International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

Transmitting Copyright-Protected Images over Low-Bandwidth Channels through FFT-Based Watermarking in E-Learning

Soumendu Banerjee, Akash Nag, Kh. Amirul Islam, Sunil Karforma

Abstract: ***In an e-learning environment, security plays an important role while transmitting information in form of image or text through an open access network like Internet. In a low-bandwidth channel, it becomes difficult to download large image files and also the checking for authentication becomes cumbersome. In our proposed methodology, the sender can successfully send large image files to the receiver through a low-bandwidth channel and also we have emphasized on the authentication of the image for originality.***

Keyword: Fast Fourier Transform, Haar wavelet transformation, digital watermarking, private key Cryptography

I. INTRODUCTION:

The three main participants in an e-learning system are administrators, teachers and students. In an e-learning environment, the situation may arise when the administrator has to send large image files to the students which should be authenticated at the student end after receiving the same. If the file size is very large, then it becomes difficult for the receiver to download the image in a low-bandwidth channel. In our proposed methodology, we have applied Haar compression technique to adjust the image size and also provide the space for verifying the authenticity to the learner.

In this paper, we have proposed an algorithm through which the administrator can send large image securely via Internet and learner can also authenticate the document after receiving. Section II covers the technique of the proposed Haar FFT Watermarking model. The architecture and algorithm of the proposed model is described in section III and IV respectively. The result of the proposed model is shown in section V and we have concluded in section VI.

II. PROPOSED HAAR TRANSFORMED FFT BASED WATERMARKING

Our proposed methodology is based on the transmission of large scale cover image file, from administrator to learner, watermarked with any logo or image to authenticate the sender, in an e-learning environment. We have divided our proposed algorithm into two sections:

Step1: Insertion of the watermark into the cover image and

Step2: Applying Haar wavelet transform to compress the watermarked image.

The watermark insertion process includes FFT (Fast Fourier Transform) based keyed watermark insertion algorithm. When the insertion process is completed[1], then the administrator opts for Haar Wavelet transform to compress the watermarked image. After the completion of the compression process, the administrator will send the compressed watermarked image to the learner along with the key[2,3]. After receiving the compressed watermarked image, learner first decompresses it and then extracts the watermark with the help of the key, provided by the administrator. Since we have applied Haar compression technique, so the extracted image will be little bit distorted compare to the image that was inserted by the administrator during the encoding process. So, learner has to verify whether both, the extracted watermark image and the inserted watermark image, are same or not. The learner will upload the watermark to the server for verification and if they are same, the server will give a positive reply, otherwise administrator will resend the image again.

To provide better authenticity and secrecy in our proposed algorithm, we have implemented the concept of a 32 bit private watermark key, which will be generated at the sender's end and will be transmitted to the receiver to extract watermark from the watermarked image. Without this key, the receiver cannot extract the watermark from the embedded image. So, if the hacker can reach the document, during transmission, can't extract the watermark due to absence of the private key. The compression has been done through Haar wavelet transformation. The Haar wavelet matrix that we have used to compress the watermark is given below.

$$H = \begin{bmatrix} 1/8 & 1/8 & 1/4 & 0 & 1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & 1/4 & 0 & -1/2 & 0 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & 1/2 & 0 & 0 \\ 1/8 & 1/8 & -1/4 & 0 & 0 & -1/2 & 0 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & 1/2 & 0 \\ 1/8 & -1/8 & 0 & 1/4 & 0 & 0 & -1/2 & 0 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & 1/2 \\ 1/8 & -1/8 & 0 & -1/4 & 0 & 0 & 0 & -1/2 \end{bmatrix}$$

Manuscript published on January 30, 2020.
* Correspondence Author
Dr. Soumendu Banerjee*, Faculty Member, Department of Computer Science at St. Xavier's College, Burdwan, India.
Faculty Member, Dept. of Computer Science, M.U.C. Women's College, Burdwan, India.
Kh. Amirul Islam, Dumkal Institute of Engineering and Technology, WBUT and MCA, University of Burdwan, India.
Dr. Sunil Karforma, Professor and Head, Department of Computer Science, University of Burdwan, India.

Here H is an 8×8 matrix (in annexure), so we also divide our watermarked image into 8×8 matrix. To decompress the image M, we apply the equation (1) to get back the original image.

Since Haar transform is a lossy compression, so we will not get back the original image.

$$A = \left(H^{T}\right)^{-1} M H^{-1} \quad (1)$$

The Fast Fourier Transform (FFT) is a Discrete Fourier Transform (DFT) algorithm and produces exactly same result much faster by reducing the time of computations from $o(n^2)$ to $o(n \log n)$. The human eye is less susceptible to change in frequency than to the change in color of each individual pixel. Therefore, the frequency domain is more suitable for watermark insertion and that is why we have opted for the FFT. Another advantage of using FFT is that it produces more accurate result compare to evaluating the DFT directly[4].

III. ARCHITECTURE OF HAAR FFT WM

Architecture of the proposed digital watermarking system related to the transmission of e-learning documents from administrator to learner is shown using Figure1.

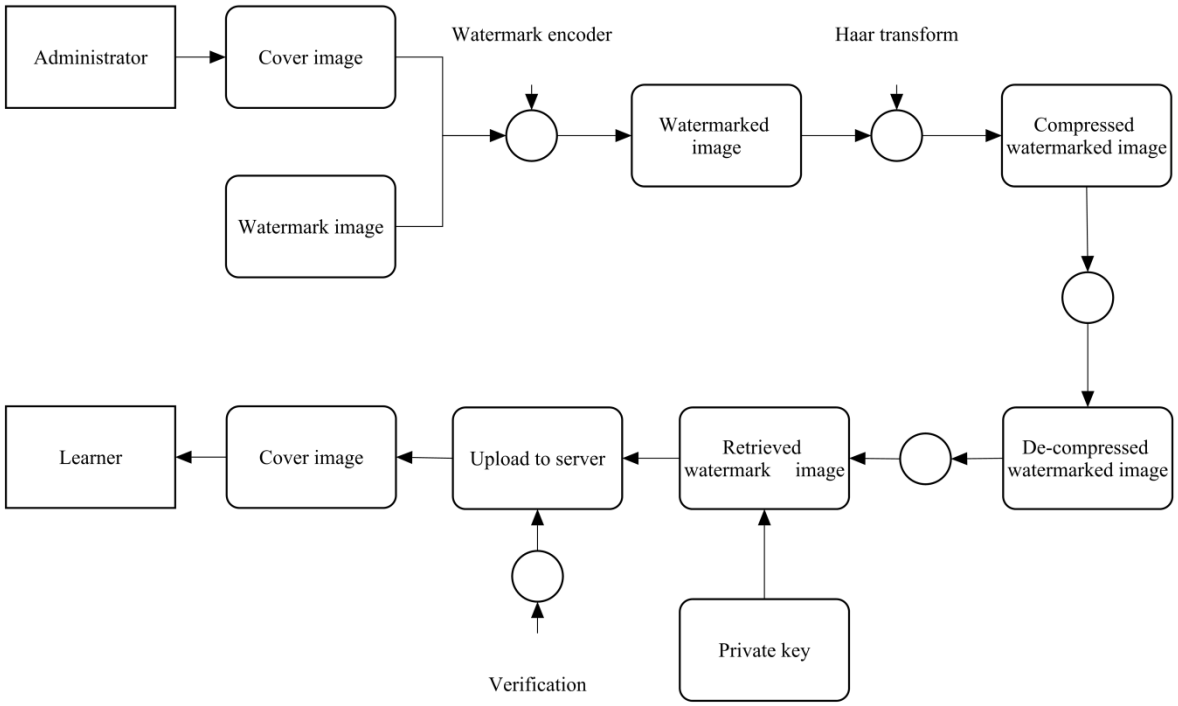


Figure1. Architecture of Haar FFT WM

IV. ALGORITHM OF HAAR FFT WM

Here, we have shown the steps of our proposed watermarking algorithm through which the watermark is inserted into the cover image and we have also shown the steps through which the watermark is extracted from the watermarked image. It is a key based FFT algorithm. The watermark insertion has been done at the administrator's end and the steps of the watermark insertion algorithm are shown below.

Step 1: Image division into blocks and Fourier transformation

The gray-scale image is first divided into blocks of 8x8 pixels. Each block is then transformed to the frequency domain using Fast Fourier Transform.

Step 2: Keyed pseudo-random permutation of the watermark

The watermark is first converted to a monochrome image containing only black and white pixels. This is then permuted randomly using a 32-bit key input by the user. The key is used as a seed to a random sequence generator to generate the permutations.

Step 3: Watermark division into blocks

The watermark is divided into as many blocks as there are image blocks. However, each block must be less than 8x8 pixels. In other words, the watermark dimensions should be strictly less than that of the image.

Step 4: Mapping of the watermark blocks to image blocks for embedding

For each block *i* of the image, the number of non-zero coefficients (real part only) of the Fourier-transformed data is computed to be M(i). For each block *j* of the watermark, the number of white pixels is computed to be W(j). Both these frequencies are then sorted in descending order and mapped according to the same rank figure2.

Image block Index (i)	M(i)	Rank
1	5	4
2	9	2
3	12	1
4	3	5
5	7	3

Watermark block index (j)	W(j)	Rank
1	3	5
2	8	3
3	13	1
4	9	2
5	5	4

Figure2. Block mapping example

Step 5: Low frequency embedding

Using the mapping, found in Step-4, each watermark block is now embedded to its mapped/corresponding image-block. This embedding is performed in the LSB of the pixels in a zig-zag fashion in order to embed into the low-frequency portions only. Figure3 shows the low frequency embedding positions clearly.

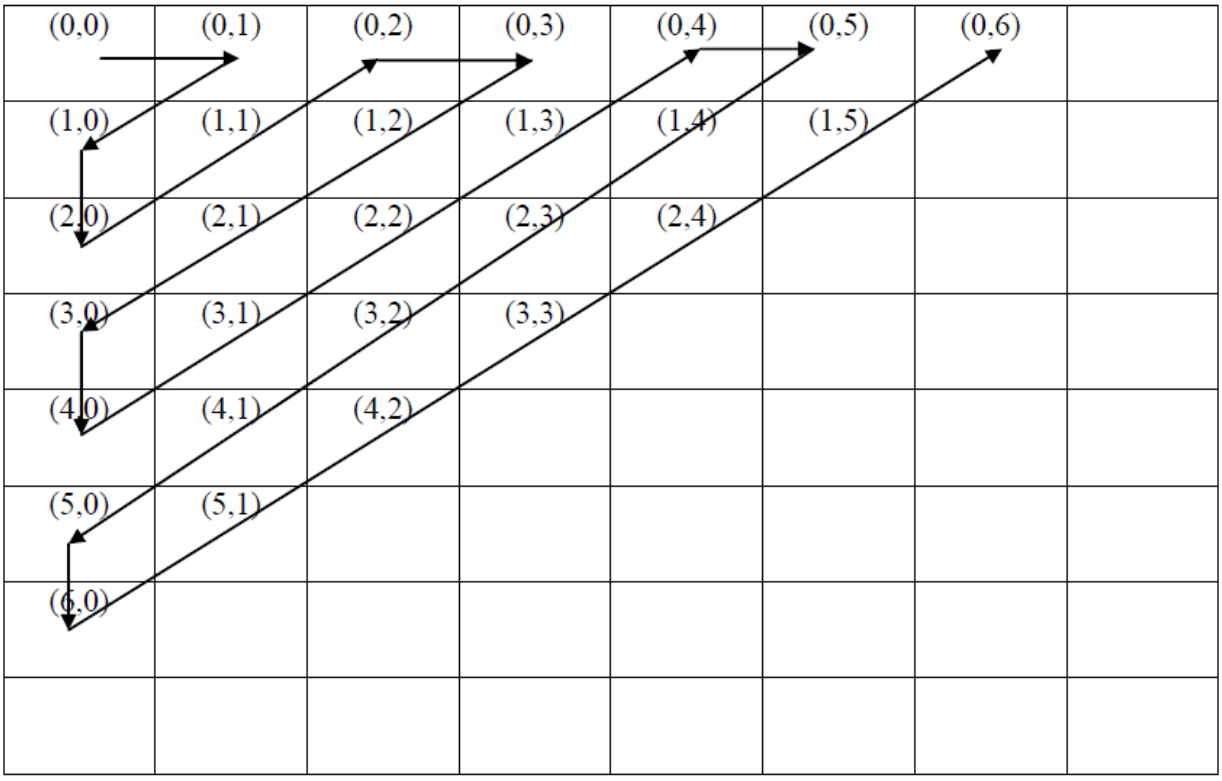


Figure3. Low frequency embedding positions

Step 6: Inverse Fourier Transformation

Each embedded image block is then transformed independently into the spatial domain using the inverse Fast Fourier Transform (FFT) algorithm. The resulting data (ignoring the imaginary coefficients) is then written out as the watermarked image.

The watermark extraction procedure has been done at the learner's end. The steps involve in performing the extraction of watermark from the embedded image are briefly discussed below.

Step 1: Transformation to frequency domain

Each block of the watermarked image is independently transformed into the frequency domain by using Fast Fourier Transform (FFT) algorithm.

Step 2: Extraction of LSB coefficients

The Least Significant Bit (LSB) coefficients are extracted in a zig-zag fashion from each image block.

Step 3: Reverse the mapping of the watermark blocks

The mapping of the watermark blocks against the image blocks are reversed to get the correct ordering of the extracted data.

Step 4: Keyed reverse permutation of the watermark

The watermark data is combined and then a reverse permutation is applied on it using the user-supplied 32 bit as the seed of a random sequence generator. The watermark is then saved as an image.

Object-Oriented modeling of any system helps the designer to improve the software quality and reduce the cost of maintainability. In the following section, we have designed UML diagrams like use case diagram, activity diagram and class diagram of Haar FFT WM.

V. RESULT AND ANALYSIS OF HAAR FFT WM

We have applied our proposed algorithm on one cover image and different payload images. We have chosen one sufficiently large image as cover image and ten different secret images; have been used as watermark images. All the images and the corresponding results are shown below.

The results we have shown here, is on the basis of one cover image shown in Figure4 and Figure5 contains the list of original watermark images which are inserted into the cover image for authentication purpose. Figure6 contains the watermarks which are extracted from the embedded image at the learner's end and will be uploaded to the server for verification.

Cameraman.png (Dimensions: 256 × 256) (Size: 32 KB)
Figure4. Cover image for Haar FFT WM

(a) logo_A.png
(64×64) (595 Bytes)

(b) logo_D.png
(240×232) (4.88 KB)

(c) logo_T.png
(160×152) (1.45 KB)

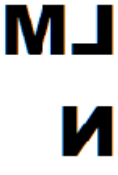
(d) logo_EW.png
(240×120) (12 KB)

(e) logo_AB.png
(128×128) (1.82 KB)

(f) logo_XY.png
(128×128) (1.01 KB)

(g) logo_ABC.png
(120×136) (1.58 KB)

(h) logo_WXY.png
(128×112) (1.98 KB)

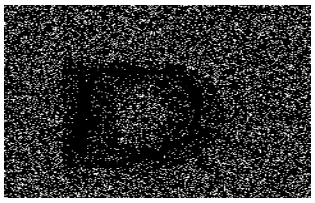


(i) logo_LMN.png
(96×120) (1.12 KB)

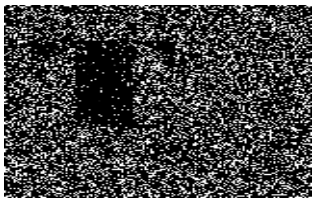
(j) logo_WXYZ.png
(112×144) (1.65 KB)

Figure5: List of watermark images before insertion

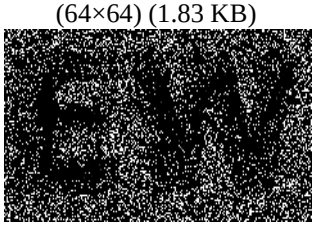
(a) extWM_A.png
(64×64) (1.83 KB)



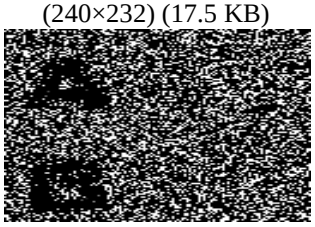
(b) extWM_D.png
(240×232) (17.5 KB)



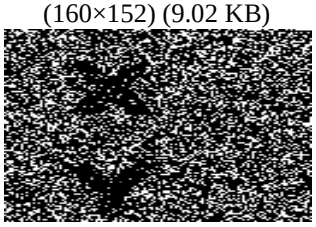
(c) extWM_T.png
(160×152) (9.02 KB)



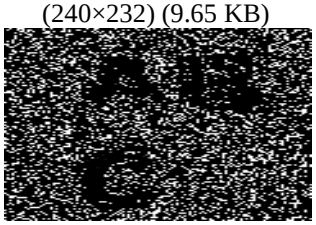
(d) extWM_EW.png
(240×232) (9.65 KB)



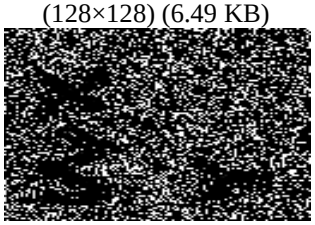
(e) extWM_AB.png
(128×128) (6.49 KB)



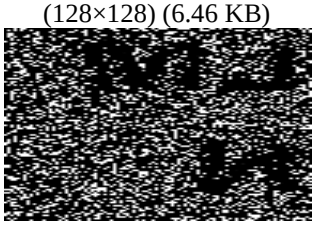
(f) extWM_XY.png
(128×128) (6.46 KB)



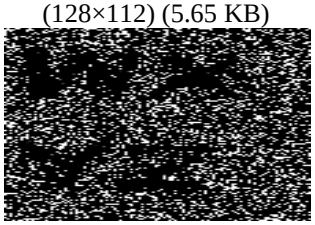
(g) extWM_ABC.png
(120×136) (6.09 KB)



(h) extWM_WXY.png
(128×112) (5.65 KB)



(i) extWM_LMN.png
(96×120) (4.47 KB)



(j) extWM_WXYZ.png
(112×144) (6.10 KB)

Figure6: List of watermark images after extraction

The figures(4 & 5) show the list original watermarks, which are may be considered as the logos of the institutes, used to authenticate the sender (here administrator) and also contains the list of extracted watermarks(Figure6) which are slightly distorted due to the compression of images as a consequence of Haar transform at the administrator's end and reverse Haar transform at the learner's end. These extractions will be done at the learner's end and after extracting the watermarked images, the learner will upload those to the server for verification. So if any kind of attacks occur during the transmission, then the watermarked image will be changed and can easily be verified at the server end.

The Table1 is used to present the compression ratio which shows the amount of compression occur by computing the ratio between the watermarked image and transformed image and actual ratio (which is always 1). This table also contains the PSNR values corresponds all those ten images which we have chosen for our experiment in the same sequence.

Table1. Compression ratio and PSNR values of Haar FFT WM

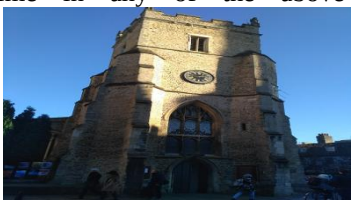
SI No.	Size of watermarked image (KB)	Size of transformed image (KB)	Compression ratio (Transformed/Watermarked):1	PSNR
(a)	34.9	23.7	1.47 : 1	54.8357
(b)	43.0	23.8	1.81 : 1	51.6383
(c)	41.5	23.8	1.74 : 1	52.5423
(d)	42.2	23.8	1.77 : 1	52.9333
(e)	41.1	23.7	1.73 : 1	52.3992
(f)	40.5	23.8	1.70 : 1	52.4021
(g)	40.7	23.7	1.71 : 1	52.3544
(h)	40.9	23.7	1.73 : 1	52.4016
(i)	40.2	23.7	1.70 : 1	52.6454
(j)	41.0	23.8	1.72 : 1	52.3645

We observe the compression ratio is lying between 1.4 and 1.8, which is quite reasonable for grayscale images in PNG format. Here we have selected only grayscale images as the cover image, but the result of the compression is too high for the color images, which can also be used as cover image. We have shown some examples of the compression ratio of our algorithm by taking some color images (shown in Figure7) in the same PNG format. The lists of images are shown below and the Table2 shows the compression ratio.

If we go through the Table3, we observe that our proposed Haar transformed FFT watermarking technique does not consume much time in any of the above cases.

(a) Lena.png

(b) CMS.png



(c) University_2.png

(d) Cat.png

Figure7. Lists of some color images

Table2. Results of compression taking some color images of Haar FFT WM

Original image size	Compressed image size	Compression ratio	Compression time (Second)	Decompression time (Second)
161 KB	42.4 KB	3.80 : 1	0.228	0.262
4.65 MB	1.40 MB	3.32 : 1	7.758	6.894
239 KB	67 KB	3.57 : 1	0.340	0.340
91.1 KB	27.8 KB	3.28 : 1	0.156	0.156

VI. CONCLUSION:

Digital watermarking is one of the most popular techniques through which authentication can be achieved in any kind of online system. Our proposed Haar transformed FFT based watermarking approach provides authenticity to the participants of e-learning system while transmitting any image files, especially for the files which are larger in size and need more time to download. There may be some places, where Internet is not so fast and in those cases if the institute follows this proposed model, especially in case of color images, then it will be easy for the learner to download the compressed file in those areas. The proposed methodologies are also applicable for any kind of online system like e-commerce, e-governance and other online systems.

REFERENCES:

1. Shih, F. Y. (2008). "Digital watermarking and Steganography: Fundamentals and techniques", London: CRC Press
2. M.Arnold, M. S. (2003). "Techniques and applications of digital watermarking and content protection.", London: Artech House
3. P. Singh and R.S. Chadha, "A survey of digital watermarking techniques, Applications and attacks", International journal of Engineering and Innovative technology, Vol:2(9), March-2013
4. K.Kaur. (2016). "Fast Fourier Transform based Hybrid image wateramrking using Android Scrambling", International journal for research in applied science andengineering technology, 204-213

AUTHORS PROFILE

Dr. Soumendu Banerjee has completed his B.Sc(H) in Mathematics, MCA and Ph.D. in Computer Science from The University of Burdwan. He is currently acting as a faculty member in the Department of Computer Science at St. Xavier's College, Burdwan.

Dr. Akash Nag completed his Bachelors in Computer Applications from the University of Burdwan, and his Masters in Computer Science from the University of Calcutta. He received his Ph.D. in Computer Science from the University of Burdwan. He is currently a faculty member in the Dept. Of Computer Science at M.U.C. Women's College, Burdwan. His research interests include algorithms and bioinformatics.

Kh Amirul Islam has completed his BCA from Dumkal Institute of Engineering and Technology, WBUT and MCA from The University of Burdwan. He has published 4 research papers in journals and conferences.

Dr. Sunil Karforma has completed B.E. (Computer Science and Engineering) and M. E. (Computer Science and Engineering) from Jadavpur University. He has completed Ph. D. in the field of Cryptography. He is presently holding the post of Professor and the Head of the Department in the Department of Computer Science, The University of Burdwan. His research interests include Network security and e-commerce. He has published numerous research papers in both National and International journals and conferences.