ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 4, No. 6, 134-139 (2019)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

Spiral Curve for Revocable Touchless Fingerprint Template Securisation

Tahirou Djara[1,2,*], Boris Sourou Zannou[1,2], Antoine Vianou[1,2]

[1]*Laboratoire d'Electronique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC), Cotonou, Bénin*

[2]*Institut d'Innovation Technologique (IITECH), Abomey-Calavi, Bénin*

ARTICLE INFO

Article history:
Received: 03 August, 2019
Accepted: 07 November, 2019
Online: 25 November, 2019

Keywords:
Revocability
Secrecy
robustness

ABSTRACT

Fingerprint data is really protected by cancelable fingerprint template because it can be revoked when compromise and a new one can be reissued. We develop a touchless cancelable fingerprint template whose algorithm was published in our previous work. We implement here the algorithm and conducted several tests on several databases to confirm the stability of the model. To justify how specific keys are used, we used the Kolmogorv-Smirnov test (K-S) and the distribution histogram of legitimate / impostor scores. We compared two systems in which users register. This is the reason for the average value of K-S (0.7812) and similarity assessment (2.4703). These results improve sufficiently (6.1636 and 0.9934 for the successive separability and the K-S test) during the evaluation of the user keys through the second device. We have tested the diversity of curves that we generate. Our proposed non-contact revocable fingerprint model has demonstrated robustness against the security challenges that fingerprint authentication systems are exposed to. We evaluated it on our own database. The requirements of revocability, diversity and security are achieved with very good performance as evidenced by the FAR (False Acceptance rate) obtained on our database (0.0015).

1. Introduction

Biometry is the identification from human characteristic and traits. The most used feature in human authentication is the fingerprint. It performs well and is unique. Minutiae are the most used representation. Nevertheless, several researches have proved that one could reconstruct the original fingerprints from some characteristics. There are problems of correspondence and paring. It should be noted that during the matching phase, the model is exposed to several intrinsic security issues including the threat of privacy, attack record multiplicity(ARM) which are the most common. ARM remains the most formidable and continues to be the focus of intensive research. Therefore the issue of securing authentication with fingerprints comes out. We design a new model for data protection enhancement protection. Our vision is therefore to deal with them by taking into the paradigms of diversity, revocability, precision and invertibility.

In [1], Author identified three major classes of fingerprint-based protection models: feature transformation, biometric cryptosystem, and hybrid. Each of these methods present its own limitation and advantages [2]. The principal requirement of a good protection template hasn't been achieved. Our interests focus on rigid transformations. Basically it will be a G transformation function with original characteristics by using a key b; the transformed template G(a, b) is then stored in the database. We use that function to transform the characteristic test c, then the transformed characteristics G(a, b) and G(c, b) will be compared in order to know yes or no if the user is the right one. Entity transformation models are classified into two main classes, namely vector-based approach and point-of-interest approach (especially those based on minutiae). This depends on the representation model that is adopted.

This article proposes a new approach that is difficult to reverse, especially for systems using minutiae as model. This technic provides revocability, diversity and security while improving performance. It should be noted, however, that to ensure security through the bio-cryptosystem or transformation of characteristics, the fingerprint device observes a delay in the accuracy or during the inversion. Our device for strengthening the fingerprint authentication has the advantage of avoiding leash dragging during the image acquisition step. Our vision is to implement a non-invertible transformation that meets the requirements of

[*] Tahirou Djara, Email: csm.djara@gmail.com

https://dx.doi.org/10.25046/aj040616

performance, diversity, revocability and security. Thus, we use information provided by the munities obtained to generate contactless curves with respect to the center of mass. Section 1 presents the introduction, then in section 2 we present the security holes in contactless biometric systems. The section 3 present our revocable and secure contactless model. Section 4 presents the experimental results to finally give the conclusion in section 5.

2. Security holes in non-contact biometric systems

Biometric systems are exposed to many security vulnerabilities [3,4]. Malicious, for example, could attack the database and recover sensitive information. In order to secure the biometric systems of the most unimaginable attacks, intensive research efforts are conducted. Many techniques have been developed for the purpose of securing biometric data.

. The basic idea of all these models is to generate revocable templates. By revocability it should be understood that in comparison to passwords that could be modified if they are damaged, the user model stored in the database could also be generated in a new (different from the previous) using the same biometric information. Diversity, security and performance are the characteristics that an ideal model of protection must have for security models. Diversity means that it is necessary to ensure that there is no correspondence between the compromised models and those newly generated in the case where a new model is generated to replace an old one Security is the impossibility for a malicious person to recover the original data of a user who was used to build his model. Performance means keeping the authentication capacity of the biometric system intact, which should not be affected by data protection. In a biometric system, instead of storing biometric templates directly, the transformed templates are stored in the database for subsequent authentication. In this technique, the biometric characteristics are transformed into another domain [6] and only the transform (signature) is stored in such a way that the details of the original biometric data cannot be revealed to a malicious person. he gets the biometric pattern. The biometric characteristic elements are transformed into another model G (a; b) which will be stored in a database for future authentication, the biometric information β of the user is transformed into G (c, b) to allow a comparison with G (a, b) to decide whether it is a malicious or an authentic one. The attacks essentially originate in the security vulnerabilities that can essentially be counted:

- Presentation attacks: fingerprint is presented at the inputs after having reproduce it;
- hacking and using data from fingerprint after bypassing Sensor
- The usurped characteristics are substituted for the originals.
- Tripatouillage in the correspondence module to use the false features

In [1], Author have cited security loopholes through a fish skeleton.

3. Literature review

Given the security weaknesses listed above, it is necessary to look for sustainable solutions. It is within this framework that solutions approaches are born. We can mention revocable biometrics without alignment and biometrics based on pre-registration. These solutions are based on the local structures of the minutiae or the taking of the munities in pairs or in a triangle because they do not vary with the rigid transformation. In the next paragraph we will go through the revocable models without alignment. In [5], Authors have proposed one of the most recent models by inserting two key factors. Their model focused on a self-alignement local structure based on textures as features. Their research was much more focused on the many possible attacks rather than dealing with algorithms managing the loss of models or two keys. Another recent technique in [5] evaluates the orientation of the munitie in the surrounding area at each reference munitie. All this is possible thanks to two functions allowing to evaluate the number of transformations around each munitie of reference. The performance of this technique drops when it comes to poor quality images.

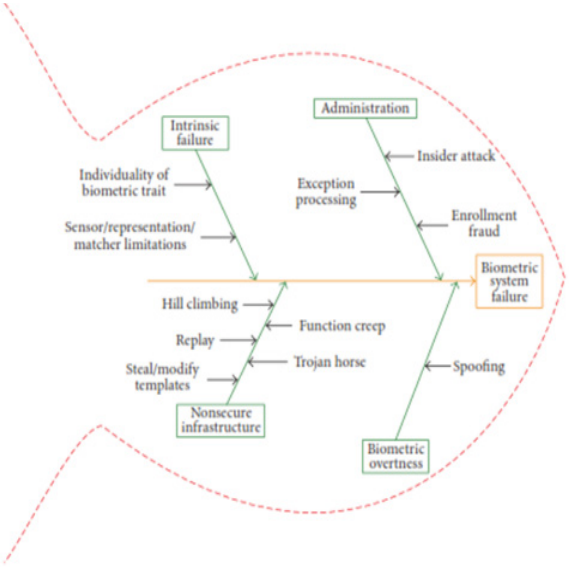


Figure 1: vulnerabilities in the form of fishbone [1]

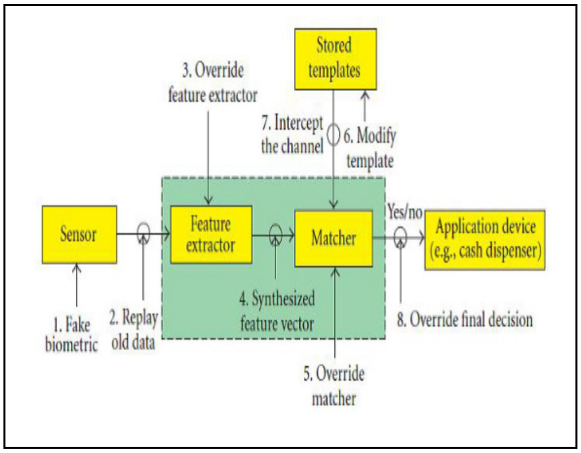


Figure 2: Attacks on Biometric System

In [6], author proposed a set of hash functions based on the position of the munities. These transformation function based on the position of the munitie, takes into account the hazardous mobility points munitie due to the sensor recording. This technique is well revocable and performs well with high complexity. The vicinity of the munities is a technique based on the dynamic random projection to secure the extracted features. It was developed by authors in [7]. The random projection matrix is dynamically assembled. The feature vector conditions the choice of projection vectors. The test results on some databases are still insufficient to prelude because this approach would be applyed to other databases. In [8], authors used a method based on the relative position between each reference munitiae. Another munitiae based template is built in a polar coordinate system whose faults reside in poor quality performance. In [9], authors developed an approach based on a characteristic vector based on a triangle. The template is formed by quantization and binarization. A descriptor based on a string of characters, allows to set up plates in the form of binary codes. This technique is called the multiline code (MLC) developed by authors in [10] and is based on the decomposition of neighborhood munities. Similarly, models referencing mapping in an infinite approach emerged with authors in [10]. They introduced the Hamming method based on graphs generating binary formats that can be revoked. Other not less powerful techniques such as reduced circular convolution [11], the partial transformation of Hadamard [12].

Despite of plethora of methods, fingerprint authentication systems have security vulnerabilities and are still vulnerable to ARMs (Multi-Object Attack) [1].

4. Touchless secured revocable template based on center of mass

Because of weaknesses of existant template we propose a spiral curve for securing contactless fingerprint template that use Zernike moment [13], Hausdorff distance modified [14, 15, 16] and the geometric moment [17]. In this section we will present our Touchless fingerprint revocable template based on center of mass. To strengthen fingerprint authentication, We plot the contactless curve using images obtained from our contactless sensors. Later we attach them to those previously stored. then we calculate the corresponding score to finally make a decision to accept or refuse.

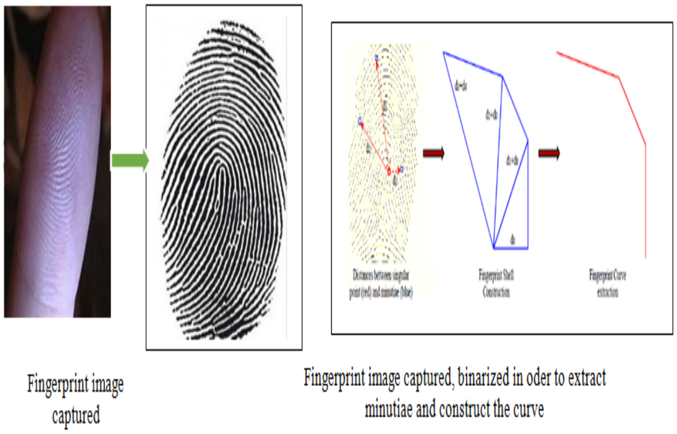

Distances between singular point (red) and minutiae (blue)
Fingerprint Shell Construction
Fingerprint Curve extraction
Fingerprint image captured
Fingerprint image captured, binarized in oder to extract minutiae and construct the curve

Figure 3: Building of the spiral curve

Our system is monomodal and is based on fingerprints. The rigid transformation [17] without modifying the extracted characteristics, protects the model stored there. Rigid transformation is a combination of translation and rotation expressed by:

$$\begin{pmatrix} u'-u_0 \\ v'-v_0 \\ 1 \end{pmatrix}=\begin{pmatrix} \cos\delta & -\sin\delta & 0 \\ \sin\delta & \cos\delta & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & b_x \\ 0 & 1 & b_y \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} u-u_0 \\ v-v_0 \\ 0 \end{pmatrix} \quad (1)$$

Where

$$\begin{pmatrix} u' \\ v' \\ 1 \end{pmatrix}=\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 \\ \beta_0 & \beta_1 & \beta_2 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} u \\ v \\ 1 \end{pmatrix} \quad (2)$$

with

$$\alpha_0 = \cos\delta \quad \alpha_1 = -\sin\delta$$

$$\alpha_2 = (1-\cos\delta)u_0 + v_0\sin\delta + b_u\cos\delta - b_v\sin\delta \quad (3)$$

$$\beta_0 = \sin\delta \quad \beta_1 = -\cos\delta$$

$$\beta_2 = (1-\cos\delta)v_0 + u_0\sin\delta + b_u\sin\delta - b_v\cos\delta \quad (4)$$

Noted that $F_0\begin{pmatrix} u_0 \\ v_0 \end{pmatrix}$ is the center of rotation, δ is the angle of rotation, $\begin{pmatrix} b_u \\ b_v \end{pmatrix}$ are the coordinate of translation vector and F' is the transformed point of F.

In oder to eliminate all the above danger, we design an new method which is implement in [3].

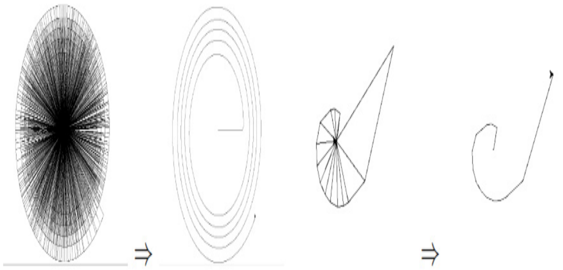


Figure 4: Different curves obtained according to the quality of the images and the number of minutiae present on these images

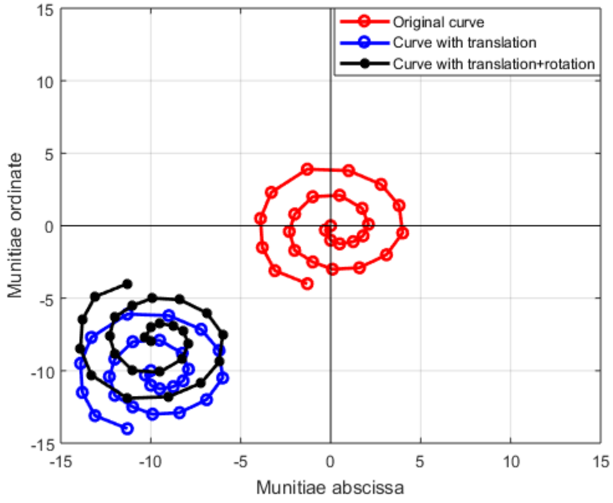


Figure 5: Construction of the secured touchless template

The requirements of revocability, diversity and security have been achieved with our new method. In reality the protection of a compromised model can go through the modification of C_0. The mismatch of the most recent curve with the old one provides diversity (see Figure 4). In reality, it is impossible to find the munities to walk a contactless curve but it is nevertheless necessary to look at the most extreme case. In this case, even if the thug gets the curve and knows how to leave the curve to recover the munities. In reality he could only recover distances that have infinite positioning. There exists only 360 positioning and 360n possible combinations with n corresponding to the number of munities. We therefore find that in the most extreme case our model remains stable and robust despite the complexity of the attacks perpetrated. Performance, Diversity and security will be further analyzed in the next subsection.

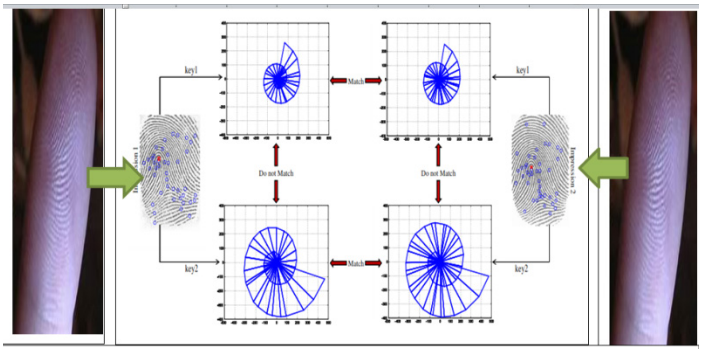


Figure 6: sample of two impressions of the same identity using two differents keys to illustrate revocability/diversity

5. Experimental results and analysis

We tested the model by using our own fingerprints database. We describe the database in Table 1. We have a fingerprint database containing 1,512 fingerprints, obtained from 378 separate fingers. We take 4 impressions from each subject. Out of 378 people, the fingerprints of the four fingerprints could be automatically captured from 1512 people. Thus only 1250 fingerprints impressions were used in experiment. In fact, due to the lack of time and people from whom we can get fingerprint images, we import some images from existant database in order to reach the number we choose. It doesn't affect the result. *We* develop our own software for the fingerprint images treatment. To appreciate how our system performs, we use false acceptance rates and false rejection rates

Due to the fact that we use two keys, we notice the amelioration of the performance of template. Our c_0.allows us to have a significant improvement of the Equal Error Rate (EER) because of the specific way of it is compute and its only one occurrence [18]. The rigid transformation applied to the curves adds a high level of randomization. Because of the fact that the key value is specific to users, the use of rigid transformation help us to have the curve unable to be rebuilt. In Figure 6, We compare FAR obtained for the proposed technique with Fingerprint Shell [17, 18] for different thresholds.

We have modified the FVC evaluation protocol to avoid the zero effort scenarios, where the adversary knows and tries to bypass the system using his own fingerprints. Impostor scores is obtain from comparison of the first curve of one single finger and the first curve of the same finger in another system that we build with reference to the identic curve. We note that they must perform 8999 attacks before succeeding one time their attacks. We compare every single print of any finger with the remaining impression of same finger. We will have at least 2799 trying before succeeding one time. In addition, we select the key randomly belonging to the interval]0, 1001[. Figure 8 describe the scenario.

Table 2: Performance comparison: existing template versus proposed template following FVC

Various Techniques	**Our collection**	**FVC2002 DB2(%)**	**FVC2002 DB1(%)**
[12]	Not tested	1.2	2.1
[15]	Not tested	3.61	7.18
[2]	Not Tested	1.01	2.03
[18]	0.001	Not tested	Not tested
Our template	0.0015	0.96	1.54

The value of FRR remains the same comparatively to fingerprint shell because of the uniqueness of the key. Let us remarks that the rightness of the curve depends on the quality of the image. More there is minutiae better is the curve, and less there is minutiae, worst is the curve (figure 9). The propose template performs well. Our model presents good results and verifies the criteria of good protection systems. Our Solution is efficient against attacks without effort or even in case of usurpation of the user key. Although, as shown in Table it presents the values EER, FMR1000 and zeroFMR obtained. Performance is only maintained in the vicinity of ERR points (4.2705% for DB1 and 1.458% for DB2). Our template are no longer accurate for thresholds that are far from ERR threshold (figure 7). In any case, we retain that (in the FMR security applications of Table 3), the systems for securing which are based on the curves are efficient only if the threshold is close to the EER point in order to limit the passage in force of the effortless attacks.

Table 3: Verification of accuracy of our template in the zero effort attack:

	FVC 2004			FVC 2005	
	EER	FMR$_{100}$		EER	FMR$_{100}$
Our touchless Secure template	4,250	26,146	Our touchless Secure template	4,250	26,146

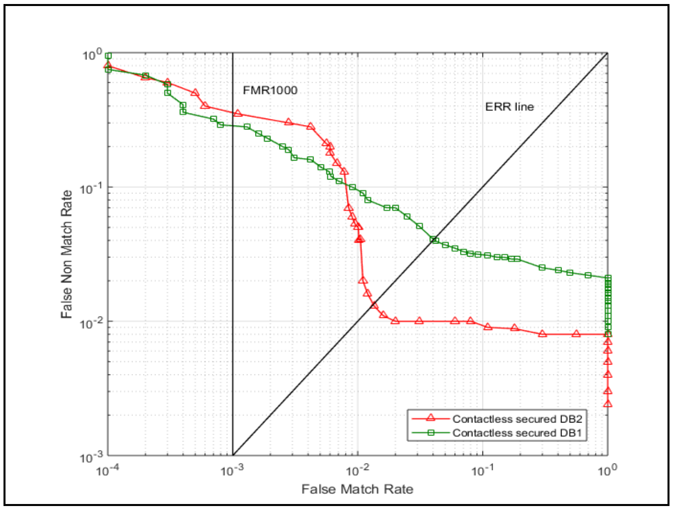


Figure 7: ROC curve in the presence of effortless attack

We remark that in high security applications based on their scheme, the systems should be operated only near the EER point to minimize the success of zero effort attacks.

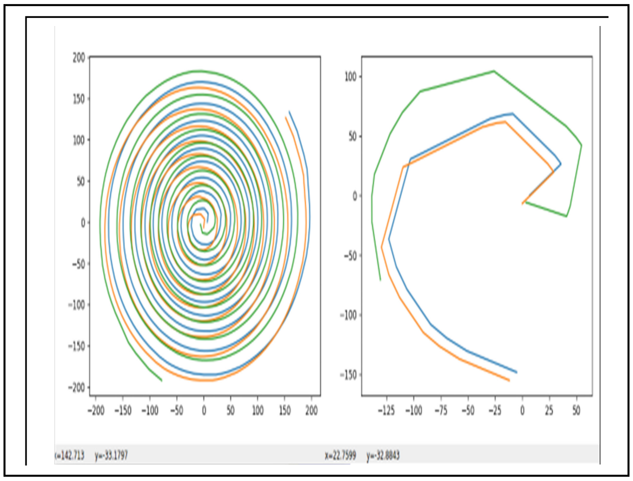


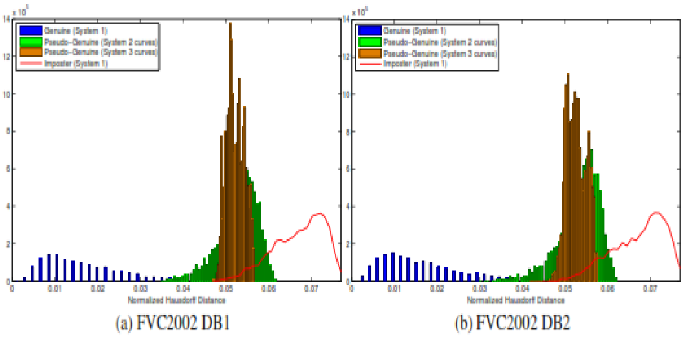
Figure 8: Sample of Template obtained from two kind of image: the first template is obtained from an image with many munitiae vs the second one is obtained from an image without enough minutiae.

Given the poor quality of some images, we observed 7 rejections for DB2 and 21 for DB1. Thus, we obtained REJDB1 = 0.75% and REJDB2 = 0.25%. With the intention of testing the opportunity to make use of C_0 particular to each user, we calculate the separability.

To justify the way in which specific keys are used, we used the kolmogorv-Smirnov test and the distribution histogram of legitimate / impostor scores. We compared two systems in which users register. In the first, the registration is done without user key, while in the second, a user key is required (the keys are drawn randomly in the interval [0; 1,5555]). We have illustrated the results in Figure 9. We can notice a form of superposition between the two distributions. This is the reason for the average value of the K-S (0.7812) and the similarity evaluation (2.4703). these results improve sufficiently (6.1636 and 0.9934 for successively the separability and the K-S test) during the evaluation of the user keys through the second device (Figure 9-b). This is proof of the improvement of discredit. In conclusion, the rate of false acceptance improves when we assigns to each user a particular key C_0. Thus, we improve the performance and accuracy of our device.

In a second step, we want to test the diversity of the curves that we generate. It will be a matter of reassuring oneself that the curve generated from one finger in one system does not coincide with another curve generated in other systems with the same finger. For this purpose, we have installed three devices that use loops. For randomly selected users in the ranges of [0,1.5555], [100,500] and [1000,2000]. The same finger is used to register in all three systems and then we look for pseudo-legitimate distribution. We conducted 6355 tests for each device, We did 6355 attempts at database DB1 and 6385 attempts for the database DB2. Figure 8 shows the results or we can clearly see that the real users and the malicious ones are well separated in the distribution of our first device. The closer they are to the distribution of the malfrats of the device 1 so the device 1 always considers the curves of the devices 2 and 3 as usurpers.

To summarize, we will say that revocability and diversity are taken into account by our device. The pseudo-distribution of the device 3 is further from the distribution of the real users of the device 1 and 2, therefore the diversity of two devices that rely on our model increases when the choice intervals of the keys are distinct.



(a) FVC2002 DB1 (b) FVC2002 DB2

Figure 9: System Histogram 1 and pseudo-legitimate distributions using systems 2 and 3

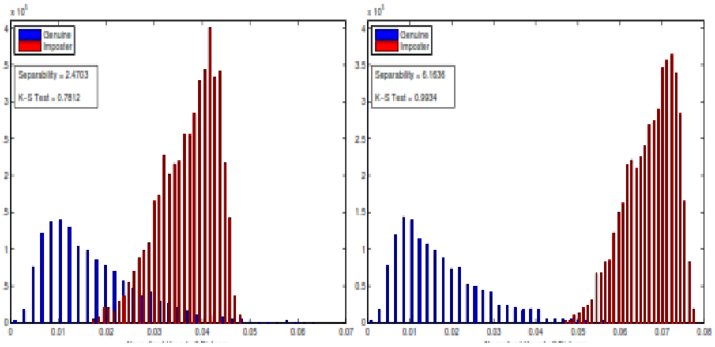


Figure 10: Histogram of Two Systems Protected by Fingerprint Shell Using FVC2002 DB1.

6. Conclusion

Our proposed contactless revocable fingerprint template has shown good robustness against the security challenges that fingerprint-based authentication systems are exposed to. It also bypasses the contagion hazards to which contact systems expose us. We evaluated it on FVC2002 DB1, DB2 and DB3 and FVC2994 DB2 and the results of the tests show that it performs very well compared to existing models in the literature review. the exisgences of revocability, diversity, security are reached with very good performances. ARM issues will be better addressed with proposals for more stable models such as exploring a combination of DFTs and dynamic projection.

Conflict of Interest

The authors declare no conflict of interest.

References

[1]. Jain, A. K., Nandakumar, K. and Nagar, A. 'Biometric Template Security', (January), pp. 1–20, 2008.

[2]. Rathgeb, C., Uhl, A., A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security 2011, 1–25, 2011

[3]. S. B. ZANNOU, T. Djara, A. Vianou, "Secured revocable contactless fingerprint template based on center of mass", 2019 3rd International conference on Bio-engineering for Smart technologies (BioSMART), 2019.

[4]. J. Breebaart, B. Yang, I. Buhan-Dulman and C. Busch. Biometric template protection. Datenschutz und Datensicherheit-DuD 33, 299–304, 2009.

[5]. S. Chikkerur, N. Ratha, J. Connell, R. Bolle, Generating registration-free cancelable fingerprint templates, in: 2nd IEEE International Conference on Biometrics: Theory, Applications and Systems, pp. 1-6, 2008.

[6]. W. Yang, J. Hu, S. Wang, J. Yang, Cancelable Fingerprint Templates with Delaunay Triangle-based Local Structures, Cyberspace Safety and Security, Lecture Notes in Computer Science. 8300 pp. 81-91, 2013.

[7]. S. Tulyakov, F. Farooq, P. Mansukhani, V. Govindaraju, Symmetric hash functions for secure fingerprint biometric systems, Pattern Recognition Letters. 28 pp. 2427-2436, 2007.

[8]. T. Ahmad, J. Hu, S. Wang, Pair-polar coordinate-based cancelable fingerprint templates, Pattern Recognition. 44 (10-11) pp. 2555-2564,2011.

[9]. P. Das, K. Karthik, B.C. Garai, A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs, Pattern Recognition. 45 (9) pp. 3373-3388, 2012.

[10]. W.J. Wong, A.B.J. Teoh, M.L.D. Wong, Y.H. Kho, Enhanced multi-line code for minutiae-based fingerprint template protection, Pattern Recognition Letters. 34 pp. 1221-1229, 2013.

[11]. C. Li, J. Hu, Attacks via record multiplicity on cancelable biometrics templates, Concurrency and Computation: Practice and Experience. 26 (8) pp. 1593-1605, 2013.

[12]. Song Wang, Wencheng Yang and Jiankun Hu, Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs Pattern Recognition 2017, http://dx.doi.org/10.1017/j.patcog.2017.01.019

[13]. Djara, ASSOGBA, NAIT ALI and Vianou, 'Fingerprint Registration Using Zernike Moments : An Approach for a Supervised Contactless Biometric System', (9), pp. 254–271, 2009.

[14]. Dubuisson, M. et al. DISTANCE Between Point Sets Research supported by a ', pp. 566–568, (1994).

[15]. Syed Sadaf Ali, Surya Prakash, 3-Dimensional Secured Fingerprint Shell, Pattern Recognition Letters, 2018, doi:10.1018/j.patrec.2018.04.017

[16]. A. A. Taha and A. Hanbury. An Efficient Algorithm for Calculating the Exact Hausdorff distance. IEEE Trans. on PAMI 37, 2153–2163, 2015.

[17]. Moujahdi, C. et al. 'Fingerprint shell: Secure representation of fingerprint template', Pattern Recognition Letters, 45(1), pp. 189–196, 2014. doi: 10.1016/j.patrec.2014.04.001.

[18]. Ali S. S. and Prakash, S. 'Enhanced fingerprint shell', 2nd International Conference on Signal Processing and Integrated Networks, SPIN 2015, pp. 801–805, 2015. doi: 10.1109/SPIN.2015.7095438.