



Original Article

Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)

Reem A. Alotaibi ^{a,b,*}, Lamiaa A. Elrefaei ^{a,c,1}^a Computer Science Department, Faculty of Computing & Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia^b Computer Science Department, Faculty of Computing & Information Technology, Taif University, Taif, Saudi Arabia^c Electrical Engineering Department, Faculty of Engineering at Shoubra, Benha University, Cairo, Egypt

ARTICLE INFO

Article history:

Received 4 March 2018

Revised 18 June 2018

Accepted 20 June 2018

Available online 23 June 2018

Keywords:

Watermarking

IWT

DCT

PSNR

ABSTRACT

Text-images still have 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 transform (IWT) and discrete cosine transform (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 Arabic 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 Arabic text-images. Also, the proposed method provides good robustness results, especially against compression and noise.

© 2018 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. 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 [3].

* Corresponding author at: King Abdulaziz University, Female Campus, Bulding No. 61 Room No. s109, P.O Box 80221, Jeddah 21589, Saudi Arabia.

E-mail addresses: reem.a.saffran@gmail.com (R.A. Alotaibi), laelrefaei@kau.edu.sa, lamiaa.alrefaai@feng.bu.edu.eg (L.A. Elrefaei).

¹ Postal address: King Abdulaziz University, Female Campus, Bulding No. 61 Room No. s109, P.O Box 80221, Jeddah 21589, Saudi Arabia.

Peer review under responsibility of King Saud University.



Production and hosting by Elsevier

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 this paper, a text-image watermarking method is proposed 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 the experimental setup. Section 6 reports the experimental results in terms of imperceptibility and robustness. Section 7 concludes the paper and highlights the future work.

2. Related 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.

2.1. Spatial domain text-image watermarking

Yang 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.

This window takes three characters each time along the line. The word space is the inter character space which is larger than the maximum space between two characters. This method achieved a high degree of transparency and improved the capacity compared to line shifting and word shifting. However, it is not robust against image attacks.

The researchers in Ref. [9] proposed a watermarking method by modifying the spaces between words in the text line. They founded that the average word spaces of multiple lines in the text-image represent a sine wave. The frequency, phase and amplitude of the sine waves used to encode the watermarking signal. 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 5×5 . The overlapping window of size 3×3 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 binarization 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: {و, ز, ذ} to encode bit “1” and remain them the same to encode bit “0”. This method is easy to use and has higher capacity

compared to line or word shifting. Another characteristic of these languages is the existence of curvaceous letters which is utilized in the watermarking process. The curvaceous letters {ح، خ، ج، چ} for watermarking are used in Ref. [18]. The researchers modified the curve of the letter with the baseline if the watermark bit is “1” and nothing is changed in case of bit “0”. This method is robust against resizing the text-image.

These methods [16–18] share the drawback of they are not robust to image attacks and require special font in the text-image.

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 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 frequency band of DWT. The sign of lower DFT-DCT coefficients to form the visual feature vector. The authors combined the feature vectors with the watermark to generate the key. The key is used in watermark extraction and authentication process. This method provides less robustness against compression and rotation attacks. The authors use the same principle, but instead of using DFT they use DCT in Ref. [21]. They found the same results with the previous one.

A watermarking method for sensitive text-image based on DCT is proposed in Ref. [22]. Linear interpolation of the watermark image and the original image is used to generate the watermarked image. This method uses a scaling parameter to specify the degree of visibility of the watermark. It is robust against compression and noise but weak against geometric attacks except rotation with 45.

The researchers in Ref. [23] proposed watermarking Technique of sensitive text-images based on SVD. The original image is decomposed into three components using SVD. The second component is interpolated with the watermark image in the watermark embedding process using linear interpolation. This method has good robustness and security. However, the inverse of SVD can result in information loss unlike to the inverse of DCT [22].

Tables 1 and 2 show a comparison of text-image watermarking methods in spatial and frequency domains respectively. Spatial methods are weak against most types of image attacks and restricted to certain font styles or sizes and some of them require complex calculations. While, transform methods showed immunity against attacks, but they poorly applied to the text-images.

We propose a text-image watermarking in the transform domain. The combination of IWT and DCT is used in the proposed method. 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. Overview of IWT and DCT transforms is presented in Section 3.

3. Preliminaries

Transforms are used to convert the original image from time to frequency domain and vice versa. Time (spatial) domain refers to

Table 1 Comparison of text-image watermarking methods in the spatial domain.

Author(s)	The used watermarking feature	Text-image	Advantages	Drawbacks
Huang and Yan (2001) [8]	Word space modification	English	Robust against interference	Low capacity
Kim et al. (2003) [9]	Words shifting	English	Blind watermarking High imperceptibility	Low capacity High complexity
Yang and Kot (2004) [10]	Word space modification	English	Blind watermarking More capacity than line and word shifting	Not robust against noise
Shirali-Shahreza and Shirali-Shahreza (2006) [16]	Points shifting	Persian Arabic	High capacity	Font dependency Not robust against image attacks
Davarzani and Yaghmaie (2009) [17]	Change the slope of {ز، ر، و}	Persian Arabic	Blind watermarking	Font dependency Not robust against image attacks
Yazdani et al. (2013) [18]	Change the curve of {ح، خ، ج، چ}	Persian Arabic	Blind watermarking Robust against resizing	Font dependency Not robust against image attacks
Yang et al. (2005) [11]	Pixel flipping	English	Blind watermarking High capacity	Time consuming
Tirandaz et al. (2009) [12]	Edge pixels flipping	English, Persian, Chinese	Blind watermarking High imperceptibility	Low robustness
Kim and Oh (2004) [3]	Modify edge direction histogram	Korean, Chinese, English	Applied in different languages	Not robust against binarization attack
Kurup et al. (2005) [13]	Entropy based	English	Blind watermarking	Time consuming Font size dependant
Khan et al. (2011) [14]	Entropy based	English	Blind watermarking Good visual quality	Font size dependant
Aslam and Alimgeer (2013) [15]	Entropy based	English	Blind watermarking Good visual quality	Font size dependant

Table 2 Comparison of text-image watermarking methods in the transform domain.

Author(s)	The used transform	Text-image	Advantages	Drawbacks
Laouamer and Tayan (2015) [22]	DCT	Arabic	Dynamic visibility	Semi blind watermarking Weak against geometric attacks
Feng and Huang (2012) [19]	DCT	Chinese	High imperceptibility	No external image watermark Weak against mean filtering
Li and Wa (2013) [20]	DWT and DFT	Chinese	High imperceptibility	Less robustness against compression and rotation attacks
Wa et al. (2015) [21]	DWT and DCT	Chinese	High imperceptibility	Less robustness against compression and rotation attacks
Laouamer and Tayan (2013) [23]	SVD	Arabic	Good robustness and security	Loss information in ISVD

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.

3.1. 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 × N in spatial domain transformed into DCT domain using the following equation:

$$F(u, v) = \frac{2}{\sqrt{MN}} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} f(x, y) \times \cos \left[\frac{\pi(2x + 1)u}{2N} \right] \cos \left[\frac{\pi(2y + 1)v}{2M} \right] \quad (1)$$

for u = 0, 1, ..., N - 1 and v = 0, 1, ..., M - 1, where

$$C(K) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{for } k = 0 \\ 1, & \text{otherwise} \end{cases} \quad (2)$$

The inverse DCT, which is used to convert the DCT image into the original one is computed as:

$$f(x, y) = \frac{2}{\sqrt{MN}} \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} C(u)C(v)F(u, v) \times \cos \left[\frac{\pi(2x + 1)u}{2N} \right] \cos \left[\frac{\pi(2y + 1)v}{2M} \right] \quad (3)$$

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.

DC	AC1	AC5	AC6				
AC2	AC4	AC7					
AC3	AC8						
AC9							
							AC63

Fig. 1. DCT coefficients matrix and frequency bands.

DCT is widely used in digital image watermarking because it is compatible with JPEG compression and its output is real matrix.

3.2. 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 represent 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 Sweldens [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.

4. 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 × n.

$$\{LL, LH, HL, HH\} = IWT(A) \quad (4)$$

Step 2: Apply 8 * 8 block DCT to LL sub-band which is of size $\frac{m}{2} \times \frac{n}{2}$ and take the coefficients from low to medium except the first coefficient DC. Each block has 64 coefficients.

$$\{DC_b, AC_{b,1}, AC_{b,2}, \dots, AC_{b,N}, \dots, AC_{b,63}\} = DCT(LL) \text{ for } b = 1 : B \quad (5)$$

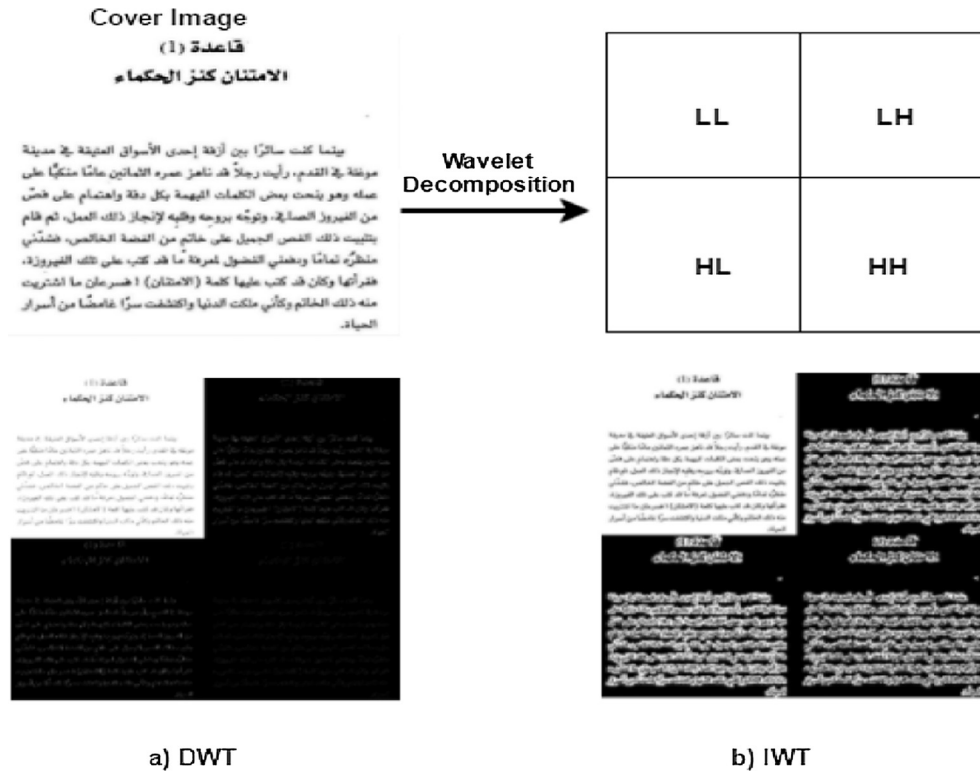


Fig. 2. Wavelet decomposition of cover image. (a) DWT and (b) IWT.

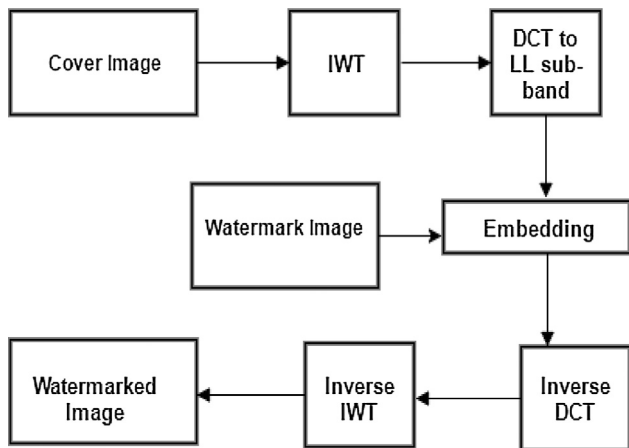


Fig. 3. Block diagram of the embedding process.

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:

$$B = \frac{m * n}{256} \quad (6)$$

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

$$r = \sqrt{B * N} \quad (7)$$

Step 4: Convert the watermark image w into a vector V of size $1 \times r^2$.

Step 5: Embed the vector V which represents the watermark image in the chosen DCT coefficients from $AC_{b,1}$ to $AC_{b,N}$ in each block using the following equation:

$$AC'_{b,i} = AC_{b,i} + (\alpha * V(i + (b - 1) * N)) \text{ for } i = 1 : N, b = 1 : B \quad (8)$$

where $AC_{b,i}$ is indicating to DCT coefficient, α indicates the scaling factor and V indicates the vector representing the watermark image.

Step 6: Inverse DCT (IDCT) to each block in the LL sub-band.

$$LL' = IDCT(\{DC_b, AC'_{b,1}, AC'_{b,2}, \dots, AC'_{b,N}, \dots, AC_{b,63}\}) \quad (9)$$

Step 7: Inverse IWT (IIWT) using the modified LL' sub-band and other bands: LH , HL and HH to get the watermarked image A_w .

$$A_w = IIWT(LL', LH, HL, HH) \quad (10)$$

4.2. Extraction process

The proposed IWT-DCT based method is a non-blind method because it needs the cover image in the extraction process. The extraction process includes IWT decomposition of the watermarked and cover images. Then, taking each LL sub-band of both. The DCT is applied and determine the number of coefficients as in the embedding process. Finally, inverse the equation to extract the watermark image. Fig. 4 illustrates the block diagram of the extraction process for the proposed IWT-DCT method.

The extraction process follows the following steps:

Step 1: Perform one level IWT to the cover image A of size $m \times n$.

$$[LL, LH, HL, HH] = IWT(A) \quad (11)$$

Step 2: Apply $8 * 8$ block DCT to LL sub-band and take the coefficients from low to medium except the first coefficient DC. Each block has 64 coefficients.

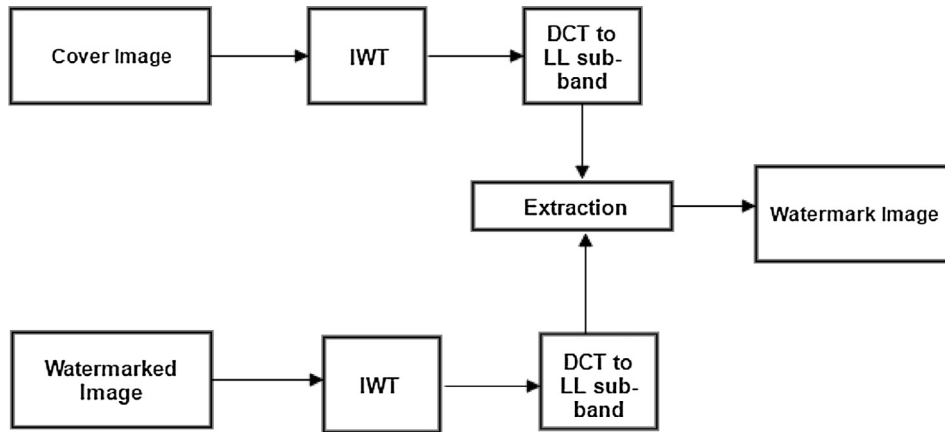


Fig. 4. Block diagram of the extraction process.



Fig. 5. GUI of watermarking text-image.

$$\{DC_b, AC_{b,1}, AC_{b,2}, \dots, AC_{b,N}, \dots, AC_{b,63}\} = DCT(LL) \text{ for } b = 1 : B \quad (12)$$

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:

$$B = \frac{m * n}{256} \quad (13)$$

Step 3: Perform one level IWT to the watermarked image A_w of size $m \times n$.

$$[LL', LH', HL', HH'] = IWT(A_w) \quad (14)$$

Step 4: Apply 8 * 8 block DCT to LL' sub-band and take the coefficients from low to medium except the first coefficient DC. Each block has 64 coefficients.

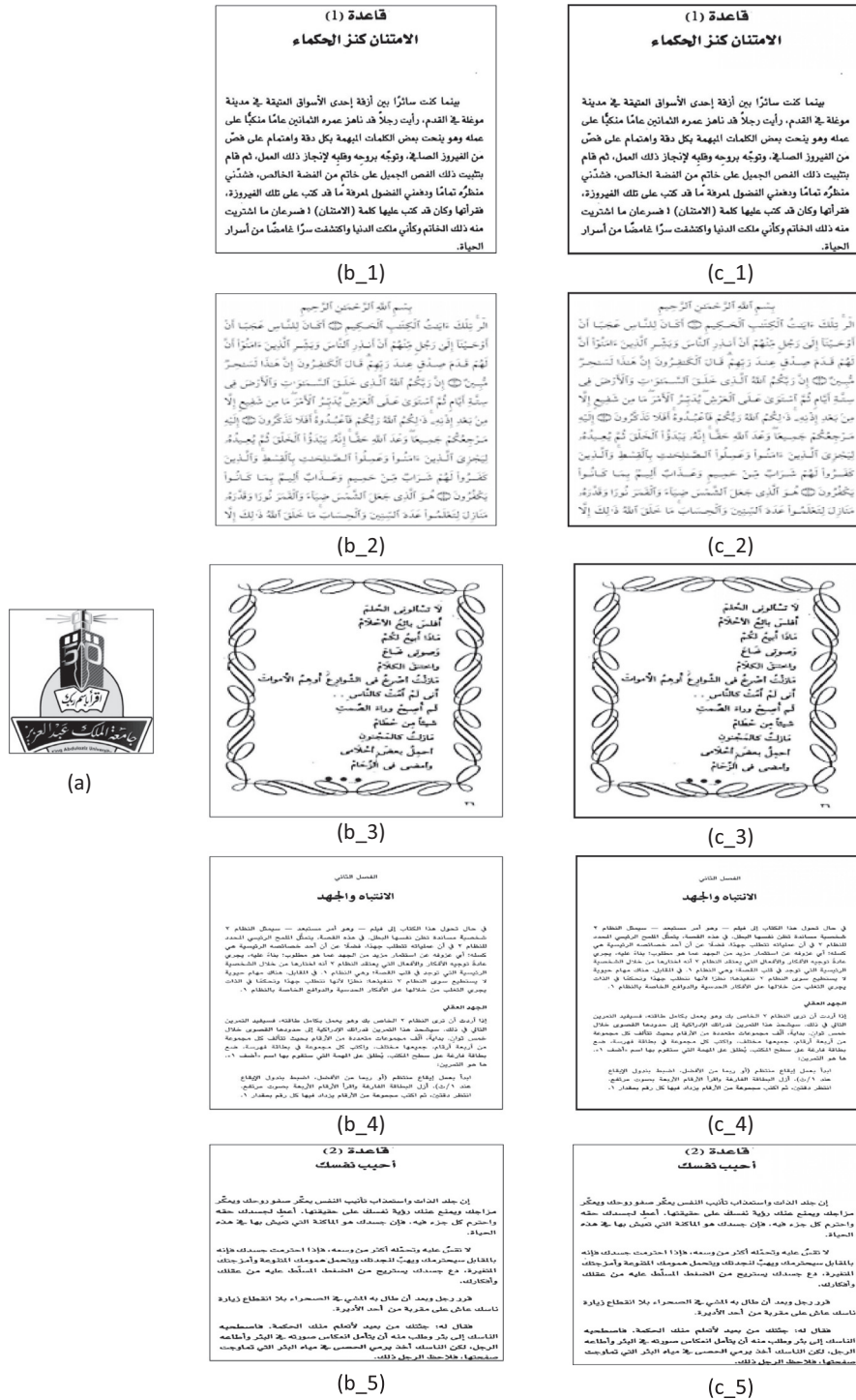


Fig. 6. (a) Watermark image, (b) Cover images, (c) Watermarked images.

$$\{DC'_b, AC'_{b,1}, AC'_{b,2}, \dots, AC'_{b,N}, \dots, AC'_{b,63}\} = DCT(LL') \text{ for } b = 1 : B \quad (15)$$

where N is the number of the chosen coefficients per block and B is the number of 8 * 8 DCT blocks.

Step 5: Extract the vector V which represents the watermark image by comparing the DCT coefficients from AC_{b,1} to AC_{b,N} from the cover image and the DCT coefficients from AC'_{b,1} to AC'_{b,N} from watermarked image using the following equation:

$$V(i + (b - 1) * N) = (AC'_{b,i} - AC_{b,i}) / \alpha \text{ for } i = 1 : N, b = 1 : B \quad (16)$$

The resulting vector V is with size of 1 × r², r² is calculated as:

$$r^2 = B * N \quad (17)$$

Step 6: Convert the vector V into watermark image w of size r × r.

Table 3
Description of image quality metrics.

Metrics	Equation	Description
Mean Squared Error (MSE) [30]	$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \sqrt{f(i,j) - f'(i,j)}$	Finds the error between original image $f(i, j)$ and watermarked image $f'(i, j)$ Both images of the same size [MxN]
Peak Signal to Noise Ratio (PSNR) [31]	$PSNR = 10 \log_{10} \left\{ \frac{255^2}{MSE} \right\}$	Measures the amount of noise in the distorted image
Universal Quality Index (UQI) [32]	$UQI = \frac{4\sigma_{xy}\mu_x\mu_y}{(\sigma_x + \sigma_y)(\mu_x + \mu_y)}$	Finds the distortion between two images based on distortions of correlation, luminance, and contrast, Where μ_x and μ_y are the averages of the original and distorted images respectively. σ_x and σ_y are the variances and σ_{xy} is the covariance
Structural Similarity Index (SSIM) [33]	$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$	Compares the structural information between original and distorted images Where c_1 and c_2 are constants
Normalized cross-correlation (NC) [34]	$NC = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [f(i,j) - \mu_f][f'(i,j) - \mu_{f'}]}{\sqrt{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [f(i,j) - \mu_f]^2} \sqrt{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [f'(i,j) - \mu_{f'}]^2}}$	Measures the similarity between two images $f(i, j)$ and $f'(i, j)$. Where μ_f and $\mu_{f'}$ are the averages of the original and distorted images respectively

Table 4
Imperceptibility results of the proposed IWT-DCT method.

Test Image	No. of bits	Metrics				
		PSNR	SSIM	MSE	NC	UQI
Test-image-1 Shown in Fig. 6 (b_1)	9	58.17	0.99	0.09	0.99	0.99
	16	57.99	0.99	0.09	0.99	0.99
	25	57.89	0.99	0.10	0.99	0.99
	36	57.45	0.99	0.11	0.99	0.99
Test-image-2 Shown in Fig. 6 (b_2)	9	58.55	0.99	0.08	0.99	0.99
	16	58.31	0.99	0.09	0.99	0.99
	25	58.19	0.99	0.09	0.99	0.99
	36	57.73	0.99	0.1	0.99	0.99
Test-image-3 Shown in Fig. 6 (b_3)	9	58.54	0.99	0.08	0.99	0.99
	16	58.29	0.99	0.09	0.99	0.99
	25	58.17	0.99	0.09	0.99	0.99
	36	57.71	0.99	0.1	0.99	0.99
Test-image-4 Shown in Fig. 6 (b_4)	9	57.93	0.99	0.1	0.99	0.99
	16	57.75	0.99	0.1	0.99	0.99
	25	57.71	0.99	0.1	0.99	0.99
	36	57.33	0.99	0.11	0.99	0.99
Test-image-5 Shown in Fig. 6 (b_5)	9	58.14	0.99	0.09	1	0.99
	16	57.94	0.99	0.1	1	0.99
	25	57.91	0.99	0.1	0.99	0.99
	36	57.51	0.99	0.11	1	0.99

The embedding and extraction processes of the proposed method are simple. IWT is applied to the cover image. Then, DCT is performed to the LL sub-band. The watermark image is embedded in the low to medium DCT coefficients. Inverse DCT followed by Inverse IWT to get the watermarked image.

For the extraction process, IWT is applied to the cover and watermarked images. Then, DCT is performed to the LL sub-band of both the cover and watermarked images. The watermark image is extracted by comparing the DCT coefficients from the cover and watermarked images.

5. Experimental setup

5.1. Studied images

The proposed IWT-DCT method has been implemented using Matlab (R2015a), Fig. 5 shows the GUI for our implementation. Five Arabic text-images with size of 512 × 512 are used as a cover image and the logo of KAU is used as a watermark image with different four sizes: 96 × 96, 128 × 128, 160 × 160 and 192 × 192. Using a logo as a watermark image has a good advantage where the extracted image can be correlated with the embedded one by a human observer [29]. Both of cover and watermark images are grayscale. These images are shown in Fig. 6. The value of alpha is set to 0.9 in the embedding and extraction processes.

5.2. Evaluation metrics

Experiments were performed to evaluate the proposed method in terms of imperceptibility and robustness. Some criteria are used to analyze the effect of embedding the watermark image in the cover image and to measure how much the watermarked image is resistant against attacks. These criteria are called image quality metrics. The most important criteria are Mean Squared Error (MSE) [30], Peak Signal to Noise Ratio (PSNR) [31], Universal Quality Index (UQI) [32], Structural Similarity Index (SSIM) [33] and Normalized cross-correlation (NC) [34]. They are described with their equations in Table 3.

6. Experimental results

6.1. Imperceptibility evaluation results

The embedding process applies to different five text-images which are shown in Fig. 6. The watermarked images preserve good visible quality as shown in Fig. 6. There is no visual distortion in the watermarked images. Table 4 shows the imperceptibility results of the proposed IWT-DCT method with a different number of the used bits. The greater number of the hidden bits, the less transparency, but with very few differences. For example

Table 5
Imperceptibility comparison results using averages PSNR.

Watermarking method	PSNR
Proposed IWT-DCT-9	58.17
Proposed IWT-DCT-16	57.99
Proposed IWT-DCT-25	57.89
Proposed IWT-DCT -36	57.45
IWT-SVD [34]	50.11
IWT-SVD [35]	43.67
DCT-DWT [36]	50.028
DWT-DCT [37]	36.52
DCT-SVD [38]	41.66
IWT-DCT [39]	45.09

IWT-DCT-9 is higher than IWT-SCT-36 because less coefficients are modified.

The imperceptibility of the proposed IWT-DCT method is about 58 dB as shown in Table 4 which is a high PSNR value. Fig. 6 shows the cover and watermarked images using the five text-images when the number of the taken coefficients is equal to 9. It is shown that no visual difference between the cover and watermarked images. Table 5 compares the imperceptibility results of the proposed IWT-DCT method with other methods: IWT-SVD [34], IWT-SVD [35], DCT-DWT [36], DWT-DCT [37], DCT-SVD [38] and IWT-DCT [39]. The averages of PSNR results of the five text-images are used in the comparison. IWT-SVD [34] used the combination of IWT and SVD. IWT is performed on the original image,

Table 6
Robustness results of the proposed IWT-DCT method against some attacks.

Attack type	Watermarked Image	Extracted watermark after attack			
		IWT-DCT-9	IWT-DCT-16	IWT-DCT-25	IWT-DCT -36
Without attack					
Histogram equalization		PSNR=57.97	PSNR=57.99	PSNR=57.83	PSNR=57.60
Median filter		PSNR=6.84	PSNR=8.77	PSNR=10.42	PSNR= 11.54
Salt & pepper noise 0.001		PSNR=35.54	PSNR=37.54	PSNR=39.06	PSNR= 40.30
		PSNR=39.82	PSNR=39.85	PSNR=39.72	PSNR=40.04

Table 7
Robustness results of the proposed IWT-DCT method against geometric attacks.

Geometric attack type	Watermarked Image	Extracted watermark after geometric attack			
		IWT-DCT-9	IWT-DCT-16	IWT-DCT-25	IWT-DCT-36
Scaling([512, 512] → [256, 256] → [512, 512])					
Scaling([512, 512] → [1024, 1024] → [512, 512])		PSNR=42.32	PSNR=40.45	PSNR=40.41	PSNR=40.48
Rotation (45°)		PSNR= 48.74	PSNR=52.42	PSNR=52.75	PSNR=52.78
Rotation (15°)		PSNR=14.76	PSNR=16.70	PSNR=18.18	PSNR=19.52
Cropping		PSNR= 13.40	PSNR= 15.12	PSNR= 16.65	PSNR= 18.05
Cropping		PSNR=57.97	PSNR= 57.99	PSNR=57.83	PSNR=57.60
		PSNR=18.03	PSNR=20.06	PSNR=21.66	PSNR= 22.97

If the number of authors on a reference is greater.

then SVD is applied in all sub-bands. The watermark image is embedded by modifying the singular values of LL, LH, HL, HH. IWT-SVD [35] also used IWT and SVD in addition to digital signature. DCT-DWT [36] applied DCT to the watermark image, then embedded it in the smooth sub-block of the high frequency DWT sub-band. The smoother sub-block is a sub-block which has a small value of entropy. DWT-DCT [37] decomposed the original image four level DWT followed by DCT. The watermark image is embedded in the coefficients of HL14 and LH24 sub-bands of DWT. DCT-SVD [38] performed DCT to the original image then applied SVD. The watermark is embedded in the middle DCT coefficients. In IWT-DCT [39], HH sub-bands of three levels of IWT are selected for embedding a binary image of size 32×32 into a cover image of size 512×512 . Integer cosine transform at 8×8 block level is performed on all selected HH3 sub-bands. The watermark bits are inserted by swapping specific DCT coefficients.

IWT watermarking has high imperceptibility as we see in IWT-SVD [34] from Table 5. DCT-DWT [36] also has high imperceptibility due to use of entropy to determine the suitable sub-block of DWT sub-band. Using multi-level IWT or DWT in DWT-DCT [37] and IWT-DCT [39] provides lower imperceptibility results compared to other methods as shown in Table 5. Also, these methods have higher complexity than the proposed IWT-DCT method

because of applying wavelet transform at multi-levels. It can be seen from Table 5 that the combination of the two transforms IWT-DCT in the proposed method gives the best results in terms of imperceptibility than others, even of these methods are used for watermarking general images not text-images.

6.2. Robustness evaluation results

Robustness is one of the most important ingredients of watermarking. The robustness of the proposed method was tested against many attacks using test-image-1 as shown in Tables 6 and 8. PSNR is used to measure the difference between original watermark image and extracted one. Common attacks like histogram equalization, scaling (enlarge or reduce), rotation, filtering, noise and JPEG compression are used in the robustness test. The robustness results of the proposed method with 9, 16, 25 and 36 DCT coefficients are convergent.

In general, the biggest coefficients used (9, 16, 25, 36) increased the robustness. IWT-DCT-36 has the highest robustness in most attacks except in compression, enlarge and noise, IWT-DCT-25 has the highest value. The averages of the five test-images are used to compare the proposed method with other methods from the literature. Fig. 7 shows the averages PSNR values of the proposed

Table 8 Robustness results of the proposed IWT-DCT method against JPEG compression attacks.

Quality factor	Watermarked Image	IWT-DCT-9	IWT-DCT-16	IWT-DCT-25	IWT-DCT-36
Q = 10		 PSNR=38.60	 PSNR= 39.34	 PSNR=39.67	 PSNR=39.48
Q = 25		 PSNR=44.47	 PSNR=44.47	 PSNR=44.65	 PSNR=44.45
Q = 50		 PSNR= 46.90	 PSNR= 46.91	 PSNR=47.12	 PSNR=46.77
Q = 75		 PSNR=46.31	 PSNR=47.31	 PSNR=47.90	 PSNR=47.52
Q = 90		 PSNR=50.62	 PSNR=51.69	 PSNR=51.10	 PSNR=50.51
Q = 100		 PSNR=53.06	 PSNR= 53.09	 PSNR=54.58	 PSNR=54.30

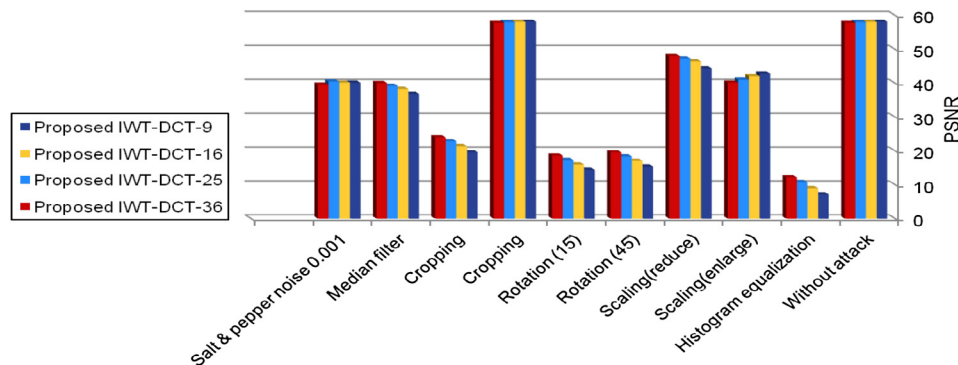


Fig. 7. The averages PSNR values of the proposed method robustness using the five test-images.

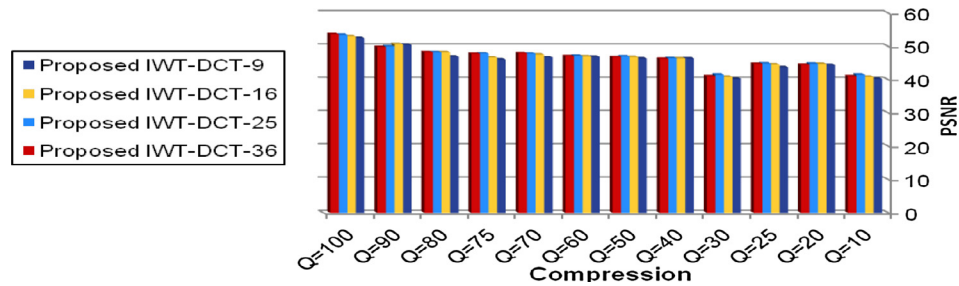


Fig. 8. The averages PSNR values of the proposed method robustness using the five test-images against compression.

Table 9

Robustness comparison results for text-image watermarking methods using PSNR.

	Proposed IWT-DCT-9	Proposed IWT-DCT-16	Proposed IWT-DCT-25	Proposed IWT-DCT-36	DWT-DFT [20]	DCT [22]	SVD [23]	DWT-DCT [21]
JPEG compression Q = 10	40.32	40.91	41.48	41.07	17.71	NA	NA	17.71
JPEG compression Q = 20	44.46	44.78	44.87	44.47	19.95	NA	NA	19.95
JPEG compression Q = 25	43.77	44.6	44.9	44.83	21.60	NA	NA	21.60
JPEG compression Q = 30	40.32	40.91	41.48	41.07	23.07	NA	NA	23.07
Rotation (15°)	14.51	15.98	17.36	18.66	5.239	NA	NA	5.239
Salt & pepper noise	40.18	40.21	40.53	39.58	NA	37.82	37.59	NA

NA: not available in the resources.

method robustness using the five test-images. Fig. 8 summarized the results obtained after JPEG compression using several quality factors using the five test-images. The proposed IWT-DCT method shows good robustness results especially against compression and noise, but weak robustness in case of rotation and histogram equalization. Table 9 compares the proposed IWT-DCT method with four text-image watermarking methods in the transform domain: DWT-DFT [20], DCT [22], SVD [23] and DWT-DCT [21]. The proposed method overcomes DWT-DFT [20] and DWT-DCT [21]. As known watermarking in DCT domain withstands compression attack. DCT [22] has a very good robustness against compression, but our proposed method improved the robustness against noise. The proposed method compared to SVD [23] has a higher robustness against compression and noise. But the main drawback is in case of rotation attack.

The data from this section shows the contribution of the study conducted. From Section 6.1 we found that the proposed IWT-DCT method is an imperceptible watermarking method. The logo is still detectable after most attacks as shown in Tables 6 and 8 from Section 6.2 except in rotation and compression with small factors. So, the proposed IWT-DCT method has achieved high imperceptibility and robustness results.

7. Conclusion

In this paper, an invisible watermarking method for text-image is proposed using the combination of integer wavelet transform (IWT) and discrete cosine transform (DCT). This hybrid method includes high robustness against most attacks from DCT and high imperceptibility from IWT. The lower coefficients from each transform are used to increase the robustness while maintaining the imperceptibility by choosing a good value for the scaling factor. Four values are used to determine the suitable DCT coefficients: 9, 16, 25 and 36. Their results are too close in imperceptibility and robustness, but differ in capacity. The more coefficients used the more capacity. The proposed IWT-DCT method overcomes other methods from literature against most attacks especially noise attack. It has higher imperceptibility compared to other

watermarking methods. However, it has low PSNR values when testing its robustness against rotation and histogram equalization.

In the proposed IWT-DCT method, the gray scale watermark image is embedded as it is. As a future work, Binary watermark image can be used and scrambled before the embedding to ensure the security. The proposed IWT-DCT method are used in watermarking Arabic text-image and can be extended for colored images. In the proposed IWT-DCT method, LL sub-band is selected with the lower DCT coefficients, other bands: HL, LH and HH can be used with the lower DCT coefficients.

References

- [1] I.I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, *Digital Watermarking and Steganography*, second ed., Morgan Kaufmann, United States, 2007.
- [2] S. Stanković, O. Irena, S. Ervin, *Multimedia Signals and Systems*, Springer, US, New York, 2012.
- [3] Y.-W. Kim, I.-S. Oh, 'Watermarking text document images using edge direction histograms, *Pattern Recognit. Lett.* 25 (2004) 1243–1251.
- [4] Practical Introduction to Frequency-Domain Analysis – MATLAB & Simulink Example – MathWorks United Kingdom, <http://www.mathworks.com/help/signal/examples/practical-introduction-to-frequency-domain-analysis.html> (accessed 14 October 2016).
- [5] S. Tyagi, H.V. Singh, R. Agarwal, S.K. Gangwar, Digital watermarking techniques for security applications, in: *International Conference on Emerging Trends in Electrical Electronics & Sustainable Energy Systems (ICETEESSES)*, 2016, pp. 379–382.
- [6] M.S. Hsieh, D.C. Tseng, Y.H. Huang, Hiding digital watermarks using multiresolution wavelet transform, *IEEE Trans. Ind. Electron.* 48 (5) (2001) 875–882.
- [7] R. Harshitha, S.S. Vidya, Robust and high limit watermarking using DWT-IWT, *Int. J. Adv. Sci. Res. Manage.* 2 (4) (2017) 18–21.
- [8] H. Yang, A.C. Kot, Text document authentication by integrating inter character and word spaces watermarking, in: *2004 IEEE International Conference on Multimedia and Expo (ICME)*, Taipei, Taiwan, June, 2004, pp. 955–958.
- [9] D. Huang, H. Yan, Interword distance changes represented by sine waves for watermarking text images, *IEEE Trans. Circuits Syst. Video Technol.* 11 (2001) 1237–1245.
- [10] Y.-W. Kim, K.-A. Moon, I.-S. Oh, A text watermarking algorithm based on word classification and inter-word space statistics, in: *Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 2003)*, Edinburgh, UK, 2003, pp. 775–779.
- [11] H. Yang, A.C. Kot, J. Liu, Semi-fragile watermarking for text document images authentication, in: *2005 IEEE International Symposium on Circuits and Systems*, Japan, 2005, pp. 4002–4005.
- [12] H. Tirandaz, R. Davarzani, M. Monemizadeh, J. Haddadnia, Invisible and high capacity data hiding in binary text images based on use of edge pixels, in:

- 2009 International Conference on Signal Processing Systems, Singapore, Singapore, 2009, pp. 130–134.
- [13] S. Kurup, G. Sridhar, V. Sridhar, Entropy based data hiding for document images, *World Acad. Sci. Eng. Technol.* (2005) 248–251.
- [14] A. Khan, M. Khanam, S. Bashir, M.S.H. Khiyal, A. Iqbal, F.H. Khan, Entropy based data hiding in binary document images, *Int. J. Comput. Electr. Eng.* 3 (2011) 503–506.
- [15] S. Aslam, K.S. Alimgeer, Entropy based data hiding on document images applied on DRDM approach, *Int. J. Technol. Res.* 1 (2013) 1–7.
- [16] M.H. Shirali-Shahreza, M. Shirali-Shahreza, A new approach to persian/arabic text steganography, in: *Proceedings of the 5th IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse (ICIS-COM SAR'06)*, Honolulu, HI, USA, 2006, pp. 310–315.
- [17] R. Davarzani, K. Yaghmaie, Farsi text watermarking based on character coding, in: *2009 International Conference on Signal Processing Systems*, Singapore, Singapore, 2009, pp. 152–156.
- [18] V. Yazdani, M.A. Doostari, H. Yazdani, A new method to persian text watermarking using curvaceous letters, *J. Basic Appl. Sci. Res.* 3 (2013) 125–131.
- [19] G. Feng, X. Huang, An improved DCT based zero-watermarking algorithm for text image, in: *2014 International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, China, 2014, pp. 1–4.
- [20] J. Li, F. Wu, Robust watermarking for text images based on arnold scrambling and dwt-dft, in: *Proceedings 2013 International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC)*, Shenyang, China, 2013, pp. 1182–1186.
- [21] F. Wu, M. Huang, J. Li, Robust watermarking for text images based on Arnold scrambling and DWT-DCT, in: *2015 International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC 2015)*, Shenyang, China, 2015, pp. 568–572.
- [22] L. Laouamer, O. Tayan, A semi-blind robust DCT watermarking approach for sensitive text images, *Arab. J. Sci. Eng. (Springer Science & Business Media BV)* 40 (2015) 1097–1109.
- [23] L. Laouamer, O. Tayan, An enhanced SVD technique for authentication and protection of text-images using a case study on digital Quran content with sensitivity constraints, *Life Sci. J.* 10 (2013) 2591–2597.
- [24] S. Mishra, A. Mahapatra, P. Mishra, A survey on digital watermarking techniques, *Int. J. Comput. Sci. Inform. Technol.* 4 (2013) 451–456.
- [25] S.D. Lin, S.-C. Shie, J.Y. Guo, Improving the robustness of DCT-based image watermarking against JPEG compression, *Comput. Stand. Interfaces* 32 (2010) 54–60.
- [26] Discrete Cosine Transform, https://en.wikipedia.org/wiki/Discrete_cosine_transform (accessed 25 November 2016).
- [27] N. Goel, G. Singh, Study of wavelet functions of discrete wavelet transformation in image watermarking, *Int. J. Eng. Sci.* 17 (1) (2016) 154–160.
- [28] W. Sweldens, The lifting scheme: a construction of second generation wavelets, *SIAM J. Math. Anal.* 29 (1998) 511–546.
- [29] L.A. Elrefaey, M.E. Allam, H.A. Kader, M. Selim, Robust blind image-adaptive watermarking, in: *Twenty Fifth National Radio Science Conference NRSC 2008*, Tanta, Egypt, 2008, pp. 1–13.
- [30] T. Samajdar, M.I. Quraishi, Analysis and evaluation of image quality metrics, in: *Information Systems Design and Intelligent Applications*, Springer, 2015, pp. 369–378.
- [31] P.B. Nguyen, M. Luong, A. Beghdadi, Statistical analysis of image quality metrics for watermark transparency assessment, in: *Pacific-Rim Conference on Multimedia: Advances in Multimedia Information Processing – PCM 2010*, Shanghai, China, 2010, pp. 685–696.
- [32] Z. Wang, A.C. Bovik, A universal image quality index, *IEEE Signal Process. Lett.* 9 (2002) 81–84.
- [33] Z. Wang, A.C. Bovik, H.R. Sheikh, E. P. Image quality assessment: from error visibility to structural similarity, *IEEE Trans. Image Process.* 13 (2004) 600–612.
- [34] N.M. Makbol, B.E. Khoo, A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition, *Digital Signal Process.* 33 (2014) 134–147.
- [35] U.M. Gokhale, Y.V. Joshi, A semi fragile watermarking algorithm based on SVD-IWT for image authentication, *Int. J. Adv. Res. Comput. Commun. Eng.* 1 (4) (2012) 217–222.
- [36] M. Jiansheng, L. Sukang, T. Xiaomei, A digital watermarking algorithm based on DCT and DWT, in: *International Symposium on Web Information Systems and Applications*, 2009, pp. 104–107.
- [37] A. Akter, M.A. Ullah, Digital image watermarking based on DWT-DCT: evaluate for a new embedding algorithm, in: *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, University of Dhaka, Dhaka, Bangladesh, 2014, pp. 1–6.
- [38] S. Mukherjee, A.K. Pal, A DCT-SVD based robust watermarking scheme for grayscale image, in: *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, Chennai, India, 2012, pp. 573–578.
- [39] S.L. Agrwal, A. Yadav, U. Kumar, S.K. Gupta, Improved invisible watermarking technique using IWT-DCT, in: *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, 2016, pp. 283–285.