Cancelable Fingerprint Recognition based on Encrypted Convolution Kernel in Different Domains

Fatma G. Hashad
Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menouf 32951, Menoufia University.

O. Zahran
Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menouf 32951, Menoufia University.

S. El-Rabaie
Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menouf 32951, Menoufia University.

Ibrahim F. Elashry
Department of Electrical Engineering, Faculty of Engineering, Kafrelsheikh University, Egypt.

Ghada Elbanby
Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menouf 32951, Menoufia University.

Moawad I. Dessouky
Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menouf 32951, Menoufia University.

Fathi E. Abd El-Samie
Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menouf 32951, Menoufia University.

Abstract— **Peoples' biometrics, such as fingerprints, are unique , as a result it can be used in many evidence security requests, such as employees' registration gate, crime investigation, and revealing smart phones. The security of fingerprints is very critical in protecting the peoples' identity. In this research, a cancelable fingerprint recognition system is proposed. The proposed system is based on comprising four biometrics in a unified biometric template for each person using Discrete Cosine Transform (DCT) compression. This unified biometric template is encrypted with different convolution kernels produced by chaotic Baker map in different domains. The Integer Wavelet Transform (IWT) and the Discrete Wavelet Transform (DWT) are used to create different transformations of the fingerprint. In case a transformed fingerprint is compromised, the biometric fingerprint transformation is reorganized with another transformation. A comparative study between different transform-domains in the occurrence of attacks shows the authority of encryption in the DWT domain with different keys. Both Equal Error Rate (EER) and Area under Receiver Operating Characteristic (AROC) curve are used for performance evaluation revealing high performance of the proposed system.**

Keywords: Biometrics, Fingerprint recognition, Cancelable biometrics, IWT,DWT.

1. Introduction

In recent years, the usage of human biological data, such as face, iris, and fingerprint biometrics, has seen an exponential progress in every aspect of our daily life. The fingerprint biometrics has the greatest developed technology and has a high user acceptance rate [1]. The problem is that, is the dependence on a single verification biometric, which reduces the trustiness of the verification results. Hence, there is a need to use multiple biometrics for trusted verification results [2-5].

For more security of the biometrics, cancelable biometrics is used. This cancelable biometrics can be easily replaced without the need to modification of the system at all. The trend of cancelable biometrics is a promising trend towards more protected biometric systems [6-7]. So, in this paper we offered the cancelable approach to generate a fingerprint based non-invertible system for secure recognition. Multiple biometrics can be acquired for the same person and used for verification with a majority voting scenario to ensure trusted verification results. So, there is a need to save all biometrics in a secure way, which allows authentication from each of them, afterwards. The storage of multiple biometrics consumes storage space. Hence, there is a need for some sort of compression to save this storage space, while keeping the discrimination ability of subjects.

Different convolution kernels produced by chaotic Baker map in different domains. The Integer Wavelet Transform (IWT) and the Discrete Wavelet Transform (DWT) are used to generate the different transformations. In case a transformed fingerprint is compromised, the biometric fingerprint is updated with another transformation. The proposed system protects the original fingerprint from stealing or tampering. Furthermore, the matching process is done in the encrypted format which prevents the attacker from stealing the fingerprint data during the decryption process.

The rest of the paper is organized as follows: Section 2 discusses the related works. Section 3 presents the proposed cancelable recognition scheme. Section 4 presents the simulation results. Finally, Section 5 presents the concluding remarks.

2. Related Work

There are some works have been presented to generate fingerprints cancelable biometrics. Wang and Hu offered a blind cancelable fingerprint recognition system based on creating binary strings for pair-minutiae vectors, and the use of their frequency samples for identification [8]. This approach is suitable for smart cards as an example of resource-limited applications. It was evaluated over FVC2002 DB1, DB2, and DB3 databases by the way of achieving good results.

Wang et al. presented an approach for cancelable fingerprints based on the segmentation of the fingerprint pattern into local zones and the deployment of a Fourier-like transform to change the guides of all minutiae inside the same local zone [9]. This methodology does not need fingerprints record-keeping. It get gaining in recognition on four different standard databases with Equal Error Rates (EERs) in the lost token situation ranging from 0.19% to 9%.

Wang et al. also presented a cancelable fingerprint biometric system based on the Hadamard transform applied on the binary design of the fingerprint minutiae [10]. The Hadamard transform is applied on the Fourier transform of binary series representing the biometric to generate complex vectors, while protective the distance between the vectors predictable prior to the application of the transform. This approach achieved EERs ranging from 1% to 5% on different standard databases. Some attempts have also been presented for fingerprint and finger-vein cancelable multi-biometric systems [11].

Zhe Jin et. al. presented a fingerprint protection technique to protected the fingerprint minutiae [12]. By combining Randomized Graph-based Hamming Embedding (RGHE), their method supports a minutiae descriptor, dubbed as minutiae vicinity decomposition (MVD) to infer a lot of randomized geometrical invariant features together with irregular projection. The randomized MVD discrimination is then improved by explicit Minutia Vicinities Collection structure ,then it will be installed into a Hamming space by methods for the Graph-based Hamming Embedding. They performed their experiment on the FVC2002-DB1 and FVC2002-DB2 and FVC2004-DB1 and FVC2004-DB2 databases, and obtained EER of 4.36%, 1.77%, 24.71%, and 21.825%.

Wang et al. presented an alignment free cancelable biometric scheme for fingerprints [13]. They used curtailed circular convolution to produce transformed template. First, fingerprint images are recorded according to the singular points. Then, curtailed convolution is applied by multiplying discrete Fourier transformation (DFT) of two series. They performed their experiment on the DB1, DB2 and DB3 of FVC2002 database and achieved EER of 2%, 3% and 6.12%, respectively.

Priyanka Das et. al. presented an alignment-free fingerprint hashing algorithm centered on comprising a minimum distance graph of the inter-minutia minimum distance vectors initiating from the core point as a feature set [14]. Matching of hashes has been activated using an equivalent search algorithm. They completed their experiment on the FVC2002-DB1a and FVC2002-DB2a databases, and obtained EER of 2.27%.

3. Proposed Cancelable Fingerprint Recognition Scheme

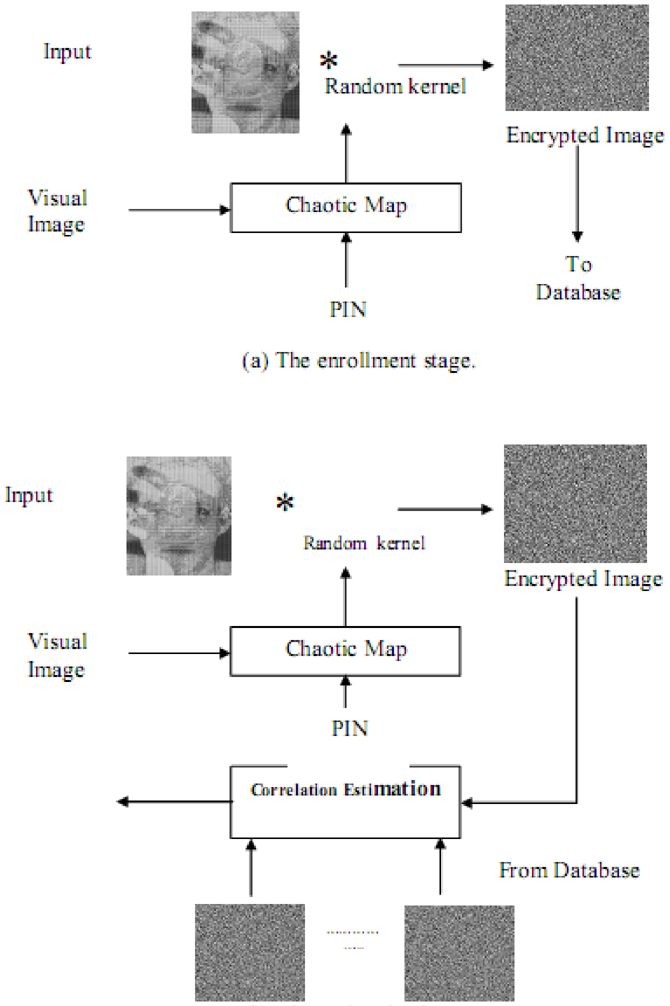
The basic idea of the proposed cancelable system is to compress four biometric images together into a single biometric template and encrypt this template as shown by utilizing 2-D chaotic Baker map in different transform domains, spatial, (IWT) and (DWT). Only, the first quartile of the DCT of each image is kept. Some sort of rotation is performed on these quartiles, and then they are arranged into a new DCT plane comprising information from all biometrics. The obtained new DCT plane is inverted to time domain to get a mixed image from all biometrics. This image is further encrypted for security purposes .The proposed framework comprises of two main stages; the enrolment stage and the authentication stage as shown in Fig. 1(a) and (b), respectively.

3.1 Enrollment Stage

In the enrollment stage, a unified biometric template is acquired and then encryption is performed by convolution with a random kernel that is generated with chaotic Baker map encryption of another image [15-17]. The objective of the random convolution process is to hide the details of the features through the convolution process. The resulting encrypted templates can be saved in a database and then used to validate the user's identity. If the system database is compromised, it is possible to generate a different convolution kernel to get a different encrypted fingerprint. If an attacker tries to reconstruct an individual's fingerprint from the compromised database, he needs to know the convolution kernel used in the enrollment stage. Moreover, the attacker essentially has to perform image de-convolution to retrieve the original fingerprint, which is extremely difficult without knowing the user's PIN, the used encrypted algorithm and also the size of the convolution kernel. Hence, this is considered a high level of security and protection for the fingerprints.

3.2 Authentication Stage

In the authentication stage, the user presents the PIN. This PIN is used to generate the convolution kernel, which is used to encrypt the user's fingerprint. The resulting encrypted fingerprint is then correlated with the encrypted fingerprint templates in the database, and the resulting correlation outputs are examined to perform authentication. The correlation values are used to express the similarity between a test fingerprint and the fingerprints in the database.



(a) The enrollment stage.

(b) The authentication stage.

Fig. 1: The two stages for the proposed cancelable fingerprint recognition scheme.

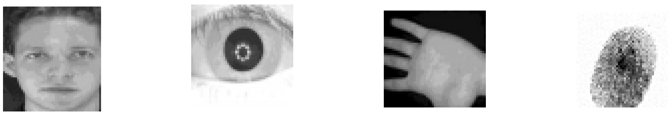


Fig. 2: Samples of the input images.

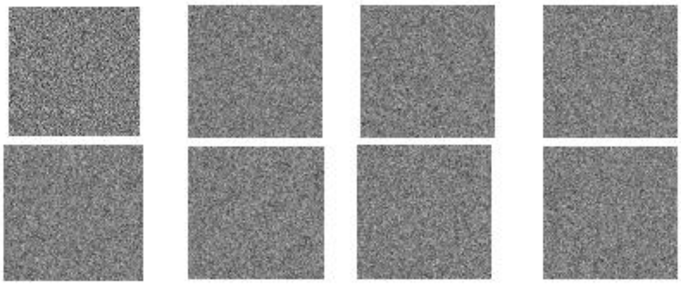


Fig. 3: Samples of equivalent kernel of each fingerprint.

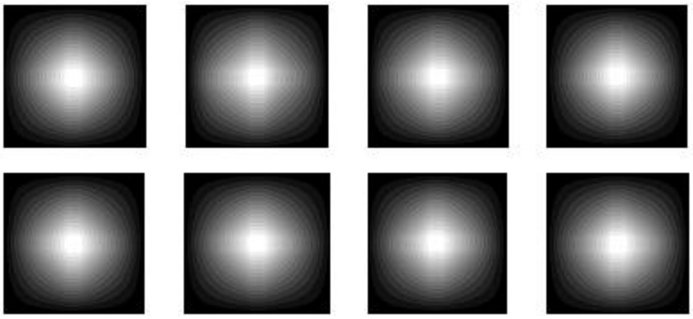


Fig. 4: Samples of encrypted training fingerprints by equivalent Kernels.

The higher the score, the higher is the similarity between fingerprints [18-20]. Accessing of the system is granted only if the score for a test user is higher than a certain threshold known as the Equal Error Rate (EER), which is estimated at the intersection of the impostor and genuine distributions. At the intersection point between these distributions, the incorrect reject and incorrect accept errors are equal [21-23].

Genuine user's score ought to dependably be higher than the scores of impostor users. But it is not always true that the fingerprint with the highest correlation is the correct fingerprint. For example, if the fingerprint scanned to the system does not belong to the database, the system will falsely identify the fingerprint of highest correlation as the correct one. To solve this problem, an EER value should separate between accepted values and non-accepted values and this should be made before checking for the fingerprint with highest correlation. Since the fingerprint in the previous example does not belong to the database in the first place, the resulted correlation should be low. The EER value puts a minimum value for acceptable correlation. If the highest correlation is less than the threshold, the system will not recognize the fingerprint (not in the database). If the value of the correlation is higher than the threshold, then the system will output the fingerprint with the highest correlation as the identified one. If impostor fingerprint generates a score that is higher than the score of a genuine one, the impostor fingerprint will be falsely accepted as a genuine fingerprint. On the other hand, if a genuine fingerprint has a correlation score lower than the threshold, then the genuine fingerprint will be falsely rejected. In the proposed fingerprint recognition system, the test data consists of both impostor and genuine fingerprints. Hence, the correlation scores of each fingerprint would be somehow distributed around a certain mean value. So, the probability distribution of the correlation metric is used to represent the score distribution of impostor and genuine fingerprints. We have Probability of True Distribution (PTD) which is the probability distribution of the correlation between the true fingerprints with the encrypted fingerprints and the Probability of False Distribution (PFD) of the correlation scores resulting in the authentication stage.

4. Simulation Results

In order to evaluate the performance of the proposed scheme, we have worked on 20 images acquired randomly from standard fingerprint images taken from the Fingerprint Verification Competition (FVC2002) database (DB1, DB2, DB3, DB4) and(FVC2004) database (DB1, DB2) [24]. Also databases of faces, iris, and palmprints are used. The used databases in these experiments are ORL database for faces [25], CASIA-V3 for iris [26], CASIA-V1 for palmprint [27]. Four different biometrics assumed to belong to the same person are used to generate a unified biometric template for that person. Samples of fingerprints from the database are shown in Fig. 2.

In the enrollment stage, each user enters his own PIN, and this generates the equivalent kernel to be convolved with the fingerprint. Figure 3 shows the kernel output. The resulting 20 encrypted biometric fingerprints are saved in the system database. Figure 4 shows samples of the encrypted database fingerprints.

In the authentication stage, two fingerprints have been tested. One belongs to a genuine user and the other belongs to an impostor user. In the two cases, the test users enter the PIN and generate the random convolution kernel and two encrypted test fingerprints have been presented. It is assumed that, the impostor user knows the right PIN for any genuine user to test the degree of security of the system. The correlation coefficients are calculated between each of the two encrypted fingerprints and the 20 encrypted fingerprints. Accessing the system is granted only if the score for the test fingerprint is higher than the EER value with an error probability. The probability of correct detection can be easily obtained from the error probability, 100 - (error probability) %. The lower the error probability, the better is the system performance. We plot the curves of the two metrics, PTD and PFD for the proposed encryption scheme in different domains to determine the threshold (EER) value and error probability as shown in Fig. 5 to Fig. 9.

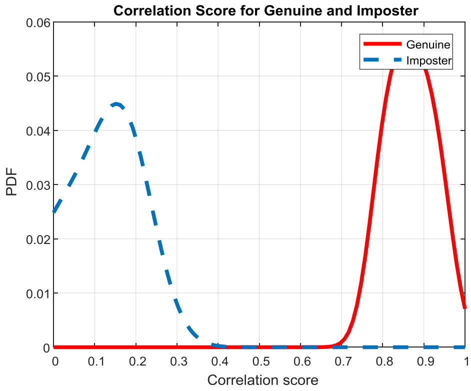


Fig. 5: Impostor and genuine distributions using the circular encryption.

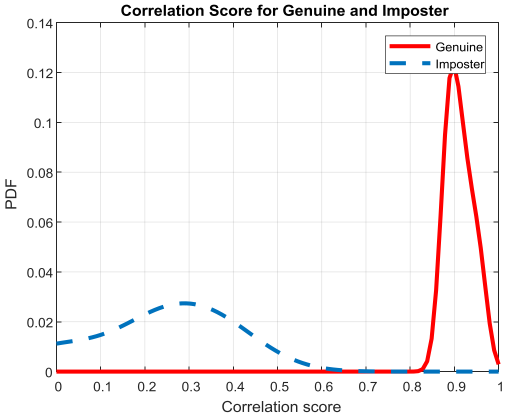


Fig. 6: Impostor and genuine distributions using the IWT encryption.

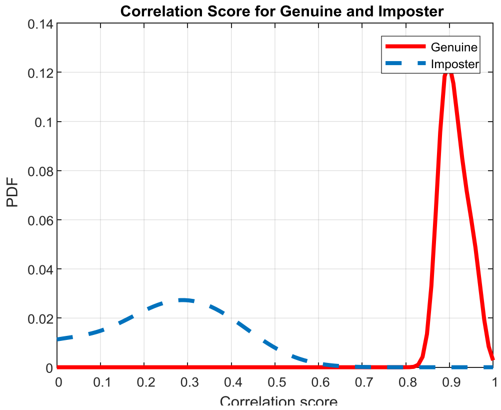


Fig. 7: Impostor and genuine distributions using the IWT domain encryption with different keys.

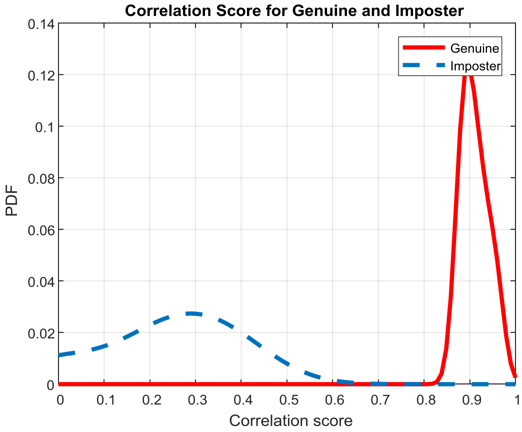


Fig. 8: Impostor and genuine distributions using the DWT encryption.

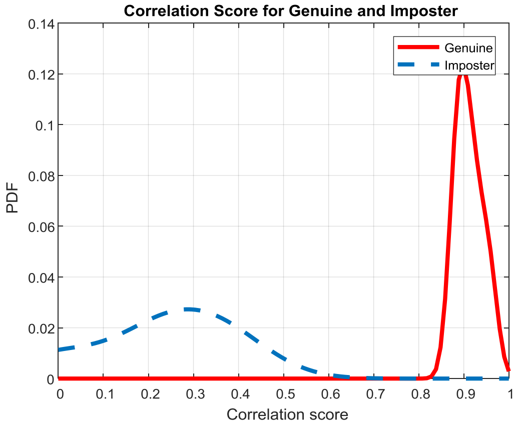


Fig. 9: Impostor and genuine distributions using the DWT encryption with different keys.

4.1 Comparison between the Proposed Fingerprint Recognition Scheme Outputs in Different Transform Domains.

The performance efficiency of the proposed cancelable biometric scheme is evaluated through calculating the EER, the lower the EER value, the more efficient the security of the system. The FPR is defined as the probability that a genuine attempt is incorrectly identified as an un-genuine one (incorrect reject). The FNR is the probability that an un-genuine attempt is incorrectly identified as a genuine one (incorrect accept). The ROC curve is a parametric relation between the True Positive Rate TPR(T) and the False Positive Rate FPR(T) with T as a varying discrimination threshold parameter [21-22]. In this paper we will use the ROC curve for performance evaluation of biometric systems. This is indicated in Fig. 10 to Fig. 14.

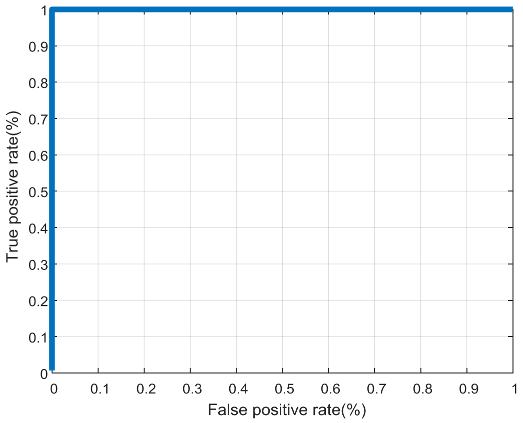


Fig. 10: ROC curve for the circular encryption.

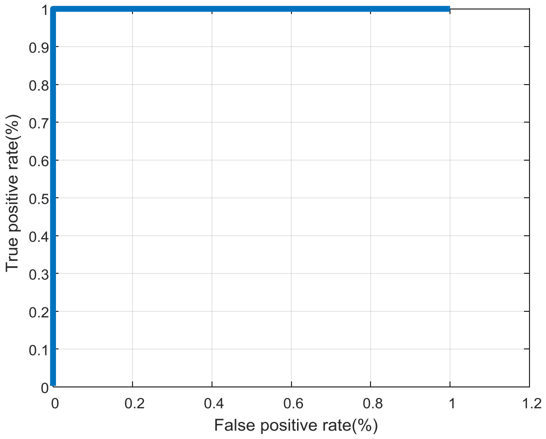


Fig. 11: ROC curve for the IWT encryption.

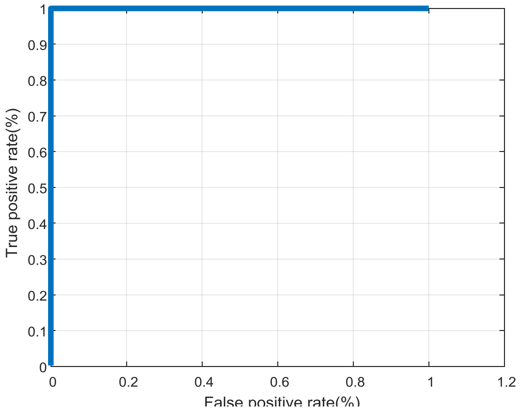


Fig. 12: ROC curve for the IWT encryption with different keys.

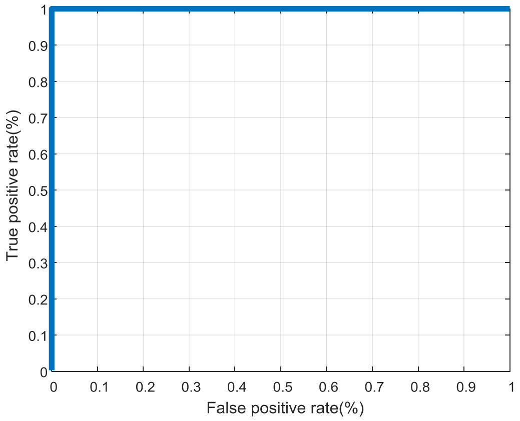


Fig. 13: ROC curve for the DWT encryption.

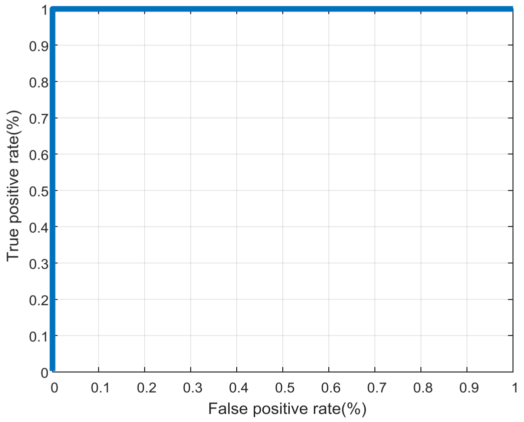
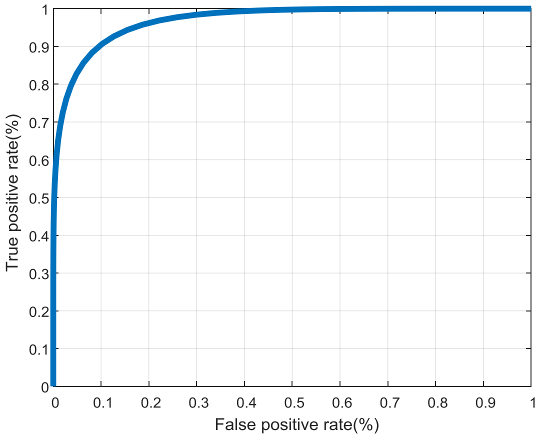


Fig. 14: ROC curve for DWT encryption with different keys.

Table 1 gives a comparison between the proposed fingerprint recognition scheme outputs in different transform domains from a numerical perspective considering the mean of genuine and impostor patterns, EER, the error probability, and the authentication time. It is clear from Table (1) that; the DWT domain with different keys succeeds in achieving high performance with a larger degree of security.

In addition, from Fig.15 to Fig.19 shows the ROC curves in the presence of noise at different levels. The results show that the noise effect at moderate noise levels is acceptable and tables from 2 to 6 give the numerical values extracted from the sensitivity-to-noise study with the different noise levels.

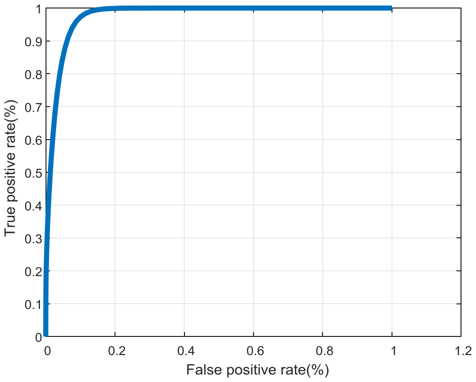


(a) Noise variance=0.02.

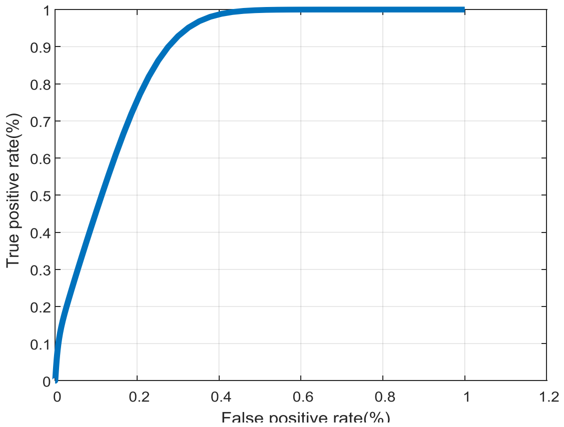
Fig. 15: ROC curves for the circular encryption in the presence of Gaussian noise.

Table 2: Evaluation metrics for the circular encryption in the presence of noise.

Noise variance	EER	AROC
0.02	0.002	0.9692



(a)Noise variance=0.01.

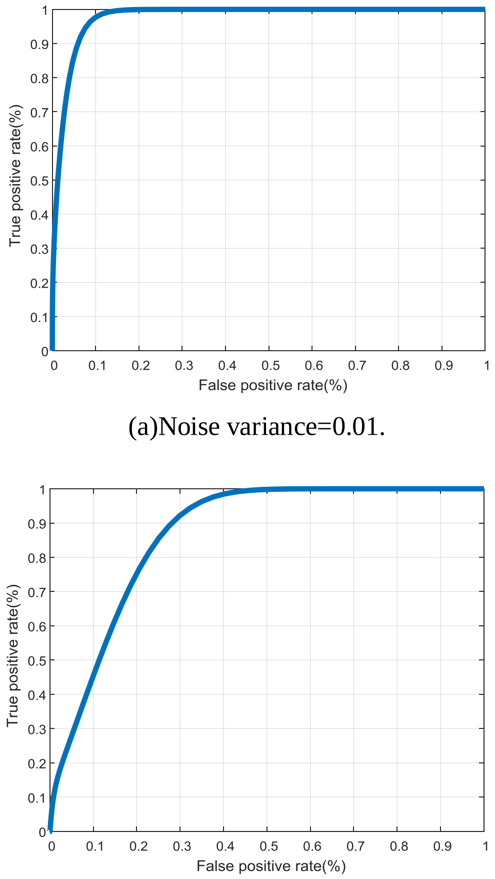


(b)Noise variance=0.02.

Fig. 16: ROC curves for the IWT encryption in the presence of Gaussian noise.

Table 3: Evaluation metrics for the IWT encryption in the presence of noise.

Noise variance	EER	AROC
0.01	0.4545	0.9764
0.02	0.3535	0.8695



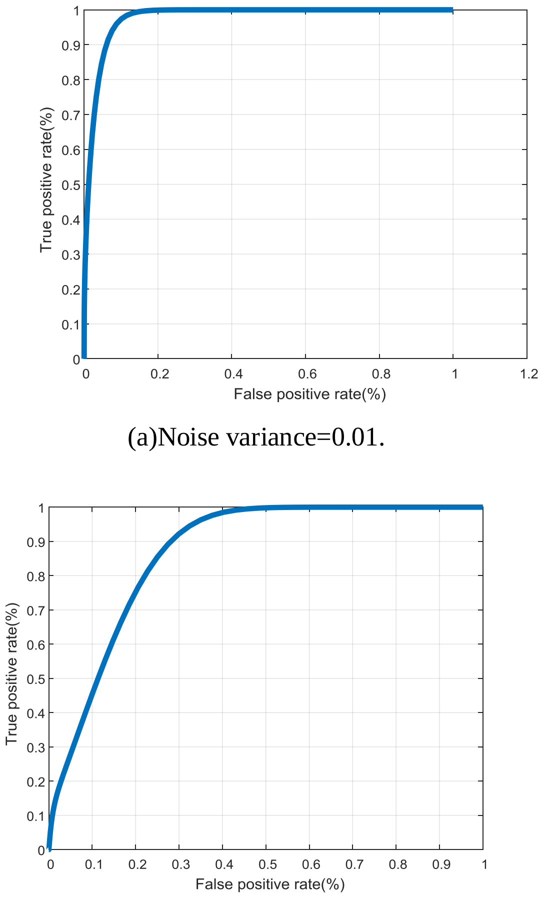
(a)Noise variance=0.01.

(b)Noise variance=0.02.

Fig. 17: ROC curves for the IWT encryption with different keys in the presence of Gaussian noise.

Table 4: Evaluation metrics for the IWT encryption with different keys in the presence of noise.

Noise variance	EER	AROC
0.01	0.4545	0.9773
0.02	0.3535	0.8683



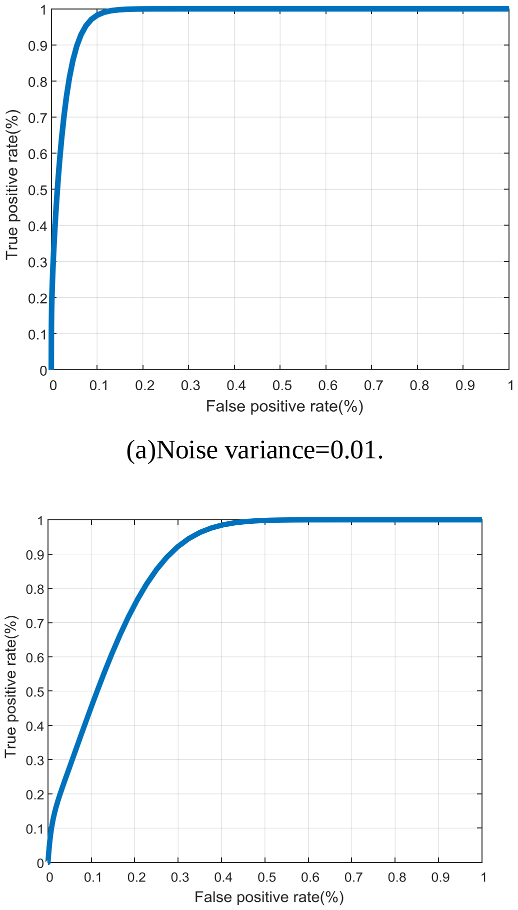
(a)Noise variance=0.01.

(b)Noise variance=0.02.

Fig. 18: ROC curves for the DWT encryption in the presence of Gaussian noise.

Table 5: Evaluation metrics for the DWT encryption in the presence of noise.

Noise variance	EER	AROC
0.01	0.4545	0.9770
0.02	0.3434	0.8698



(a)Noise variance=0.01.

(b)Noise variance=0.02.

Fig. 19: ROC curves for DWT encryption with different keys in the presence of Gaussian noise.

Table 6: Evaluation metrics for the DWT encryption with different keys in the presence of noise.

Noise variance	EER	AROC
0.01	0.4545	0.9779
0.02	0.3535	0.8765

Finally, a comparison between the proposed cancelable fingerprint recognition scheme (using DWT domain with different keys) and some of the state-of-the-art schemes is given in Table 7. These results reveal the superiority of the proposed scheme.

5. Conclusion

This paper offered a multi-biometric security system that depends on merging different biometrics for the same person based on the DCT and encrypting the composite image generated using different convolution kernels produced by chaotic Baker map in different domains. This system performs the authentication directly in the encrypted domain (i.e., no compelling reason to decrypt the images during authentication). This helps to guard against any type of attacks, where the attacker might try to steal the decrypted image during the authentication stage, as would be the case in standard recognition. Moreover, if a transformed version of the fingerprint is leaked, we can simply replace it the fingerprint in another transform domain.

The effect of the chaotic map in different domains on the threshold value, error probability, and the authentication time has been studied in detail. A comparison between all the transformations used in this paper was demonstrated, and the effect of noise on the proposed system has been studied. The DWT transform with different keys has the smallest error probability among all encryption domains and confirm lowest EER values, and highest AROC values compared to other transforms. Hence, the cancelable biometric system using the DWT domain transform with different keys has the best performance. Also simulation and comparison results obtained for the fingerprint cancelable biometric scheme ensure low EER values, and high AROC values compared to other traditional schemes. We can come to a conclusion that it is possible to identify the person from the biometrics involved in the proposed security system with high recognition rates even in the presence of channel degradation effects.

Table 1: The encryption domain effect.

Domain	mean of		EER	Error probability	probability of correct detection	Authentication Time (Sec)
	genuine patterns	impostor patterns				
Spatial domain	0.1030	0.8660	0.0033	1 %	99%	0.281733
IWT domain	0.2303	0.9897	0.0304	1%	99%	0.553501
IWT domain with different keys	0.2291	0.9897	0.0271	1%	99%	0.476315
DWT domain	0.2303	0.9897	0.0027	1%	99%	0.279902
DWT domain with different keys	0.1291	0.9897	0	0.9%	99.1%	0.274335

Table 7: Comparison of EER for different encryption algorithms.

Method	EER(%)					
	FVC2002				FVC2004	
	DB1	DB2	DB3	DB4	DB1	DB2
Hadamard transform [10]	1	2	5.2	-	-	-
Non-invertible randomized graph-based Hamming embedding [12]	4.36	1.77	-	-	24.71	21.825
Curtailed circular convolution[13]	2	3	6.12	-	-	-
Minimum -distance graph [14]	2.27	3.97	-	-	-	-
Proposed scheme using DWT domain with different keys	0	0.4	1	0.6	1	0.8

References

[1] A. K. Jain, A. A. Ross, and K. Nandakumar, " *Introduction to Biometrics*," Springer, 2011, http://www.csee.wvu.edu/ross/BiometricsTextBook.

[2] Ritu and M. Garg, "*A Review on Fingerprint Based Identification System*," SBIET College IJARCCE, Vol. 3, No. 3, 2014.

[3] L. Kocarev, S. Lian, "*Chaos-Based Cryptography*", Algorithms and Applications, vol. 354, Berlin 2011.

[4] C.C. Chang, M.S. Hwang, T.S. Chen, "*A New Encryption Algorithm for Image Cryptosystems*," Proceedings of the Journal of Syst. Software, vol. 58, pp. 83–91, 2001.

[5] Alfalou A, Alkolidi A (2005) "Implementation of an all- optical image compression architecture based on

[6] fourier transform which will be the core principle in the realization of DCT", Proc. SPIE 5823, pp. 183: 190V. M. Patel, N. K. Ratha, and R. Chellappa, "*Cancelable biometrics: A Review*," Proceedings of the IEEE Signal Processing Magazine 32(5), 54-65, 2015.

[7] A. Sarkar and B. K. Singh "*Cancelable biometric based key generation for symmetric cryptography*," International Conference on Inventive Communication and Computational Technologies (ICICCT),doi:10.1109/icicct.2017.7975229,2017.

[8] H. Kaur and P. Khanna, *"Non-invertible biometric encryption to generate Cancelable biometric templates,"* Proceedings of the world Congress on Engineering and Computer Science, San Francisco USA I, October 25-27, 2017.

[9] Wei-Chao Liu and Hong-tao Guo, *"Occluded Fingerprint Recognition Algorithm Based on Multi Association Features Match,"* Proceedings of the Journal Of Multimedia, Vol. 9, No. 7, pp. 910 - 917, 2014.

[10] S. Wang, G. Deng, and J. Hu, *"A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations,"* Proceedings of the Pattern Recognition Vol. 61, pp. 447-458, 2017.

[11] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "*A fingerprint and finger-vein based cancelable multi-biometric system,* " Proceedings of the Pattern Recognition Vol. 78, pp. 242-251, 2018.

[12] Z. Jin, M.H.Lim, A.B.J.Teoh, B.M.Goi, *"A non-invertible randomized graph- based Hamming embedding for generating cancelable fingerprint template,"* Pattern Recognit. Lett., Vol. 42, pp. 137–147, 2014.

[13] S. Wang and J. Hu, *"Design of alignment-free cancelable fingerprint templates via curtailed circular convolution,"* Proceedings of the Elsevier J. Pattern Recognition. Vol.47, no. 3, pp. 1321- 1329, 2014.

[14] P. Das, K. Karthik and B. C. Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs," Proceedings of the Elsevier J. Pattern Recognition. Vol. 45, no. 9, pp. 3373-3388 , 2012.

[15] Carmen Pellicer- Lostao, Ricardo Lopez-Ruiz, "Notions of Chaotic Cryptography, Sketch of a Chaos based Cryptosystem", Proceedings of the Applied Cryptosystem and network Security (Intech Books), 1st Edition, pp. 267-294, March 2012.

[16] G. Bhatnagar, and Q. Wu, *"Chaos-Based Security Solution for Fingerprint Data during Communication and Transmission,"* Proceedings of the Instrumentation and Measurement, IEEE Transactions on, Vol. 61, No. 4, pp. 876-887, 2012.

[17] Ensherah A. Naeem, Mustafa M. Abd Elnaby , Naglaa F. Soliman , Alaa M. Abbas, Osama S. Faragallah, Noura Semary, Mohiy M. Hadhoud f, Saleh A. Alshebeili, Fathi E. Abd El-Samie, " Efficient implementation of chaotic image encryption in transform domains", Proceedings of the Journal of Systems and Software, Vol. 97, pp. 118–127 , 2014.

[18] B. V. K. V. Kumar, A. Mahalanobis, and R. D. Juday, *"Correlation Pattern Recognition,"* Cambridge Univ. Press, 2005.

[19] A. Sarkar, B. K. Singh, and U. Bhaumik, *"Cryptographic Key Generation Scheme from Cancellable Biometrics,"* Progress in Computing Analytics and Networking 265–272.doi:10.1007/978-981-10-7871-2_26, 2018.

[20] Soliman RF, Amin M, Abd El-Samie FE ," A double random phase encoding approach for cancelable Iris recognition," Springer, Optical and Quantum Electronics no.50, Vol.326, pp.1–12,2018.

[21] S. Wang, and J. Hu, *"A blind system identification approach to cancelable fingerprint templates,"* Proceedings of Pattern Recognition Vol. 54, pp. 14-22, 2016.

[22] Technical Document about FAR, FRR and ERR, Version 1.0, by SYRIS Technology Corporation, 2004.

[23] Wu, J. C., and Wilson, C. L., *"An empirical study of sample size in ROC-curve analysis of fingerprint data,"* Proceedings of the

Biometric Technology for Human Identification III (SPIE), Vol. 6202, DOI: 10.1117/12.665601, 2006.

[24] Fingerdata base http://bias.csr.unibo.it/fvc2002/databases.asp ,Accessed July 2018.

[25] CASIA-Iris V3 Database, http://www.cbsr.ia.ac.cn/ English/Iris Data base.asp. Accessed December 2018.

[26] CASIA Palmprint Database, http://biometrics.idealtest.org / Accessed July 2018.

[27] ORL database: https://www.cl.cam.ac.uk/research/dtg/ attarchive /facedatabase.html, Accessed July 2018.