In what way is it possible to impersonate you bypassing fingerprint sensors?

Benoit Vibert, Jean-marie Le Bars, Christophe Charrier and Christophe Rosenberger[3]

Abstract: In this study, we want to determine if an attacker with different *a priori* information on the sensor parameters during the enrollment process can impersonate an individual. We have tested different apriorism such as the fingerprint class, sensor type, image resolution and the number of minutiae. Two different matching algorithms have been used on specific designed databases generated with SFinge. Two attack scenarii have been tested. Obtained results show that the knowledge of fingerprint class and resolution influence the attack success.

Keywords: Fingerprint; Minutiae template; Attack; Logical attack

1 Introduction

Since it is not possible to revoke biometric data in case of attack, these information are very sensitive. This is why in this paper, we address the fingerprint template is often saved inside a Secure Element (SE). Due to size and computation capability limitation, this template only embeds minutiae information stored following the ISO Compact Card II representation [IS]. This representation is used for the matching between the reference and captured templates. One classical attack of on-card-comparison biometric systems consists in sending random minutiae templates (brute force) to try to impersonate an individual [UJ04, Ma06]. Digital fingerprints are generally classified following the Henry classes among Arch, Left Loop, Right Loop, Tented arch and Whorl [JPH99, ZY04]. The aim of our paper is to know how the fingerprint class or sensor type or resolution of the image and number of minutiae in the template used as reference can help any attacker to succeed? With regards to security, a biometric On-Card-Comparison (OCC) have many vulnerabilities. Ratha et *al.* [RCB01] have classified attacks of a generic biometric system into 8 ways: 1) falsified biometric data, 2) interception of biometric data during its transmission, 3) attack on the extraction module parameters, 4) altered extracted parameters, 5) matching module replaced by a malicious software, 6) man in the middle attack between the database and the matching module, 7) alteration of the database and 8) alteration of the verification decision.

[3] Normandie Univ, ENSICAEN, UNICAEN, CNRS, GREYC 14000 Caen, France, {benoit.vibert, christophe.rosenberger}@ensicaen.fr, jean-marie.lebars, christophe.charrier}@unicaen.fr

For each above mentioned point, there are different types of attacks. Figure 1 shows the locations of attacks considering a generic biometric system. Uludag and Jain [UJ04], Martinez [Ma06] and Soutar [So02] consider point 2 and 4 by performing a hill-climbing attack. This latter may be performed by an application that sends random templates (which are perturbed iteratively) to the system. The application reads the output match score and continues with the perturbed template only when the matching score increases until the decision threshold is accepted without considering the type of the associated fingerprint in any way. To our knowledge, no study on fingerprint attacker apriorism have been investigated to impersonate a person. In this study we consider attacks on points 1 and 2 (cf. Figure 1). To perform such an attack, we need to replace the sensor module by our own mechanism to control all the parameters of the sensor: fingerprint class, sensor type, resolution of the image and the number of minutiae extracted. Our hypothesis is that an attacker has a logical access on the system and sends his own information to the Secure Element. To evaluate the impact of these apriorism on the efficiency of an attack, we use the EVABIO platform to characterize its impact on the matching decision. In the literature, only few platforms exist for assessing the performance and security of biometric systems. We can cite the NIST platform [Gr11], FVC-Ongoing platform [Ma13a] and the BEAT (Biometric Evaluation And Testing) [Ma13b] European project. The main drawbacks of these platforms are the loss of modularity and the difficulty to evaluate any algorithm embedded on Secure Elements [Vi15b].

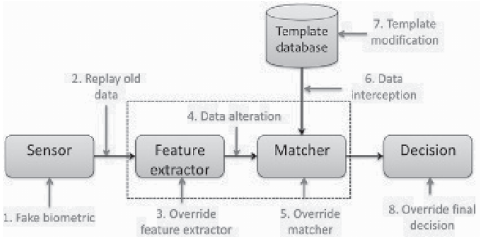


Figure 1: Vulnerabilities locations of a biometric system (defined from [RCB01])

2 EVABIO Platform - Security Analysis Module

EVABIO platform (see Figure 2) improve the one developped in [VRN13, Vi15a] providing a new functional Attack module. It offers to developers or researchers different methods to attack when comparing two fingerprints. In addition, the platform allows to test the attacks on real OCC or on computers. We take advantage in this paper of the modularity of EVABIO platform to only modify the Security Analysis module to quantify the benefit has an attacker to know the fingerprint class to impersonate an individual. The platform uses active mechanisms of communication by event allowing multiple modules simultaneously access data exchanged between the client application and the OCC, thus offering analysis of results ”on the fly”. All the modules are detailed in [Vi15b]. In this study, the `Security analysis` module will be updated since it contains methods which permit to test the knowledge the attacker has on the sensor type or the resolution of the image extracted by the sensor, or the minutiae template class, or the number of minutiae

extracted from the image. Considering all those informations, we may assume that this kind of knowledge is of importance for any attacker to impersonate people. This module also contains a method to generate a random biometric template respecting the ISO format using SFinge software [CMM04], that can be usefull for brute force attack. With this method it is possible to generate as much as needed random fingerprint templates to hack the biometric matcher algorithm.

Figure 2: General scheme of EvaBio platform (defined from [Vi15a])

3 Proposed approach

We assume that an attacker may only replace the sensor module by its own Fake sensor block: 1) by changing the resolution of the output sensor images that impacts the minutiae extraction part, or by fixing the fingerprint template class or having information on the sensor type used during the enrollment process; 2) when the attack is performed just after the minutiae extraction process, the attacker can know the number of extracted minutiae saved as reference in the matching module. All extracted minutiae are stored into a template described with 4 data $(x_i, y_i, T_i, \theta_i), i = 1 : N_j$, where the coordinates (x_i, y_i) correspond to the location of the *i-th* minutiae in the image, T_i corresponds to the *i-th* minutiae type (bifurcation, ridge ending), θ_i is the *i-th* minutiae orientation in degree (related to the ridge) and N_j the number of minutiae for the sample j of the user. We want to quantify how the knowledge of an attacker has on the sensor parameters increases a successful attack probability. This probability is based on the False Acceptance Rate (FAR) that can be interpreted as the probability of a successful attack. Let b_z the reference template of user z and D a matching algorithm between biometric templates, the success of an attack by an impostor is given by equation 1 where FAR_A is the probability of a successful attack for a decision threshold fixed to ε. The A_z biometric query is built by the impostor by taking into account all information he/she knows on user z or on the biometric system. Our purpose is to estimate the benefit an attacker has to compute A_z knowing the fingerprint class C_z, or the sensor type S_z, or the minutiae number MN_z or the resolution of the image R_z of user z.

$$FAR_A(\varepsilon) = P[D(b_z, A_z) \leq \varepsilon)] \tag{1}$$

4 Experimental setup

4.1 Databases

We use the SFinge software [CMM04] to generate different databases since we do not have access to databases providing acquisition from different types of sensor, different resolution of images and different numbers of minutiae. For each one of the four apriorisms, two kinds of database are designed :
Reference database: this database simulates the reference templates for some users. We generated 1 sample per user for 500 individuals. This database contains 500 fingerprints ;
Attack database: we generated a database with 1000 different fingerprint templates (1 sample per user). This database serves as attack database.

Using SFinge, we can choose the sensor type among two types (Capacitive and Optical). This induces the construction of four databases (1 reference DB and 1 attack DB per choice). Considering the resolution level, we selected 3 values (250dpi, 500dpi, 1000dpi) inducing 6 databases. Considering the number of minutiae, we selected 2 classes (number of minutiae < 38 or > 38) inducing 4 databases. Finally, when considering the fingerprint class (Arch, Left loop, Right loop, Tented and Whorl), 10 databases are generated (two per class). In order to estimate the decision threshold ε, used in equation 1, to compute the Error Equals Rate (EER) value, we generated a dedicated database using SFinge with default settings. The only parameters we fixed are the number of users (100) and the number of template per user (8). Finally, a total of 800 fingerprints is obtained. This is an arbitrary choice, this functioning point is always reachable for any matcher.

4.2 Matching algorithms

Bozorth3 [Wa07]: This matcher uses only the locations and orientations of the minutia points to match the fingerprints. The EER value of this matcher has been computed using the FVC2002DB3 database [Ma02] to ensure the reproducibility of results. The obtain value is equal to 1.03% for a decision threshold value $\varepsilon = 26.8$;
Minutia Cylinder-Code (MCC) algorithm [CFM10]: Thanks to the cylinder invariance, fixed-length, and bit-oriented coding, some simple but very effective metrics can be defined to compute local similarities and to consolidate them into a global score. The EER value of this matcher has been computed using the FVC2002DB3 database. The obtain value is equal to 0% for a decision threshold value $\varepsilon = 0.0315$.

4.3 Protocol

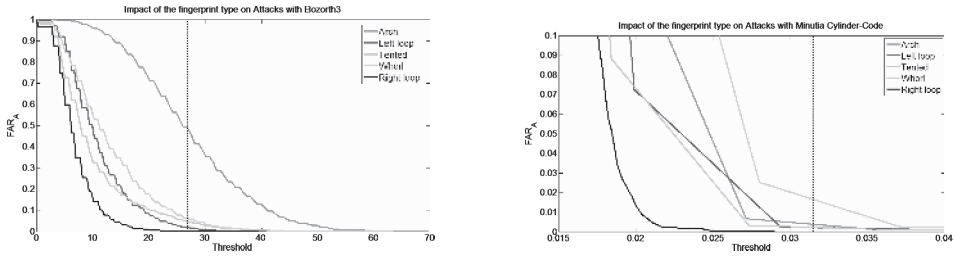
For any attack, an impostor provides a query in order to be authenticated as the legitimate user. Two scenarii are defined to simulate an attack:
Scenario 1: We simulate the brute force attack. 500 templates are randomly selected from the database constructed to estimate the ε value and will define the reference database. The

attack database is generated constructing 1000 random biometric templates respecting the ISO format.
Scenario 2: For a given apriorism, each reference database is compared to all test databases.

5 Results

5.1 Attacker knowing the fingerprint class

From the fingerprint class knowledge, we compute the value FAR_A for the two scenarii when we set the decision threshold value with respect to the used matching algorithm as described in section 4.2. Using Bozorth3, the probability of successful attack equals 3% with Brute force and 4.7% knowing the fingerprint class. When the MCC matcher is considered, the probability of successful attack equals 1.7% with Brute force and 2.6% knowing the fingerprint class. We can deduce that the knowledge of the genuine fingerprint class helps an attacker to impersonate him. Yet we need to investigate how this knowledge impacts the efficiency of the attack. In order to analyze its impact we apply the following approach: we consider only scores between reference and attack templates of the same fingerprint class to compute the FAR value for each fingerprint class. In this case, we have 5 sets of $4 \times 800 = 3200$ matching scores yielding us to compute the FAR_A value. Results are shown in Figure 3. Considering Bozorth3 matching algorithm (Figure 3.a), we can deduce that the Arch class presents the highest success attack rate whereas the Right loop class presents the lowest rate. Considering MCC matching algorithm (Figure 3.b), we observe that the Whorl loop presents the highest successful attack rate and the lowest successful rate concerns the Right loop. We can formulate a first remark: fingerprints belonging to the Right loop class are the hardest to impersonate. Table 1 gives the value of the probability of successful attack FAR_A for each fingerprint class for the two matchers. We can clearly see that some fingerprints related to their class are more easy to attack depending of the used matcher. As example, with Bozorth3, arch fingerprints can be impersonated in 50% cases.



(a) Bozorth3 (b) Minutia Cylinder-Code (MCC)

Figure 3: Evolution of the efficiency of attacks considering all the trial fingerprint classes for both biometric systems

Matcher	Arch	Right loop	Left loop	Tented arch	Whorl
Bozorth3	50 %	0 %	2 %	5 %	6.3 %
Minutia CC	0.6 %	0 %	0.2 %	0.2 %	2 %

Table 1: Value of the probability of successful attack FAR_A for each fingerprint class for the two matchers.

5.2 Attacker knowing the sensor type or the number of minutiae in the reference template

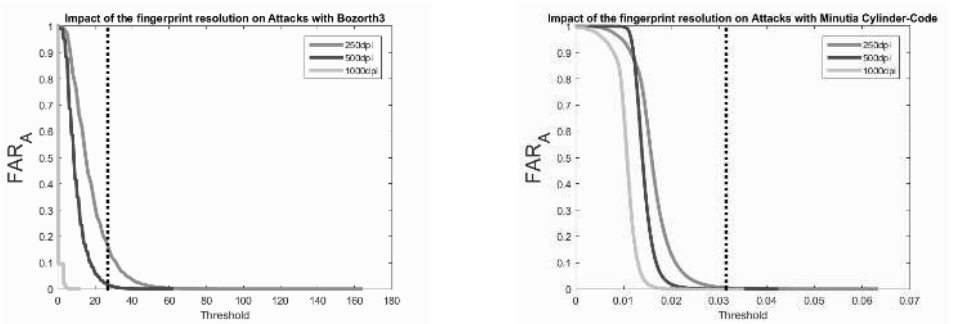
Considering the sensor type or the number of minutiae in the reference template knowledge, we compute the value FAR_A for the two scenarii when we set the decision threshold value with respect to the used matching algorithm as described in section 4.2. The benefit for an attacker when he/she knows the sensor type or the number of minutiae in the reference template is not very important. Table 2 give the value of the probability of successful attack FAR_A for each sensor type and each number of minutiae class for the two matchers. We can see clearly that this kinds of knowledge for the attacker is not relevant.

Matcher	Capacitif	Optic	< 38	> 38
Bozorth3	0.0158 %	0.016 %	0.0038 %	0.0391 %
Minutia CC	0.13×10^{-3} %	0.23×10^{-3} %	0.8×10^{-4} %	2.5×10^{-4} %

Table 2: Value of the probability of successful attack FAR_A for each sensor type and each number of minutiae class for the two matchers.

5.3 Attacker knowing the resolution of the original image

Concerning the original image resolution knowledge, we compute the value FAR_A for the two scenarii when we fix the decision threshold to obtain the EER value. We can see in both case the little benefit for an attacker to know the resolution of the original image extracted by the sensor. For Bozorth3, the probability of successful attack equals 0.019% with Brute force and 0.035% knowing the resolution of the original image. For the MCC matcher, the probability of successful attack equals 0.51×10^{-3}% with Brute force and 0.8×10^{-3}% knowing the resolution of the original image. In order to analyze if the resolution of the original image has an impact on the efficiency of this attack, we apply the following scheme: we consider only scores between reference and attack templates of the same images resolution. In this case, we have 3 sets of $4 \times 800 = 3200$ matching scores. We can compute the value FAR_A for each image resolution class (see Figure 4). For Bozorth3 matching algorithm, we can see that it is quite impossible to succeed for high resolution image (1000dpi), whereas it is easier for low resolution image (250dpi). The same remark can be formulated for MCC algorithm. Table 3 gives the value of the probability of successful attack FAR_A for each resolution of image for the two matchers. We can see clearly that low resolution help an attacker with more 3 times successful attack than medium resolution.



(a) Bozorth3 (b) Minutia Cylinder-Code (MCC)

Figure 4: Evolution of the efficiency of attacks considering all the trial sensor resolutions for both biometric systems

Matcher	250dpi	500dpi	1000dpi
Bozorth3	0.165 %	0.047 %	0 %
Minutia CC	0.45×10^{-3} %	0.176×10^{-3} %	0 %

Table 3: Value of the probability of successful attack FAR_A for each resolution of the original images for the two matchers.

6 Conclusion

We showed which knowledge helps an attacker to impersonate an individual or to bring some information to reach a successful attack such as the fingerprint class and the resolution. Our experiments show that if we know the fingerprint class for enrolled people in the system, we increase the chance to impersonate him by 50%. However the number of minutiae or the type of sensor (capacitive or optical) is not very usefull for an attacker. In future works, we will investigate how much the combination of different knowledges may improve the efficiency of the successful attack probability.

References

[CFM10] Cappelli, Raffaele; Ferrara, Matteo; Maltoni, Davide: Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(12):2128–2141, 2010.

[CMM04] Cappelli, Raffaele; Maio, D; Maltoni, D: SFinGe: an approach to synthetic fingerprint generation. In: International Workshop on Biometric Technologies (BT2004). pp. 147–154, 2004.

[Gr11] Grother, P; Salamon, W; Watson, C; Indovina, M; Flanagan, P: MINEX II "Performance of Fingerprint Match-On-Card Algorithms" Phase IV : report NIST Interagency Report 7477 (Revision II). 2011.

[IS] ISO: . ISO/IEC 19794-2. Information technology - biometric data interchange format format - part 2 : Finger minutiae data, 2011. ISO.

[JPH99] Jain, Anil K; Prabhakar, Salil; Hong, Lin: A multichannel approach to fingerprint classification. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 21(4):348–359, 1999.

[Ma02] Maio, Dario; Maltoni, Davide; Cappelli, Raffaele; Wayman, James L; Jain, Anil K: FVC2002: Second fingerprint verification competition. In: Pattern Recognition, 2002. Proceedings. 16th International Conference on. volume 3. IEEE, pp. 811–814, 2002.

[Ma06] Martinez-Diaz, Marcos; Fierrez-Aguilar, J; Alonso-Fernandez, Fernando; Ortega-García, Javier; Siguenza, JA: Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification. In: Proceedings 2006 40th Annual IEEE International Carnahan Conferences Security Technology. IEEE, pp. 151–159, 2006.

[Ma13a] Maio, D; Maltoni, D; Capelli, R; Franco, A; Ferrara, M; Turroni, F: FVC-onGoing: online evaluation of fingerprint recognition algorithms. URL https://biolab. csr. unibo. it/fvcongoing/UI/Form/Home. aspx, 2013.

[Ma13b] Marcel, Sébastien: BEAT–biometrics evaluation and testing. Biometric technology today, 2013(1):5–7, 2013.

[RCB01] Ratha, Nalini K.; Connell, Jonathan H.; Bolle, Ruud M.: Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3):614–634, 2001.

[So02] Soutar, Colin et al.: Biometric system security. White Paper, Bioscrypt, http://www. bioscrypt. com, 2002.

[UJ04] Uludag, Umut; Jain, Anil K: Attacks on biometric systems: a case study in fingerprints. In: Electronic Imaging 2004. International Society for Optics and Photonics, pp. 622–633, 2004.

[Vi15a] Vibert, B; Yao, Z; Vernois, Sylvain; Le Bars, Jm; Charrier, Christophe; Rosenberger, Christophe: EvaBio Platform for the evaluation biometric system: Application to the optimization of the enrollment process for fingerprint device. In: International Conference on Information Systems Security and Privacy. 2015.

[Vi15b] Vibert, Benoit; Yao, Zhigang; Vernois, Sylvain; Le Bars, Jean-Marie; Charrier, Christophe; Rosenberger, Christophe: EvaBio a New Modular Platform to Evaluate Biometric System. In: Information Systems Security and Privacy, pp. 234–250. Springer, 2015.

[VRN13] Vibert, Benoit; Rosenberger, Christophe; Ninassi, Alexandre: Security and performance evaluation platform of biometric match on card. In: Computer and Information Technology (WCCIT), 2013 World Congress on. IEEE, pp. 1–6, 2013.

[Wa07] Watson, C. I.; Garris, M. D.; Tabassi, E.; Wilson, C. L.; Mccabe, R. M.; Janet, S.; Ko, K.: Users guide to nist biometric image software (nbis). Technical report, NIST, 2007.

[ZY04] Zhang, Qinzhi; Yan, Hong: Fingerprint classification based on extraction and analysis of singularities and pseudo ridges. Pattern Recognition, 37(11):2233–2243, 2004.