ISSN: 0067-2904

Robust Blind Watermarking Technique Against Geometric Attacks for Fingerprint Image Using DTCWT-DCT

Mohamed Lebcir[1], Suryanti Awang[*1], Ali Benziane[2]
[1]Soft Computing & Intelligent System Research Group (SPINT), Faculty of Computing, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300, Kuantan, Pahang, Malaysia
[2]Faculty of Science and Technology, University of Djelfa, Algeria

Received: 31/10/2019 Accepted: 31/3/2020

Abstract

In this research paper, a new blind and robust fingerprint image watermarking scheme based on a combination of dual-tree complex wavelet transform (DTCWT) and discrete cosine transform (DCT) domains is demonstrated. The major concern is to afford a solution in reducing the consequence of geometric attacks. It is due to the fingerprint features that may be impacted by the incorporated watermark, fingerprint rotations, and displacements that result in multiple feature sets. To integrate the bits of the watermark sequence into a differential process, two DCT-transformed sub-vectors are implemented. The initial sub-vectors were obtained by sub-sampling in the host fingerprint image of both real and imaginary parts of the DTCWT wavelet coefficients. The basic difference between the relevant sub-vectors of the watermarked fingerprint image in the extraction stage directly provides the inserted watermark sequence. It is not necessary to extract watermark data from an original fingerprint image. Therefore, the technique suggested is evaluated using 80 fingerprint images from 10 persons, from both CASIA-V5-DB and FVC2002-DB2 fingerprint database. For each person, eight fingerprints are set as the template and the watermark are inserted in each image. A comparison between the obtained results with other geometric robust techniques results is performed afterwards. The comparison results show that the proposed technique has stronger robustness against common image processing processes and geometric attacks such as cropping, resizing, and rotation.

Keywords: Fingerprint, Fingerprint image watermarking, DTCWT, DCT, Geometric robust.

Introduction

A fingerprint is demonstrated on the surface of a fingertip by the interpretation of the ridge and valley pattern. The combination of their minutiae points determines the exclusivity of a fingerprint [1, 2]. Because of their distinctiveness, fingerprint images are generally used for user authentication purposes. Thus, it is essential to protect the fingerprint's authenticity. Digital watermarking can be used to verify the authenticity of a fingerprint sample [3]. The basic idea of the digital watermarking approach lies in embedding watermark data into the original fingerprint image in order to maintain fingerprint ownership security. In addition, the watermark data can be encrypted before entrenching the watermark as a second layer of protection [4]. A secret key is used to determine the locations where the watermark would also be inserted in the fingerprint image. If the user wants to check the fingerprint images that could have been corrupted or skewed, the embedded watermark sequence can be retrieved on the basis of the secret key used to encode the watermark. Thus, the operator's key role is preventing attackers from gaining access to the watermark data.

*Email: suryanti@ump.edu.my

There are two main impediments to the fingerprint watermarking algorithms that may obstacle the fingerprint images watermarking process. Firstly, the features of fingerprint may likely be mainly affected by the integrated watermark. Secondly, fingerprint rotations and displacements guide to various sets of characteristics [5]. Thus, challenges of protecting the authenticity of the fingerprint images using watermarking techniques are becoming increasingly important to be faced by researchers.

Depending on the area in which the watermark pattern is integrated, the methods of watermarking can be categorised within three embedding areas. The domains include the spatial domain, frequency domain and multiresolution domain. Firstly, the spatial domain acts in embedding fingerprint watermark directly into the pixels of the host image [6]. A common technique used for watermarking in the spatial domain involves the substitution of the least significant bits (LSBs) with more significant bits in the image pixel [6]. The technique has several advantages such as fewer complications coupled with a high payload. However, they are not sufficiently robust against the common forms of image processing attacks such as compression. In addition, this approach is highly vulnerable to piracy attacks as the watermark can be easily modified during the process of watermarked image transmission between a sender and a receiver.

Secondly, the frequency domain denotes the rate of change in the values of the pixel at the spatial domain. In the frequency domain, insertion of watermarks is made into the image transform coefficients. An inverse transformation is used to rebuild the watermarked image [7]. The commonly used watermarking transformation techniques in the frequency domain are the Fast Fourier Transform (FFT) technique and the Discrete Cosine Transform (DCT) [7]. The use of DCT algorithms to embed watermark into a fingerprint image proved to be sufficient against compression attacks. However, it does not reveal sufficient robustness against geometric transformations such as rotations or translations. Moreover, this transformation often affects the coefficient of many DCT algorithms. Hence, fingerprint watermarking through DCT algorithm in the frequency domain is limited in its efficiency.

Finally, the multiresolution domain presents an embedding domain to the watermark, both in the spatial and the frequency domains. The notable transformations used in the multiresolution domain are the contourlet transform (CT) and the Discrete Wavelet Transform (DWT) [7]. It was observed that the highlighted techniques offer better robustness and higher image imperceptibility. Specifically, for digital image watermarking, the DWT was used more regularly. This is based on the features of its time/frequency decomposition that are considered to be more identical to the human visual systems theoretical models as compared to the other transform from previous methods [7].

Besides the general approach of embedding watermark in a single domain, there are other studies wherein two domains (hybrid domains) have been explored such as hybrid spatial and frequency domain, hybrid spatial and multiresolution domain, or hybrid frequency and multiresolution domain [7]. Based on the results that have been recorded in fingerprint image watermarking techniques, both multiresolution and hybrid (frequency / multiresolution) domains are proved to be the best, especially due to their capability to preserve the minutiae number at the extraction stage. These embedding domains offer good verification performances. In addition, they present a desirable compromise between robustness and imperceptibility. However, the underlying challenge now is on how to enhance the robustness of the fingerprint watermarking procedure against most of the geometric attacks, such as translations or rotations, without a need for the original fingerprint template at the extraction stage (blind). This would help to provide higher security and robustness without corrupting minutiae points.

Overall, the most important bit is not a favoured section in which to entrench a robust watermark because perceptually it may possibly affect the watermark where the watermark may become noticeable [8]. Therefore, identifying where to embed the watermark is a compromise between robustness and perception.

Therefore, in this paper, we proposed to utilize the advantages of frequency and multiresolution domains by combining DTCWT and DCT to produce a robust blind watermarking technique. Being robust means that our method is able to maintain the originality of the fingerprint from geometric attacks. Being blind means that our method works without a need for the original fingerprint image to extract the watermark and, thus, beefing up the robustness of watermark data and the security of the fingerprint recognition system.

The next sections of this paper will discuss related work based on other watermarking techniques that dealt with geometric attacks, as well as a discussion about DTCWT and DCT, followed by the methodology of our watermarking technique, and ends with experimental results and discussion.

Related Work

Robustness is a key issue in many prospective applications of watermarking fingerprint image technologies. Usually, the hybrid (frequency / multiresolution) domains are the best due to their capability to preserve the minutiae points and better robustness against attacks on watermark data [9].

In the multiresolution domain, DWT has become the most advanced choice among all the multiresolution domains for image watermarking techniques. This is because the magnitude of DWT coefficients is larger in the lowest band at each level of decomposition; it is possible to use a larger scaling factor for watermark embedding [10]. In addition, DWT is very suitable to identify the areas in the host image where a watermark can be embedded effectively. In particular, this property allows exploitation of the masking effect of the human visual system. For example, in case a DWT coefficient is modified, only the region corresponding to that coefficient will be modified [11]. In the DWT, the image is divided into four sub-bands named LL, LH, HL, and HH at level 1. The LH and HL signify the horizontally and vertically high-frequency details, respectively. The HH contains the noise and edge information. Whilst, LL signifies low-frequency input signal coefficients [12]. The disintegration of the LL band is performed more frequently until the desired decomposition stage found by the technique is reached.

The features of the fingerprint can likely be affected by the entrenched watermark, rotations of fingerprints and displacements which lead to numerous sets of features. The DWT has two drawbacks. Firstly, it lacks shift invariance, which means small shifts in input signal can cause big changes in the energy distribution of wavelet coefficients. Secondly, the DWT has poor directional selectivity for diagonal features, which is obvious from the impulse responses of the filters' individual sub-bands. On the other side, the complex wavelet transform (CWT) is efficient and effective, and has only a modest redundancy quantity; It still provides approximate shift invariance and better directional selectivity [13, 14]. In opposition to the conventional DWT, which uses three directions (horizontal, vertical and diagonal), the CWT uses a single tree (one-dimensional ;1-D) of filters with complex coefficients. Enhanced implementation of the CWT is a dual-tree complex wavelet transform (DTCWT) [15]. It is an improvement version of the wavelets transforms that provides 12 direction wavelets, six for the actual tree and six for the imaginary tree at the angles of ±5, ±10, and ±15 in two dimensions. Fingerprint image watermarking that implemented DTCWT has achieved a good result [16]. That implementation was founded on dual-tree complex wavelet transformation (DTCWT) for embedding a binary image into fingerprint by an encrypted password in order to prevent it from possible effects on the embedded watermark. In addition, it embeds the watermark in all parts of the fingerprint image without affecting the features and is able to retain mostly the same array of fingerprint features even after some rotations have been made to the fingerprint images. However, the proposed algorithm in the above mentioned study [16] requires the original fingerprint template at the extraction stage (not blind). Thus, the attackers can easily use the original secure data to attack the system.

To address this problem, a combination of DTCWT and DCT domains is presented in our proposed technique. Two DCT-transformed sub-vectors are used to integrate the watermark sequence bits into a differential system. During the extraction stage, the simple difference between the correlating sub-vectors of the watermarked fingerprint image effectively results in an integrated watermark sequence. No original fingerprint image is needed to extract watermark information (blind). On the other hand, DCT-based watermarking is based on two facts. Firstly, much of the signal energy lies at low frequencies sub-band which contains the most important visual parts of the image. Secondly, high-frequency components of the image are removed through compression and noise attacks. The watermark is therefore embedded by modifying the coefficients of the middle-frequency sub-band, so that the visibility of the image will not be affected, and the watermark will not be removed by compression.

Based on the related works, we noticed that DTCWT and DCT technique have advantages in the fingerprint image watermarking technique. Thus, we provide further explanation about these two techniques in the following subsections.

Dual-Tree Complex Wavelet Transform (DTCWT)

The dual-tree hybrid complex wavelet transform requires two real DWTs. The two transforms together provide an overall transform. The first transform of the DWT identifies the real part and the second transform identifies the imaginary part. The actual two wavelets incorporated together with the two actual wavelet transforms are demonstrated as $W_r(s)$ and $W_i(s)$. After the filters are produced, the complex wavelet is roughly expected as follows:

$$W(s) = W_r(s) + jW_i(s) \tag{1}$$

where $W_r(s)$ is the real part and $jW_i(s)$ is the imaginary part. In the 2-D DTCWT, the 2-D wavelet function $W(a,b) = W(a).W(b)$ is integrated with the row-column of the wavelet transform, where (a) is a complex wavelet represented by

$$W(a) = W_r(a) + jW_i(a) \tag{2}$$

$W(a,b)$ is obtained from the equation:

$$\begin{aligned} W(a,b) &= [W_r(a) + jW_i(a)][W_r(b) + jW_i(b)] \\ &= W_r(a)W_r(b) - W_i(a)W_i(b) + j[W_r(a)W_i(b) + W_i(a)W_r(b)] \end{aligned} \tag{3}$$

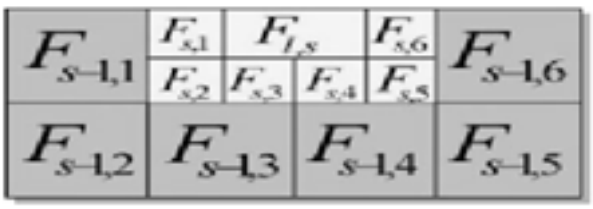
The real part of the complex wavelet is taken, and then the sums of two separable wavelets are obtained:

$$\text{RealPart}\{ W_r(a,b) \} = W_r(a)W_r(b) - W_i(a)W_i(b) \tag{4}$$

The watermark has a checkerboard style pattern. The directional filter of DTCWT is added to the watermarked image for decomposition purposes. The subsequent images are the output of the one-directional filter from the high pass and low pass filters. The DTCWT decomposition's real and imaginary parts of the fingerprint image are presented in Figure-1

Figure 1- Image of fingerprint (a), Fingerprint of the imaginary part (b), Fingerprint of the real part (c).

The coefficients of the DTCWT obtained from the primary filter bank are called the actual part and the coefficients derived from the other filter are named the imaginary part. The actual part of the image consists of less significant data than the imaginary part containing additional information.
Recently, DTCWT [13,17] is used for watermarking [14, 15] due to its property of nearly shift-invariance and better direction selectivity. The coefficients of DTCWT possess 6 directions, i.e., ±15, ±45 and ±75, compared with the three directions exhibited by the normal DWT, i.e., 0, 90 and ±45. The positioning of the coefficients of DTCWT is illustrated in Figure-2. In that Figure, $F_{l,s}$ is the low pass frequency coefficient at level s and $F_{s,1}$ to $F_{s,6}$ represent the high-pass frequency coefficients of level s at directions 1 to 6.



<table>
<tr><td rowspan="2">HLR1</td><td>HLR2</td><td>LLR2</td><td>LLI2</td><td>HLI2</td><td rowspan="2">HLI1</td></tr>
<tr><td>HHR2</td><td>LHR2</td><td>LHI2</td><td>HHI2</td></tr>
<tr><td>HHR1</td><td colspan="2">LHR1</td><td colspan="2">LHI1</td><td>HHI1</td></tr>
</table>

1,2: Decomposition level

H: High Frequency Bands

L: Low Frequency Bands

R: Real Wavelet Coefficients

I: Imaginary Wavelet Coefficients

Figure 2- Positioning of the coefficients in a 2-level decomposition of DTCWT.

Overall, it is difficult to embed the watermark in the low frequency components, since arbitrarily changing the low frequency coefficients may result in an important change in the visual quality of the image. Four bands of low frequency coefficients can be attained due to the dual-tree decomposition of the DTCWT, in which each one is a shifted version of another [18]. Typically, high-pass complex coefficients of DTCWT correspond to the edges and fine details of the images in six various directions. Embedding the watermark in these locations is not simply noticeable to the human eyes.

In the embedding process, the input image is initially decomposed into level s, where s=1 is chosen. Let us represent the complex coefficients as

$$F_{s,d} = C_{s,d,r} + jC_{s,d,i} \tag{5}$$

where s and d denote the level of decomposition and directions of the coefficients, respectively, d∈{1, 2, 3, 4, 5, 6}; $C_{s,d,r}$ and $jC_{s,d,i}$ represent the real and imaginary coefficients obtained from decomposing using DTCWT with two different trees, respectively [18].

Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) is one of the most common linear transformations in digital signal process technology. The most common DCT definition of a 1-Dimension sequence x of length N is:

$$c(k) = \alpha(k) \sum_{i=0}^{N-1} x(i) \cos\left[\frac{(2i+1)}{2N}\right] \tag{6}$$

where

$$\alpha(k) = \begin{cases} \sqrt{2/N} & for \quad k=0 \\ \sqrt{2/N} & for \quad k=1,2..N-1 \end{cases}$$

The corresponding inverse transformation for 1- Dimension sequence x of length N is:

$$x(i) = \sum_{k=0}^{N-1} \alpha(k) c(k) \cos\left[\frac{(2i+1)k\pi}{2N}\right] \tag{7}$$

The middle frequency sub-band is the appropriate part in DCT domain decomposition to embed the watermark. The lower frequencies sub band contains the most visually parts of the image. Furthermore, it's easy to remove components of the image through compression and noise attacks in the high frequency bands. Consequently, the embedded watermark in the middle frequency sub- band will not affect cover image visibility and will not be removed it by compression.

Two DCT-transformed sub-vectors are implemented, obtained by sub-sampling in the host fingerprint image of both real and imaginary parts of the DTCWT LL sub-band wavelet coefficients. The

differential embedding of the watermark in the resulting two transformed sub-vectors of the DCT guarantees the blind extraction of the watermark.

Methodology: DTCWT-DCT

The new proposed fingerprint image watermarking algorithm is extended from combining the idea of K. Ramani *et al*. [10] and Benoraira *et al*. [12], that uses the hybrid domain of DTCWT and DCT, with the differential embedding method. The technique of differential embedding depends on two DCT transformed sub-vectors to ensure the blind extraction of the watermark. The blindness and robustness of watermarking fingerprint image depends on the hybrid domain of DTCWT and DCT. The proposed method is achieved under the biometric image (fingerprint), which means that it concentrates on biometric features. These features are combined between unique ridges and minutia points for the purpose of improving the security of biometric data, whilst the proposed method by Ramani *et al*. [10] concentrated on the copyright protection of digital images. In addition, it was based on the differential method to choose the best place of the embedded watermark without affecting minutia points within the cover fingerprint image. Furthermore, achieving the blindness means that there is no needed for the original cover image to extract the embedded watermark. While, K. Ramani *et al*. [10] did not mention this method (differential method) in his algorithm. On the other hand, the choice of the embedding of the coefficient sub-bands in the proposed DCT-DTCWT algorithm is far more adjustable than those used in the study of Benoraira *et al*. [12] (the used frequency domain is not the same) because of the proprieties of the used transform domain.

To insert the watermark within the fingerprint image, this hybrid algorithm is proposed where each transform has its own advantages for the watermarking scheme. The transform DCT permits to divide the image into different blocks and to insert easily the watermark in the blocks selected. While, the transform DTCWT uses the fingerprint images of parallel lines (ridges) at varying angles. This algorithm inserts the watermark within the fingerprint image, in other words, the imaginary and real parts. This is chosen because if an attack occurs while it is being broadcasted, it can quickly be identified. Likewise, if only the actual part is used for the embedding of a watermark and the unauthorized body manages to remove a watermark, the data on the minutiae point will not be changed since the actual part contains less information.

In using imaginary and real parts, an attack can be recognized although the distribution of minutia will be changed. In addition, this algorithm has a perfect reconstruction; its shift invariance is approximate while its directional advantage is selective.

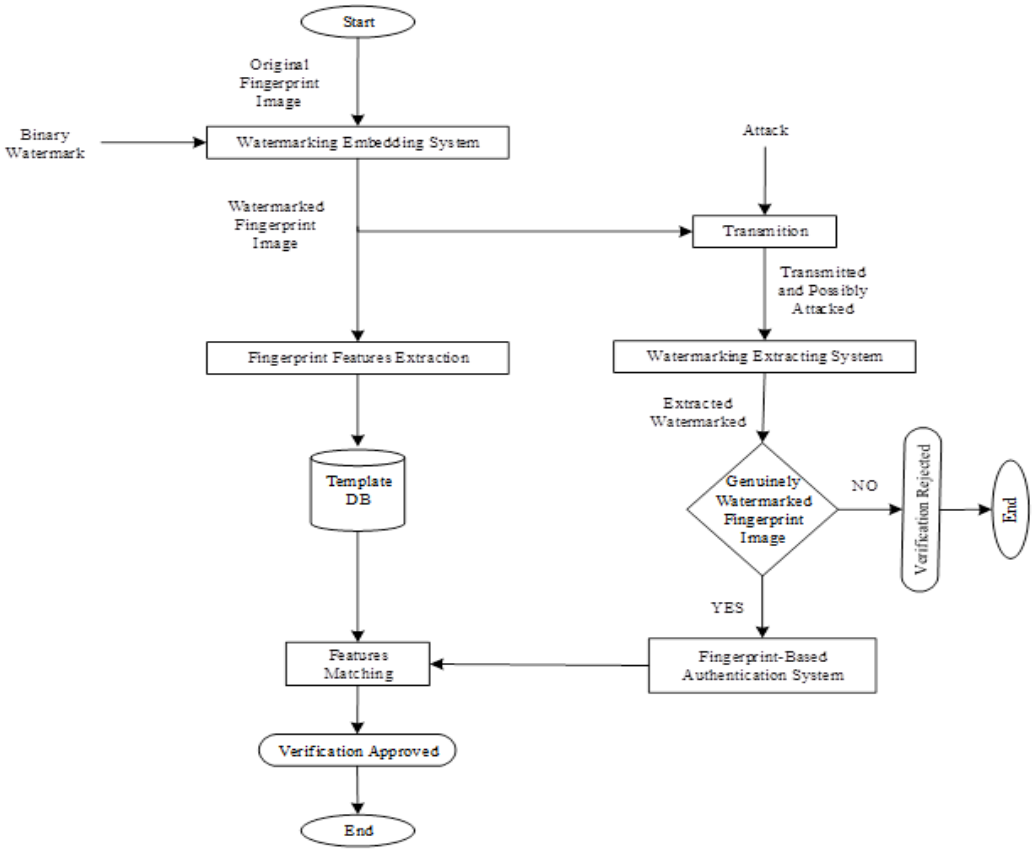


Figure 3- Fingerprint Identification/Verification System using Digital Watermarking.

The flowchart shown in Figure-3 represents the fingerprint verification system using digital watermarking in general. It is divided into two interrelated sections, which are fingerprint image watermarking system and fingerprint-based authentication system. The verification process begins with the verification system using watermarking technique on fingerprint image, which is the study subject in this paper, and the process is completed with identification by the fingerprint-based authentication system. The following is a brief explanation of the most important steps of the research proposal methodology shown in Fig. 3. The watermarking embedding system begins with performing a fingerprint scan using a fingerprint scanner to acquire a fingerprint image. The embedding process consists of implementing on the fingerprint image that contains valid features, as a host image, and the bipolar {-1,1} binary sequence W of size L, as a watermark. This is performed using DTCWT, DCT, and the differential embedding method which will be explained in detail later on. In this stage, the watermark data is embedded in a fingerprint image to be used in the fingerprint-based authentication system.

The next process in the watermarking embedding system is the feature extraction of fingerprint features. The extracted features are stored in the database to be used during the feature matching. The watermark is embedded to measure if the fingerprint image may be attacked by attackers during the transmission stage. The assumption is that they may be intended for watermark detection, counterfeiting, or image processing operations, such as compression, noise or geometric attacks such as cropping and rotation.

Prior to the fingerprint-based authentication system, the watermarking extracting system is implemented and the watermark is extracted from the watermarked fingerprint image, which may have been attacked. The extracting of the watermark does not need the original fingerprint image (blind), whereby, only the differential extracting method will be used and explained in details.

Finally, the extracted watermark is compared with the original image. If the extracted watermark is not genuine, the verification process is rejected and the process is ended. Otherwise, the extracted watermark is sent to the fingerprint-based authentication system to be matched with the genuine features in the database and the process is ended with the approved verification.

DTCWT-DCT

Based on the general fingerprint verification system using digital watermarking as described in Fig. 3, the watermarking system with the DTCWT-DCT as a watermark embedding method is proposed as shown in Fig. 4. The advantages of the DTCWT-DCT depend on DTCWT and DCT; DTCWT preserves ridge angles and it is characterized with perfect reconstruction, its shift invariance is approximate, and its directional advantage is selective; while DCT permits to divide the image into different blocks and to easily embed the watermark into selected blocks. It is also sufficient for compression attacks. The main steps of the proposed watermark embedding procedure can be described as follows:

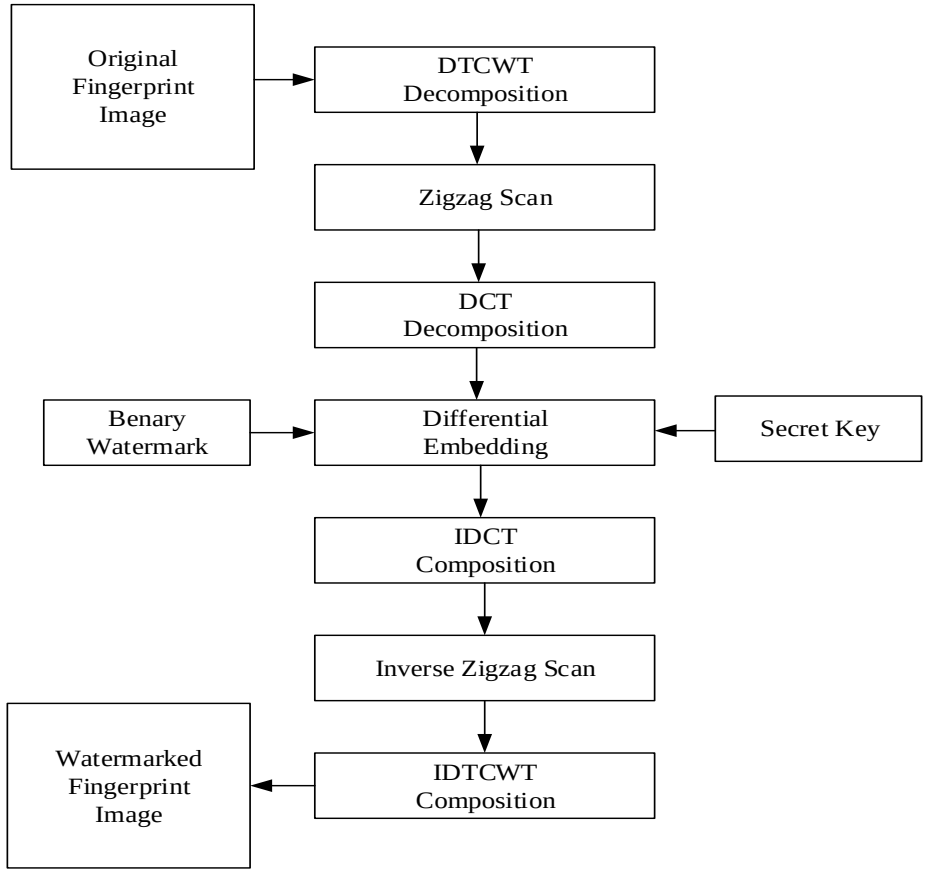


Figure 4- The embedding procedure of the proposed DTCWT-DCT technique.

A. Watermark Embedding Process

The first process in DTCWT-DCT method is the proposed watermark embedding process, as shown in Fig. 4. The process can be described as follows:

Step 1: DTCWT is performed on the input fingerprint image F_o. to obtain DTCWT coefficients of fingerprint image which is referred to as follows:

$$Z_{m.n} = X_{m.n} + jY_{m.n} \tag{8}$$

where F_o is the original fingerprint image, X, Y and Z are the real, imaginary and complex coefficients at either scale of decomposition, respectively, while $n = 1 \ldots N$ is the number of coefficients attained at either scale m of decomposition. The high value coefficients for fingerprint image decomposition define the ridges, short ridges and other transition points. These points are known as "minutia points" that correspond with high values coefficients, while low values correspond with continuous lines; this is when applying DTCWT decomposition in fingerprint image. The middle of the fingerprint usually contains minutiae points. The transform DTCWT decomposes the fingerprint image by using two 2D DWT to obtain additional coefficients. One collection of them speaks to the genuine part, and the other speaks to the imaginary part. The benefit of additional coefficients is that if

modifications happen in one coefficient, the other will adapt with these modifications. Thus, it will be easy to restore the original fingerprint image without being affected by the watermarking process.

Step 2: A zigzag scanning is performed on a complex coefficients matrix which is obtained from DTCWT decomposition. The aim is to convert it into a vector of complex coefficients $Z(n)$ to easily process the watermarking, where $n=1\ldots N$ and N is the size of the complex coefficients matrix.

Step 3: The coefficients vector Z is decomposed within two (related) sub-vectors, z_1 and z_2, to allow applying the differential embedding technique (will be explained in details in the next steps) as follows:

$$z_1(k)=Z(2k) \tag{9}$$

$$z_2(k)=Z(2k-1) \tag{10}$$

where $k=1\ldots N/2$.

Step 4: DCT is performed on z_1 and z_2 to create their DCT changed forms, Z_1 and Z_2, which permit an image to be decomposed into various blocks in such way that making it much easier to embed the watermark into selected blocks.

$$Z_1 = DCT(z_1) \tag{11}$$

$$Z_2 = DCT(z_2) \tag{12}$$

Step 5: The watermark (binary sequence W of size L) sequence bits $W(i)$ for $i=0,2\ldots L-1$ is inserted within the changed vectors Z_1 and Z_2 using a differential embedding method that is a mathematical equation, as describe in equations 13 and 14. It allows including the watermark randomly into the transformed vectors Z_1 and Z_2 obtained from DCT transform, to be used in the extraction stage without the need for the original data (blind). This will output two changed (by watermarking) sub-vectors z'_1 and z'_2 as follows:

$$Z'_1\left(i'\right)=1/2\left[Z_1\left(i'\right)+Z_2\left(i'\right)\right]+\alpha W(i) \tag{13}$$

$$Z'_2\left(i'\right)=1/2\left[Z_1\left(i'\right)+Z_2\left(i'\right)\right]-\alpha W(i) \tag{14}$$

where α is the gain factor and i' are the random places into the highly strength band of Z_1 and Z_2 within the watermark bits are integrated. These spots are the elements of a vector r which can be produced by the usage of an arbitrary change operation:

$$i'=r(i) \tag{15}$$

$$r=RandPerm(S,a,b) \tag{16}$$

where S is the grain of the related Pseudo Random Number Generator (PNRG), a and b are the beginning and the ending places, respectively, of the highly strength band applied to be put in the watermark, as shown in Fig. 5. Therefore, the user's secret key is $K=(S,a,b)$, which prevents the watermark from tempering or unauthorized access by attackers.

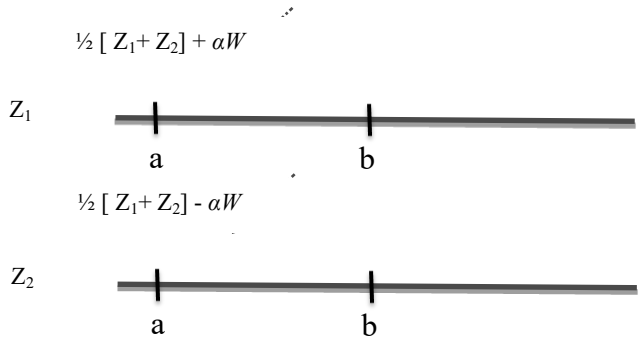


Figure 5- The differential embedding of the watermark in the high energy band of the transformed sub-vectors

Z_1 and Z_2 [18]

Step 6: The inverse DCT $IDCT$ is performed on z'_1 and z'_2 using the following equations 17 and 18. The purpose of performing the $IDCT$ is to reconstruct the vector of complex coefficients Z embedded by the watermark.

$$z'_1 = IDCT(Z'_1) \quad (17)$$

$$z'_2 = IDCT(Z'_2) \quad (18)$$

Step 7: The two changed sub-vectors z'_1 and z'_2 are combined in the composing step using the opposite operation in equations 7 and 8 in order to produce the modified vector Z' to reconstruct the complex coefficients vector embedded by the watermark:

$$Z'(2k) = z'_1(k) \quad (19)$$

$$Z'(2k-1) = z'_2(k) \quad (20)$$

where $k = 1 \ldots N/2$.

Step 8: The modified vector is converted within the matrix employing the inverse of the zigzag scanning operation to reconstruct the complex coefficients matrix embedded by the watermark.

Step 9: The DTCWT coefficients are changed and the opposite wavelet transform IDTCWT is executed to attain the watermarked fingerprint image F_w. The perfect image reconstruction has been assisted by using the redundancy of data (real/imaginary components) presented in the DTCWT algorithm. In fact, if the DTCWT coefficients have been slightly modified, we should be able to reconstruct a very similar image to the original one [14]. Thus, the controlled watermark embedding in the wavelet coefficients of the fingerprint image is unlikely to be altering its main features, and the identification phase using the image minutia can be performed without concern.

Note 1: The parameters a and b should be chosen to satisfy the following conditions:

--First, a > 0: the DC-components of the transformed sub-vectors Z_1 and Z_2 must remain unchanged in order to preserve the quality of the watermarked image.

--Second, b - a ≥ L: the insertion band has to be wide enough to insert all the watermark's bits.

--Third, b ≤ N/2: the watermarking is done in the height energy band of Z_1 and Z_2 in order to guarantee the robustness of the method.

Note 2: While the normal differential embedding would be as follows: $Z'_1 = Z_1 + \alpha w$ and $Z'_2 = Z_2 - \alpha w$ (by omitting the insertion locations), the fact that the transformed sub-vectors Z_1 and Z_2 in (11) and (12) are highly correlated [18], allowing us to assume that $Z_1 \approx Z_2 \approx 1/2\,[Z_1 + Z_2]$. This will guarantee that Z_1 and Z_2 are similarly adding to the new changed ones Z'_1 and Z'_2 so that the consequent manipulation on the watermarked image will be limited. It is also clear that the distinction between Z'_1 and Z'_2 will bring an augmented (by 2) amount of the integrated watermark array (αW) which is the essential aspect of this distinct integrating method.

B. Watermark Extraction Process

The mechanism of watermark extraction pursues the likewise stride as the integrating process, until reaching Step 4 where the extraction is taking place, as shown in Figure-6.

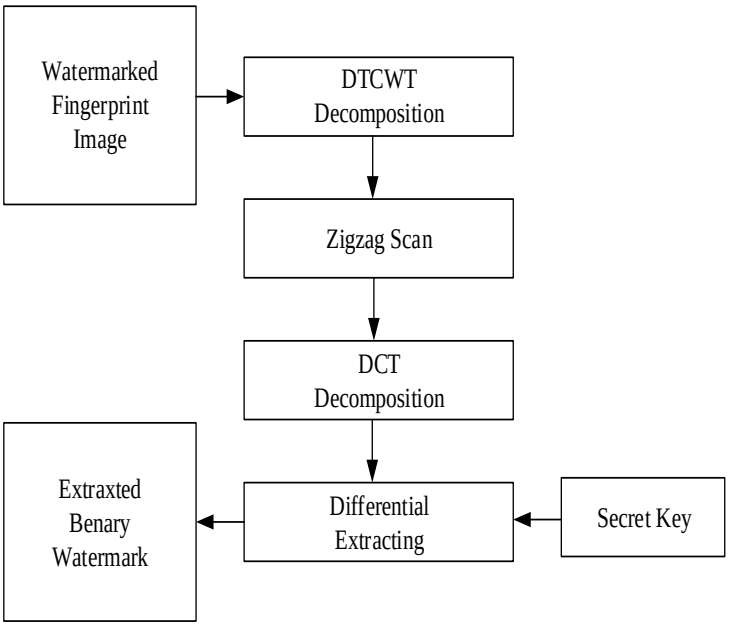


Figure 6-The procedure of extraction of the proposed DTCWT-DCT technique.

Step 1: Perform DTCWT on the input watermarked fingerprint image F_w.

Step 2: Execute a zigzag scanning on complex coefficients matrix which has been obtained from DTCWT decomposition. The aim is to convert it into vector of complex coefficients $Z'(n)$, to achieve an easy process of watermarking, where $n = 1 \ldots N$ and N is the size of complex coefficients matrix.

Step 3: Decompose the vector of coefficients Z' into two related sub-vectors z'_1 and z'_2. The decomposition of sub-vectors is based on equations 22 and 23.

$$z'_1(k) = Z'(2k) \tag{22}$$

$$z'_2(k) = Z'(2k-1) \tag{23}$$

for $k = 1 \ldots N/2$.

Step 4: Perform DCT on z'_1 and z'_2 to produce their DCT-transformed forms Z'_1 and Z'_2.

$$Z'_1 = DCT(z'_1) \tag{24}$$

$$Z'_2 = DCT(z'_2) \tag{25}$$

If the enter fingerprint image is the watermarked one, and by using analogy with the embedding operations, the extraction operations will deliver 2 sub-vectors Z'_1 & Z'_2 as proven in equations 24 and 25 duly. Appropriately, the distinction between them has a corresponding dating with the watermark array W:

$$\Delta Z(i) = Z'_1(i') - Z'_2(i') = 2\alpha W(i) \tag{26}$$

where $i = 1 \ldots L$ and i' are the arbitrary spots in which the watermark bits are integrated. These spots are clearly defined by recreating the vector r and the usage of the user selected secret key and the arbitrary permutation, as shown in equations 13 and 14. Finally, because the difference $\Delta(i)$ may vary from $+1/-1$ values, therefore, a difficult challenge characteristic is implemented on it to be able to restore the source bits of the watermark:

$$W'(i) = \begin{cases} +1 & if \quad \Delta Z(i) \geq 0 \\ -1 & otherwise \end{cases} \tag{27}$$

After that, a comparison between the two watermarks W and W' is performed. If there is a similarity between W and W', then fingerprint-based authentication system is launched.

Overview of the Experiment

Some experiments were performed in this section to test the quality of the proposed watermarking scheme. The performance of the fingerprint image-watermarking algorithm is evaluated by employing two fingerprint image databases (CASIA-V5-DB and FCV2002-DB2) which are publicly available, and comparing it with previous works that had used the same database. In the given experiment, 80 fingerprint images from 10 characters, with sizes of 328 × 356 and 388 × 374 pixels for CASIA-V5-DB and FCV2002-DB2 fingerprint databases, respectively, have been tested. Eight fingerprint images for each person are set as a template then the sequence binary, with a size of 160 bits as watermark, is embedded into each one. The process starts with comparing the input original fingerprint images in both databases against its corresponding watermarked fingerprint images to find positive matching results between them for minutia points and watermark data. Then, the input fingerprint images watermarked against common image processing are tested along with geometric attacks such as cropping, resizing, and rotation. The process is completed with comparing the original watermark embedded to the extracted watermark, that may be attacked, to find positive results between them. Thus, stronger robustness against common attacks of image processing and geometric is achieved, compared to previous methods, especially cropping, resizing, and rotation.

The hybrid domain DTCWT-DCT with the differential embedding in the proposed method is used to integrate watermark within original fingerprint images. The watermarked fingerprint images are compared with their corresponding original fingerprint images in both databases. To qualify the quality of the watermarked fingerprint image, the peak signal to noise ratio (PSNR) is used. Fingerprint recognition tools are used to measure the rate of similarities between fingerprints features. The Purpose of the similarity measurement is to find a positive score of minutia points matching between original fingerprint images in databases and their corresponding's, which have been possibly attacked and distorted. PNSR represents the ratio noise between the fingerprint image before and after the watermarking operation. This ratio can be used to determine the percentage of deformation on the original fingerprint image caused by the embedding of the watermark.

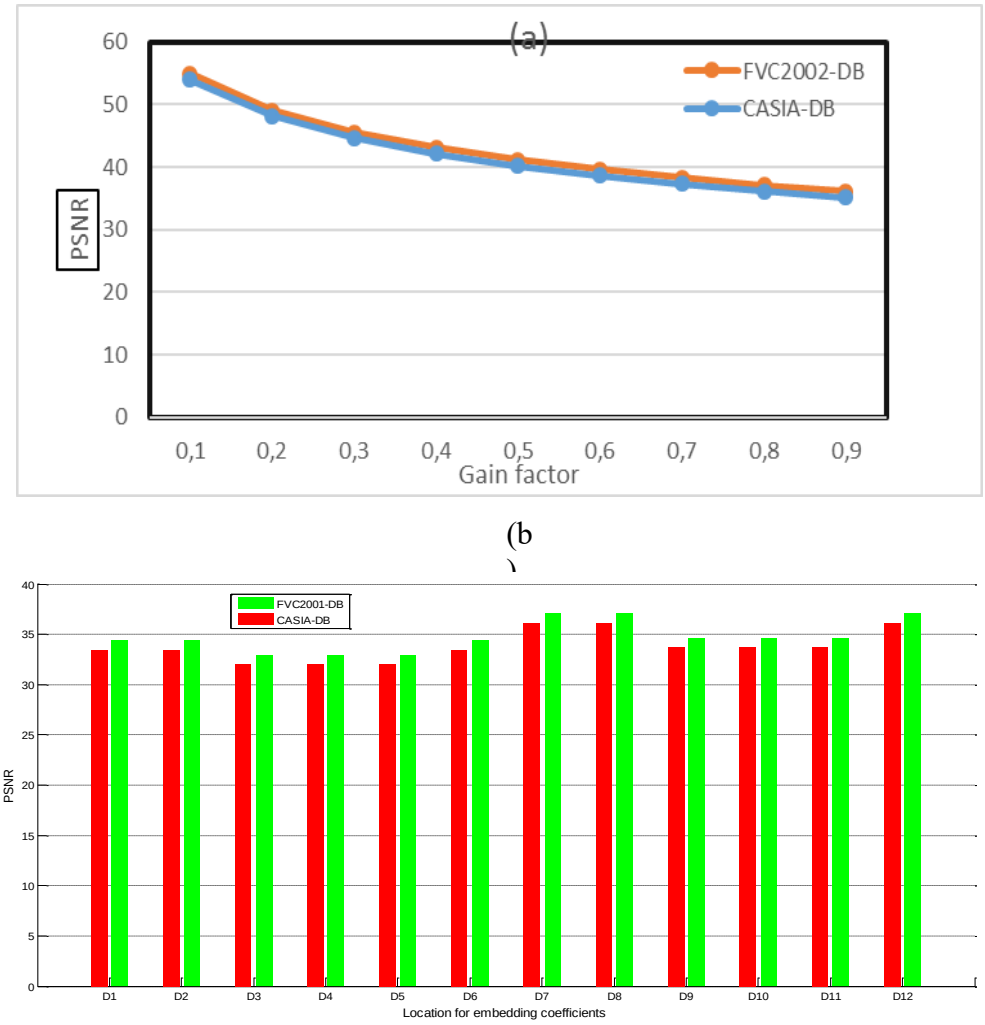


Figure 7- PSNR of fingerprint images versus the gain factor α (a), PSNR of fingerprint images versus the different directions for DTCWT (b).

The high ratio of *PNSR* means that the watermarked fingerprint image quality is high, thus, the similarity between the watermarked fingerprint image and the fingerprint image before watermarking operation implies high imperceptibility. Fig. 7 shows *PSNR* values obtained from our experiments versus the gain factor α and different directions for DTCWT to purpose embedding coefficients. It is obvious from Fig. 7(a) that higher α values result in lower PSNR of the watermarked fingerprint images. The $PSNR$ is determined as:

$$PSNR\left(I_{org},I_w\right)=10\log_{10}\left(\frac{R^2}{MSE\left(I_{org},I_w\right)}\right) \tag{28}$$

with R is the top grey scale of the image (for an 8-bit image $R=255$) and MSE is determined as:

$$MSE\left(I_{org},I_w\right)=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[I_{org}\left(i,j\right)-I_w\left(i,j\right)\right]^2 \tag{29}$$

where M,N are the dimensions of the original image, I_{org} is the fingerprint image before watermarking operation and I_w is fingerprint image after it.

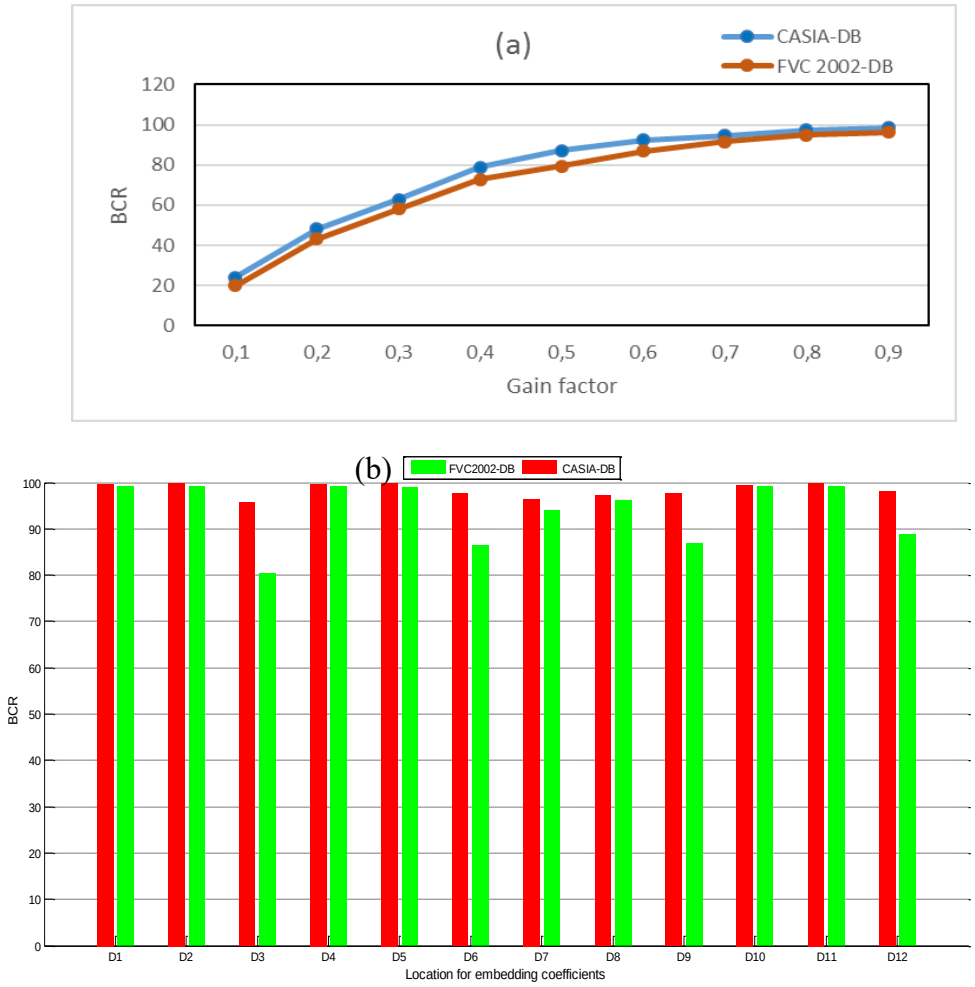


Figure 8- BCR rates of the derived watermark opposed to the gain factor α after rotation attack (angle = 0.25°) (a). BCR rates of the extracted watermark versus different directions for DTCWT after rotation attack (angle = 0.25°) (b).

The hybrid domain DTCWT-DCT with the differential extracting method is used to extract watermark embedded into the watermarked fingerprint image, that might be attacked by common image processing and geometric attacks; the extracted watermark is compared with its corresponding original watermark which does not need the original fingerprint image based on new proposed algorithm. To estimate the quality of derived watermark, the bit-correct ratio (BCR) is accepted to measure the sameness between the source watermark W and the derived watermark W'. The usage of this measurement became common lately as it grants more specific scale of values; BCR is characterized as the scale of precise extracted bits to the total number of integrated bits [19].

. It has been chosen to measure the similarity of watermark data that have been used as sequence binary in the proposed method. If the rate of BCR is equal to 100%, the extracted watermark will be identical to the original, which means achieving stronger robustness against common image processing and geometric attacks. Fig. 8 shows BCR rates of the extracted watermark obtained from our experiments versus the gain factor α and different directions for DTCWT after rotation attack (angle = 0.25°). It is apparent from Figure-8(a) the sameness (BCR %) of the source watermark and the derived watermark improved for higher values of α.

The BCR is defined as:

$$BCR = \frac{100}{L} \sum_{n=0}^{L-1} \begin{cases} 1, & W'_n = W_n \\ 0, & W'_n \neq W_n \end{cases} \quad (30)$$

where L is the length of watermark, W_n is the bit number n of original watermark W and W'_n is the bit number n of extracted watermark W'.

A. Gain Factor Selection

Several experiments have been conducted on the proposed method (DTCWT-DCT) for the purpose of evaluating its performance as compared to the other approaches that will be explained with detail in the section of discussion. The aim is to select the proper values of the gain factor α in equations 13 and 14 that fulfil both the inconspicuousness and the toughness demands of the watermarking. In addition, due to the random permutation value in equation 15, the experiments are deployed 15 times with what is agreed with our random algorithm for embedding the watermark data in order to obtain good and stable results. Furthermore, the watermark data has been embedded in various locations to increase the security against intentional attacks. The proposed algorithm is based on both databases, FCV2002-DB2 and CASIA-V5-DB, which has been tested on 80 fingerprint images from 10 persons, 8 fingerprint images each. As shown in Figure-7 and Figure-8, if we match between them, the best exchange between ocular aspect and watermark toughness is accomplished with the value of α = 0.8. We set α = 0.8 as the standard gain factor value.

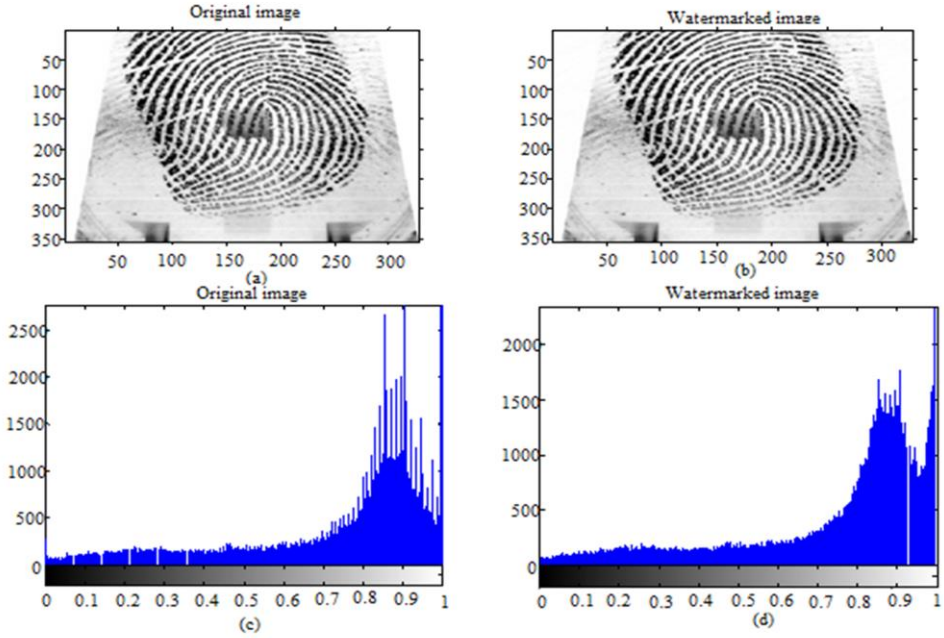


Figure 9- The original cover image (a), watermarked image (b), histogram of the original cover image (c), and watermarked image (d) for CASIA-V5-DB.

Figure-9 and Figure-10 show the original and the watermarked images along with their corresponding histograms in both databases, CASIA-V5-DB and FCV2002-DB2, respectively. The minutia points in the fingerprint image combine the ridges, short ridges, and other transition points that represent a high value in image decomposition. As show in the histograms in Figure-9(c) and Figure-10(c), most of the coefficients are centred around 0.7 and 1 values for CASIA-V5-DB database as well as 0.9 and 1 values for FCV2002-DB2 database. In the watermarked image, the wavelet coefficients range increases as compared to the original fingerprint image coefficients in both databases, as shown in Figure-9(d) and Figure-10(d).

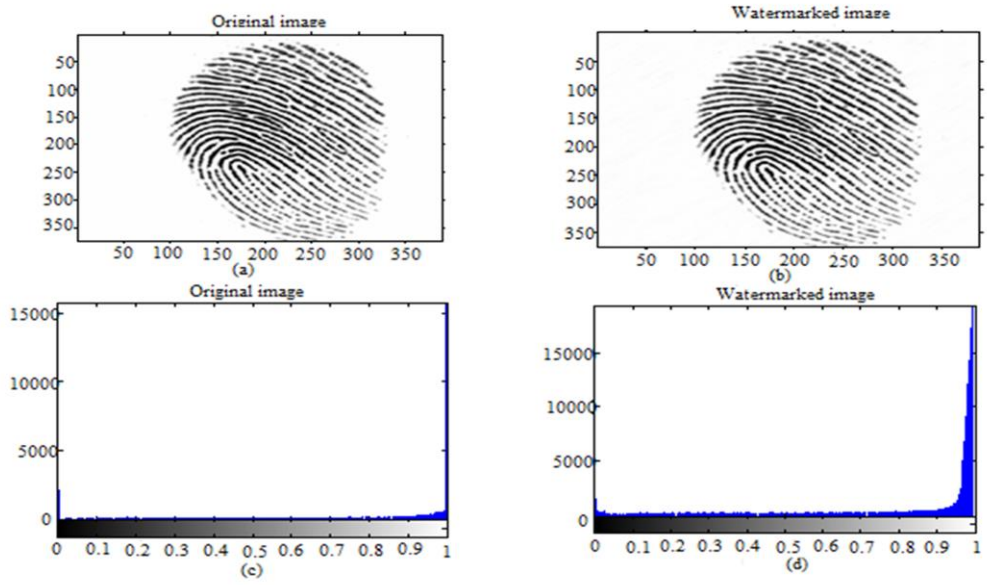


Figure 10- The original cover image (a), watermarked image (b), Histogram of the original cover image (c), and the watermarked image (d) for FVC2002-DB.

We can clearly see that the visual quality of the fingerprint image has not been affected by the watermarking process, as shown in Fig. 9 and Fig. 10. Furthermore, values of *PNSR* and the matching score that have been obtained in the experiments, as shows in Table- 1, prove that the fingerprint image has not been affected by the watermarking process.

Table 1- PSNR Values, BCR Rate and the Matching Score Value of the Proposed DTCWT-DCT Technique

Data Base	PSNR	BCR (%)	Matching Score
FCV2002-DB2	37.10	99.99	0.99
CASIA-V5-DB	36.15	99.96	0.98

Based on the good results obtained from the experiments of the proposed fingerprint image technique without attacks, it is clear that it has achieved, in the watermarking process, the visual quality of the fingerprint image without affecting watermark data robustness.

B. Robustness Tests

The robustness of the proposed system is measured against common digital image watermarking attacks such as image geometrical attacks, image compression, image processing and low-pass filtering attacks. This evaluation is observed based on the average of PSNR values, BCR rates and the matching score values between the original fingerprint images and the corresponding ones which have been the possibly attacked and distorted.

On the other hand, to evaluate the performance of the proposed DTCWT-DCT method, we have implemented the proposed watermarking algorithm on the standard image used in [10], 'lena', as a cover image with a size of 512x512, and the sequence binary with a size of 1000 bit, as a the watermark data. The robustness against different types of attacks is compared based on PSNR value and normalized cross correlation values (NCC).

1. Robustness Against Geometrical Attacks

The proposed method is evaluated against geometric attacks based on the results obtained from this experiment. The experiments have tested three types of geometric attacks (Resizing, cropping and rotation) and their results are shown in Table- 2.

Table 2-BCR Rate and the Matching Score Value of The Given DTCWT-DCT Method Under Geometrical Attacks

Attack	BCR (%)		Matching Score	
	FCV2002-DB2	CASIA-V5-DB	FCV2002-DB2	CASIA-V5-DB
Resizing (Q=1/2)	85.91	82.49	0.90	0.90
Resizing (Q=2)	99.86	99.57	0.97	0.98
Cropping (15 %)	99.78	99.07	0.92	0.95
Cropping (25 %)	98.82	97.25	0.83	0.86
Rotation (0.25°)	93.18	95.87	0.95	0.95

For resizing (Q=2), cropping (15 %,10%), and rotation (angle =0.25), the proposed method could almost be able to fully recover the watermark without affecting fingerprint image features. While, resizing (Q=1/2) failed to fully recover all the watermark data, as appeared for the BCR rate and matching score results in Table-2.

Furthermore, from the obtained results shown in Table-3, it seems that the proposed method succeeded to show strength against the geometric attacks of resizing and cropping compared the previously proposed method [10]. The choices of the embedding coefficient sub-bands in the proposed DCT-DTCWT method are far more adjustable than those used in the previous method [10] because the proprieties of the used hybrid transform domain under proposed algorithm with differential method.

Table 3- Comparisons of PSNR and NCC between the Proposed Method and the Previously Proposed Method in [10]

Attack	K. Ramani et al [10]		Proposed method	
	PSNR	NCC	PSNR	NCC
Resizing (20%)	7	0.48	**24.14**	0.52
Resizing (25%)	7.9	0.64	**27.55**	0.56
Resizing (75%)	8	0.73	**28.85**	0.58
Cropping (20 %)	7	0.48	**14.33**	**1**
Cropping (25 %)	7.8	064	**13.37**	**1**
Cropping (75 %)	8	0.73	**8.54**	**0.98**

Under Geometrical Attacks (scaling and cropping).

In the next experiments, some rotations have been added to the watermarked fingerprint images. The original image is set as the template for the purpose of comparison and it is rotated on six various rotation angles ±5°; ±10°; ±15°. Table- 4 shows the average of matching score values between the template images in both databases compared to the watermarked images with rotations.

Table 4- The Matching Score Values of the Given DTCWT-DCT Method Under Geometrical Attacks.

Angle	Matching Score	
	FCV2002-DB2	CASIA-V5-DB
Rotation(+5°)	0.87	0.87
Rotation(-5°)	0.87	0.85
Rotation(+10°)	0.85	0.84
Rotation(-10°)	0.84	0.85
Rotation(+15°)	0.84	0.81
Rotation(-15°)	0.83	0.82

Based on the previous table, our proposed method proved to be robust against geometrical attacks as shown from their obtained results in Tables- 2 and 3. In particular, it performs well against rotation attacks that did not affect the fingerprint features, as it appears in the results in Table-4.

2. Toughness Versus Image Compression

The BCR rate of the derived watermarks and score matching of minutiae points under JPEG lossy and JPEG2000 compression attacks are given in Table- 5. As for JPEG lossy compression, the quality factor (Q) varies from 70 to 80, whereas for JPEG2000 the compression ratio r varies from 4 to 8. The JPEG lossy compression image in order to compression factor is more 80, and the JPEG2000 compression image in order to compression ratio is lower 8. The watermark extracted is almost similar to the original. Furthermore, the watermarked fingerprint images have not been affected by image compression process, as revealed through the higher rate of similarities between fingerprints features for the matching score, as shown in Table-5.

Table 5- BCR Rate and the Matching Score Values of the Given DTCWT-DCT Method Under Compression Attacks

Attack	BCR (%)		Matching Score	
	FCV2002-DB2	CASIA-V5-DB	FCV2002-DB2	CASIA-V5-DB
JPEG 2000 (r = 4)	99,81	98,79	0,98	0,97
JPEG 2000 (r = 8)	93,66	94,22	0,97	0,96
JPEG lossy (Q = 70)	92,26	96,95	0,97	0,97
JPEG lossy (Q = 80)	95,73	99,01	0,98	0,97

In addition, the proposed method has been tested on a standard image under different JPEG compression factors, as shown in Table-6

Table6- Comparisons of PSNR and NCC Between the Proposed Method and Previously Proposed Method in [10]Under Compression Attacks

Attack	K. Ramani et al [10]		Proposed method	
	PSNR	NCC	PSNR	NCC
JPEG lossy (Q = 20)	26.1	0.74	**32.91**	0.64
JPEG lossy (Q = 30)	28	0.77	**34.97**	0.69
JPEG lossy (Q = 40)	29.9	0.88	**34.93**	0.75
JPEG lossy (Q = 50)	31.1	0.90	**35.28**	0.83
JPEG lossy (Q = 60)	33.5	0.93	**35.05**	0.92
JPEG lossy (Q = 70)	36	0.95	35.12	**0.96**

Acceptable results have been obtained from the proposed method under JPEG lossy and JPEG2000 compression. On the other hand, as shown in Table- 6, for JPEG compression, the quality factor (Q) varies from 20 to 80. The watermark extracted is almost similar to the original for compression factors of 50 and 70, as demonstrated by NCC values. Moreover, the proposed method succeeded to improve the results under compression images, as compared to the previous method [10]. The proposed method proved its robust performance in compression watermarking fingerprint images compression process.

3. Robustness Against Image Processing Attacks

We also evaluated the proposed method against noise addition attacks to measure its robustness against some noise that can be produced, for example, by the sensor and circuitry of a scanner or digital camera. Concerning the three groups of evaluated noises attacks (Speckle, Gaussian, and salt and pepper); we added them to the watermarked fingerprint image with different noise densities. It can be observed that the given technique is adequately robust versus noises with medium variances, although, for high variance noises, the technique gives adequate achievement, considering that the BCR values are above 90 % for the larger part of experiments. In addition, the watermarked fingerprint images have not been affected, as it could be noticed from the high percentages of similarities between fingerprints features for matching score, as shown in Table-5.

Table 7- BCR Rate and the Matching Score Values of the Given DTCWT-DCT Method Under Noise Addition Attacks

Attack	BCR (%)		Matching Score	
	FCV2002-DB2	CASIA-V5-DB	FCV2002-DB2	CASIA-V5-DB
Gauss noise (var = 0.005)	97.94	99.38	0.94	0.94
Gauss noise (var = 0.01)	95.64	98.47	0.91	0.93
Gauss noise (var = 0.02)	90.42	95.60	0.89	0.89
Salt and pepper (var = 0.01)	99.40	99.74	0.96	0.95
Salt and pepper (var = 0.02)	98.26	99.36	0.93	0.93
Speckle noise (var = 0.01)	96.30	99.06	0.92	0.95
Speckle noise (var = 0.02)	92.06	97.55	0.90	0.93

On the other hand, compared with the results obtained in the previosu method [10], the proposed method performs well under different noise densities, as shown Table 8.

Table 8- Comparisons of PSNR and NCC Values Obtained After Different Types of Image Noises Between Proposed Method and Previously Proposed Method in [10].

Attack	K. Ramani et al [10]		Proposed method	
	PSNR	NCC	PSNR	NCC
Gauss noise (var = 0.01)	20	0.97	19.85	**1**
Gauss noise (var = 0.05)	18.7	0.93	13.60	**0.95**
Gauss noise (var = 0.1)	16.3	0.86	11.35	**0.87**
Salt and pepper (var = 0.01)	25.5	0.97	24.77	**1**
Salt and pepper (var = 0.05)	23.9	0.96	18.33	**0.99**
Salt and pepper (var = 0.01)	20	0.92	15.43	**0.96**

Based on the obtained results, it can be observed that the proposed technique has an acceptable robustness against noises (Gaussian and salt and pepper) with medium variances. The NCC values were above 90 % for the larger part of experiments and it succeeded to improve their results compared with that in the previous method [10] .

Thus, in rapport to the results given in Tables- 7, 8, the shown method has proven better performance against the three groups of the evaluated noises attacks (Speckle, Gaussian, and salt and pepper).

4. Robustness Against Low-Pass Filtering Attacks

Table-9 demonstrates the results of the experiment to observe the robustness of the proposed method against low-pass filtering. Gaussian filter and Wiener filter produced the highest BCR, with values of 90% to 92%, respectively, for the database FCV2002-DB, unlike the Average filter and Median filter for which the BCR rate was weak. However, the percentage of the matching score between fingerprint features was higher than 85% for all low-pass filtering attack experiments. This implies that they are acceptable results according to the values accepted by fingerprint recognition tools that we used in our proposed method.

In addition, for standard images that were used in previous studies [20, 21], our method has better performance against Gaussin filter, as shown in Table-13.

Table 9- BCR Rate and the Matching Score Values of the Given DTCWT-DCT Method Under Low-Pass Filtering Attacks

Attack	BCR (%)		Matching Score	
	FCV2002-DB2	CASIA-V5-DB	FCV2002-DB2	CASIA-V5-DB
Average filter (3x3)	72.58	68.73	0.85	0.88
Median filter (3x3)	76.69	64.77	0.88	0.90
Wiener filter (3x3)	92.19	84.96	0.89	0.92
Gauss filter (3x3) (var=1)	90.71	88.78	0.87	0.90

Gauss filter (3x3) (var=1.5)	81.75	78.78	0.86	0.89

According the results presented in Table- 9 for the tested low-pass filtering attacks, the proposed method has proven better performance against Gaussian filter and Wiener filter attacks. However, it exhibits weak robustness against the other low-pass filtering attacks.

C. Similarity with Other Techniques

To begin with this subsection, we have conducted diver's experiments to evaluate the achievements of the given DTCWT-DCT method compared with other fingerprint image watermarking approaches. The approach in a previous study [20] proposed embedding of the face features (watermark) into the fingerprint image (cover) via a generated secret key to locate the pixels to be watermarked while preserving the fingerprint minutia points under the FVC2002-DB2 fingerprint database. While, both of the previous approaches [20, 21] have been tested using the CASIA-V5-DB fingerprint image database. Ghany *et al*.[20] proposed a wavelet-based approach to embed a multi-bit watermark, based on DNA data into fingerprint images. In the other study [21], the proposed watermarking scheme was based on inserting, in the fingerprint image, a binary image from an encrypted password using Dual Tree Complex Wavelet Transform. Although, the previous works have some advantages for fingerprint image watermarking process which achieved the combination between imperceptibility, the payload of the watermark embedded and achieving an only high score of matching between original fingerprint images in databases and its corresponding which the possibly attacked and distorted. However, the extracted watermark after the watermarking process not found for its recover, as shown in Table- 10.

Table10- Comparisons Among Different Robust Fingerprint Image Watermarking Methods in Terms of Peak Signal-to-Noise Ratio (PSNR), The Bit-Correct Ratio (BCR), Matching Score

Items	Ghany et al. [20]	Alkhathami et al. [21]	Bousnina et al. [22]	Proposed Method
Watermarking techniques	DWT-DNA	DTCWT	OLPP	DTCWT-DCT
Embedding domain	Multiresolution	Multiresolution	Spatial	Hybrid domain
Watermark	Sequence Binary DNA	-Text -Binary Image	Face features	Sequence Binary
Databases	CASIA-V5-DB	CASIA-V5-DB	FCV2002-DB2	CASIA-V5-DB
PSNR (dB)	26	36.23	33.75	36.15
The Matching scores	1	1	1	1
BCR(%)	-	-	-	100

On the other hand, these previous techniques focus only on authentication and not provide robustness of the extracted watermark after watermarking process. The extracted watermark is used to certainly identify the real owner of the fingerprint that was possibly attacked or distorted.

In addition, the conducted experiments of the previous works have been tested only under some several attacks, such as image processing. While, the other geometrical attacks had not been tested. For example, rotation attacks, when tested it to prove proposed method able or cannot retain the features of fingerprint and watermark data though some rotations have been made on the fingerprint images. However, Alkhathami's approach [21] has achieved good results under geometrical attack. Nevertheless, it requires the original fingerprint template at the extraction stage (not blind). Conversely, our proposed approach was blind, which implies the non-requirement to the original fingerprint image to extract the watermark and, thus, beefing up the robustness of watermark data and the security of the fingerprint recognition system.

Furthermore, the proposed algorithm has been tested under different several common attacks such as image processing, compression and geometrical attacks. Good quality of the watermarked fingerprint images was achieved compared with the other methods [20-22], as shown in Table- 10. This is clear since the PSNR value was almost greater than 36 dB in the majority of the experiments for all tests on the fingerprint images in CASIA-V5-DB, while its value was greater than 37 dB for FVC2002-DB2. The BCR rate achieved 100% for all the extracted watermarks after watermarking process.

Table 11- The Coordinating score between the Template and Rotated Images Obtained by DTCWT and our Proposed Method

Technique	Image No	Rotation Angles						
		0	**+5**	**+10**	**+15**	**-5**	**-10**	**-15**
Alkhathami et al[22]	1	0.86	0.86	0.86	0.86	0.86	0.86	0.86
	2	0.78	0.78	0.78	0.78	0.78	0.78	0.78
	3	0.80	0.80	0.80	0.80	0.80	0.80	0.80
	4	0.83	0.83	0.83	0.83	0.83	0.83	0.83
	5	0.85	0.85	0.85	0.85	0.85	0.85	0.85
Proposed method	1	1	0.87	0.92	0.91	0.87	0.86	0.87
	2	1	0.94	0.93	0.93	0.92	0.92	0.97
	3	1	0.90	0.81	0.86	0.88	0.89	0.90
	4	1	0.80	0.89	0.88	0.75	0.92	0.83
	5	1	0.89	0.85	0.69	0.71	0.75	0.78

The proposed method achieved a high score of matching fingerprint features compared to the previously proposed method [21], as shown in Table- 11. We used five random comparison results that have been obtained from five watermarked fingerprint images and rotated them on six different rotation angles (±5°; ±10°; ±15).

Although the method proposed in this paper have been tested under some of the same attacks with a strong factor as that in the previous methods, and obtained unsatisfactory results compared with the results of these methods. However, the proposed method has achieved the combination of imperceptibility, robustness and security, all with a simplicity in the application when using a weak factor of the same attacks; in addition, it was tested under others attacks which had not been used in the previous methods. One of the previously proposed methods [22] focused only on the PSNR values of watermark, which achieved good results, without testing PNSR values for the cover image under these attacks. This is contrary to the other proposed method [20], which focused only on the PSNR values of the cover image, which also achieved a good result against the noise attacks, without evaluating the extracted watermark. In the third previously proposed method [21], the focus was on hiding the watermark into the fingerprint image without any attacks tested.

On the other part, as show in Table- 8 that contains the obtained results of PSNR values after Gaussian and salt and pepper noise attacks, it can be observed that the proposed technique is low of imperceptibility compared to the other previously reported technique [10]. The proposed method has been tested on the biometric image (fingerprint) in order to preserve the embedded watermark without affecting minutia points of the cover fingerprint image (not the cover fingerprint image). Thus, robustness for watermark data was achieved and security of biometric data was improved. When we tested our proposed algorithm on standard images (which do not have features biometric), logically, we had a decrease in PSNR and acceptable values of NCC.

Table 12- Comparisons of PSNR Values Obtained After Different Types of Image Noises Between Proposed Method and Previous Proposed Method in [22]

Technique	Image No	Salt & Pepper (0.2 noise density)	Speckle (0.04 Parameter value)	Poisson
Alkhathami et al[22]	1	36.23	18.64	27.21
	2	35.76	18.61	27.20

	3	36.02	18.30	27.06
	4	34.82	18.42	27.09
	5	35.72	18.72	27.26
	6	34.42	18.82	27.34
Proposed method	1	11.22	17.68	36.58
	2	11.19	17.71	36.60
	3	10.96	17.76	36.61
	4	11.03	17.74	36.61
	5	11.14	17.47	36.58
	6	11.08	17.74	36.61

Based on the comparison results of the fingerprint image watermarking, the proposed method in this paper shows that the best exchange between visual quality and watermark toughness is accomplished without attacks. While, when tested against some common several attacks such as image processing, compression and geometric attacks, the watermark was not completely recovered for some attacks, as shown by the high strength JPEG2000 or JPEG lossy compression. However, better matching score between minutiae points for all watermarked fingerprint images have been achieved compared to the previous methods, as shown in Table- 12. In addition, depending on the related results provided in Table- 11, the suggested algorithm shows high solidity towards a rotation attack**.**

On the other hand, to evaluate the performance of the proposed DTCWT-DCT method, a comparison is performed with other recent watermarking approaches that use standard images. The implementation proposed watermarking algorithm on standard images used by techniques in previous reports [25, 26, 27] with a cover image size of 512x512 and a sequence binary with watermark data size of 512 bit. Different classes of images such as the standard images of Lena, Mandril, Peppers, Barbra have been considered in this comparison. These images are collected from CVGUGR image database and USC-SIPI image database. Figure-11 shows PSNR values obtained from four standard images under the proposed DTCWT-DCT and different recent watermarking methods proposed in the above mentioned studies. It has been observed that one of the proposed methods [25] is almost providing the better imperceptibility. However, the PSNR values of our suggested DTCWT-DCT stayed stable and acceptable in the four standard images compared to the other methods. This may be due to the fact that the proposed algorithm focuses on choosing the location of embedding to achieve better imperceptibility and h robustness against many different image's attacks.

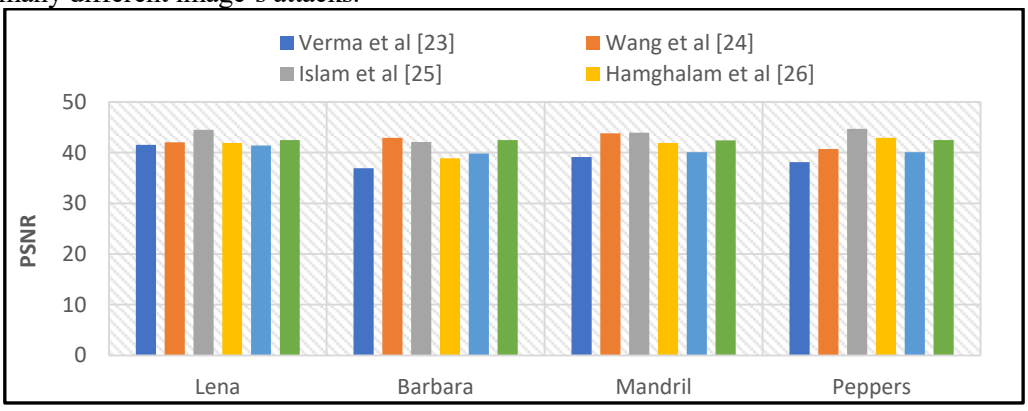


Figure 11- Comparison of Imperceptibility with different methods.

The robustness against different types of attacks is compared based on bit error rate (BER), as calculated previously [23], between the original watermark and the extracted watermark. The robustness values have been compared with those of the previous methods [25, 28], as shown in Table-13.

Table 13- The comparison of the results with previous methods [28, 25] for different attacks in terms of BER

Attacks	Lena			Peppers			Mandril		
	Mehtael al [28]	Islam et al [25]	Proposed	Mehtael al [28]	Islam et al [25]	Proposed	Mehtael al [28]	Islam et al [25]	Proposed
SPN(0.005	0.0566	0.0253	**0,0001**	0.0557	0.0351	**0,0001**	0.0518	0.0390	**0,0002**

)									
SPN (0.01)	0.1152	0.0429	**0,0011**	0.1230	0.0703	**0,0030**	0.1025	0.0625	**0,0025**
SPN (0.02)	0.1638	0.0859	**0,0129**	0.1973	0.1250	**0,0175**	0.1768	0.1445	**0,0187**
GN (0.001)	0.0547	0.0351	**0**	0.0557	0.0390	**0**	0.0684	0.0429	**0**
GN (0.005)	0.2490	0.2089	**0,0084**	0.2637	0.1933	**0,0111**	0.2480	0.2226	**0,0141**
GN (0.01)	0.3584	0.3476	**0,0432**	0.3635	0.3535	**0,0521**	0.3281	0.3105	**0,0517**
IS	0.0107	0.0020	**0**	0.0107	0.0136	**0**	0.0557	0.0410	**0**
AF (3 × 3)	0.0039	0.0664	0,7379	0.0078	0.0391	0,7197	0.0410	0.1601	0,6374
GF (3 × 3)	0	0.0039	**0**	0.0020	0.0195	**0**	0.0315	0.0153	**0**
JPEG 50	0.0020	0.0020	0,0507	0.0020	0.0020	0,0756	0.0256	0.0059	0,1102
JPEG 70	0	0	0,0092	0	0	0,0133	0.0049	0	0,0495

Based on the results obtained from the comparison show in Table-13, the proposed DTCWT-DCT method provides improved robustness against some attacks. It showed an improvement in its strength against image processing attacks like salt and pepper noise (SPN), Gaussian noise (GN), Gaussian filtering (GF) and image sharpening (IS). While, it stays weak against other attacks like compression attacks, as compared to the other proposed methods [25, 28]. However, the proposed method gives also better solution to prove ownership claim under diverse attacks.

Conclusions

This research paper shows a vison-less, solid and simple watermarking system relying on the mixture of DTCWT and DCT spheres. In the integrating phase, the differing technique is applied to two transformed sub-vectors such that the removal of the watermark is carried out using the distinction of the corresponding watermarked sub-vectors only.

Generally, the experimental findings show that our system offers a tremendous solidity versus numerous image attacks such as image processing, compression, and geometrical

attacks. Moreover, the nature of the watermarked fingerprint image is adequate in the condition of preserving fingerprint features (minutiae points) as just the *PSNR* per watermarked image is above 36 dB, and the achieving high strong of security in terms of correlation of extracted watermark data as the accepted results obtained of *BCR* values of derived watermark and score matching of minutiae points for cover image.

Furthermore, the necessity of the mixture of the DTCWT and DCT transforms have been investigated over the idea of the previously proposed methods [10, 22] that depended only on the DTCWT transform. The proposed blind method which is based on DTCWT-DCT hybrid transform has a higher robustness than Alkhathami 's method [23] which is based only on DTCWT transform with the requirement of the original fingerprint template at the extraction stage (non-blind). In addition, the proposed algorithm shows a high robustness against rotation attacks. Furthermore, compared with a previous method [10], our results showed an improvement in its strength against several different image attacks like scaling, cropping and other image processing attacks like salt and pepper and Gaussian noise. While, it stays weak against some other attacks such speckle and poison techniques, compared with the proposed methods. However, the proposed method gives also a better solution to prove ownership claim under diverse attacks. The outcomes of the tests have also shown that the suggested (DTCWT-DCT) method has enhanced the robustness and high security compared to the other prior fingerprint image watermarking schemes. Thus, the proposed technique will add a validation factor in the authorisation process by integrating user identification and bio-metric features with high security, particularly when the transformation of the fingerprint image between the sender and receiver is made.

Acknowledgment

We would like to show our gratitude to the Ministry of Higher Education of Malaysia, under the Fundamental Research Grant Scheme vote number FRGS/1/2019/ICT02/UMP/02/1 for supporting this study.

References

1. Jain, A.K., Prabhakar, S., Hong, L., Pankanti, S. **2000**. Filterbank-based fingerprint matching, *IEEE Transactions on Image Processing*. **9**: 846–859.

2. Awang, S., Sulaiman, J., Noor, N., Mohd, K. and Bayuaji, L. **2017**. Comparison of accuracy performance based on normalization techniques for the features fusion of face and online signature. *Advanced Science Letters*, **23**(11): 11233-11236.

3. Noore, R., Singh, M. and Vatsa, M.M. **2007**. Enhancing security of fingerprints through contextual biometric watermarking, *Forensic Science International*. **169**(2007): 188–194.

4. Mousavi, S.M., Naghsh, A. and Abu-Bakar, S.A.R. **2014**. Watermarking techniques used in medical images: a survey, *Journal of Digital Imaging*. **27**: 714–729.

5. Alkhathami, M. **2015**. Watermarking techniques for genuine fingerprint authentication.

6. Shih, F.Y. and Wu, S.Y.T. **2003**. Combinational image watermarking in the spatial and frequency domains, *Pattern Recognition*. **36**: 969–975.

7. Thanki, R. and Borisagar, K. **2015**. Sparse Watermarking Technique for Improving Security of Biometric System, *Procedia Computer Science*. **70**: 251–258. doi: 10.1016/j.procs.2015.10.083.

8. Kundur, D. Hatzinakos, Toward robust logo watermarking using multiresolution image fusion principles, *IEEE Transactions on Multimedia*. **6**(2004): 185–198. doi:10.1109/ TMM. 2003. 819747.

9. Lebcir, M. and Awang, S. **2018**. Fingerprint Image Watermarking in Spatial, Frequency and Multiresolution domain: Techniques and challenges, In: Proceedings Book: National Conference for Postgraduate Research (NCON-PGR 2018), 28-29 August 2018, Universiti Malaysia Pahang, Gambang, Pahang. pp. 1-7.

10. Ramani, K., Prasad, E.V. and Varadarajan, S. **2010**. Protecting Digital Images Using DTCWT-DCT, in: *Communications in Computer and Information Science*, **2010**: 36–44. doi:10.1007/978-3-642-15766-0_6.

11. Lebcir, M., & Awang, S. **2019**. A Review on Type of Attacks on Fingerprint Image and Watermarking Techniques. In IOP Conference Series: Materials Science and Engineering (Vol. 551, No. 1, p. 012071). IOP Publishing.

12. Benoraira, A., Benmahammed, K., & Boucenna, N. **2015**. Blind image watermarking technique based on differential embedding in DWT and DCT domains. *Eurasip Journal on Advances in Signal Processing*, **2015**(1). https://doi.org/10.1186/s13634-015-0239-5.

13. Selesnick, I.W., Baraniuk, R.G., Kingsbury, N.G., Selesnick, I.W., Baraniuk, R.G. and Kingsbury, N.G. **2005**. The dual-tree complex wavelet transform, *IEEE Signal Processing Magazine*. **22**(2005): 123–151. doi:10.1109/MSP.2005.1550194..

14. Loo, P. and Kingsbury, N. **2000**. Digital watermarking using complex wavelets, in: Image Processing, 2000. *Proceedings. 2000 International Conference On*, **2000**: 29–32.

15. Coria, L.E., Pickering, M.R., Nasiopoulos, P. and Ward, R.K. **2008**. A video watermarking scheme based on the dual-tree complex wavelet transform, *IEEE Transactions on Information Forensics and Security*. **3**(2008): 466–474.

16. Yang, H., Jiang, X. and Kot, A.C. **2010**. Image watermarking using Dual-Tree Complex Wavelet by coefficients swapping and group of coefficients quantization, in: 2010 IEEE International Conference on Multimedia and Expo, ICME 2010, 2010: pp. 1673–1678. doi:10.1109/ICME.2010.5582958.

17. Kingsbury, N. **2000**. A dual-tree complex wavelet transform with improved orthogonality and symmetry properties, *IEEE International Conference on Image Processing*. **2**(2000): 375–378. doi:10.1109/ICIP.2000.899397.

18. H.-C. Huang, S.-C. Chu, J.-S. Pan, C.-Y. Huang, B.-Y. Liao. **2011**. Tabu search based multi-watermarks embedding algorithm with multiple description coding, Information Sciences. **181**: 3379–3396. doi:10.1016/j.ins.2011.04.007.

19. Zhao, Y., Campisi, P. and Kundur, D. **2004**. Dual domain watermarking for authentication and compression of cultural heritage images, *IEEE Transactions on Image Processing*. 13 (2004) 430–448. doi:10.1109/TIP.2003.821552.

20. K.K.A. Ghany, G. Hassan, A.E. Hassanien, H.A. Hefny, G. Schaefer, A.R. Ahad. **2014**. A Hybrid Biometric Approach Embedding DNA Data in Fingerprint Images, 2014 International Conference on Informatics, Electronics & Vision (ICIEV). 1–5. doi:10.1109/iciev.2014.6850836.

21. M. Alkhathami, F. Han, R. Van Schyndel. **2013**. Fingerprint Image Watermarking Approach Using DTCWT without Corrupting Minutiae, 2013 6th International Congress on Image and Signal Processing (CISP): 1717–1723. doi:10.1109/cisp.2013.6743953.

22. N. Bousnina, S. Ghouzali, M. Lafkih, O. Nafea, M. Mikram, W. Abdul, D. **2016**. Aboutajdine, Watermarking for protected fingerprint authentication, 2016 12th International Conference on Innovations in Information Technology (IIT): 127–131. doi:10.1109 /innovations .2016. 7880039.

23. V.S.Verma, R.K. Jha and A. Ojha. **2015**. Digital watermark extrac- tion using support vector machine with principal component analysis based feature reduction, *Journal of Visual Communication and Image Representation*, **31**(2015): 75–85.

24. X.Y. Wang, Y.N. Liu, H. Xu, A.L. Wang and H.Y. Yang. **2016**. Blind optimum detector for robust image watermarking in non-subsampled shearlet domain, *Information Sciences*, **372**: 634–654.

25. M. Islam, A. Roy, R.H. Laskar. **2018**. Neural network based robust image watermarking technique in LWT domain, *Journal of Intelligent & Fuzzy Systems.* **34**: 1691–1700. doi:10.3233/JIFS-169462.

26. M. Hamghalam, S. Mirzakuchaki and M.A. Akhaee, Geometric modelling of the wavelet coefficients for imagewatermarking using optimum detector, IET Image Processing 8(3) (2014), 162–172.

27. G. Kasana and S.S. Kasana. **2017**. Reference based Semi Blind Image Watermarking Scheme in Wavelet Domain, *Opti*k, **142**: 191–204.

28. Mehta, R., Rajpal, N. and Vishwakarma, V.P. **2016**. LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR, Multimedia Tools and Applications 75(7) (2016), 4129–4150.