8 blocks E_{ij}^{*} and find the threshold value T_{ij}^{*}.
5. Select the 8 x 8 blocks C_{ij}^{*} whose entropy value is greater than threshold value.
6. Apply HT to the selected 8 x 8 blocks $C_{ij}^{*}=.^{*}=(H_n[C_{ij}^{*}]H_n)/N$.
7. Extract the watermark blocks W_{ij} from the respective blocks C_{ij}^{*} using constant factor.
8. Apply IHT to the respective 8 x 8 blocks
$C_{ij}^{*}=H_n^{-1}[C_{ij}^{*}]H_n^{*}= C_{ij}^{*}=(H_n[C_{ij}^{*}]H_n)/N$.
9. Rearrange the watermark blocks W_{ij} and original 8 x 8 blocks C_{ij}.
10. Integrate the 8 x 8 blocks to get original red component R and watermark blocks to display the watermark image W.
11. Integrate original red component R with unmodified green and blue component.
12. Develop an original video sequence A using different extracted frames.

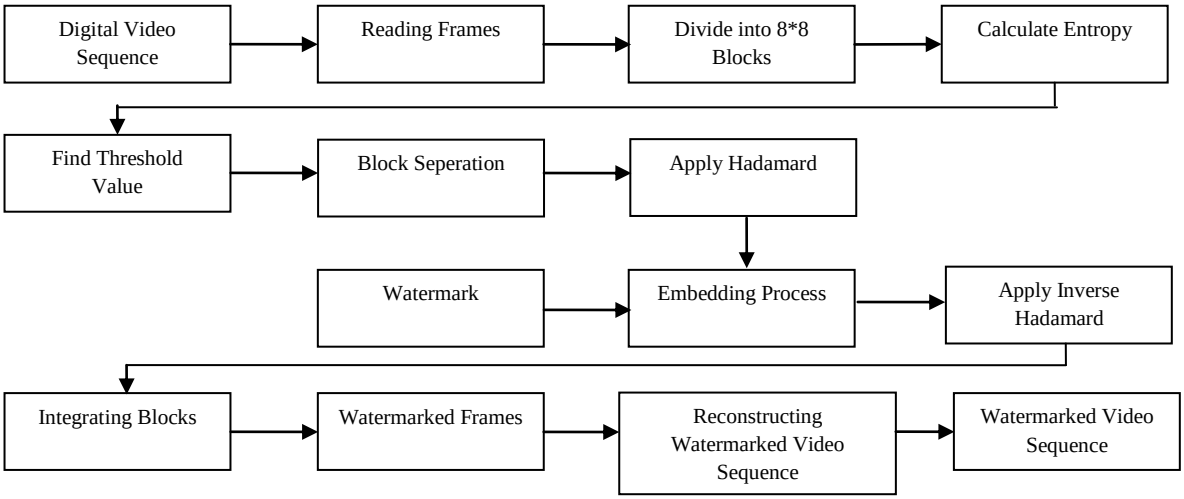


Fig.1 Embedding of watermark

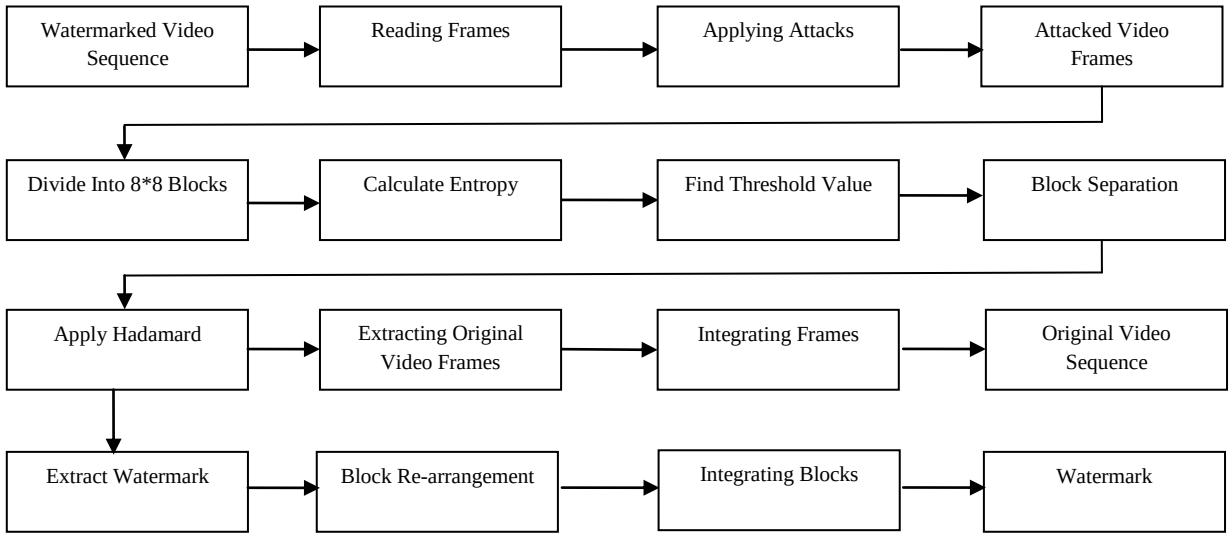
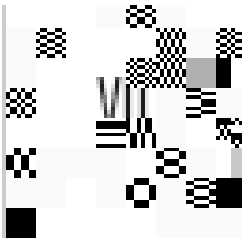
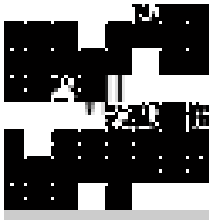
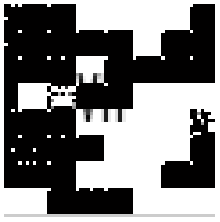
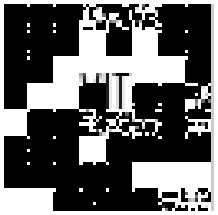
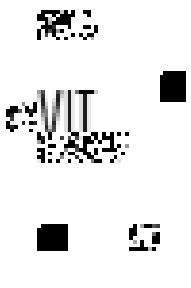
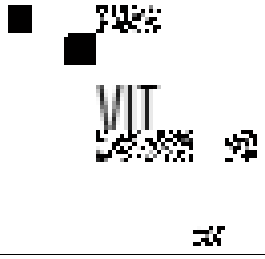
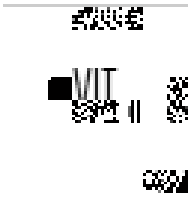
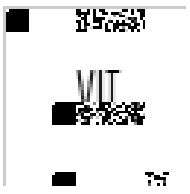
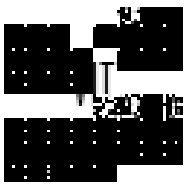
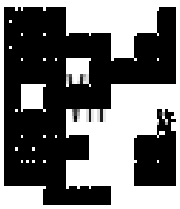
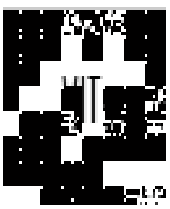


Fig.2 Extraction of watermark

6. PERFORMANCE EVALUATION

EXTRACTED WATERMARK FROM WATERMARKED IMAGE

Variation	0.0001	0.01	0.1
			
Salt and pepper noise attack	Psnr=43.1359	Psnr=25.1527	Psnr=15.1685
Variation	0.00001	0.0001	0.01
Gaussian noise attack	Psnr=47.1021	Psnr=45.2443	Psnr=30.0092
Variation	0.00001	0.0001	0.01
Speckle noise attack	Psnr=46.7222	Psnr=44.0469	Psnr=27.2283
Variation	270	180	90
			
Rotational attack	Psnr=12.2816	Psnr=12.0405	Psnr=12.2809
Variation	Nil	Nil	Nil
			
Poisson noise attack	Psnr=28.1683	Psnr=28.1666	Psnr=28.1674

			
Salt and pepper noise attack	Psnr=43.1248	Psnr=25.1224	Psnr=15.1618
Variation	0.00001	0.0001	0.01
Gaussian noise attack	Psnr=47.0813	Psnr=45.2323	Psnr=30.0128
Variation	0.00001	0.0001	0.01
			
Speckle noise attack	Psnr=46.7043	Psnr=44.0427	Psnr=27.2384
Variation	270	180	90
			
Rotational attack	Psnr=12.2322	Psnr=11.9960	Psnr=12.2315
Variation	Nil	Nil	Nil

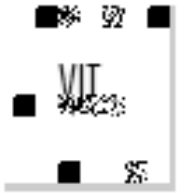
			
Poisson noise attack	Psnr=28.1759	Psnr=28.1739	Psnr=28.1742

TABLE.2 PSNR VALUES OF VARIOUS ATTACKS WITH VARIATIONS IN MPG VIDEO SEQUENCE

PSNR=57.4062

The performance of the algorithm is tested by simulating it using MATLAB software. A test video sequence and a watermark of size 64x64 are used to test the performance. The quality of the watermarked video is objectively measured using PSNR and it is observed that quality of the watermarked video both in AVI & MPG format is good. The measured PSNR value for AVI format is 47.2754db and for MPG format is 47.2534. The similarity measure or the normalized correlation coefficient of original and extracted watermark from undistorted watermarked image is 1. The psnr value is calculated using the eq. 4.

$$MSE = \frac{1}{MN}\sum_{i=1}^{m}\sum_{j=1}^{n}(f(i,j) - f(i,j))2 \quad (4)$$

$$PSNR = 10\ log_{10}\left(\frac{255^2}{MSE}\right) \quad (5)$$

$f(i,j)$ and $f^{'}(i,j)$ represent the pixel values of original host frame and the watermarked frame respectively and parameters *m,n* specify row and column size of images respectively. To test the robustness of the algorithm various attacks are introduced to the video. Initially the noise addition attack is introduced and it is observed that algorithm is robust if the variance is 0.001and 0.01. Various noises such as salt and pepper, Gaussian noise and speckle noise are added and robustness is tested. It is found that the algorithm is withstanding noise addition attacks. To check the quality of the extracted watermark from the distorted video the similarity measure is used. To check the similarity normalized correlation (NC) between original and extracted watermark is calculated using Eq. 7. If normalized correlation value is high

then the quality of the extracted watermark is considered as good. If the value of NC goes below 50%, it is assumed that the algorithm is not robust to that particular attack.

$$NC = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} w(i,j) * w_e(i,j)}{\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m} w^2(i,j)}\ \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{m} w_e^2(i,j)}} \quad (7)$$

Algorithm is also tested with attacks like rotation and poisson. The tampered video and extracted watermark is shown in table1 and table 2 for both AVI & MPG format respectively.

7. CONCLUSION

This work has probed a simple, efficient watermark embedding and extraction algorithm for digital video sequence. Test results of the algorithm indicate how the algorithm is robust and fragile to various kinds of attacks made by the external attackers over the video sequence to destroy the watermark. It gives the comparison of PSNR values of MPG and AVI video sequence. This system successfully prevents the watermark from damage, when different kinds of attacks are introduced to the watermarked video sequence and robust to most of the attacks. In future the Hadamard transformation based watermarking work is extended to test robustness against geometric attacks like translation scaling and Rotation and shearing for video sequences.

8. REFERENCES

[1] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques", in proc. of the IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.

[2] Ali Al-Haj, "Combined DWT-DCT Digital Image Watermarking", Journal of computer science 3 (9), 740-746, ISSN, 2007.

[3] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for data hiding", IBM Systems Journal**,** vol.35, no. 3&4, pp. 313-336, 1996.

[4] I. J. Cox, J. Killian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, December 1997.

[5] J. J. K. 0 Ruanaidh, W. J. Dowling and F. M. Boland, "Watermarking digital images for copyright protection", IEEE Proceedings - Vision, Image and Signal Processing, vol. 143, no. 4, pp. 250-256, August 1996.

[6] M. D. Swanson, M. Kobayashi and A. H. Tewfik, "Multimedia data-embedding and watermarking techniques", Proceedings of the IEEE**,** vol. 86, no. 6, pp.1064-1087, June 1998.

[7] Navas K A,Ajay Mathews Cheriyan, Lekshmi. M, Archana Tampy.S, Sasikumar M, "DWT-DCT-SVD Based Watermarking", 3rd International Conference on Communication Systems Software and Middleware and Workshops, 2008.

[8] Anthony T.S. Ho, Jun Shen, Soon Hie Tan, Alex C. Kot, "Digital Image-in-Image Watermarking For Copyright Protection Of Satellite Images Using the Fast Hadamard Transform", IEEE International Geosciences and Remote Sensing Symposium, vol. 6, pp. 3311-3313, 2002.

[9] Anthony T.S. Ho, Jun Shen, Andrew K.K. Chow, Jerry Woon, " Robust digital image-image watermarking algorithm using fast Hadamard transform", International Symposium on circuits and systems, vol. 3, pp. III-826-III-829, May 2003.

[10] Yasunori Ishikawa, Kazutake Uehiraand Kazuhisa yanaka, "Illumination Watermarking Technique Using Orthogonal Transforms", Industry Applications society Annual Meeting, pp. 1-4, October 2009.

[11] B. J. Fnlkowski and Lip-San Lim, "Image watermarking using Hadamard Transforms**"**, Electronics Letters, vol. 36, no. 3, pp. 211-213, February 2000.

[12] Bogdan J. Falkowski and Lip-San Lim, "Image Watermarking Using the Complex Hadamard Transform", IEEE International Symposium on Circuits and Systems, vol. 4, pp. 573-576, Geneva, Switzerland, May 2000.

[13] Tang Xianghong, Yang Lianjie, YueHengli, Yin Zhongke, **"**A Watermarking Algorithm Based on the SVD and Hadamard Transform", International Conference on Communications, circuits and system, vol. 2-877, May 2005.

[14] Aris Marjuni, Rajasvaran Logeswaran, M. F. Ahmad Fauzi, "An image watermarking scheme based on fast Walsh Hadamard transformation and discrete Cosine transformation", International Conference on Networking and Information Technology, pp. 289-293, June 2010.

[15] Bogdan J. Falkowski, "Multi-Polarity Complex Hadamard Transforms for Phase Watermarking Algorithm", 6th International Conference on Information Communication and Signal Processing, pp. 1-5, December 2007.

[16] Gaurav Bhatnagarl and Balasubramanian Raman2, "Robust Watermarking in Multiresolution Walsh-Hadamard Transform", International Advance Computing Conference (IACC 2009),Patiala, India, pp. 894-899, March 2009.

[17] Roumen Kountchev Mariofanna Milanova Charles Ford Stuart Rubin, **"**Multimedia Watermarking with complex Hadamard transform in the inverse pyramidal decomposition", International conference on Information Reuse and Integration, pp. 305-310, October 2003.

[18] Yasunori Ishikawa, Kazutake Uehira, and Kazuhisa Yanaka, "Practical evaluation of illumination watermarking technique using orthogonal transforms", Journal of Display Technology, vol. 6, no. 9, pp. 351-358, September 2010.

[19] Emad E. Abdallah, A. Ben Hamza, and Prabir Bhattacharya, "Robust block based image watermarking scheme using fast Hadamard transformation and single value decomposition", The 18th International Conference on Pattern Recognition , vol. 3, pp. 673-676, 2006.

[20] Elijah Mwangi, "A wavelet based image watermarking scheme with a cdma/Hadamard embedding technique**",** 9th International Symposium on Signal Processing and its Applications, pp. 1-4, February 2007.