Reversible Watermarking Technique for Fingerprint authentication based on DCT

Mohamed Lebcir¹, Suryanti Awang¹, and Ali Benziane²

¹Soft Computing & Intelligent Systems Research Group (SPINT), Faculty of Computing, University Malaysia Pahang, UMP, Lebuhraya Tun Razak 26300, Kuantan, Pahang, Malaysia.

²Faculty of Science and Technology, University of Djelfa, Algeria.

mlebcir78@gmail.com

Abstract. In this paper, a new reversible and blind fingerprint image watermarking technique based on the differential method and discrete cosine transform (DCT) domains is presented. The focus is to increase the security of the fingerprint image in authentication systems. Two DCT-transformed sub-vectors are employed to embed the bits of the watermark sequence in a differential scheme. The original sub-vectors are acquired by the DCT transform on the host fingerprint image. In the extraction process, a minor variance between the sub-vectors that correspond to the watermarked fingerprint image directly allows access to the embedded watermark sequence; therefore, the extraction process doesn’t require an original fingerprint. The original fingerprint image is then recovered from the watermarked fingerprint image based on the reversible watermarking technique. The similarity between the reversible fingerprint image and the original is considered, and we could extract minutiae points from it without a problem. The proposed technique is evaluated using 80 fingerprint images from 10 persons for each from FVC2002 fingerprint database. Eight fingerprint images have been taken from each person to be used as the template then the process was followed by embedding the watermark into each fingerprint image. The experimental results validate the proposed method able to give promising results in preserving the fingerprint image security.

Keywords: Fingerprint, Fingerprint image watermarking; Frequency Domain; DCT; Reversibility

1. Introduction

Automated systems with the implementation of Artificial Intelligence techniques widely used in many areas to enhance the quality of the system [1,2,3]. It’s becomes more popular from late 1990 until now. An authentication system based on fingerprint image also does not left behind in this trend. A fingerprint image indicates the process of impressing the ridges and valleys pattern on the fingertip surface; the combination of their minutiae points then determines the uniqueness of a fingerprint [4,5] which permits the use of the fingerprint images in the user authentication process due to their uniqueness [6]. Thus, it is essential to protect the fingerprint’s authenticity. In order to avoid issues of compromised fingerprint recognition system, three different research domains, namely fingerprint biometric for authentication, cryptosystem for confidential data and reversible watermarking for the integrity.
Digital watermarking could be used to check a fingerprint sample authenticity [6]. This approach is used to embed the watermark data into the original fingerprint image in the purpose of maintaining fingerprint ownership security. As an additional protection layer, we may encrypt the watermark data before the watermark is embedded [7]. Thus, the operator’s key role is preventing attackers to gain access to the watermark. The reversible watermarking technique extracts minutiae points from fingerprint image watermarked without problem.

We may classify the watermarking techniques into three embedding domains after watermark pattern embedding location of the domain [7]. The domains are spatial domain, frequency domain and the multiresolution domain. Spatial domain of embedding fingerprint watermark directly into the pixels of the host image. 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 [8]. The technique has several advantages such as less complication coupled with 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.

Whereas, frequency domain denotes the rate of change in the values of 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 [9]. The commonly used watermarking transformation techniques in frequency domain are the Fast Fourier Transform (FFT) technique, and the Discrete Cosine Transform (DCT) [10]. The use of DCT algorithms for embedding watermark into fingerprint image is sufficiently for compression attacks. Thus, in this paper, DCT is implemented that based on reversible watermarking technique to enhance the security of the fingerprint recognition system for authentication purposes.

The next section of this paper will discuss about related work that combined watermarking and fingerprint biometrics for enhancing the security on fingerprint recognition system, followed by our watermarking technique methodology and ends with experimental results and discussion.

2. Related work
There are some notable researches in a combination of watermarking and fingerprint biometrics for enhancing the security purpose in fingerprint recognition system. A fragile authentication technique for watermarking fingerprint images was proposed by Pankanti and Yeung [11]. In their research, an authentication key was used to embed a watermark into a fingerprint image in the spatial domain. The method proposed has the ability pinpoint any part of the fingerprint image which has been altered. Their watermarking approach does not present observable loss to the process of the fingerprint authentication. However, the technique is not suitable for protected fingerprint sample transmission over network which is not secure. This is due to the high vulnerability of embedded watermarks towards attackers.

In another research, a method was presented by Gunes et al. [12] and Uludag et al. [13]. This method safeguards the orientation of the quantized gradient in the domain of the embedded watermark. Two techniques for fingerprint image watermarking in the spatial domain were described by Gunes et al. The first approach makes use of gradient orientation analysis during the process of embedding the watermark. Hence, none of the features extracted by making use of gradient information is altered. Likewise, the second technique conserves the singular points within the fingerprint image. Therefore, there is no disruption to the classifications of the fingerprint image that is watermarked using this approach. In similar manner, Uludag et al. put forward a spatial method for embedding watermarking fingerprint images without ruining the features of the fingerprint. With this approach, the characteristic features of the fingerprint are first detected. The watermark is then embedded into the fingerprint image in such a way that the fingerprint features are not distorted by the watermark. It is questionable if this method could trigger potential changes in the features of the fingerprint after the incorporation of the watermark data, or whether the features shall be retained. However, the entire single points as well as features of the fingerprint which were extracted using gradient information are secured within the fingerprint image.
In a different research, incorporation of a facial image was proposed to be hidden in the fingerprint image by A. K. Jain et al. [14]. This method involves inserting a user face’s eigenface coefficients in the fingerprint image. Hence, during the process of decoding, the recovered facial image may be used to ascertain the originality of the image. In their research, the information from the user face was primarily used to verify the fingerprint image. A secret key is randomly generated and one-bit stream of the coefficients of the eigen face is then inserted into the pixels of selected fingerprint image. The process of embedding the face is in the spatial domain. Thus, it does not depend on the original image in order to extract the watermark (blind). The main disadvantage of this approach is it mainly works in the spatial domain, whereby, the embedded watermark is highly vulnerable to attack. This is because spatial domain makes use of direct values of image pixels.

In a similar approach, a scheme of watermarked spatial fingerprint which utilizes eigenfaces was proposed [15]. The watermark was embedded into the fingerprint through steganography in the ‘sailboat’ image. The solution was aimed at inscribing black squares around the minutiae in order to denote the ones that need to be dodged during the watermarking phase. After evaluation, this technique was proven to reveal good performance especially towards authentication and protection of fingerprint minutiae following the watermarking process. However, there is the challenge of computational complexity. This is mainly due to the long duration of time would be required to process a combined watermarking and steganography procedure. Other than that, this approach is the spatial embedding domain that was not sufficiently resistant to factors such as compression, noise as well as filtering attacks. This is associated with the pixels were changed thereby sacrificing the image quality.

A new watermark embedding method has been presented by Bousnina et al.; it consists of generating a secret key that can be used to designate the pixels to be watermarked. The fingerprint minutia points, thus, would be protected and security would be enhanced along the extraction stage of the watermark. The following step consists of inserting the face features (watermark) into the fingerprint image (cover); the fingerprint minutia points, thus, would be protected via Orthogonal Locality Preserving Projections (OLPP) method [16]. Although this approach resistance efficiency was not checked to confront other potential attacks such as geometric attacks, it was able to prevent the intentional attacks where the attacks would acquire the secret key in watermark extracting.

Ghany et al.’s based on wavelet approach, on the other hand, consists of embedding DNA data based multi-bit watermark into fingerprint images using DWT [17]. This method proved its robustness and straightforwardness, yet the original fingerprint template is required at the stage of extraction (non-blind). This method proved to be robust with high imperceptibility; however, the need for the original fingerprint when extracting the watermark decreased its security.

Another method was proposed by Abraham et al.; the technique is simple and blind, and it uses DWT in watermarking and in detecting digital image [18]. This method is characterised as blind which implies the unneccessity of the original fingerprint template along the extraction stage (blind). The embedded information robustness of in this approach proved to be acceptable.

Alkhathami et al.’s approach proposed a watermarking algorithm which can be embedded with the unique minutiae into fingerprint images so as to protect it from possible effects of the embedded watermark [19]. A new Dual-tree Complex Wavelet Transform (DTCWT) is used in this technique which had the advantages of preserving the fingerprint minutiae from potential embedded watermark effects. This technique, however, is non-blind; the watermark extraction process requires the the original image.

Alkhathami et al., adding to the last algorithm, introduced two watermarking techniques [20,21] in which both DWT and DCT techniques features are combined. These two techniques consist of combining the fingerprint of owner’s grayscale facial image and other identification details in the model of binary text image into the fingerprint image [20]. While, in [21], Discrete Cosine Transform (DCT) algorithm is used in which two watermarks are combined for embedding into fingerprint images. These techniques achieved successful payload capacity without corrupting the minutiae points. Through this technique, more authentication factors will be added based on the watermark messages. However, this
The technique is characterised as non-blind due to the necessity for the original fingerprint image during the watermark data extraction stage.

Therefore, based on the related works, we can see that most of the researchers focus on non-blind watermarking. However, the problem with non-blind is that it prone to lack of security to the fingerprint image because original fingerprint image is needed in extracting the watermark data. Thus, we come out with our proposed solution in this paper that will utilize blind watermarking in frequency domain with reversible watermarking technique.

3. Methodology
The proposed algorithm is extended from the idea of Benoraira et al [2] that used the hybrid of DWT and DCT algorithms in line with the differential embedding technique. The technique of differential embedding depends on two DCT transformed sub-vectors to ensure the blind extraction of the watermark. Furthermore, the proposed algorithm added the Reversible Watermarking Technique for Fingerprint authentication based only on DCT blind that Benoraira et al. not used it in their method.

To embed watermark into fingerprint image, the reversible watermarking algorithm that based on Discrete Cosine Transform (DCT) is used in this proposed method. The transform DCT permits to divide the image into different blocks and easily embedding the watermark into selected blocks. In addition, this algorithm based on differential embedding technique that depends in two DCT transformed sub-vectors to ensure the blind extraction of watermark. Further, new idea has been added in this algorithm, could recovering the original fingerprint image from the watermarked fingerprint image based on reversible watermarking technique. Thus, could extracting minutiae points easily from reversible fingerprint image that seem as copy than the original.

The most common \(DCT\) definition of a 1-Dimension sequence \(x\) of length \(N\) is:

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

where

\[
\alpha(k) = \begin{cases} 
\sqrt{\frac{2}{N}} & \text{for } k = 0 \\
\sqrt{\frac{2}{N}} & \text{for } k = 1, 2, \ldots, N-1
\end{cases}
\]

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

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

DCT based watermarking is split into three levels: low, middle and high. The lower frequencies sub band includes the image most important visual parts where the majority of the signal energy lies. Compression and noise attacks delete the image high frequency component. The watermark is embedded through changing the middle frequency sub-band coefficients. This, therefore, will not affect the image visibility and the compression will not remove the watermark [23]. DCT is applied on the fingerprint image to obtain two sub-vectors for purpose watermarking and reversibility process based on embedding technique. The extraction is therefore blind due to differential embedding of the watermark in the resulting two DCT transformed sub-vectors.

The flowchart that shown in in figure 1 represents fingerprint authentication system using reversible watermarking technique. There are 3 major processes; watermarking embedding process, watermarking extracting process and reversibility watermarking process in the respective systems. The watermarking embedding system begins with performing a fingerprint scan using a fingerprint scanner to acquire a fingerprint image and the extracted features are stored in the database to be used during the feature matching. The embedding process is 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. Using DCT and the differential embedding method which will be explained in detail later. Here, the watermark is embedded into fingerprint image for further use in the fingerprint-based authentication system that the possibly attacked. The next process, the extracted watermark is compared with the original watermark. If the extracted watermark is not genuine, the verification process is rejected, and the process is ended. Otherwise, the reversible watermarking system to extract new features from reversible watermarked fingerprint image, the new extracted features from reversible watermarking system are sent with the genuine features in the database to achieve matching together and the process is ended with the approved verification.

Figure 1. Fingerprint authentication system using reversible watermarking technique

The main steps of the proposed watermark embedding procedure can be described as follows:

3.1. Watermark Embedding Process:
This is the first process in proposed method. The proposed watermark embedding process is shown in figure 2 and the embedding process can be described as follows:

- **Step 1**: perform a zigzag scanning on coefficients matrix which obtained from receiving original fingerprint image $F_o$. The aim is to convert it into a vector of complex coefficients $Z_n$ to easily process of watermarking. Where $n=1,...,N$, and $N$ size of coefficients matrix.
- **Step 2**: the vector of coefficients $Z$ is decomposed into two (correlated) sub-vectors $z_1$ and $z_2$ to allow applying differential embedding technique (will explain it on details in next steps) as follow:
The 6th International Conference on Software Engineering & Computer Systems
IOP Conf. Series: Materials Science and Engineering 769 (2020) 012070  doi:10.1088/1757-899X/769/1/012070

\[
z_1(k) = Z(2k) \quad (3)
\]
\[
z_2(k) = Z(2k - 1) \quad (4)
\]

where \( k = 1 \ldots \frac{N}{2} \).

**Figure 2.** The embedding procedure of proposed reversible watermarking method

- **Step 3:** DCT is performed on \( z_1 \) and \( z_2 \) to produce their DCT transformed 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.

\[
Z_1 = DCT(z_1) \quad (5)
\]
\[
Z_2 = DCT(z_2) \quad (6)
\]

- **Step 4:** The watermark (binary sequence \( W \) of size \( L \) ) sequence bits \( w(i) \) for \( i = 0, 2 \ldots L - 1 \), is inserted into the transformed vectors \( Z_1 \) and \( Z_2 \) using a differential embedding method that is a mathematical equation will describe in equations 7 and 8. It allows to include the watermark randomly into the transformed vectors \( Z_1 \) and \( Z_2 \) which obtained from DCT transform to use in extraction stage without need the original data (blind). This will output two changed (by watermarking) sub-vectors \( Z'_1 \) and \( Z'_2 \) as follows:

\[
Z'_1(i') = Z_1(i') + \alpha w(i) \quad (7)
\]
\[
Z'_2(i') = Z_2(i') - \alpha w(i) \quad (8)
\]

where \( \alpha \) is the gain factor and \( i' \) are the random places into the highly strength band of \( Z_1 \) and \( Z_2 \) are the embedded watermark bits. These places are the elements of a vector \( r \) which can be generated the usage of a random permutation operation:

\[
i' = r(i) \quad (9)
\]
\[
r = RandPerm(S,a,b) \quad (10)
\]
where $S$ is the seed of the associated Pseudo Random Number Generator (PNRG), $a$ and $b$ are the beginning and the ending places of the highly strength band applied to put in the watermark. Therefore, the user’s secret key is $K = (S, a, b)$, which prevents the watermark from tempering or unauthorized access by attackers.

**Step 5:** The inverse DCT $ICDT$ is performed on $Z'_1$ and $Z'_2$ using the following equations 11 and 12. The purpose of performing the $ICDT$ is to reconstruct vector of complex coefficients $Z$ embedded by watermark.

$$z'_1 = IDCT(Z'_1)$$  \hspace{2cm} (11)  \\
$$z'_2 = IDCT(Z'_2)$$  \hspace{2cm} (12)  \\

**Step 6:** the two changed sub-vectors $z'_1$ and $z'_2$ is combined in the composing step using the opposite operation in equations 3 and 4 in order to produce the modified vector $Z'$ to reconstruct complex coefficients vector embedded by watermark.

**Step 7:** The modified vector is converted into the matrix employing the inverse of the zigzag scanning operation to reconstruct coefficients matrix embedded by watermark, to attain the watermarked fingerprint image $F_w$.

There are small modifications in original coefficients matrix. During the embedding process, the coefficients of the fingerprint image are modified but still can obtained almost the original fingerprint image without affected their features that had been due to the embedded watermark.

### 3.2. Watermark Extraction Process:

The watermark extraction process follows the same steps as the embedding process until Step 3 where the extraction is taking place as shown in figure 3.

![Watermark Extraction Process Diagram](image)

**Figure 3.** The extraction procedure of proposed reversible watermarking method

- **Step 1:** perform a zigzag scanning on coefficients matrix which obtained from watermarked fingerprint image $F_w$. The aim is to convert it into a vector of complex coefficients $Z(n)$ to easily process of watermarking. Where $n = 1..N$, and $N$ size of complex coefficients matrix.

- **Step 2:** Decompose the vector of coefficients $Z'$ to two related sub-vectors $z'_1$ and $z'_2$ is performed next.

- **Step 3:** perform DCT on $z'_1$ and $z'_2$ to produce their DCT-transformed forms $Z'_1$ and $Z'_2$.

If the enter fingerprint image is the watermarked one, and by using analogy with the embedding operations, the extraction operations will deliver two sub-vectors $Z'_1$ and $Z'_2$. Consequently, the difference between them has a proportional dating with the watermark sequence $W$:
\[ \Delta Z(i) = Z_1(i) - Z_2(i) = 2aW(i) \]  

with \( i = 1..L \); and \( i \) are the random places in which the watermark bits are embedded. These places are determined clearly by using recreating the vector \( r \), the usage of the user-selected secret key and the random permutation as shown in equations 7 and 8.

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 recover the source bits of the watermark:

\[
W'(i) = \begin{cases} +1 & \text{if } \Delta Z(i) \geq 0 \\ -1 & \text{otherwise} \end{cases}
\]  

After that, a comparison between tow watermarks \( W \) and \( W' \) is performed. If there is a similarity between it, then begins work of extracting features from watermarked fingerprint image through reversible watermarking process for using in fingerprint-based authentication system.

3.3. Reversible Watermarking Process:
The reversible watermarking process begin as the same step 4 in the embedding process, where we replace the original watermark with the extracted watermark obtained from watermark extraction process as shown in figure 4.

**Figure 4.** The reversibility procedure of the proposed reversible watermarking method

• **Step 1:** The extracted watermark (binary sequence \( W' \) of size \( L \) ) sequence bits \( W'(i) \) for \( i = 0..2..L-1 \), is inserted into the transformed vectors \( Z_1 \) and \( Z_2 \) using a differential embedding method that is a mathematical equation will describe in equations 21 and 22. It allows to include the watermark randomly into the transformed vectors \( Z_1 \) and \( Z_2 \) which obtained from \( DCT \) transform to use in extraction stage without need the original data (blind). This will output two changed (by watermarking) sub-vectors \( Z'_1 \) and \( Z'_2 \).

**Step 2:** The inverse DCT IDCT is performed on \( Z'_1 \) and \( Z'_2 \) using the following equations 9 and 10. The purpose of performing the IDCT is to reconstruct vector of coefficients \( Z' \) embedded by extracted watermark.
Step 3: The two changed sub-vectors $z_1'$ and $z_2'$ is combined in the composing step using the opposite operation in equations 27 and 28 in order to produce the modified vector $Z'$ to reconstruct coefficients vector embedded by extracted watermark.

Step 4: The modified vector is converted into the matrix employing the inverse of the zigzag scanning operation to reconstruct coefficients matrix embedded by extracted watermark, to attain the reversible fingerprint image $F_r$.

There are small modifications compared of original coefficients matrix. Thus, during the second embedding process by extracted watermark, the coefficients of the reversible fingerprint image obtained are modified but it is very close to the original, we could extract minutia without problem.

4. Results and discussion

Several experiments in this section have been conducted aimed at evaluating the performance of the adopted watermarking technique. The performance of the reversible fingerprint image-watermarking algorithm is evaluated by employing a benchmark fingerprint image database FCV2002-DB2 and compare it with previous works that had used the same database. To conduct this experiment, 80 fingerprint images have been taken from 10 persons from which the template is set using eight fingerprint images of each person; after that, the watermark is embedded into each of the taken fingerprint images.

Firstly, we compare the input original fingerprint images in databases against its corresponding watermarked fingerprint images to find positive matching results between them for minutia points and watermark data. Secondly, we embed the extracted watermarked into watermarked fingerprint image based on embedding equation that shown in equations 21 and 22 to obtain the reversible fingerprint image. Finally, we compare the reversible fingerprint image against its corresponding original fingerprint image to extract minutia easily without problem. It is because the reversible fingerprint image is very close to the original, as proved from the experiments results. In order to evaluate the obtained reversible and watermarked of fingerprint image quality, we utilised the peak signal to noise ratio (PSNR) [16].

Fingerprint recognition tools is 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 its corresponding which the possibly attacked and distorted. PSNR represents the ratio noise between the fingerprint image before and after operations of watermarking and its reversibility. This ratio can be used to determine the percentage of deformation on the original image caused by the embedding of the watermark. The high ratio of PSNR means the watermarked and reversible of fingerprint image quality is high, thus, the watermarked and reversible image is similar to the original image after operations of watermarking and its reversibility means good imperceptibility. figure 5 shows PSNR values obtained from our experiments versus the gain factor $\alpha$ to purpose embedding coefficients.
Looking at figure 5(a), the higher $\alpha$ values make lower PSNR of the watermarked fingerprint images. In contrast, for reversible fingerprint image, the PSNR value increases with $\alpha$ values until it stabilizes at value ($\alpha=0.2$) as show in figure 5(b).

The DCT with the differential extracting method is used to extracting watermark embedded into fingerprint image watermarked which may be affected due to watermarking process, the extracted watermark is compared with its corresponding original watermark which not need the original fingerprint image. We used the bit-correct ratio (BCR) in the process of evaluating the extracted watermark quality by measuring the rate of the similarity between the original and the extracted watermarks $W$ and $w$ respectively. The bit-correct ratio (BCR) is the ratio of correct extracted bits to the total embedded bits number. It is worth mentioning that since BCR generates further values detailed scale, it is getting widely spread and used. [17]. Thus, it was chosen as to measure the similarity of watermark data that have used as sequence binary in the proposed method, if the rate of $BCR$ is equal to 100%, it’s means that the extracted watermark is equal to the original. That means, the technique is achieving stronger robustness against watermarking process. figure 6 shows BCR rates of the extracted watermark obtained from our experiments versus the gain factor $\alpha$. Based on that figure, the BCR is getting better at $\alpha$ value of 0.2 and higher.

Figure 5. PSNR fingerprint watermarked image (a), PSNR reversible fingerprint image (b) for the proposed reversible watermarking method
4.1. Gain Factor Selection:
Other than above experiment, several experiments are conducted to observe the invisibility, robustness and reversibility. These experiments are under the gain factor selection experiment. The aim of this experiment is to observe if the proposed technique able to increase the security of the fingerprint recognition system. In order to select the suitable values of the gain factor in equations 5, 6, 20 and 21 that fulfil both the invisibility, the robustness and reversibility requirements of the watermarking. In addition, due to the random permutation value in equations 8 and 23, the experiment is deployed 20 times with what is agreed with our random algorithm for embedding the watermark data in order to obtain good stable results. Further, embedding the watermark data in various location to increase the security against intentional attacks. In the proposed algorithm based on databases, FCV2002-DB2 which were tested on 80 fingerprint images from 10 persons and there are 8 fingerprint images for each person. As shown in figure 5 and 6, the best trade-off between visual quality and watermark robustness is achieved with the value of $\alpha = 0.2$. Therefore, value of $\alpha = 0.2$ is used as the default value of the gain factor. figure 7 shows the original, the watermarked image and reversible image along with their corresponding histograms in databases FCV2002-DB2. It is clearly noticeable that watermarking process reversibility has not affected of the fingerprint image visual quality as shown in each if the histogram graphs. Furthermore, values of $PNSR$ and Matching score that obtained in experiments as shows in Table 1, prove that the fingerprint image has not been affected by reversibility of watermarking process.
Figure 7. The original cover image (a), watermarked image (b), The reversible watermarked image (c), histogram of the original cover (d), histogram of the watermarked image (e) and histogram of the reversible watermarked image (f).

The average of PSNR values, BCR rates and the matching score values between the original fingerprint images and its corresponding in database is shown in Table 1. Looking at that table, PSNR results obtained for reversible and watermarked fingerprint image from our experiments are acceptable, where, proposed method achieved over 47 dB for PSNR value of the watermarked image and 301dB for reversible image in database. Whereas, the BCR rates of the extracted watermark and the minutia score matching of watermarked fingerprint images without attacks are almost achieved 100% for all experiments.

Table 1. PSNR values, BCR rate and the Matching score value of the proposed reversible watermarking technique

| DB         | PSNR watermarked image | PSNR reversible image | BCR    | Matching score |
|------------|------------------------|-----------------------|--------|----------------|
| FVC2002-DB2 | 47,53                  | 301,67                | 99,61  | 1              |

5. Conclusions

Briefly, this paper introduces a blind, robust but simple technique of reversible watermarking based on DCT domains. A differential technique is performed on both transformed sub-vectors during the embedding process stage in order to fulfil the extraction of the watermark by using the difference of the corresponding watermarked sub-vectors. Then, the extracted watermarked in another embedding process based on differential technique is used to obtain a reversible fingerprint image. The reversible fingerprint image is very close to the original, as proved from the experiments results. All in all, the results obtained from the experiments confirms that the adopted technique achieves a high visual quality of the watermarked and reversible fingerprint image marking over 47 dB for PSNR per watermarked image, and over 301dB for reversible fingerprint image. Thus, extracting minutiae will be easy without problem. Besides, the achieving high strong of security in terms of correlation of extracted watermark data as the accepted results obtained of BCR values of extracted watermark and score matching of minutiae points for fingerprint image (cover image). The proposed technique will add a factor of authentication to the authorization process by combining both identity of the user and biometric features with a high security when access to the fingerprint recognition system.
Acknowledgment

We would like to show our gratitude to Universiti Malaysia Pahang (RDU vote number RDU180380) for supporting this study.

References

[1] Awang, S., Azmi, N. M. A. N. (2018). Vehicle Counting System Based on Vehicle Type Classification Using Deep Learning Method. In IT Convergence and Security 2017 (pp. 52-59). Springer, Singapore

[2] Al-Saffar, A., Awang, S., Tao, H., Omar, N., Al-Saiaigh, W., Al-bared, M. (2018). Malay sentiment analysis based on combined classification approaches and Senti-lexicon algorithm. PloS one, 13(4), e0194852.

[3] W. M. Syahrir, A. Suryanti, N. N. Ain, N. N. (2007, September). Egg_s Bloodspot Detection Using Image Processing. In Second International Conference on Innovative Computing, Informatio and Control (ICICIC 2007) (pp. 424-424). IEEE.

[4] A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, Filterbank-based fingerprint matching, IEEE Trans. Image Process. 9 (2000) 846–859.

[5] S. Awang, J. Sulaiman, J., N. Noor, K. Mohd, L. Bayuaji (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.

[6] G. Balamurugan, A Fingerprint Based Reversible Watermarking System For The Security Of Medical Information, 2016 World Conf. Futur. Trends Res. Innov. Soc. Welf. (Startup Conclave). (2016) 1–6. doi:10.1109/STARTUP.2016.7583901.

[7] A. Noore, R. Singh, M. Vatsa, M.M. Houck, Enhancing security of fingerprints through contextual biometric watermarking, Forensic Sci. Int. 169 (2007) 188–194.

[8] S.M. Mousavi, A. Naghsh, S.A.R. Abu-Bakar, Watermarking techniques used in medical images: a survey, J. Digit. Imaging. 27 (2014) 714–729.

[9] M. Lebcir, S. Awang, Fingerprint Image Watermarking in Spatial , Frequency and Multiresolution domain : Techniques and challenges, 2018. http://umpir.ump.edu.my/id/eprint/23029/7/Fingerprint Image Watermarking in Spatial1.pdf.

[10] F.Y. Shih, S.Y.T. Wu, Combinational image watermarking in the spatial and frequency domains, Pattern Recognit. 36 (2003) 969–975.

[11] M.M. Yeung, S. Pankanti, Verification watermarking on fingerprint recognition and retrieval, J. Electron. Imaging. 9 (2000). doi:10.1117/12.344704.

[12] B. Günsel, U. Uludag, A. Murat Tekalp, Robust watermarking of fingerprint images, Pattern Recognit. 35 (2002) 2739–2747. doi:10.1016/S0031-3203(01)00250-3.

[13] U. Uludag, B. Günsel, M. Ballan, A Spatial Method for Watermarking of Fingerprint Images., in: PRIS, 2001: pp. 26–33.

[14] L.R. Haddada, I.H. Trimech, N.E. Ben Amara, A biometric watermarking approach of fingerprint images by DLDA Gabor face features without altering minutiae, IPAS 2016 - 2nd Int. Image Process. Appl. Syst. Conf. (2017) 1–6. doi:10.1109/IPAS.2016.7880135.

[15] A. K. Jain, U. Uludag, R.-L.H.R.-L. Hsu, Hiding a face in a fingerprint image, Object Recognit. Support. by User Interact. Serv. Robot. 3 (2002) 756–759. doi:10.1109/ICPR.2002.1048100.

[16] N. Bousmina, S. Ghouzali, M. Lafkaï, O. Nafea, M. Mikram, W. Abdul, D. Aboutajdine, Watermarking for protected fingerprint authentication, in: 2016: pp. 127–131.

[17] K.K.A. Ghany, G. Hassan, A.E. Hassanien, H.A. Hefny, G. Schaefer, A.R. Ahad, A Hybrid Biometric Approach Embedding DNA Data in Fingerprint Images, (2014) 1–5.

[18] J. Abraham, V. Paul, A blind watermarking method for fingerprinting digital images, in: 2016 Int. Conf. Data Min. Adv. Comput., IEEE, 2016: pp. 145–149. doi:10.1109/SAPIENCE.2016.7684124.

[19] M. Alkhathami. (2015). Watermarking techniques for genuine fingerprint authentication.
[20] M. Alkhathami, F. Han, R. Van Schyndel, Fingerprint authentication enhancement using combination of DWT and DCT, Proc. 2015 10th IEEE Conf. Ind. Electron. Appl. ICIEA 2015. (2015) 387–392. doi:10.1109/ICIEA.2015.7334144.

[21] M. Alkhathami, F. Han, R. Van Schyndel, Fingerprint image protection using two watermarks without corrupting minutiae, Proc. 2013 IEEE 8th Conf. Ind. Electron. Appl. ICIEA 2013. (2013) 1151–1155. doi:10.1109/ICIEA.2013.6566540.

[22] 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.

[23] K. Ramani, E. V Prasad, S. Varadarajan, DWT Based Watermarking For Biometric Data, Indian J. Inf. Sci. Technol. 3 (2007) 35–41.