Adv Syst Sci Appl 2022; **01**; 117-129
Published online at https://ijassa.ipu.ru.

Robust Reversible Watermarking Application for Fingerprint Image Security

Rasha Thabit[1], Bee Ee Khoo[2*]

[1)] *Department of Computer Techniques Engineering, Al-Rasheed University College, Baghdad, Iraq*

E-mail: rashathabit@yahoo.com

[2)] *School of Electrical and Electronic Engineering, Engineering Campus, Universiti Sains Malaysia, 14300, Nibong Tebal, Penang, Malaysia*

E-mail: beekhoo@usm.my

Abstract: Fingerprint biometric systems can automatically identify individuals based on their fingerprint characteristics. Different image watermarking schemes have been applied to fingerprint images for security and protection purposes. The previous schemes are either robust watermarking schemes or reversible watermarking schemes. In order to ensure the intactness of the minutiae, this work applies the robust reversible watermarking scheme for fingerprint images which can recover the original image after the watermark extraction process and provide robustness against different kinds of attacks. The proposed scheme embeds the identification number (ID) of the person in his fingerprint image to provide security while saving and exchanging the image. The scheme has two stages of security; in the first stage, the ID of the received image is extracted and compared with the saved ID in the database, if they are identical the system proceeds to the second stage in which the matching score between the received fingerprint and the saved fingerprint is calculated to authenticate the received image. The experimental results proved the efficiency of the proposed scheme in terms of visual quality, robustness, reversibility, and intactness of the fingerprint's minutiae.

Keywords: information security, fingerprint images protection, robust reversible watermarking, image authentication, biometric data security

1. INTRODUCTION

Biometrics technology has been used to differentiate between authorized and unauthorized people in personal identification systems. For instance, the biometrics signals such as fingerprint, iris, face, and voice have been used as an input to the automated biometrics-based person authentication systems [1-4]. These biometrics signals can be acquired from the user, either locally or remotely. The biometrics-based verification system needs to verify that the biometric data came from the legitimate person at the time of enrollment, therefore, the security and integrity of the biometrics data became important issues [5,6]. Different data hiding and watermarking techniques have been applied to protect biometrics signals and provide a secure transmission of their related data [7-12].

Fingerprint-based authentication system is one of the most mature biometrics authentication systems. The main processes in these systems are acquisition, representation, feature extraction, and matching [13]. In order to present a suitable watermarking technique for fingerprint images, the watermarking process should not affect the features (i.e., minutiae) of the image and should not affect the fingerprints matching process.

[*] Corresponding author: beekhoo@usm.my

Over the years, different wavelet transforms have been applied in many different applications such as in [14-17] because of their efficiency. Most of the watermarking and data hiding schemes for fingerprint images have concentrated on the robustness of the watermark to withstand different kinds of attacks [7-10,18-20]. In [10], a wavelet-based watermarking scheme for fingerprint images has been presented. The horizontal and vertical high frequency subbands have been used to carry the watermark. The scheme has robustness against Gaussian noise, filtering, and JPEG2000 compression. In [9], a wavelet-based watermarking method has been applied to embed the fingerprint minutiae data in the fingerprint image in order to increase the level of security. The horizontal, vertical, and diagonal DWT coefficients have been selected to carry the watermark bits. The scheme provides robustness against JPEG compression, additive noise, and filtering. In [7,8], the fingerprint image has been divided into two regions called region of interest (ROI) and region of non-interest (RONI). Only ROI (ridges area) has been used to carry the watermark bits in order to provide robustness against cropping attack. In addition, the schemes have robustness against Wavelet Scalar Quantization (WSQ) compression, filtering, and additive white Gaussian noise (AWGN). In [18,19], image watermarking schemes have been presented to hide the minutiae data or text data in fingerprint images. The horizontal, vertical, and diagonal DWT coefficients have been selected to carry the watermark bits. The schemes have robustness against salt & pepper noise, Gaussian noise, filtering, and JPEG compression. In [20], the method used DCT and Neural Network-Particle Swarm Optimization (NN-PSO) to watermark host gray scale fingerprint images with their corresponding facial images. The scheme divides the image into blocks and the NN is used to find the features of the block. Then, the output of the NN is used as input in the PSO module to find the best DCT coefficients' locations in that block where the secret facial image data can be embedded. The scheme has robustness against different kinds of attacks.

On the other hand, some fragile watermarking techniques have been presented for fingerprint images [21-24]. In [21], at the sender side, the SHA-256 hash of the original fingerprint image and sensitive personal information are encrypted and embedded into the fingerprint image using lossless data hiding. At the receiver, the fingerprint image can be recovered without loss. In [22], a reversible watermarking based on difference expansion (DE) [25] and Rotational Replacement of the LSB has been presented to hide text watermark in fingerprint image. The scheme can recover the original image after extracting the embedded text and it obtained better visual quality in comparison with the scheme in [25]. In [23], the watermarking process has been applied to the template of the fingerprint (the template is found after the feature extraction process). Any tampering in the template will destroy the watermark and thus the absence of the watermark makes the template unauthentic. According to the reported results, the method did not affect the verification process of the fingerprint images (except for only three images among the test images that have been used in the experiments). In [24], a fragile image watermarking technique has been used to hide the watermark into the fingerprint images by changing the least significant bit value of randomly chosen pixels of the image. The results proved that the presented scheme did not affect the verification system except for three test images.

The schemes in [7-10,18-20] obtained robustness against different kinds of attacks, however, the process of embedding the watermark in the fingerprint images causes distortions in these images and the original images cannot be recovered after the watermark extraction process (i.e., irreversible watermarking). In addition, there is no test for the effect of the watermarking process on the number of the fingerprint minutiae and the matching process. The schemes in [21,22] are reversible watermarking techniques where the original fingerprint image can be recovered without loss; the schemes in [23,24] are irreversible but they tested the effect of the watermarking on the fingerprints matching process. However, the watermarks of the schemes in [21-24] are fragile and they can be destroyed if the watermarked image undergone unintentional attacks.

Recently, the researches in the reversible watermarking techniques highlighted the need for reversible watermarking techniques that can withstand the unintentional attacks such as channel noise and compression which are unavoidable attacks [17,26-31]. Therefore, this paper suggested the use of robust reversible watermarking (RRW) method as a better candidate for fingerprint images watermarking because this kind of watermarking can recover the original image after the watermark extraction process and at the same time provide robustness against unintentional attacks.

The proposed scheme embeds the identification number (ID) of the person in his fingerprint image. Embedding the ID using RRW in the fingerprint image has the following advantages: (a) provides security where the personal information has been embedded in a cover image and thus it will not be a clear text for any user, (b) provides direct link between the image and its related information, (c) the embedded ID is used for database authentication and the absence of the ID means the image is not authentic and it may come from illegal alteration in the database, (d) the scheme is reversible watermarking, thus the original image can be recovered correctly after extracting the hidden data, and (e) the scheme is robust and the embedded ID can withstand different attacks.

The rest of this paper is structured as follows: Section 2 explains the details of the proposed robust reversible watermarking (RRW) technique for fingerprint image watermarking. Section 3 presents the experimental results for several fingerprint images. The conclusions are drawn in Section 4.

2. PROPOSED SCHEME

As mentioned before, the RRW schemes have been suggested as better candidates for the practical applications because they can recover the original image after the watermark extraction process and can withstand attacks [27,32,33]. In this paper, we suggest using robust reversible watermarking for fingerprint images which is based on our previous work in [34]. The RRW scheme in [34] has been studied for different types of images, different block sizes, and different threshold values and the results proved that it has better performance in comparison with previous RRW schemes. In this paper, the proposed RRW scheme is applied for a specific type of images (i.e., fingerprint images). To find the best block size for dividing the fingerprint image, we will modify our previous algorithm [34] to automatically calculate the best block size according to the number of bits in the ID number and the size of the fingerprint image. A general block diagram for the watermark embedding and extraction processes is shown in Fig. 2.1. The procedures of the watermark embedding and extraction process are explained in the following subsections.

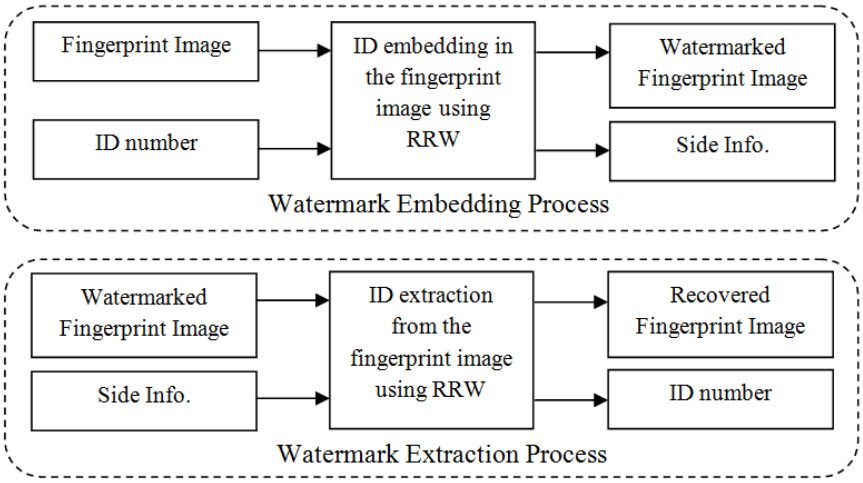

Fig. 2.1. Proposed RRW for Fingerprint Images

2.1. Watermark embedding algorithm

The flow chart of the proposed algorithm for embedding the ID number in the fingerprint image is shown in Fig. 2.2 which can be summarized in the following steps (for more details about the original RRW algorithm the reader can refer to [34]):

Step 1: Input the ID number and the fingerprint image. The current format of the Malaysian National Registration Identity Card (NRIC) number which contains 12 digits has been used in the proposed scheme as an example. The ID number is written in a text file. The software reads the ID text file and the fingerprint image.

Step 2: Convert the ID number to binary sequence. Each digit in the ID number is converted from decimal number to 8 bits binary number. Then, the binary numbers are reshaped to form a sequence of binary bits. (i.e., 12 digits × 8 bits gives a binary sequence of length 96 bits).

Step 3: Selecting the best block size for dividing the fingerprint image. The best block size is selected according to the size of the fingerprint image and the length of the ID binary sequence. According to our RRW scheme [34], better robustness and better visual quality can be obtained with the larger block size (*bsize*). At the same time, the larger *bsize* gives lower capacity. The capacity depends on the size of the fingerprint image and *bsize*. The algorithm must search for the largest *bsize* that can be used by calculating the available capacity at a specific *bsize* and comparing it with the length of the binary sequence. The best *bsize* is found using the following algorithm:

a) Read the size of the fingerprint image, denote the height and width by h and w, respectively.
b) Set the (*bsize*) to 64 (which means the block size is 64×64).
c) Calculate the capacity using $C=\lfloor (h\times w)/(bsize)^2 \rfloor$, where $\lfloor\ \rfloor$ refers to the floor function in which the result is the nearest integer number that is less than or equal to the element inside the function.
d) Compare C with the length of the binary sequence (*Lseq*) as follows:
e) If $C \geq Lseq$ then stop
f) Else divide *bsize* by 2 and repeat steps c and d.
g) The final *bsize* is chosen for dividing the fingerprint image.

Step 4: Divide the fingerprint image into non-overlapping blocks (size *bsize* × *bsize*).

Step 5: Transform each block using Slantlet transform (SLT) matrix as shown in the following equation:

$$S = SLT_N \quad s \quad SLT_N^T, \tag{2.1}$$

where (s) is the image block, (S) is the Slantlet transform of the block, (SLT_N) is an N×N Slantlet matrix, and T is the transpose of matrix. Note that s, S, and SLT_N have the same size.

Step 6: Divide the resultant coefficients. The resultant coefficients in the matrix (S) into four subbands and select the high frequency subbands (High-Low (HL) and Low-High (LH)) to carry the ID bits.

Step 7: Apply the modification rules according to the bit value as explained in [34]. This process will generate some side information.

Step 8: Replace the original high frequency subbands by the modified subbands.

Step 9: Apply inverse SLT to obtain the watermarked blocks using the following equation:

$$s = SLT_N^T \; S \quad SLT_N. \tag{2.2}$$

Step 10: Rearrange the blocks to obtain the watermarked fingerprint image.

Step 11: Apply post-processing as explained in [34] to prevent the overflow/underflow of the pixel values.

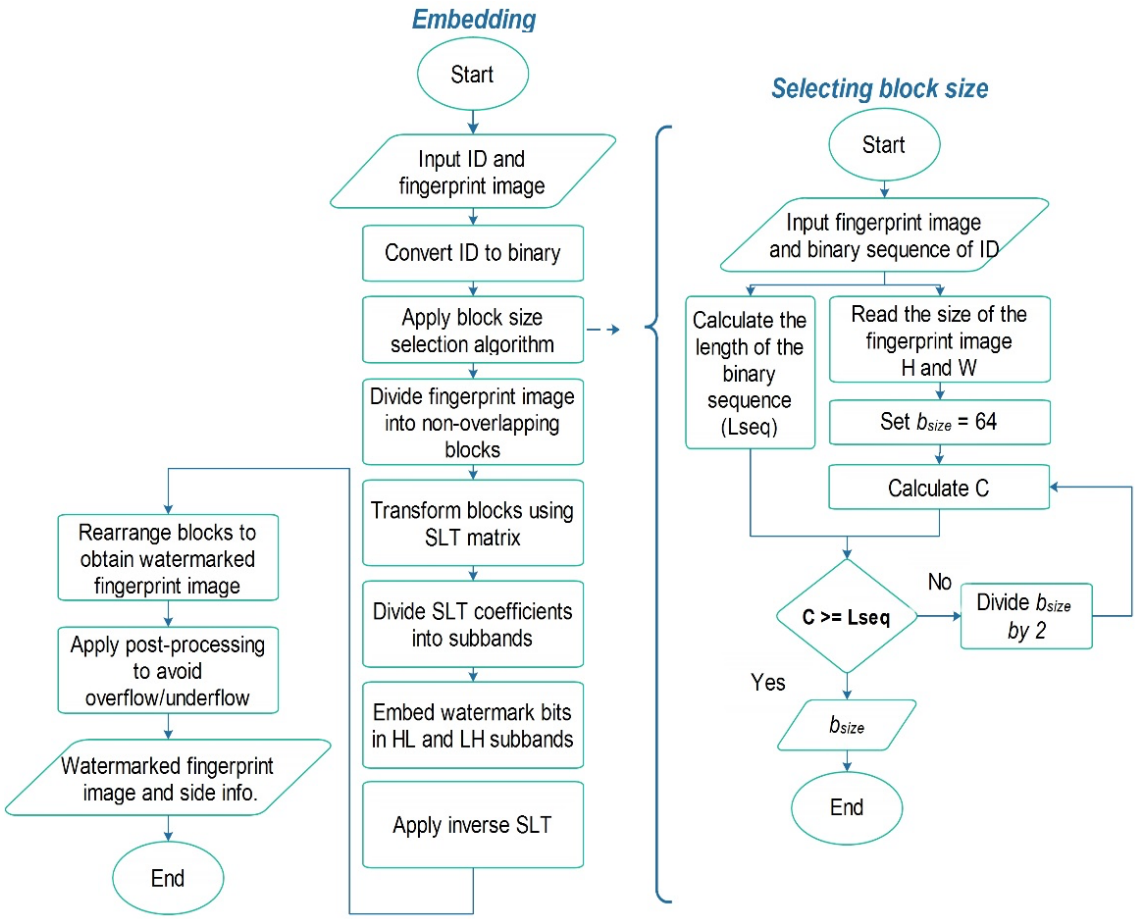

Fig. 2.2. Proposed ID embedding algorithm

2.2. Watermark extraction algorithm

The flow chart of the proposed algorithm for extracting the ID number from the watermarked fingerprint image is shown in Fig. 2.3 which can be summarized in the following steps (for more details about the original RRW algorithm the reader can refer to ([34]):

Step 1: Input the side information and the watermarked fingerprint image.
Step 2: Return the pixel values (that have been adjusted) to their places.
Step 3: Divide the resultant fingerprint image into non-overlapping blocks.
Step 4: Transform each block using SLT matrix.
Step 5: Select the high frequency subbands (High-Low (HL) and Low-High (LH)) to extract the ID bits.
Step 6: Apply the extraction rules as explained in [34].
Step 7: Recover the original transform domain blocks according to the side information and the extracted bits.
Step 8: Apply inverse SLT to obtain the original spatial domain blocks.
Step 9: Rearrange the blocks to obtain the original fingerprint image.
Step 10: Recover the ID number from the extracted binary sequence.
Step 11: Compare the recovered ID with the saved ID in database, if they are equal then continue to the next step, else show a message that notify the receiver about the inauthenticity of the received fingerprint image and end the algorithm.
Step 12: Calculate the matching score, if the minutiae of the received fingerprint image is identical to the saved one then show a message that notify the receiver about the authenticity of the received fingerprint image.

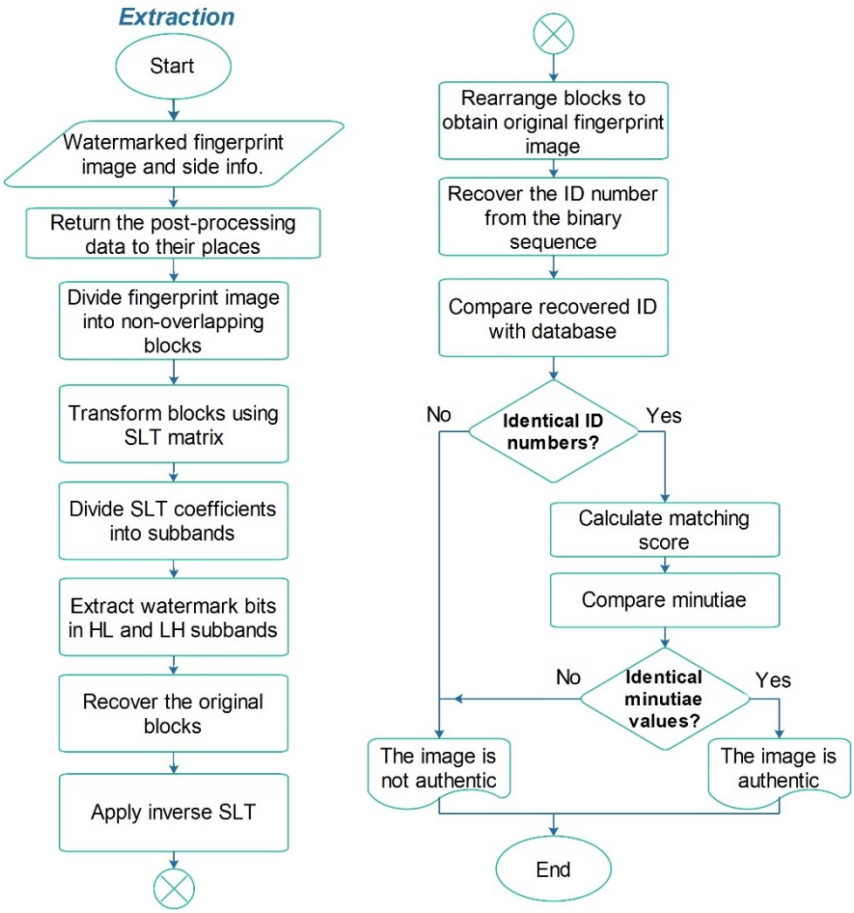

Fig. 2.3. Proposed extraction algorithm

3. RESULTS AND ANALYSIS

To evaluate the proposed scheme, different fingerprint images have been collected from [FVC2000 and FVC2004 databases] [35]. Each database contains four sub-databases (DB1, DB2, DB3, and DB4). In each sub-database, there are 80 fingerprint images. Thus, the total number of fingerprint images that are used in the experiments is (640 fingerprint images). Samples of the test images are shown in Fig. 3.1. The experiments are conducted to evaluate the visual quality of the watermarked fingerprint images, the reversibility of the watermarking scheme, the robustness against attacks, and the effect of the proposed watermarking process on the features (i.e., minutiae) of the fingerprint images.

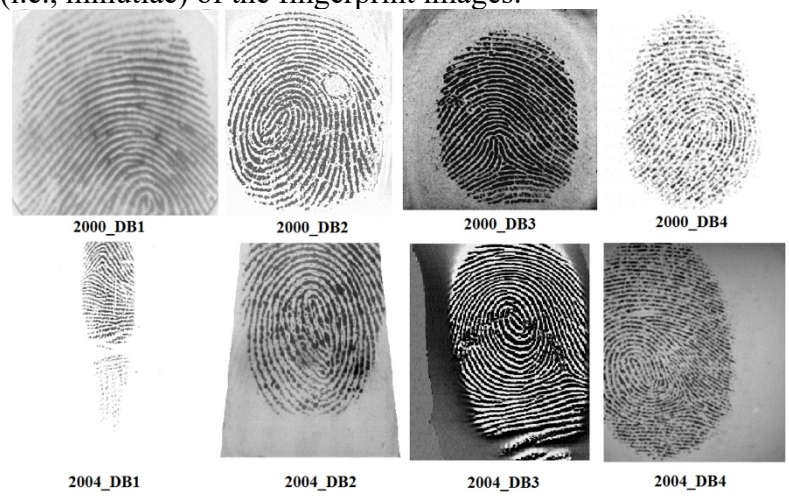

Fig. 3.1. Sample test images from each database

3.1. Visual Quality Evaluation

To evaluate the visual quality, the Peak-Signal-to-Noise ratio (PSNR) and the Structural Similarity Index (SSIM) are calculated for each image in each sub-database of fingerprint images. A sample ID number has been embedded in the images. The average PSNR values and the average SSIM values have been calculated for each sub-database (for 80 images in each sub-database). The threshold value affects the visual quality of the watermarked image therefore the visual quality of the scheme has been tested at different threshold values. Fig. 3.2 shows samples of the watermarked images that have been obtained at different threshold values. The PSNR values and SSIM values for each watermarked image are in Table 3.1. Table 3.2 and Table 3.3 contain the average values for each sub-database. The results proved that the proposed scheme does not affect the visual quality of the image. As shown in the results, when the threshold value increased, the visual quality decreased.

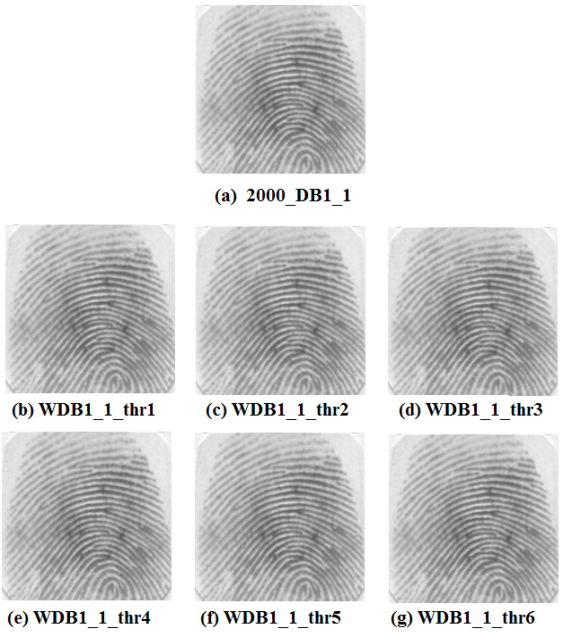

Fig. 3.2. (a) Original fingerprint image, Watermarked images at different threshold values: (b) at T=1, (c) at T=2, (d) at T=3, (e) at T=4, (f) at T=5, (g) at T=6.

Table 3.1. The PSNR and SSIM values for the watermarked images in Fig. 3.2

Image name	PSNR (dB)	SSIM
WDB1_1_thr1	59.6101	0.9995
WDB1_1_thr2	55.2978	0.9986
WDB1_1_thr3	52.3700	0.9973
WDB1_1_thr4	50.2032	0.9957
WDB1_1_thr5	48.4958	0.9937
WDB1_1_thr6	46.9980	0.9912

Table 3.2. The average PSNR(dB) values at different threshold values

Name of database	Size	T=1	T=2	T=3	T=4	T=5	T=6	T=7
2000_DB1	300×300	59.872	55.526	52.544	50.362	48.610	47.114	45.768
2000_DB2	256×364	51.532	50.155	48.885	47.731	46.674	45.702	44.802
2000_DB3	448×478	55.058	52.020	49.628	47.687	46.055	44.657	43.436
2000_DB4	240×320	55.419	53.292	51.349	49.831	48.419	47.234	46.087
2004_DB1	640×480	60.234	56.532	53.813	51.763	50.030	48.548	47.259

2004_DB2	328×364	54.174	50.507	47.805	45.691	43.941	42.468	41.192
2004_DB3	300×480	48.227	46.797	45.452	44.220	43.082	42.037	41.076
2004_DB4	288×384	54.115	50.156	47.343	45.182	43.402	41.905	40.617

Table 3.3. The average SSIM values at different threshold values

Name of database	Size	T=1	T=2	T=3	T=4	T=5	T=6	T=7
2000_DB1	300×300	0.9995	0.9987	0.9974	0.9958	0.9938	0.9913	0.9883
2000_DB2	256×364	0.9996	0.9993	0.9990	0.9985	0.9980	0.9974	0.9967
2000_DB3	448×478	0.9996	0.9990	0.9982	0.9971	0.9957	0.9940	0.9921
2000_DB4	240×320	0.9997	0.9992	0.9986	0.9979	0.9969	0.9958	0.9944
2004_DB1	640×480	0.9997	0.9991	0.9981	0.9969	0.9954	0.9935	0.9912
2004_DB2	328×364	0.9992	0.9978	0.9958	0.9932	0.9897	0.9857	0.9810
2004_DB3	300×480	0.9991	0.9982	0.9968	0.9951	0.9929	0.9903	0.9873
2004_DB4	288×384	0.9990	0.9969	0.9937	0.9896	0.9843	0.9780	0.9709

3.2. Reversibility Evaluation

The image reversibility is evaluated by comparing the pixel values in the original image with the pixel values in the recovered image after the watermark extraction process. Consider the original image (I_O) and the recovered image (I_R) are both of size (H×W), if the two images are equal then the image reversibility is '1' else the image reversibility is '0'. The image reversibility is calculated using the following equation:

$$Image\ Reversibility = \begin{cases} 1 & if\ I_O(i,j) = I_R(i,j), \\ 0 & if\ I_O(i,j) \neq I_R(i,j), \end{cases} \tag{3.1}$$

where $I_O(i,j)$ is the pixel value at the coordinates (i,j) in the original image, $I_R(i,j)$ is the pixel value at the coordinates (i,j) in the recovered image, $i = 1, 2, \dots, H$, $j = 1, 2, \dots, W$.

Table 3.4 shows the average image reversibility results for each database. As illustrated in the results, the proposed scheme obtained complete reversibility for all test images at different threshold values.

Table 3.4. The average SSIM values at different threshold values

Name of database	Size	T=1	T=2	T=3	T=4	T=5	T=6	T=7
2000_DB1	300×300	1	1	1	1	1	1	1
2000_DB2	256×364	1	1	1	1	1	1	1
2000_DB3	448×478	1	1	1	1	1	1	1
2000_DB4	240×320	1	1	1	1	1	1	1
2004_DB1	640×480	1	1	1	1	1	1	1
2004_DB2	328×364	1	1	1	1	1	1	1
2004_DB3	300×480	1	1	1	1	1	1	1
2004_DB4	288×384	1	1	1	1	1	1	1

3.3. Robustness Evaluation

The robustness is evaluated by calculating the bit error rate (BER) in the extracted watermark after different kinds of attacks (i.e., additive Gaussian noise (AGN), JPEG/JPEG2000 compression, histogram equalization, wiener filtering, and median filtering). Fig. 3.3 shows samples of the results from the fingerprint images database (2000_DB1) where the average BER against the mentioned attacks is calculated at different threshold values. Fig. 3.3(a) shows the robustness results against additive Gaussian noise (AGN) with zero-mean and the variance equals to (0.001, 0.002, …, 0.01) for different threshold values. Fig. 3.3(b) shows the robustness results against JPEG compression with the quality factor equals to (40, 50, …, 100)

for different threshold values. Fig. 3.3(c) shows the robustness results against JPEG2000 compression with the rate equals to (0.2, 0.4, …, 2) for different threshold values. Fig. 3.3(d) shows the robustness results against histogram equalization, wiener filtering (3×3), and median filtering (3×3). As shown in the results, the higher the threshold value the better the robustness.

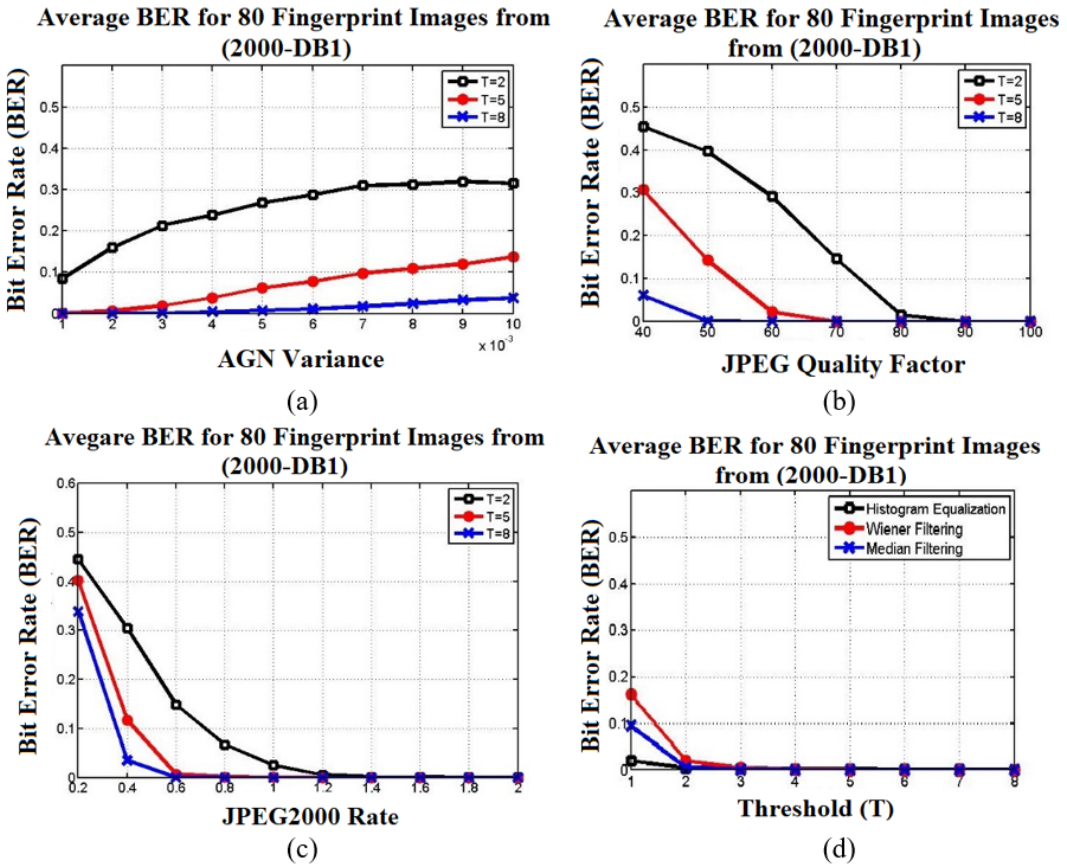

Fig. 3.3. Robustness results at different threshold values against (a) AGN, (b) JPEG compression, (c) JPEG2000 compression, and (d) Histogram equalization, Wiener filtering, and Median filtering.

3.4. Similarity Measure

The number of the extracted minutia from the original fingerprint images and the recovered fingerprint images after the watermark extraction process has been calculated. The matching process between the original and the watermarked images are based on calculating the similarity measure [36] of the extracted minutiae in both images. The similarity measure value is (0 to 1), the more similar the minutiae the higher the similarity measure; when the minutiae of both images are identical the similarity measure equals 1. The proposed algorithm is completely reversible therefore the number of the minutiae is identical for each test image. Table 3.5 shows the average similarity measure results for all fingerprint images databases at different threshold values.

Table 3.5. The average similarity measure at different threshold values

Name of database	Size	T=1	T=2	T=3	T=4	T=5	T=6	T=7
2000_DB1	300×300	1	1	1	1	1	1	1
2000_DB2	256×364	1	1	1	1	1	1	1
2000_DB3	448×478	1	1	1	1	1	1	1
2000_DB4	240×320	1	1	1	1	1	1	1
2004_DB1	640×480	1	1	1	1	1	1	1
2004_DB2	328×364	1	1	1	1	1	1	1
2004_DB3	300×480	1	1	1	1	1	1	1
2004_DB4	288×384	1	1	1	1	1	1	1

3.5. General comparison with previous fingerprint image watermarking schemes

This section contains a general comparison between the proposed robust reversible watermarking scheme and the previous schemes in [7-10,18-20,22-24,37]. As mentioned in the introduction section, the previous fingerprint image watermarking schemes are either robust or reversible therefore the proposed scheme can be considered as a better candidate for fingerprint images. Table 3.6 summarizes the differences between the proposed scheme and the previous schemes. The proposed scheme is better than the scheme in [7-10,18-20] in terms of reversibility where these schemes cannot recover the original image after the watermark extraction process. In comparison with the schemes in [22,37], the proposed scheme is better in terms of robustness where these schemes are fragile and the watermark cannot withstand attacks. The proposed scheme is better than the schemes in [23,24] in terms of robustness and reversibility.

Table 3.6. The average similarity measure at different threshold values

Scheme	Domain	Robustness	Reversibility	Tested Minutiae
[7]-[10], [18], [19]	Transform Domain DWT	Have robustness against different attacks	Irreversible	No test for the effect of watermarking process on the fingerprint features.
[20]	Transform Domain DCT	Have robustness against different attacks	Irreversible	No test for the effect of watermarking process on the fingerprint features.
[37]	Comparative study for different domains (LSB, DCT, and DWT)	Fragile The watermark cannot withstand any attack.	Reversible	The scheme is reversible therefore the minutiae of the fingerprint images have not been changed.
[22]	Transform Domain DCT	Fragile The watermark cannot withstand any attack.	Reversible	The scheme is reversible therefore the minutiae of the fingerprint images have not been changed.
[23], [24]	Spatial domain	Fragile The watermark cannot withstand any attack.	Irreversible	The effect of the watermarking process has been tested and the verification process has been affected for only some images.
Proposed Scheme	Transform Domain SLT	Have robustness against different attacks	Reversible	The effect of the watermarking process has been tested and the verification process has not been affected for all test images.

4. CONCLUSION

The proposed scheme in this paper protects the fingerprint image by embedding the ID number in the fingerprint image using RRW without destroying fingerprint features. The scheme based on applying the Slantlet transform (SLT) on fingerprint image's blocks and modifying the SLT coefficients to carry the watermark bits. The proposed scheme is completely reversible therefore the matching process has not been affected. The experiments proved that the proposed scheme obtained high visual quality, good robustness results against different attacks, and it performs better in comparison with the previous fingerprint image watermarking schemes, therefore, it can be considered as a good candidate for practical applications.

ACKNOWLEDGEMENTS

The authors would like to acknowledge Universiti Sains Malaysia under Research University Individual Grant (RUI Grant No. 1001/PELECT /8014111) for the financial support.

REFERENCES

1. Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An Introduction to Biometric Authentication Systems. *Biometric Syst.*, pp. 1–20. doi: 10.1007/1-84628-064-8_1.
2. Pato, J. N., & Millett, L. I. (2010). *Biometric Recognition: Challenges and Opportunities.* Washington: The national academies press.
3. Nugraha, U., & Wahyu, A. P. (2019). Implementation of biometric data on information security systems. *J. Adv. Res. Dyn. Control Syst.*, vol. 11, no. 2, pp. 950–956.
4. Ratha, N. K., Connell, J. H., & Bolle, R. M. (2000). Secure data hiding in wavelet compressed fingerprint images. *In ACM Multimedia Workshop Marina Del Rey CA USA,* pp. 127–130, doi: 10.1145/357744.357902.
5. Anchalia, U., & et. al. (2019). Study and Design of Biometric Security Systems: Fingerprint and Speech Technology. Lect. Notes Electr. Eng., vol. 556, pp. 577–584, doi: 10.1007/978-981-13-7091-5_47.
6. Henniger, O., Scheuermann, D., & Kniess, T. (2010). On security evaluation of fingerprint recognition systems. *Int. Biometric Perform. Test. Conf.,* no. Section 2, pp. 1–10,, [Online]. Available: http://private.sit.fraunhofer.de/~henniger/publ/HSK10.pdf.
7. Zebbiche, K., & Khelifi, F. (2008). Region-Based Watermarking of Biometric Images: Case Study in Fingerprint Images. *Int. J. Digit. Multimed. Broadcast*, vol. 2008, pp. 1–13, doi: 10.1155/2008/492942.
8. Zebbiche, K., Khelifi, F., & Bouridane, A. (2008). An efficient watermarking technique for the protection of fingerprint images. *Eurasip J. Inf. Secur.,* vol. 2008, doi: 10.1155/2008/918601.
9. Zebbiche, K., Ghouti, L., Khelifi, F., & Bouridane, A. (2006). Protecting Fingerprint Data Using Watermarking. *In First NASA/ESA Conference on Adaptive Hardware and Systems (AHS'06),* pp. 451–456, doi: 10.1109/AHS.2006.61.
10. Ghouti, L., & Bouridane, A. (2006). Data hiding in fingerprint images. *In 2006 14th European Signal Processing Conference,* pp. 1–4.
11. Bedi, P., Bansal, R., & Sehgal, P. (2012). Multimodal Biometric Authentication using PSO based Watermarking. *Procedia Technol.,* vol. 4, no. December 2012, pp. 612–618, doi: 10.1016/j.protcy..05.098.
12. Jain, A. K., Uludag, U., & Hsu, R.-L. (2002). Hiding a face in a fingerprint image. In Object recognition supported by user interaction for service robots, vol. 3, pp. 756–759, doi: 10.1109/ICPR.2002.1048100.
13. Jain, K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proc. IEEE,* vol. 85, no. 9, pp. 1365–1388, doi: 10.1109/5.628674.
14. Raza & Khan, A. (2019). Haar wavelet series solution for solving neutral delay differential equations. *J. King Saud Univ. - Sci.,* vol. 31, no. 4, pp. 1070–1076. doi: 10.1016/j.jksus.2018.09.013.
15. Nasab, K., Atabakan, Z.P., Ismail, A. I., & Ibrahim, R.W. (2018). A numerical method for solving singular fractional Lane–Emden type equations. *J. King Saud Univ. - Sci.,* vol. 30, no. 1, pp. 120–130. doi: 10.1016/j.jksus.2016.10.001.

16. Nury, H., Hasan, K. & Bin Alam, M. J. (2017). Comparative study of wavelet-ARIMA and wavelet-ANN models for temperature time series data in northeastern Bangladesh. *J. King Saud Univ. - Sci.,* vol. 29, no. 1, pp. 47–61. doi: 10.1016/j.jksus.2015.12.002.
17. Thabit, R. & Khoo, B. E. (2014). Capacity improved robust lossless image watermarking. *IET Image Process.,* vol. 8, no. 11, doi: 10.1049/iet-ipr.2013.0862.
18. Chouhan, R. & Khanna, P. (2011). Robust Minutiae Watermarking in Wavelet Domain for Fingerprint Security. *World Acad. Sci. Eng. Technol.,* vol. 5, no. 12, pp. 1612–1619.
19. Chouhan, R., Mishra, A., & Khanna, P. (2012). Fingerprint Authentication by Wavelet-based Digital Watermarking. *Int. J. Electr. Comput. Eng.*, vol. 2, no. 4, pp. 519–528. doi: 10.11591/ijece.v2i4.505.
20. Bansal, R. Sehgal, P. & Bedi, P. (2012). Securing fingerprint images using a hybrid technique. *In ICACCI'12: Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, pp. 557–565.
21. Xuan, G., Shi, Y., & Ni, Z. (2004). Lossless data hiding using integer wavelet transform and spread spectrum. *IEEE Int. Work. Multimed. Signal Process.,* pp. 2–5.
22. Thampi, S. M. & Jacob, A. J. (2011). SECURING BIOMETRIC IMAGES USING REVERSIBLE WATERMARKING Sabu. Int. J. Image Process., vol. 5, no. 4.
23. Gothwal, J. K., & Singh, R. (2012). Hiding Additional Information in Fingerprint Images using Fragile Watermarking Technique. *Int. J. Eng. Res. Dev.,* vol. 2, no. 7, pp. 52–61.
24. Jitendra, K. G., & Singh, R. (2014). Applying Information Hiding into Fingerprint Verification System using Fragile Watermarking Technique. *Int. J. Emerg. Sci. Eng.,* no. 8, pp. 12–18.
25. Tian, J. (2003). Reversible Data Embedding Using a Difference Expansion. *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, doi: 10.1109/TCSVT.2003.815962.
26. An, L. Gao, X. & Deng, C. (2010). Reliable embedding for robust reversible watermarking. *Proc. 2nd Int. Conf. Internet Multimed. Comput. Serv. ICIMCS'10*, pp. 57–60, doi: 10.1145/1937728.1937742.
27. An, L., Gao, X., Li, X., Tao, D., Deng, C. & Li, J. (2012). Robust reversible watermarking via clustering and enhanced pixel-wise masking. *IEEE Trans. Image Process.,* vol. 21, no. 8, pp. 3598–3611, doi: 10.1109/TIP.2012.2191564.
28. An, L. Gao, X. Yuan, Y. Tao, D. Deng, C. & Ji, F. (2012). Content-adaptive reliable robust lossless data embedding," Neurocomputing, vol. 79, pp. 1–11, doi: 10.1016/j.neucom.2011.08.019.
29. Thabit, R. & Khoo, B. E. (2014). A new robust reversible watermarking method in the transform domain. *Lect. Notes Electr. Eng.*, vol. 291 LNEE, doi: 10.1007/978-981-4585-42-2_19.
30. Mohammed, R. T. & Khoo, B. E. (2013). Robust reversible watermarking scheme based on wavelet-like transform. *In IEEE ICSIPA 2013- IEEE International Conference on Signal and Image Processing Applications*, doi: 10.1109/ICSIPA.2013.6708032.
31. Mousavi, S. M., Naghsh, A., & Abu-Bakar, S.A.R. (2014). Watermarking Techniques used in Medical Images: a Survey. *J. Digit. Imaging,* vol. 27, no. 6, pp. 714–729, doi: 10.1007/s10278-014-9700-5.

32. An, L., Gao, X., Yuan, Y., & Tao, D. (2012). Robust lossless data hiding using clustering and statistical quantity histogram. *Neurocomputing*, vol. 77, no. 1, pp. 1–11, doi: 10.1016/j.neucom.2011.06.012.
33. Thabit, R., and Khoo, B. E. (2014). Robust reversible watermarking scheme using Slantlet transform matrix. *Journal of systems and software,* vol. 88, no. 1, doi: 10.1016/j.jss.2013.09.033.
34. Thabit, R. & Khoo, B. E. (2015). A new robust lossless data hiding scheme and its application to color medical images. *Digit. Signal Process. A Rev. J.,* vol. 38, doi: 10.1016/j.dsp.2014.12.005.
35. Maltoni, D., Maio, D., Jain, A. K. & Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. 2nd ed. London.
36. Abraham, J. Kwan, P. & Gao, J. (2011). *Fingerprint Matching using A Hybrid Shape and Orientation Descriptor*. In book: State of the art in Biometrics, Publisher: InTech, Editors: Jucheng Yang, Loris Nanni.
37. Xuan, G., et al. (2005). *A Secure Internet-Based Personal Identity Verification System Using Lossless Watermarking and Fingerprint Recognition*. Berlin, Heidelberg: Springer Berlin Heidelberg.
38. Xuan, G., Zhu, J., Chen, J., Shi, Y. Q., Ni, Z. & Su, W. (2002). Distortionless data hiding based on integer wavelet transform," Electron. Lett., vol. 38, no. 25, pp. 1646–1648, doi: 10.1049/el:20021131.

