

Design and Development of Text-Image Watermarking Based on Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT)

PhD Scholar Arpana Bhandari

Rabindranath Tagore
University Bhopal, India
arpanabhandari08@gmail.com

Associate Professor Dr. Shailja Shukla

Rabindranath Tagore
University Bhopal, India
shailja@gmail.com

Professor Dr. Rajiv Shrivastava

SIRTE BHOPAL
rajiv@gmail.com

Asst. Professor Dr. Vijay Bhandari

Dept. CSE
SIRTE
vijaysirt@gmail.com

Abstract - This paper investigates Text-images still has a great importance, despite the spread of electronic texts. Text-images are protected using digital watermarking. This paper proposes a watermarking method applied to text images. This method integrates two transforms: integer wavelet transforms (IWT) and discrete cosine transforms (DCT). For the watermark embedding, IWT is performed on the cover image and DCT is applied to the low frequency sub-band LL. The watermark image is inserted in the lower to medium DCT coefficients to achieve a high degree of robustness and imperceptibility. Experiments using different English text-images are performed to evaluate the proposed method in terms of imperceptibility and robustness. Results show that the proposed method has higher imperceptibility compared to other existing methods applied to English text-images. Also, the proposed method provides good robustness results, especially against compression and noise..

Keywords - Quantization, Transformation, MSE, PSNR, NAE, DCT.

I. INTRODUCTION

With the rapid development of electronic communication technologies, it has become easy to access and share information, and as a result, online piracy has spread. Textual information is the most widely used in comparison to images, audio and video. It represents the easiest way to translate speech. It is the main component of publications and contributes greatly to the educational process. Text-images are no less important than electronic text. They are still in use in official transactions and some authors publish their books as a text-image. However, text-images face some issues related to the protection of intellectual rights and unauthorized use. Watermarking technology is used to solve these issues. Using digital watermarking technology depends on stashing data in a digital media. The media may be an image, text, video or audio. The stashed data called a watermark, the watermark describes the information regarding the owner of the digital media. The watermarking method may be visible like logos or invisible. In invisible watermarking, the watermark is embedded or stashed in the cover media in a way that the human eyes cannot noticed the embedded watermark [1]. Two basic stages of any watermarking method: embedding and extraction processes. The basic watermarking requirements are robustness,

imperceptibility, security and capacity [2]. The watermarking method which is resistant against attacks is called a robust method. Otherwise, it is called a fragile method. Imperceptibility means that the watermark does not affect the value of the media or causes distortion. The watermarked media must look like the cover or original media. Security includes keeping the watermark, embedding and extraction processes secure. Capacity is the amount of embedded data compared to the cover media. Text-image watermarking has many challenges and difficulties. The text-image has a little information redundancy for watermark embedding compared to general images. Normal or general images contain a lot of details that can be exploited for watermark insertion without notice by the human eye. However, text images have a difference or contrast between the background and the typed text. Simple changes in a text-image can be noticed because it has a clear separation between foreground and background. Text-image watermarking methods are classified based on the domain into spatial and transform methods [4]. Spatial domain methods add watermark bits by directly changing the pixels values in the image while watermarking methods based on transform modify the coefficients of the transform.

Currently, text-image watermarking based on the spatial domain are not resistant enough to lossy image compression and other image processing operations

[5,6]. Some of these methods require high complexity or font size/style dependency. Recently, watermarking text image is done in transform domain because of its huge robustness compared to spatial domain methods. Not all methods applied to the general images could be performed on the text-images. The text image needs a watermarking method which satisfies the imperceptibility requirement and balanced with the robustness at the same time. The problem is how to embed watermark bits into the text image without noticeable degradation and satisfy high robustness against possible attacks in the frequency domain with the contribution of using the combination of two transforms IWT and DCT. Discrete Wavelet Transform (DWT) watermarking methods provide high imperceptibility because DWT transform is compatible with the Human Visual System (HVS) [6]. It means that the human eye is less sensitive to changes in the image (the inserted watermark). Integer wavelet transform (IWT) watermarking can exploit the characteristics of DWT with more advantages. IWT is much faster because it deals only with integers. The image can be reconstructed without any loss using IWT and can be stored without rounding off the errors [7]. Discrete cosine transform (DCT) watermarking methods are more robust than spatial domain watermarking methods [5]. DCT watermarking methods have high robustness against compression and image processing. Also, it is a fast transform. So, the using of IWT and DCT is suitable for text-image watermarking. This combination is used to achieve acceptable results of robustness and imperceptibility. The embedding is done in the lower frequency coefficients to increase the robustness. The LL sub-band (low frequency sub band) is selected after applying IWT which has the lower frequencies. The lower to medium coefficients are taken after applying DCT. In the experiments, four different numbers of coefficients are tested to find the relationship between the number of coefficients and imperceptibility and robustness. The rest of the paper is organized as follows: Section 2 discusses the related methods towards text-image watermarking. Section 3 presents an overview of the used transforms in the proposed watermarking method. The proposed method is discussed in Section 4 with its embedding and extraction processes. Section 5 presents conclusion. Structure of the paper consists of introduction, related work, proposed work, comparing results based on different parameters and conclusion.

II. EXISTING WORK

In this section, watermarking methods which performed on text-image will be discussed and compared. Text-image watermarking methods in the spatial domain are presented first, then watermarking methods which are performed in the transform domain.

• Spatial domain text-image watermarking

Ang and Kot [8] proposed a blind watermarking method in the Latin text-image by integrating spaces between characters and word space. The watermark is embedded by shifting the character into right or left to denote “0” or “1” using overlapping window.

The watermarking method is implemented in both blind and non-blind algorithms. This method suffers from low coding capacity. A new word shifting method based on word classification was developed in Ref. [10]. The words are classified depending on its width. A group of adjacent words composes a segment; the segments are classified based on word class information within each segment. The words are shifted left or right to encode the watermark data. This method has higher imperceptibility than traditional word shifting, since it shifts a small amount using the statistics. However, it consumes more time for calculations. Yang et al. [11] developed a blind watermarking method in binary text-images by flipping pixels. The binary image is divided into blocks of size 5 by 5. The overlapping window of size 3 is used to determine the ability of a pixel to flip.

This watermarking method consumes the time very much and needs lots of calculations. The authors in Ref. [12] also used the flipping of pixels to watermark binary text-image. They flip only the edge pixels of the connected components. The watermark is embedded in the outer boundary of a character using vertical and horizontal edges. The visible distortion is less than in Ref. [11] but, it decreases the capacity.

Kim and Oh [3] inserted the watermark in grayscale text images using edge direction histograms. They divide the image into sub-blocks, the first three blocks considered as mother blocks. The watermarking is done in the remaining blocks. Each block is used to encode one watermarking bit. The length of diagonal edge directions is modified and then compared to the lengths in mother blocks to extract the watermark. This algorithm is not robust against finalization attack. The principle of entropy is used in Ref. [13] to identify the suitable location of watermark embedding in the binary text-images. The image is divided into sub-blocks and the entropy is calculated for each block. Entropy variation is used to find smaller font size regions which have a higher occurrence in the document. The watermark is embedded in these regions as ASCII values of a small text. This method does not require anything else the watermarked image in the extraction phase. However, it has a lot of calculations. The researchers in Ref. [14] proposed a blind watermarking algorithm in binary text-images based on entropy. They reduced the complexity of the previous method [13] and enhance the imperceptibility. Watermark data is embedded in the central pixels of blocks having small fonts. Aslam and Alimgeer [15] developed a new entropy-based watermarking method in grayscale text images. They flipped the pixels which are in the small

size regions. Only the minimum pixel values are used after computing XOR of the desired blocks. This method overcomes the previous similar methods [13,14] in terms of capacity and imperceptibility. Little text-image watermarking researches [16–18] are done on Arabic and Persian images in the spatial domain. The authors in [16] proposed a watermarking method by shifting the points which are located above or under the Arabic/Persian letters. This method has a high capacity since most of their letters have points. Davarzani and Yaghmaie [17] changed the slope of the letters: to encode bit “1” and remain them the same to encode bit “0”. This method is easy to use and has higher capacity.

2.2 Transform domain text-image watermarking

A zero-watermarking method for text-images based on DCT is developed in Ref. [19]. The watermark is generated from the text-image using the lower frequency coefficient of each DCT block and logistic mapping. Then, the watermark is registered as the copyright of the text-image. This method provides very high imperceptibility since nothing added actually to the original image. However, the watermark is not only generated from the original image nor external image or text watermarks are used. It is robust against compression and noise but weak against mean filtering. Li and Wu [20] developed a watermarking method in binary text-images using both DWT and DFT. The feature vectors are obtained from the original image by firstly applying one level DWT then DFT to the lower.

III. PRELIMINARIES

Transforms are used to convert the original image from time to frequency domain and vice versa. Time (spatial) domain refers to the variation of the signal over time, while frequency domain refers to the distribution of the signal's energy over a range of frequencies [4]. Transforms do not change the image data, but represent it in another way suitable for some analysis. Image watermarking methods in transform domain are more robust than methods in spatial domain. They are also compatible with human visual system (HVS) [24]. Discrete cosine transform (DCT), and integer wavelet transform (IWT) are the used transforms in the proposed method. They are explained in the following subsections.

• Discrete cosine Transform (DCT)

DCT is a mathematical transform which converts the function from time domain into the frequency domain. It results with many coefficients: single direct current (DC) and a set of alternating currents (AC). Fig. 1 shows the DCT matrix bands in 8 * 8 block. Low frequency coefficients located in the upper left corner of DCT matrix. The coefficients in the middle are medium frequency coefficients. The coefficients in the lower right corner are high frequency coefficients [25]. The image $f(x,y)$ with size M by N in spatial domain

transformed into DCT domain using the following equation:

There is common mathematical statement for a 1D (N numbers items) DCT is explained by the subsequent mathematical statement shown in below eq no 1.

$$F(u) = \frac{1}{\sqrt{2N}} \sum_{i=0}^{N-1} A(i) \cos \left[\frac{\pi}{2N} u(2i+1) \right] f(i) \quad (1)$$

and the resultant inverse 1D DCT transmode is plain $F^{-1}(u)$, i.e.:

where

$$A(i) = \begin{cases} 1/\sqrt{2} & \text{for } i=0 \\ 1 & \text{otherwise} \end{cases} \quad (2)$$

The common mathematical statement for 2D (n by m picture) DCT is defined by the subsequent mathematical statement:

$$F(u,v) = \frac{1}{\sqrt{2N}} \frac{1}{\sqrt{2M}} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} A(i) A(j) \cos \left[\frac{\pi}{2N} u(2i+1) \right] \cos \left[\frac{\pi}{2M} v(2j+1) \right] f(i,j) \quad (3)$$

The resultant inverse 2D DCT transmode is simple $F^{-1}(u,v)$ as shown below eq. no. 4.

where

$$A(i) = \begin{cases} 1/\sqrt{2} & \text{for } i=0 \\ 1 & \text{otherwise} \end{cases} \quad (4)$$

$F(0,0)$ is the DC coefficient, which involves the most energy of the image. The high frequency coefficients represent the edge and detailed information of the image. The details are increased by moving to the bottom right [26]. Low frequency coefficients are modified in robust watermarking method, while in imperceptible watermarking method the high frequency coefficients are changed.

• Discrete wavelet transform (DWT)

DWT is a mathematical analytical method used to address signals for many applications. It captures both spatial and frequency image information. DWT is used widely in image watermarking and compression since it provides a good visual image. DWT decompose the image into one low frequency sub band (LL) and three high frequency sub bands (LH, HL, and HH). LL contains the most image information and this band is closer to the original image. LH represents the horizontal details, HL represents the vertical details and HH represents the diagonal details of the image. The

image is reconstructed from these sub bands using inverse DWT. The image also could be decomposed more than one time, LL decomposed into four sub band and so on [27]. The outputs of DWT are floating point coefficients. The rounding error of the coefficients may lead to data loss. Also, dealing with floating point numbers in the watermark embedding and extraction requires high computations. Integer wavelet transform (IWT) maps the original image into integer coefficients. It is implemented by modifying DWT using lifting scheme proposed by Sweden's [28]. It is faster, easier to invert and does not require auxiliary memory compared to DWT. Fig. 2 shows the difference between DWT and IWT applied to text-image.

IV. THE PROPOSED IWT-DCT BASED METHOD

The goal of this research work is to find a watermarking method for text-images using transforms. Watermarking using DCT provides high robustness against compression, especially JPEG. DWT watermarking has good imperceptibility, reconstruction and more compatible with HVS. IWT overcomes DWT, while it is faster and has no rounding errors (dealing only with integers). 4.1. Embedding process The cover image is decomposed into four sub-bands: LL, LH, HL and HH after applying IWT. The LL image is very close to the cover image which means that it contains the most energy and other bands contain the details. This is the first step to develop a robust watermarking method. Then DCT is applied to the LL sub-band and again taking the lowest coefficients. The numbers of the chosen coefficients in each DCT block are: 9, 16, 25 and 36. In the proposed IWT-DCT-9, the first 9 pixels in the watermark image are embedded in the 9 DCT coefficients (the first coefficient (DC) does not change) in the first block. The second 9 pixels in the watermark image are embedded in the 9 DCT coefficients (the first coefficient (DC) does not change) in the second block, and so on until the last DCT block in the LL sub-band. The proposed IWT-DCT-16, proposed IWT-DCT-25 and proposed IWT-DCT-36 follow the same procedure with changing the number of the chosen DCT coefficients. Fig. 3 shows the block diagram of the embedding process for the proposed IWT-DCT method. The embedding process follows the following steps:

Step 1: Perform one level IWT to the cover image A of size m by n. (LL; LH; HL; HH)IWT(A)

Step 2: Apply $8 * 8$ block DCT to LL sub-band which is of size $m/2 * n/2$ and take the coefficients from low to medium except the first coefficient DC. Each block has 64 coefficients. {DCb;ACb;1;ACb;2;...;ACb;N;...;ACb;63 = DCT(LL) for $b : 1 : B$

Where N is the number of the chosen coefficients per block and B is the number of $8 * 8$ DCT blocks which is calculated as:

$$B = m * n / 256$$

Step 3: Resize of the watermark image w to be of size $r * r$.

$$r = \lceil \sqrt{B * R} \rceil$$

step 4 Convert the watermark image w into a vector V of size $1 * r^2$

step 5 Embed the vector V which represents the watermark image in the chosen DCT coefficients from ACb,1 to ACb,N in each block using the following equation

$$AC'_{b,i} = AC_{b,i} + (a * V_i * b^{-1} * N \text{ for } i : 1 : N; b : 1 : B$$

Montage image means the image produced by ordering many small blocks to form a vibrant larger image. The purpose of Information hiding using montage images is new way of securing information so that the data can be send in a private and secure manner. The aim of this paper is to provide efficient and better embedding algorithm as compare to all related previous technique. The covert image is first divided into number of blocks called "Tiles" and then these tiles are placed on the single image called "TARGET image" which we are selecting from our database on some similarity measure with our covert image. We are creating our own database here to overcome the drawback of managing large database. To create a montage image we have to place each and every tiles of the covert image over the target image with the efficient embedding algorithm on the particular region. The embedding of the tiles should be in format. We are using a DCT algorithm for embedding.

It involves following steps:

First we take covert image divide into tiles, which will convert each tile image into a binary value through $16*16$ quantization then we prepare a form of covert value by combining all the value, then embed this covert value in the original image through $16*16$ quantization, after embedding we go through sender who will send information to receiver, at the other side receiver who will extract the covert value inverse algorithm it can see in figure 1.2.

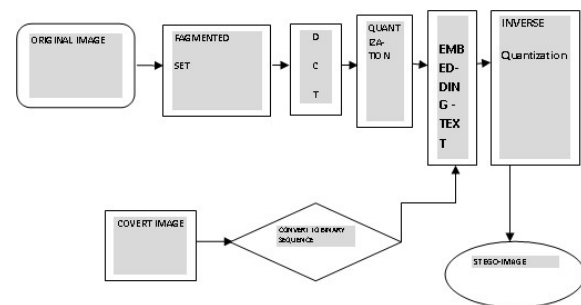


Fig.1. Outline of the Proposed Work.

- **Result analysis of Existing Work and Results analysis of proposed work**

Here Result can be seen in table 1.1 which have MSE,NSS,NAE,PSNR values.

No. of paniles	MSE	*NAE	NCC	PSNR
6	0.22	0.0017	1.0007	54.8
12	0.21	0.0018	1.0010	54.81
15	0.31	0.0016	1.0011	55.82
18	0.29	0.0019	1.0012	54.32
20	0.30	0.0020	1.0005	55.94

Table no. 1- Result analysis of Existing Work and Results analysis of proposed work

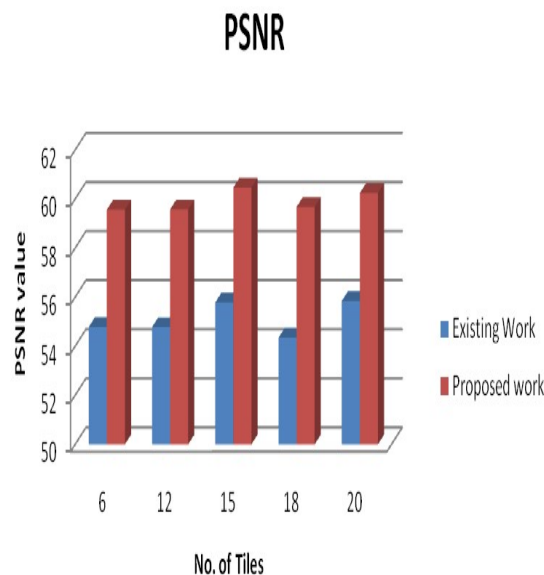
• Comparison Based on the Error Rate

Here comparison can be seen in table 1.2 which have error rates based on no. of tiles which have shown in table no. 1.2.

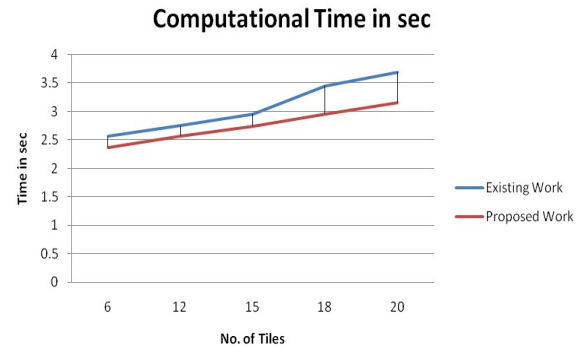


Fig.2. Comparative Analysis of Error Rate.

• Comparison Based on the computation Time



• Computation Time in Sec



V. CONCLUSION

The work that we proposed provides less compression time. This technique M-secure here provides a more efficient technique to authenticating the user to access the original image. By the different parameter we calculated here we find our proposed work is more efficient with Ya-Lin Lee. we have generated graphs and tables which is generated and tested through MATLAB.

REFERENCE

- [1]. Ching-Nung Yang et al.: Extended color visual cryptography for black and white covert image, Elsevier, Theoretical Computer Science, 2016, pp 143-161.
- [2]. Dawen Xu et al.: Separable and error-free reversible data hiding in encrypted images Elsevier 2016 ,pp 9-21.
- [3]. Moacir Ponti .: Image quantization as a dimensionality reduction procedure in color and texture feature extraction. Elsevier 2015,pp 1-12.
- [4]. Angel Rose et al.:A secure verifiable scheme for covert image sharing. Elsevier ,Second International Symposium on Computer Vision and the Internet 2015, pp 140 – 150.
- [5]. Tong Qiao .:Steganalysis of jsteg algorithm using hypothesis testing theory. Springer open journal EURASIP Journal on Information Security, 2015, pp 1-16.
- [6]. Chih-Wei ,Shiu, Yu-Chi Chen ,Wien Hong.: encrypted image-based reversible data hiding with public key cryptography from difference expansion. Published by Elsevier, 2015.
- [7]. Wen-Chung Kuoa,et al.: high capacity data hiding scheme based on multi-bit encoding function. Elsevier , 2015.
- [8]. Rina Mishra, et al. :An edge based image steganography with compression and encryption.IEEE 2015,International

- Conference on Computer, Communication and Control.
- [9]. Amrita manjreka.: A novel approach for data transmission technique through covert fragment visible montage image. in Springer ,Emerging Research in Computing, Information, Communication and Applications, 2015.
 - [10]. Edwina Alias T., Dominic Mathew.: Steganographic technique using secure adaptive pixel pair matching for embedding multiple data types in images. IEEE 2015 pp 426-429.
 - [11]. Rina Mishra et al.:A review on steganography and cryptograph. 2015 international conference on advances in computer engineering and applications” IEEE 2015.
 - [12]. Xingyu Li et al.: A complete color normalization approach to histo-pathology images using color cues computed from saturation-weighted statistics. 2015 IEEE.
 - [13]. Ya-Lin Lee et al.: A new secure image transmission technique via covert-fragment-visible montage images by nearly reversible color transformations. IEEE transactions on circuits and systems for video technology, vol. 24, NO. 4, APRIL 2014,Pp 695-704.
- Yicong Zhou, et al.:(n, k, p)-Gray Code for Image Systems. IEEE transactions on cybernetics, VOL. 43, NO. 2, APRIL 2013 pp 515-525.