A Watermarking Algorithm Based on HT-DWT-TGF for Security Applications

C. SUBBA RAO M.E., (PhD) Associate Professor, ECE

PVP Siddhartha Engineering College

Phone No: 9290876076, Vijayawada.

Abstract: - This research paper, scopes a Reversible watermarking scheme for digital images based on DWT & Triangular Generator functions (TGF) and Hardmard Transform. The two key aspects of Reversible watermarking schemes are copyright protection and robustness. The proposed watermarking algorithm divides the image into sub bands. There are different types of level decompositions such as level 1, level 2, level 3. In this design of the project we are using level 3 decomposition. To every pixel of the image three basic techniques (DWT, TGF, and HT) is applied and then XOR operation for the three basic technique is performed. The performance of watermarking algorithm based on peak to signal noise ratio (PSNR), Normalized coefficient (NC), Image Enhancement Factor (IEF) is obtained. The system applies a triangular number generating function to strengthen the binary watermark and employs for watermark synchronization. Experimental results show that the proposed system provides good fidelity of watermarked and recovered images and robustness to certain geometrical and non geometrical attacks.

Index Terms— Discrete Wavelet Transform (DWT), Frequency domain, Hardmard Transform, Reversible Watermarking, Triangular Generating Function.

I. INTRODUCTION

Today digitization develops day by day, the protection of digital information is important. In order to resist different kinds of infringement, a new technology that called watermarking had been put forward to in the international scope. Watermark is sequence carrying information about the copyright owner

To embed into the digital image [1], audios and videos in order that owners can read it out while unauthorized **B.V.LAKSHMI** (Mtech) ,ECE PVP Siddhartha Engineering College.

> Kanuru, Vijayawada Phone No: 9704335849,

users cannot easily read it. There are many methods to embed the watermark. It can be divided into two classes: Spatial-domain watermarks and transform-domain watermarks. The spatial domain is so simple that the watermark can be damaged easily, but the transform-Domain algorithm can be resist intensity attack, watermark information can't be damaged easily. The Transform algorithm includes chiefly DWT, DFT and DCT [2, 3, and 4]. Wavelet transform is superior to timefrequency transform for its inner predominance. For example, wavelet has the character of multi-resolution, which can avoid the rectangle brought by DCT. In fact, it has more application fields in engineering and computer science. In this paper, a new reversible watermarking algorithm that embeds a meaningful binary image into the color images is proposed based on HT-DWT-TGF.Some important types of watermarking based on difference watermarks [3] are given below:

Visible watermarks:

It is a simple, analogous to stamping a mark on paper. The data is digitally stamped. This is applicable only to images.

Example: On television channels visible watermarking is seen when their logo is visibly superimposed in the corner of the screen.

Invisible watermark:

It is a complex concept. It is most often used to copyright data such as author, distributor etc.



"Fig. (1) Digital Watermarking system"

II. PROBLEM DESCRIPTION

The main purpose of this paper is to contribute in study of comparison of frequency domain techniques are used for image processing as for reservable blind watermarking. Section III describes Basic principle and theoretical part of watermarking. Section IV Describes DWT method for proposed purpose. Section V shows experimental output and comparison result. Section VI concludes the paper in which DCT and DWT techniques.

III. DISCREET WAVELET TRANSFORM PRINCIPLES

Wavelet transform is a time-frequency domain combined analysis method. It has multiresolution analysis features. Each level of the wavelet decomposition has four subimages with same size. Let the LL_k stands for the approximation sub-image and LH_k , HL_k , HH_k stand for the horizontal, vertical and diagonal direction high frequency detail sub-image respectively. Where the variable $k=1, 2, 3, (k \in N)$ is the scale or the level of the wavelet decomposition. After wavelet decomposition, many signal processing, such as compression and filter are likely to change the highfrequency wavelet coefficients. If the watermark sequence is embedded into this part, its information may be lost in the processing in sequence, which will reduce the robustness of the watermark [3]. In order to ensure the watermark has a better imperceptibility and the approximation sub-image LL3 robustness, coefficients are chosen to embed watermark. We can achieve the transform of the separable wavelet as in Figure 1.

IV PROPOSED WATERMARKING ALGORITHM BASED ON TRIANGULAR NUMBER GENERATOR FUNCTIONS

Here, the readable watermark is a qq binary image. We arrange the binary image to 0, 1 watermark sequence wm. And the length of wm is the pXq. Original image is a mXn.



"Fig. (2) Proposed Watermarking 3 level discrete wavelet Transform"

V WATERMARK EMBEDDING SCHEME

Consider the Hardmard matrix for the watermarking process are given below Dimensional discrete

Hadamard transform positive transform and inverse transform, such as the definition of formula (1) and (2) [5]:

$$H(u,v) = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) (-1)^{\sum_{i=0}^{N} (b_i(x_i)b_i(u) + b_i(y)b_i(v))}$$
(1)

$$f(x, y) = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} H(u, v) (-1)^{\sum_{i=0}^{N} (b_i(x_i)b_i(u) + b_i(y)b_i(v))}$$
(2)

H(0,0) is called image block the DC component hardamard transform domain. Using an interactive relationship can generate higher

Order transform matrix of Hadamard transform, such as the formula (3) below.

$$\mathbf{H}_{2} = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}, \mathbf{H}_{2^{k+1}} = \begin{bmatrix} \mathbf{H}_{2^{k}} & \mathbf{H}_{2^{k}} \\ \mathbf{H}_{2^{k}} & \mathbf{H}_{2^{k}} \end{bmatrix}, k = 1, 2, 3....(3)$$

Step1 `A one-dimension chaotic sequence is originated from a logistic mapping $X_{n+1} = uX_n (1 - X_n)^{-1}$ [4]. The sequence has the same size as the length of the wm. Apply a threshold value, and then get 0-1 sequences A*. The program performs a *XOR* operation of this wm with the binary watermark image. X_0 and u are password. The sequence of the binary watermark image after encrypting is:

Step2 Extracting the triangular components and the from original image. It is divided into square blocks of size 8×8 pixels. Then the HT is applied in each block. Then the DC value $H_{i,j}(1,1)$ *H* of each block is collected together to get a new matrix $I = \begin{bmatrix} H_{1,1}(1,1) & H_{1,2}(1,1) & \dots & H_{1,k1}(1,1) \\ H_{2,1}(1,1) & H_{2,2}(1,1) & \dots & H_{2,k1}(1,1) \\ \dots & \dots & \dots & \dots \\ H_{k2,l}(1,1) & H_{k2,2}(1,1) & \dots & H_{k2,k1}(1,1) \end{bmatrix} (5)$

Where $k1 = \frac{n}{8}$, $k2 = \frac{m}{8}$

Step3 Make the new matrix *I* to do a one-scale twodimension discrete wavelet transform with haar. According to quantization step value s, make the low coefficient LL to qualified adjustment, then embed the watermark value. The detailed process is as follows:

The quantified value q(i, j) of the low-frequency wavelet coefficient can be obtained by:

$$q(i,j) = \begin{bmatrix} LL(i,j) \\ s \end{bmatrix}$$
(6)

The process of embedding watermark information is as follows:

If mod(q(i, j), 2) = w(k) adjust the lowfrequency wavelet coefficient to

$$LL'(i,j) = q(i,j) \times s + \frac{s}{2} \qquad (7)$$

if $mod(q(i, j), 2) \neq w(k)$ adjust the lowfrequency wavelet coefficient to

If
$$LL'(i, j) - q(i, j) \times s \in +(0, \frac{s}{2})$$

then $LL'(i, j) = (q(i, j) - 1) \times s + \frac{s}{2}$
else $LL'(i, j) = (q(i, j) + 1) \times s + \frac{s}{2}$
where $i = 1, 2, \dots, \frac{m}{16}, j = 1, 2, \dots, \frac{n}{16}, k = 1, 2, 3, \dots, p \times q$
Step 4 Make wavelet inverse transform.

Step 5 The $H_{i,j}(1,1)$ of each block can be obtained by extracting the corresponding value the wavelet inverse transform matrix, then make HT inversetransform each sub-block. Changing the doubleprecision real number to unsigned 8-bit integer. Thus, obtain the color components in which watermark are embedded. Finally, we transform the image from threebasic-color image into true color RGB space. Then we will get the watermarked color image. دد



"Fig. (3) Proposed Watermarking Extraction

Technique"

VI WATERMARK EXTRACTING SCHEME:

The processes of watermark extracting and embedding are reverse. When extracting watermark, the detailed ways is as follows:

Step1 Extracting the green components (G), it is divided into 8×8 sub-block. Then the HT is applied in each block. Then the DC value, $H_{i,j}(1,1)$ of each block is collected together to get a new matrix I'

$$i = 1, 2, \dots, \frac{m}{8}, \quad j = 1, 2, \dots, \frac{n}{8}$$
$$I^{1} = \begin{bmatrix} H^{1}_{1,1}(1,1) & H^{1}_{1,2}(1,1) & \dots, H^{1}_{1,k1}(1,1) \\ H^{1}_{2,1}(1,1) & H^{1}_{2,2}(1,1) & \dots, H^{1}_{2,k1}(1,1) \\ \dots & \dots & \dots \\ H^{1}_{k2,1}(1,1) & H^{1}_{k2,2}(1,1) & \dots, H^{1}_{k2,k1}(1,1) \end{bmatrix}$$
(8)

Where
$$k1 = \frac{n}{8}, \quad k2 = \frac{m}{8}$$

Step2 Make the matrix *I* ' to do a one-scale

Two-dimension discrete wavelet transforms with haar, and extracts the watermark from low-frequency wavelet coefficient LL. The detailed way is as follows:

$$q(i,j) = \begin{bmatrix} LL(i,j) \\ s \end{bmatrix}$$
(9)

$$\operatorname{mod}(q(i,j),2) = w^{1}(k) \qquad (10)$$

where
$$i = 1, 2, \dots, \frac{m}{16}, j = 1, 2, \dots, \frac{n}{16}, k = 1, 2, 3, \dots, p \times q$$

The word s refers to quantization step value, and W(k) refers to extracted watermark sequences.

Step3 The watermark sequences which are extracted carry on chaotically decryption. Then it can be transformed into a binary image.

Here we use the normalized correlation (NC) to measure Here we use the normalized correlation (NC) to measure the similarity between original image W and the detected watermark image W' [6].

$$NC = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} W(i, j) . W^{1}(i, j)}{\sum_{i=1}^{n} \sum_{j=1}^{n} W(i, j) . W(i, j)}$$
(11)

In order to get rid of the impact of subjective factor, this paper adopts peak signal-to-noise ratio (PSNR) to measure the fidelity between the original image and the image which watermark is embedded.

VII PEAK TO SIGNAL NOISE RATIO:

Peak Signal to noise ratio (PSNR) is one of the Performance measure of the proposed method [6] and is calculated as follows

$$PSNR = 10\log 10 \left(\frac{A^2}{\frac{1}{M*N} \sum_{i=1}^{N} \left[f(i,j) - f^1(i,j) \right]^2} \right)$$



Fig. (4) Graphical representation of PSNR vs. Normalized coefficient

From the graph we can observe a plot is made between PSNR and Normalized Coefficient(NC).asPSNRincreases the NC also increases because both the linearly related **Table: 1 Comparison of PSNR values with standard**

value in db

Host image		Data set	Data set	Data
		1	2	set 3
Method				
		jpg	tiff	bmp
Proposeds	8X8	39.24	37.397	34.399
ystem				
Shereen et al.		41.25	41.2612	41.27
H.Song et al		35.25	36.65	34.98

THE TABULAR COLUMNS GIVES VALUES OF PSNR OF 8*8 PIXEL OF DIFFERENT IMAGE TYPES

VIII SIMULATION RESULTS:



"Fig. (5) Cover Image"



"Fig. (6) MSB of cover

Image"





"Fig. (7) Watermark image"

"Fig. (8) Watermarked







"Fig. (9) MSB of watermark ""Fig. (10) MSB of

Watermarked image"



"Fig.(11) shifted watermark " "Fig.(12) LSB

combined with MSB of watermark"



"Fig.(13) LSB of cover image" "Fig.(14) LSB extracted"





"Fig.(15) predicted watermark" "Fig.(16) Regenerated

cover image"

Table: PSNR Value comparison between HT-DWT-TGf

Host	Data	Data set	Data	Data
Image	set 1	2	set 3	set 4
Metho				
	Bmp	Jpg	Tiff	Grey
	16*16	16*16	16*16	
UT				
	25.5	26.7	27.6	22.5
IGF				
DWT	21.0	23.0	19.1	17.9

The tabular column gives PSNR values comparing between HT-DWT-TGF and DWT FOR different types of image types.

TABLE: NORMALIZED COEFFICIENT VALUECOMPARISON BETWEEN HT-DWT-TGF AND DWT

Host Image	Data	Data	Data	Data
Method	set 1	set 2	set 3	set 4
	Bmp	Jpg	Tiff	Grey
	16*16	16*16	16*16	
HT-DWT- TGF	0.29	0.88	0.17	0.83
DWT	0.05	0.06	0.24	0.59

The tabular column gives NC values comparing between HT-DWT-TGF and DWT FOR different types of image

IX CONCLUSIONS

The essential conclusion that comes from the proposed technique is the high robustness to (almost) attacks that may be implemented by media forgers. In most of the attacks, the hidden watermark could be always extracted either complete or incomplete, i.e. there is always a recognizable watermark. The proposed technique may be embedded into image, video, or audio. Another important conclusion is that, the proposed fading technique produces an exact (100%) extracted watermark when rotation with (45, 90, 180, 270, 360) degrees. As a future step, the proposed technique could be embedded into video and audio watermarking. According to the experimental results and high error metrics, the novel proposed fading technique proven that it is very simple and robust against multiple attacks. Furthermore, the novel technique is the first of its type that embed a watermark that has the same dimensions with the original cover image. It must be mentioned that the payload of the proposed technique is high, i.e. the embedded watermark does not affect the size (in Kilobytes) of the cover image.

X REFERENCES

[1] I.J.Cox, J.Kilian, F.T.Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multimedia", IEEE Trans. Image Processing, vol .6, pp. 1673-1687, December 1997.

[2] G.Langelaarand, R.Lagendijk, "Optimal differential energy watermarking of DCT encoded images and video", IEEE Trans., vol .10,pp.148-158,January 2001.

[3] J.W.Huang, Yun Q.SHI, W.D.Cheng, "Image watermarking in DCT: an embedding strategy and algorithm", Journal of Electronic, vol .28,pp.57-60, April 2000

[4] Z.M.Zhang, L.Wang, "Semiblind image watermarking algorithm in DCT domain with chaotic encryption", Computer Engineering, vol.29,pp. 9-11, October 2003.

[5] Pankaj U.Lande, Sanjay N.Talbar., "FPGA
 Implementation of Adaptive Watermarking Using
 Human Visual Model", ICGST-PDCS Journal,
 vol.9, pp. 17-21, January 2009

[6] L.C.Li, Z.Y.Lu, "Desynchronization attack on digital watermarks and their counte measures," Journal of image and graphics, vol .10,pp.403-409, October 2005.

[8] F. Hartung, B. Girod, Watermarking of uncompressed and compressed video, Signal Process. 66(3) (1998) 283–301.

[9] C.W. Tang, H.M. Hang, A feature-based robust digital image watermarking scheme, IEEE Trans. Signal. Process

[10]C.W. Tang, H.M. Hang, A feature-based robust digital image watermarking scheme, IEEE Trans. Signal.Process.