Improved watermarking scheme based on Red channel selection using discrete slantlet transform (DST)

Asst. Lect. Myasar Mundher Adnan
Islamic University College

***Abstract*— this paper is allocated to digital watermarking is created as a method to solve this kind of problems. There are two issues which are embedded watermark image in the host image without causing any kind of degradation, achieve and improve both imperceptibility and robustness of watermarked image before and after attacks. Digital watermarking is a process to embed the secret information into digital data for verifying identity of the owners by making assertion about the data and image authentication applications that provide security to watermark, W which is converted to a sequence of random binary R of size n adopted to encrypt the watermark. The adaptation process uses a pseudo-random number generator to determine the pixel to be used on a given key. In this paper, The RGB colour image watermarking is proposed using by Discrete Slantlet Transform (DST) to generate higher degree of robustness and imperceptibility of watermarked image. After applying 2-level DST on the host image to Red channel. The experimental results show that the proposed approach provides extra imperceptibility, robustness and security against JPEG compression and different noises attacks compared to the previous methods.**

***Index Terms*— Watermarking, R channel, Discrete Slantlet Transform (DST) technique**

1) INTRODUCTION

Nowadays, most of the transactions and operations have been done in the digital form due to the rapid growth of internet. With the speeding evolution of technology, multimedia applications field and distribution of multimedia contents are getting more advanced. Multimedia data has become less protected in this digital world. With this continued rise of sharing internet, everybody could access these digital data easily through internet and may use them without permission from original owner. Many copyright violations happened recently. Thus, owners need to protect their media contents from theft, reproduction and bad representation. Digital watermarking is a solution to this kind of problems and help to protect the copyright of multimedia data or bad representation.

watermarking technique is very useful in our digital life. The research motivation is the widely uses of watermarking to avoid illegal duplication of digital data without the consent of original owner by hiding the watermark in the digital data as a token of ownership. Since there are possible intelligent attacker performed various attacks on the images to remove the watermark for using them unauthorized, thus this study is conducted to improve the imperceptibility and robustness of watermarked image which resists various possible attacks. Further investigation will be carried out to study the possibility to using Discrete Wavelet Transform (DWT) and Discrete Slantlet Transform (DST) to improve the imperceptibility and robustness of image watermarked. .

2) PROBLEM BACKGROUND

In internet-related life today, it is getting more difficult to prevent the copyright infringement of digital data. Everybody could access them and even use them for their personal purpose. This behavior is actually violating the copyright and content authentication. Many users abused these contents by forgery and piracy. Therefore, the digital watermarking methods have been identified as a possible solution to the copyright protection, and have become an area of increased research activity over the last decade (Gang Liu, 2010). There are two issues need to be concerned with

1) How to embed watermark image in the host image without causing any kind of degradation?
2) How to achieve and improve both imperceptibility and robustness of watermarked image before and after attacks?

3) RESEARCH METHODOLOGY

In this paper, RGB colour image watermarking using Discrete Slantlet Transform (DST) is proposed to generate higher degree of robustness and imperceptibility of watermarked image. Generally, the proposed technique involved four main phases, namely pre-processing, embedding, attack mechanism and extraction. These stages are implemented incorporate aspects of HVS in order to produce higher quality of watermarked image. The major purpose of pre-processing stage is

finding the best quadrant of RGB host image in red channel host image for embedding the watermark.

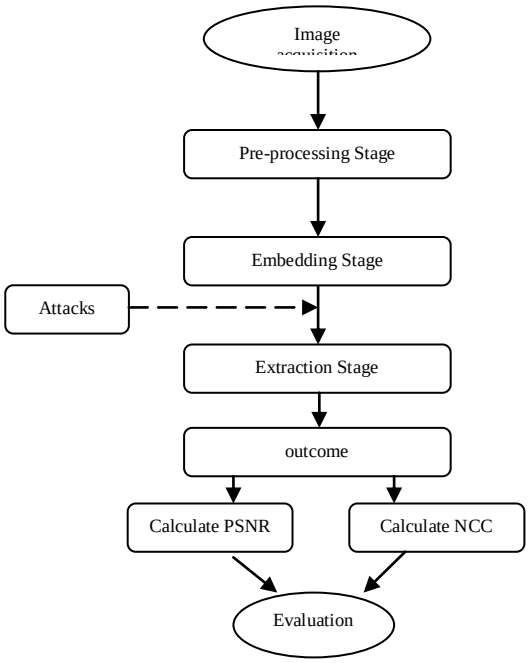


Figure (1): General stage of digital watermarking

3.1) PRE-PROCESSING STAGE

The pre-processing stage is RGB colour image which is used as cover image and the output is a secret key contains best quadrant of host image. This stage includes the steps like image partitioning which illustrate pre-processing stage of the watermarking technique as shown in Figure2. The following figure shows the five stages of reading the RGB which begin by starting step and then reading the RGB image, the second step is dividing the selected channel into four parts and selected the low frequency sub-bands for embedding and terminate from there.

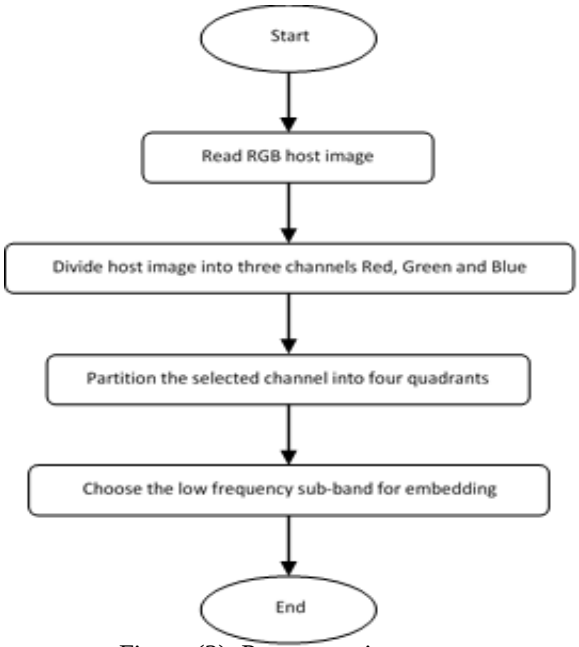
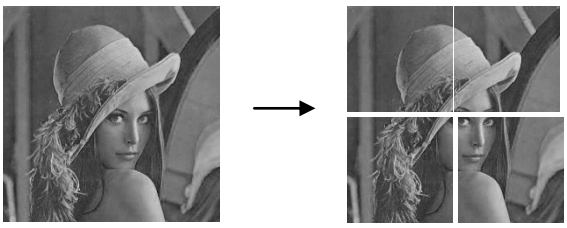


Figure (2): Pre-processing stage



Host image before partitioning after partitioning

Figure (3). Partitioning of the selected channel

3.2) EMBEDDING STAGE

The Figure 3 below shows the stage of embedding of watermarking technique and the section that follows describes the details of the stages. The process of embedding stage describes in the figure below has nine steps ,the first is the starting stage, followed by applying DST on the chosen channel for the image. The sub-bands frequency was evaluated. Once the sub-bands frequency is evaluated the embedded watermark parts chosen into the best selected sub-bands. Applying Inverse Discrete Slantlet Transform (IDST) on selected quadrant is the next process in order to get the watermarked image to merge all quadrants.

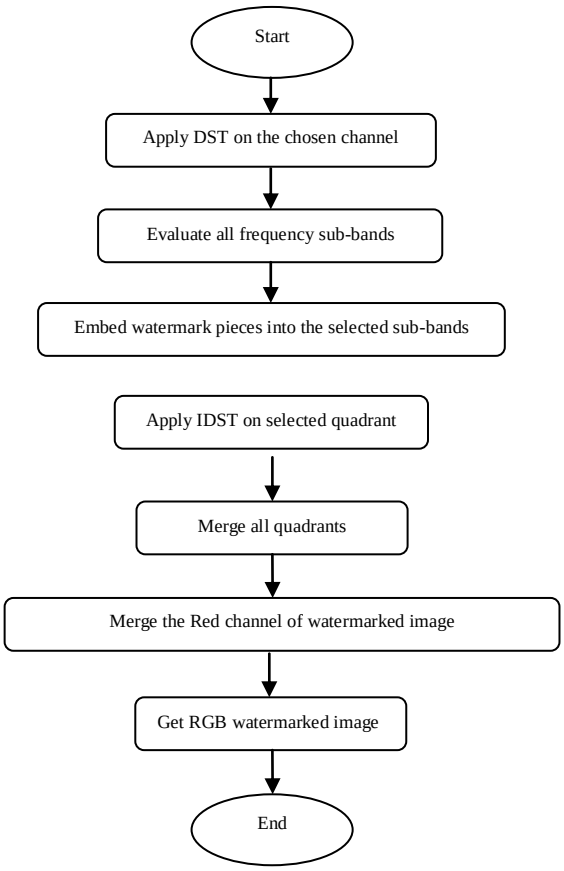


Figure (3): Embedding stage

3.2.1) APPLYING DST

In this watermarking technique DST, a gray scale image as watermark image is being hidden in host image. The embedding stage was used selected best quadrant as input.

3.2.2) EMBEDDING WATERMARK PIECES

The major purpose of partitioning watermark into four pieces before embedding in cover image is to embed the watermarked. The pixel of each watermark quadrant is transformed to bit stream into a sequence Y_i to Y_n, where *n* is the length of the bit stream. To obtain the watermark image, the perform embedding by modifying DST coefficients Intended to obtain higher robustness of watermarked image, watermark pieces are respectively embedded in the low frequency sub-band (LL) by using the following formula:

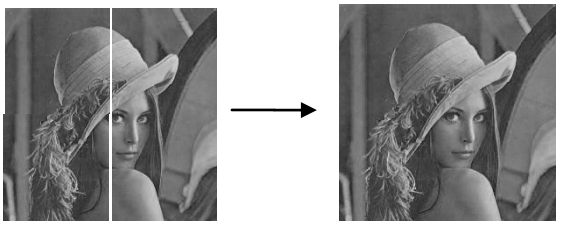
$$W_i^{'} = W_i + \alpha Y_i \quad (1)$$

Where:

$W_i^{'}$ = The Watermarked image.
W_i =The Coefficients of partitioned original image.
Y_i = The Watermark image bit (-1's or 1's).
a =The Alpha, the strength of the watermark.

3.2.3)APPLYING IDST

After embedding has been done, assemble all the frequency sub-bands by applying IDST to inverse the frequency based quadrant to regain spatial domain quadrant. This step is to reconstruct all sub-bands in the selected quadrant using inverse steps of DST [19]. A quadrant of watermarked image will be the output after IDST process. The quadrant of watermarked image is then combined with the other three quadrants to generate a watermarked image as new B channel. The following Figure 4 illustrates the merging of all quadrants.



Four quadrants of image — new channel of watermarked image

Figure (4): Merging of all quadrants

4) IMPERCEPTIBILITY MEASURING

To measure the quality between the original image and the watermarked use Peak signal to noise ratio (PSNR) Peak signal to noise ratio (PSNR) used to measure the quality between original and watermarked image, increasing PSNR related to the quality of reconstructed watermarked image. The following is PSNR formula[15].

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

Where, m n is the image size of watermark and host image, I (i , j) is the Host image pixel value, K (i , j) is the Watermark image pixel value, MSE is Mean Square Error for (I , K).

4.Robustness Measuring

The similarity between the original and extracted watermark can be measured as follows equation 3.

$$NCC = \frac{\sum_x \sum_y (W_{xy} \times W'_{xy})}{\sum_x \sum_y (W_{xy})^2} \quad (3)$$

Where, W i j and W ' i j are the pixel values at the position (i, j) of the original and the extracted watermark by that $1 \leq (i, j) \leq 32$, respectively.

5) RESULT AND DISCUSSION

In proposed technique a watermark embedded in the cover image using discrete slantlet transform, The evaluation of these results presented in this paper by using standard images which are Lena as a host images as shown in Figure 5 The watermark image that used for embedding is a gray scale image namely UTM logo. There are two type of measurement were done which are PSNR and NCC for the purpose of evaluating the performance of the watermarking technique. perform experiments. In the experiments, the research will embed the digital watermarks in the frequency domain of still images. Then, evaluate the degradation in image quality caused by the insertion of a watermark. NCC value is also calculated to measure the robustness of watermarked image before and after attacks. Experimental results are summarized in regard to the PSNR value of each watermarked image and the bit error of the watermark extracted from attacked images. The minimum value for PSNR should not be less than 30 for perceptual fidelity according to (Chin et al., 2007).

Figure (5): Lena original image

6) IMPLEMENTATION OF RESULT

In this paper, we reached that the original image and watermarked image is quite similar such that we are unable to differentiate them with regular eyes. Embedding watermark image in the host image without causing any kind of degradation and able to extract from watermarked image as Figure 6.


Original image


Watermarked image

Figure (6): Lena original image and watermarked image

Figure (7). Embedded watermark image

6.1) IMPERCEPTIBILITY TESTING

The evaluation used PSNR to measure the quality ratio between the signal of original host image and watermark image [9]. The output of imperceptibility testing is a value in decibel scale. The Equation (3) of PSNR calculation.
The MAX is the maximum possible pixel value of the image. The equation shows the MAX value is 255 where the pixels are represented using 8 bits plane.

$$MAX = 2^8 - 1 = 255 \quad (4)$$

MSE is the mean squared error for gray scale images I and K which is defined as:

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left[(I_{ij} - K_{ij}) \right]^2 \quad (5)$$

Where
m x n = Size of original host image and watermarked image
I_{ij} = Pixel value of original host image
K_{ij}= Pixel value of watermarked image

Larger PSNR value will indicate that higher quality of the watermarked image. Normally the PSNR value must exceed 30dB such that it will prove the good quality of watermarking technique which is pointed out by Xiaojun (2004).

6.2) IMPLEMENTATION

The watermark image used for embedding is a gray scale image known as UTM logo and to evaluate the proposed algorithm software method. Figure 8 show the main interface of the software.


Original image


Red channel


Applying DST


Watermarked

Figure (8). Sample results of PSNR

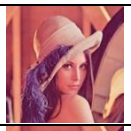
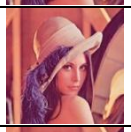
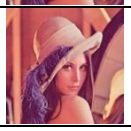
Channel	Selected part	Watermarked Image	PSNR(db)
Red	LL2		45.32
Red	LL3		41.51
Red	LL4		43.32

Figure (8). Value of PSNR

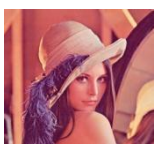
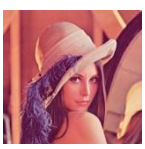
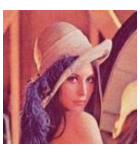
	Original image	Watermarked before attack	Watermarked after attack
Lena			

Table (1): Dataset images by applying Poisson noise attack

	Original image	Watermarked before attack	Watermarked after attack
Lena			

Table (2): Dataset images by applying Salt and Pepper attack

Attack	Before Attack		After Attack	
	Extracted Watermark	NCC	Extracted Watermark	NCC
Poisson		1		0.6500
Salt and Pepper		1		0.9660

Table (3): NCC result of Lena image

7) CONCLUSION

This paper introduces a digital watermark algorithm based on discrete slantlet transform (DST) technique a watermark embedded in the cover image, and convert to Red channel. Then applying 2-level DST on this channel for embedding. The results prove the red channel is good based on Figure (8) for embed evaluate by using peak signal noise ratio (PSNR). The experimental results revealed that the PSNR and NCC values were greater than 30db and 0.6 respectively, which was considered very encouraging. The strategy helps in developing imperceptibility and robustness at the same time. This paper method proved its imperceptibility is acceptable and its robustness against the attacks. In addition, the watermark embedded, as the busiest of the areas are less sensitive to human visual system.

8) REFERENCES

1-Ahire, V. K. and Kshirsagar, V. (2011). Robust Watermarking Scheme Based on Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images. IJCSNS International Journal of Computer Science and Network Security. 11 (8), 208-213.

2- Al-Haj, A. (2007). Combined DWT-DCT Digital Image Watermarking. Journal of Computer Science 3 (9), 740-746

3- Al-Otum, H. M., Samara, N. A.(2010). A robust blind color image watermarking based onwavelet-tree bit host difference selection. Signal Processing 90 (8), 2498-2512.

4- Ali, A. and Ahmad, M and Lama, B. (2011). DWT-Based Audio Watermarking. *IAJIT Journal*.(8), 326-333

5- Anthony, T.S.H., Shen, J., Tan, S.H. and Kot, A.C.(2002). Digital image-in-image watermarking for copyright protection of satellite images using the fast hadamard transform. IEEE International Geoscience and Remote Sensing Symposium, 6 (25), 3311-3313.

6- Baithoon, N. Y. (2011). Combined DWT and DCT Image Compression Using Sliding RLE Technique. *Baghdad Science Journal*. 8 (3), 238-238.

7- Bas, P. Chassery, J. M. and Macq, B.(2004). Image watermarking : *An evolution to content based approaches* . Neuve: Belgium.

8- Bauschke, H. H. (2003). Recompression of JPEG images by requantization. Image Processing, IEEE Transactions on image processing. 12 (7), 843-849.

9- Bender, W., D. Gruhl, M., N. and Lu, A. (1996). *Techniques for data hiding. IBM Systems Journal*, 35, 3-4.

10- Berghel, H. (1998). Digital watermarking makes it mark Networker: The craft of network computing, 2 (4), 30-39. Basu, D., Sinharay, A. and Barat, S. (2010).

11-Bit Plane Index Based Fragile Watermarking Scheme for Authenticating Color Image. *ICIIC '10 Proceedings of the First International Conference on Integrated Intelligent Computing*, 136-139.

12- Bloom, J. M. (1999). Revolution by the Ream: A History of Paper. *Saudi Aramco World*. 26-39.

13- Chaelynne M. W. (2001). Digital Watermarking. School of Computer and Information Sciences : Nova Southeastern University.

14- Chai, D. and Bouzerdoum. A. (2000). A Bayesian Approach to Skin Classification in YCbCr Color Space. IEEE. School of Engineering and Mathematics Edith Cowan University Perth, Australia.

15- Chin, C. C., Yung. C. C. and Tzu, C. L. (2007). A Semi-blind Watermarking Based on Discrete Wavelet Transform. Proceddings of 9th International Conference Information and Communications Security, Zheng zhou, China, 164-176.

16-Cox, I. J. and kalker, T.(2004). Digital Watermarking. Third international workshop, IWDW, UK.

17- Cox, I.J., Miller, Bloom, M.L.A., Fridrich, J. and Kalker, T.(2008). Digital watermarking and steganography, second edition, Morgan Kaufmann publishers.

18- Myasar Mundher, Dzulkifli Muhamad,elc B.B.(2014). Digital Watermarking for Images Security using Discrete Slantlet Transform. Applied Mathematics & Information Sciences.

Ass. Lec.: Myasar mundher adnan, Bachelor of computer science from Kufa University / Iraq in 2010. In addition, holds a master's degree in computer science from UTM in 2014. Assistant Lecturer at Islamic University College - Iraq