https://doi.org/10.31449/inf.v42i3.1855 Informatica **42** (2018) 369–373 **369**

Cancelable Fingerprint Features Using Chaff Points Encapsulation

Mokhled S. Al-Tarawneh
Computer Engineering Department, Faculty of Engineering, Mutah University, B.O.Box (7), Mutah 61710, Jordan
E-mail: mokhled@mutah.edu.jo

Keywords: fingerprint, feature extraction, minutiae, cancelable, encapsulation, chaff points

Received: September 20, 2017

Recently, biometrics imaging is widely used in several security areas such as security monitoring, database access, border control and immigration, and for reliable personal verification, identification and recognition schemes. To determine or confirm the identity of an individual's based on their physiological and/or behavioral characteristics, biometric features must be used. The aim of this paper is to review cancelable biometric generation and protection schemes. An approach for generating chaff points for fingerprint template features encapsulation as fingerprint cancelability infrastructure has been presented. Results show that strong positive correlation of original minutiae scores go with high decapsulated minutiae scores. To test the given cancelable approach performance two indexes are used, FAR (false accept rate) and FRR (false reject rate).

Povzetek: Razvita je nova biometrična metoda za prepoznavanje prstnih odtisov, temelječa na računalniškem algoritmu.

1 Introduction

Biometrics increasingly forms the basis of identification and recognition across many sensitive applications[1]. Biometrics is statistical analysis of people's physical and behavioral characteristics, It is more convenient for users, reduces fraud and is more secure. Fingerprint is commonly used modality compared to traditional identification and verification methods, such as plastic identification card, or traditional passwords [2]. Fingerprint authentication has two phases, enrolment and authentication (or verification). Enrolment involves measuring an individual's biometric data to construct a template for storage. Authentication involves a measurement of the same data and comparison with the stored template [3]. The core of any biometric system is the extracted template, where the matcher algorithms in this systems depends on template matching in one to one (verification) and one to many (identification) modes. It has become critical to protect fingerprint templates in the widespread biometric community. One way for doing this is using cancelable techniques, which transforms original templates in a non-invertible way and uses those transformed templates to verify a person's identity. Securing a stored fingerprint template and image is of paramount importance because a compromised fingerprint cannot be easily revoked. That why fingerprint template should be protected, where an ideal biometric template protection scheme should possess the following four properties [2]. 1) Diversity: if a revoked template is replaced by a new model, it should not correspond with the former. This property ensures the privacy. 2) Revocability: It should be possible to revoke a compromised template and replace it with a new one based on the same biometric data. 3) Security: It must be computationally hard to obtain the original template from the protected template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template. 4) Performance: The biometric template protection scheme should not degrade the recognition performance, false acceptance rate (FAR) and false rejection rate (FRR) of the biometric system[4]. Due to some biometric vulnerabilities, lack of security because it is impossible to revoke biometric unlike password or token, and therefore if biometric is leaked out once and threat of forgery has occurred, the user cannot securely use his biometric anymore. The only remedy is to replace the template with another biometric feature. However, a person has only a limited number of biometric features [5]. In order to overcome the vulnerabilities of biometric systems, both biometrics and crypto research communities have addressed some of the challenges, one of them is cancelable biometric which gained a lot of interest in recent years [6]. The concept behind the cancelable biometrics or cancelability is a transformation of a biometric data or extracted feature into an alternative form, which cannot be used by the imposter or intruder easily, and can be revoked if compromised. This paper proposed a cancelability method based on chaff point encapsulation to cope with biometric drawbacks. The method was tested according to performance evaluation factors.

2 Related works

Cancelable biometric generation has gained a lot of interest in recent years, and it is studied from different point of views, it could be categorized as:

1- Biometric Crypto Systems, this approach is used key binding or key generation schemes, where key binding is a user specific key or a helper data which is independent to the biometric data,

while key generation is generating the helper data from the biometric data using specific notations of crypto systems[7] [8] [9] [10].

2- Biometric Transformations: This approach is based on the transformations of biometric features, where it is categorized into two ways: Bio-Hashing which is used an external key source (PIN or Password) and other functional parameter representation to generate Hash value of the biometric data, it stores the Hash value alone in the data base [11] [12] [13] and Non-invertible transformation [14] [15], such that no information can be revealed from the cancelable biometrics template, which is stored in databases for personal identification/verification, or using biometric data to transform its cancellable domain by polynomial functions and co-occurrence matrices[16].

The proposed method will use encapsulation techniques to protect biometric template. Thus, cancelable template can be attained by template chaff point's encapsulation, where the principal objectives of cancellable biometrics templates can be checked, such as diversity, cancelability, reusability, non-invertability, and performance of technique.

3 Fingerprint feature extraction

The information carrying features in a fingerprint are the line structures, called ridges and valleys[17]. Figure 1, the ridges are black and the valleys are white. It is possible to identify two levels of detail in a fingerprint. Based on carried ridge and valleys minutiae points could be extracted. The minutiae provide the details of the ridge-valley structures, like ridge-endings and bifurcations. Minutiae are subject to post- processing to verify the validity of that are extracted using standard minutiae extraction algorithms. In this study the needed information to be extracted are minutiae coordination's (x, y), type of minutiae (ridge ending or bifurcation), and orientation. Table 1, shows some extracted samples from FVC2004, DB1_B database.

Figure 1: Minutiae-based Fingerprint Extraction.

Due to the importance of extracted fingerprint features (minutiae) and it is criticality as a major step in designing a secure biometric system. The protection of feature templates of the users those are stored either in a central database or on smart cards. If it is compromised, it leads to serious security and privacy threats, it is not possible for a legitimate user to revoke his biometric identifiers and switch to another set of uncompromised identifiers, that why we were looking for a technique to protect this extracted temples, encapsulation technique could solve previous problems. A FVC2002 database[18] with best extraction algorithm based on high scores on distributions, acceptance and rejection rates was chosen to be based for cancelable encapsulation algorithm. For accurate algorithms in extracting minutiae features for creating encapsulation cancelable based system, a comparison result of performance evaluation according to values of False acceptance rate (FAR), False rejection rate (FRR) and Error equal rate (EER) was explored, Table 1, all comparison algorithms took coordination, type and orientation as parameters for extracted features.

FVC2002,DB1_1,101_1				FVC2002,DB1_1,107_1			
X	Y	Type	Orient	X	Y	Type	Orient
216	46	3	0.5030	254	38	1	0.7503
190	49	1	3.5827	218	58	3	0.5566
146	64	1	3.2684	160	68	3	2.6141
247	80	1	0.7002	187	74	1	6.1710
173	86	1	0.3665	155	79	1	5.5414
302	93	1	0.8371	162	87	1	2.3393
176	127	3	0.2761	140	130	1	4.9955
227	131	3	0.5634	107	138	3	5.1562
164	135	1	3.3159	156	139	1	1.8174
117	140	1	5.7642	245	139	1	1.0242
196	181	1	3.7386	195	140	3	0.4140
176	187	3	0.4612	195	151	3	3.7130
151	195	1	5.7175	225	156	3	0.9941
285	215	3	0.7886	196	165	1	4.5301
227	218	1	0.8160	151	186	1	4.7262
152	219	1	2.2884	295	188	3	0.9923
169	233	1	4.1407	135	200	3	4.7436
147	242	1	4.6064	241	218	1	4.1310
186	250	1	4.1676	287	239	3	0.7131

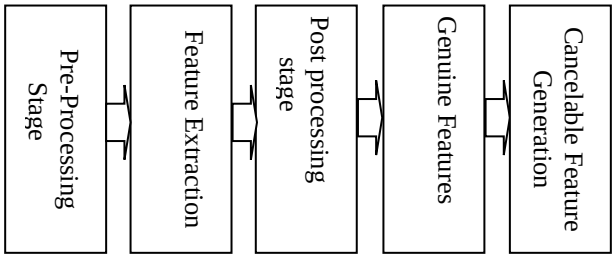
Table 1: Extracted minutiae points with data(x, y, t, Φ).

That why minutiae extraction points with previous references (x, y, t, Φ) was taken as a fundamental step for proposed framework and future method of cancelability.

4 Proposed framework

A novel method is proposed in this section. It is name as encapsulation protection method. It includes the building blocks of phases such as preprocessing, minutiae extraction, post processing and cancelable and irrevocable template generation. The proposed method uses fingerprint biometric to generate cancelable template. The system level design of the proposed method is given in figure 2.

Figure 2: System level design for fingerprint cancelable template generation.



In preprocessing stage a feeding input is the original fingerprint image taken from database DB1_1 [18], where automatic cropping technique was applied based on image background to detect the region of interest (ROI) of target image. ROI image was given to enhancement step as a part of pre-processing stage because the quality of fingerprint structure (ridge, valley) is an important characteristic. An enhancement technique applied in pre-processing phases as normalization, ridge segmentation, structure orientation estimation, frequency enhancement estimation and thinning to get binarization image which is pre extracting feature identification figure 3. After binarization and thinning process, a Cross Number algorithm (CN) described in [19, 20] was applied to get minutiae extraction. The CN algorithm is working on pixel representation to detect all minutiae, while the false minutiae can be eliminated at the post-processing stage by validating algorithm to get only genuine features.

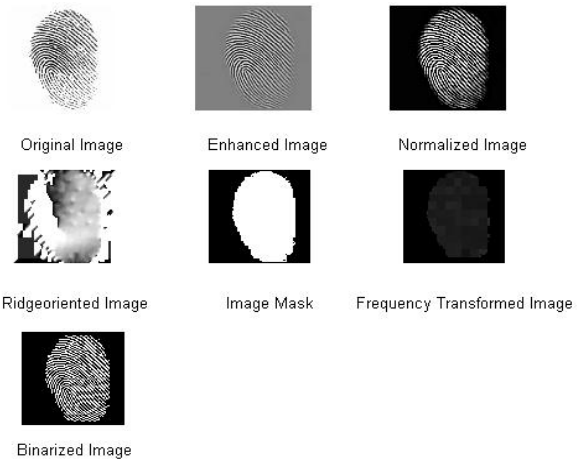


Figure 3: A result of proposed frame work, original, enhanced, normalized, filtered and binarized images.

5 Cancelable feature generation

The basic idea of cancelable feature generation as encapsulation method is to compute encapsulation chaff points (ECP) based on original extracted minutiae, where it used to recover the enrolled template on transmission stage, as well matching on the same stage. Pseudo-code of ECP is given in Algorithm 1:

Algorithm 1: Encapsulation method based on cancelable feature generation.

Input Extracted minutiae template with (x,y) coordinates, T-type of minutiae {3 bifurcation, 1 ridge ending}, Φ-orientation, m number of minutiae, X(x, y, T).

Step 1: Perform chaff points

For k=1: m

Y=change X(x → y, y → x, T=T+1)

End for

Step 2: Mix new chaff point with original minutiae

Z=(X, Y) concatenate

Output Z(x,y,T)

End Algorithm

A representation of original extracted minutiae for FVC2002, DB1_1,101_1 from table1 shown in figure 4.

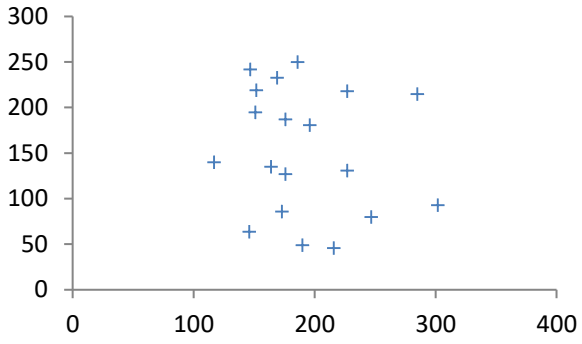


Figure 4: Original extracted minutiae representation.

Applying this algorithm on FVC2002, DB1_1,101_1 from table 1 will give figure 5. a chaff points, while a mixing encapsulation result will be shown in figure 6.

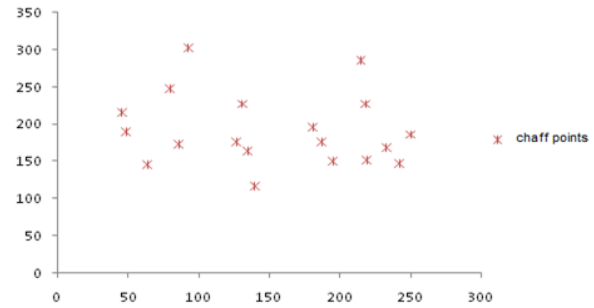


Figure 5: Chaff points representation.

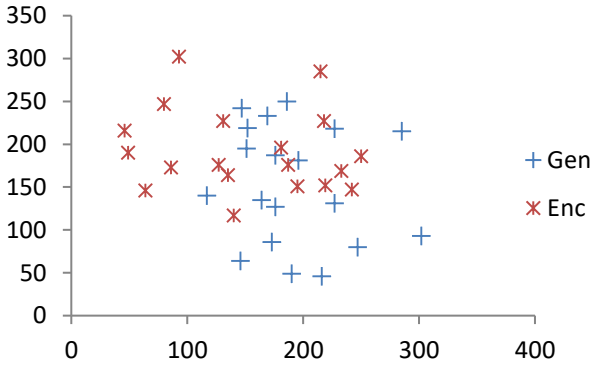


Figure 6: Mixing encapsulation of original minutiae and chaff points representation.

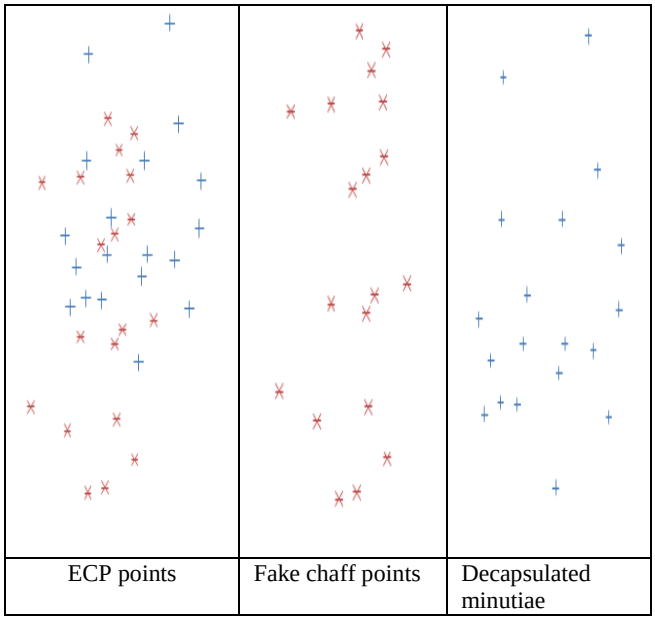
A Decapsulation part of proposed frame work is used to open up transmitted encapsulated data, separate faked chaff points from original minutiae points. The following algorithm explaining the procedure of computing decasulation chaff points (DCP), Pseudo-code of DCP is given in Algorithm 2:

Algorithm 2: Decapsulation method to wrap up genuine minutiae points.

Input Encapsulated template with (x, y) coordinates, T-type of minutiae {3 bifurcation, 1 ridge ending, 2 and 4 fakes}, Φ-orientation, m number of minutiae, X(x, y, T).

Step 1: Read transmitted encapsulated template

X= Find fake chaff points



ECP points	Fake chaff points	Decapsulated minutiae

Figure 7: Decapsulation method to wrap up genuine minutiae points.

Step 2: Y= divide a template on base of chaff point with their types

Z=(X, Y) separate

Output Z(x,y,T)

End Algorithm

A representation of this process is shown in figure 7.

6 Experimental study

An empirical study is performed to test the cancelability and irrevocability of the proposed method using linear correlation test of general original clear minutiae with decapsulated minutiae scores, the strength and nature of the linear relationship between two scores of clear and decapsulated minutiae. Applying linear coefficient (R) formula on given results, the value of R is found to be 0.9999. This is a strong positive correlation, which means that high original minutiae scores go with high decapsulated minutiae scores (and vice versa) figure 8. Another test was done to check the performance of proposed method; it was evaluated by calculating false acceptance rate (FAR) as well false reject rate (FRR) for scenario, original extracted and decapsulated templates. Sequence of experiments is made on the proposed method using benchmark databases such as FVC (Fingerprint Verification Contest) in 2002, 2004 figure 9, figure 10.

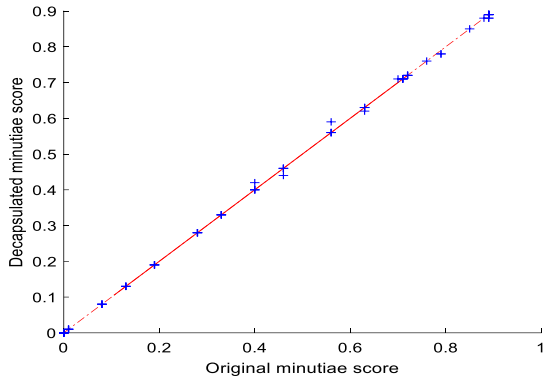


Figure 8: A correlation scores of original minutiae and chaff points representation.

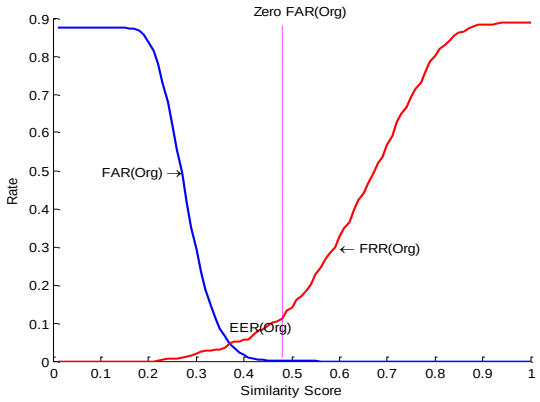


Figure 9: FAR/FRR of the dual fingerprint matcher that employs original minutiae template.

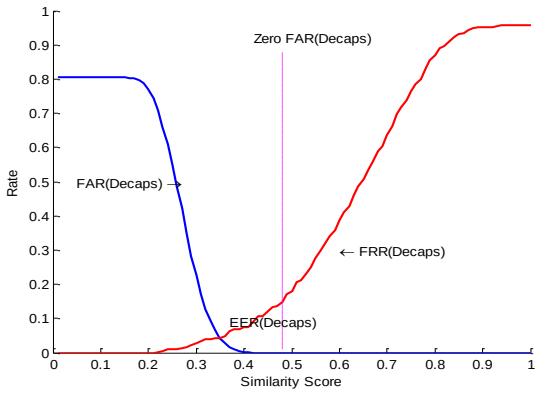


Figure 10: FAR/FRR of the dual fingerprint matcher that employs cancelable template.

7 Conclusion

An approach for generating chaff points for fingerprint template features encapsulation as fingerprint cancelability infrastructure has been presented. The approach takes advantage of fingerprint extracted information (minutiae points) to provide a novel way of generating chaffs from original ones. In addition this approach provides encouraging prospects to be used as platform of cancelable fingerprint feature extraction. From all the results, it could be able to prove that this approach with the usage of general extracted minutiae based new chaff points gave a better performance results and it is experienced as an efficient method for irrevocability and cancelablity of fingerprint template encapsulation.

8 References

[1] Punithavathi, P. and G. Subbiah, *Can cancellable biometrics preserve privacy*. Biometric Technology Today, 2007. 7: p. 8-11. https://doi.org/10.1016/S0969-4765(17)30138-8

[2] Jain, A., K. Nandakumar, and A. Nagar, *Biometric Template Security.* EURASIP Journal on Advances in Signal Processing, 2008: p. 1-17. https://doi.org/10.1155/2008/579416

[3] Ang, R., R. Safavi–Naini, and L. McAven, *Cancelable key-based fingerprint templates*, in Proc of the Australasian Conf. on Information Security and Privacy ACISP'05,242-252 2005. https://doi.org/10.1007/11506157_21

[4] Moujahdi, C., et al., *Spiral Cube for Biometric Template Protection*, in Image and Signal Processing. 2012. p. 235-244. https://doi.org/10.1007/978-3-642-31254-0_27

[5] Hirata, S. and K. Takahashi, *Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching,* ICB 2009,LNCS, Tistarelli, M and Nixon, M.S. (Eds), Springer, 2009. **5558**: p. 868-878. https://doi.org/10.1007/978-3-642-01793-3_88

[6] Patel, V.M., N.K. Ratha, and R. Chellappa, *Cancelable Biometrics: A Review.* IEEE Signal Processing Magazine, 2015. **32**(5): p. 54-65. https://doi.org/10.1109/MSP.2015.2434151

[7] Reiter, M., et al. *Cryptographic key-generation from voice*. in IEEE Computer Society Symposium on Research in Security and Privacy. 2001. USA. https://doi.org/10.1109/SECPRI.2001.924299

[8] Uludag, U., et al., *Biometric cryptosystems: issues and challenges.* Proceedings of the IEEE, 2004. **92**(6): p. 948-960. https://doi.org/10.1109/JPROC.2004.827372

[9] F.Hao, R. Anderson, and J. Daugman. Combining crypto with biometrics effectively. in IEEE Transactions on Computers 2006. https://doi.org/10.1109/TC.2006.138

[10] Ratha, N.K., et al., *Generating Cancelable Fingerprint Templates.* IEEE Transactions on Pattern Analysis and Machine Intelligence, 2007. **29**(4): p. 561-572 https://doi.org/10.1109/TPAMI.2007.1004

[11] Viellhauer, C., R. Steinmetz, and A. Mayyerhofer. *Biometric hash based on statistical features of online signatures*. in the International conference on Pattern Recognition. 2002. https://doi.org/10.1109/ICPR.2002.1044628

[12] Goh, A. and D.C.L. Ngo, *Computation of Cryptographic Keys from Face Biometrics,* in Communications and Multimedia Security. Advanced Techniques for Network and Data Protection: 7th IFIP-TC6 TC11 International Conference, CMS 2003, , A. Lioy and D. Mazzocchi, Editors. 2003, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 1-13. https://doi.org/10.1007/978-3-540-45184-6_1

[13] R.Ang, R.Safav-Naini, and L.McAven. Cancelable *Key-based Fingerprint Templates*. in 10th Australian Conf, Information Security and Privacy. 2005. https://doi.org/10.1007/11506157_21

[14] Ratha, N.K., et al., *Generating Cancelable Fingerprint Templates.* IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, 2007. **29**: p. 561-572. https://doi.org/10.1109/TPAMI.2007.1004

[15] Nagar, A. and A.K. Jain. *On the security of non-invertible fingerprint template transforms*. in 2009 First IEEE International Workshop on Information Forensics and Security (WIFS). 2009. https://doi.org/10.1109/WIFS.2009.5386477

[16] Dabbah, M.A., W.L. Woo, and S.S. Dlay. *Secure Authentication for Face Recognition*. in IEEE Symposium on Computational Intelligence in Image and Signal Processing. 2007. USA. https://doi.org/10.1109/CIISP.2007.369304

[17] Palmer, L.R., et al. *Efficient fingerprint feature extraction: Algorithm and performance evaluation*. in 2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing. 2008. https://doi.org/10.1109/CSNDSP.2008.4610735

[18] FVC2002, F.w.s. [cited; Available from: http://bias.csr.unibo.it/fvc2002].

[19] Zhao, F. and X. Tang. *Preprocessing for skeleton-based fingerprint minutiae extraction*. in Proc. Int'l Conf Imaging Science, Systems, and Technology (CISST). 2002. https://doi.org/10.1016/j.patcog.2006.09.008

[20] Sudiro, S.A., M. Paindavoine, and M. Kusuma. *Simple Fingerprint Minutiae Extraction Algorithm Using Crossing Number On Valley Structure*. in IEEE Workshop on Automatic Identification Advanced Technologies, 2007. 2007. https://doi.org/10.1109/autoid.2007.380590