Capture Biases in Fingerprint Systems

Abdarahmane Wone, Joël Di Manno, Christophe Rosenberger, Christophe Charrier

Capture Biases in Fingerprint Systems

Abdarahmane WONE*†, Joël DI MANNO*, Christophe ROSENBERGER† and Christophe CHARRIER†
*FIME EMEA, 14000 Caen, France
abdarahmane.wone@unicaen.fr, joel.dimanno@fime.com
†Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
christophe.rosenberger@ensicaen.fr, christophe.charrier@unicaen.fr

***Abstract*—Fingerprint recognition is a common solution for user authentication in Cybersecurity. This paper deals with the context of the certification of fingerprint biometric systems. The increasing use of biometric systems makes their certification a mandatory step in their development to assess their behavior in a real situation use. It has been shown that certain parameters such as environmental conditions can have a significant impact on the performance of biometric systems. However, there are also non-controlled parameters that depend on the user's state such as the quality of his biometric samples. In this paper, we propose a study that explores the performance of fingerprint systems across these parameters.**

***Index Terms*—Certification, Biometrics, fingerprints, biases.**

I. Introduction

Biometrics is more and more employed for user authentication to secure the access to digital services or computers/smartphones. The fingerprint modality is a very popular one as we can estimate that 80% of smartphones embed a fingerprint sensor. This biometric solution is very easy to use and is largely used (70% of biometric systems in the US use digital fingerprints). As this kind of system is designed to avoid attacks, it should meet security and privacy constraints. The certification of systems is a process whose objective is to verify how these constraints are fulfilled.
The certification of a biometric system is an important step during the development and use of a biometric system. During this test, a biometric system is subject to many tests in order to establish its conformance to a certain test plan (performance, robustness to attacks, time). Indeed, these tests are done by independent laboratories, the testing scenarios are defined by the testing authority. The testing of biometric systems is mainly based on ISO 19795-2 standard [1].

In [2], it has been demonstrated that environmental conditions (e.g temperature and humidity) can impact significantly the performance of a fingerprint system. This work showed that enrolment and matching in the same conditions improve performance and can reduce the vulnerabilities of a fingerprint system to attacks. The test scenarios that are used by certification schemes and laboratories to test biometric systems provide the tests to be conducted under monitored but not controlled conditions. The used dataset is mainly heterogeneous, which does not allow the isolation of particular situations as these cases are smoothed by the rest of the test population.

In this work, we propose to study the impact of non-controlled parameters on the performance of a fingerprint system. The studied parameters concern capture biases, i.e. the intrinsic quality of the fingerprint sample (related to the capture or to the quality of the person's fingerprint) and related to the sensing technology (capacitive or optical solution). The main contribution of the proposed paper is to establish the existence of biases during the capture of fingerprint samples. For example, depending on the type of sensor, do we obtain similar performance for the same user?

The paper is organized as follows: Section II briefly describes the motivations of this work and the related works. In section III, we present the proposed method to evaluate capture biases in fingerprint systems. Experimental results are provided in section IV. In section V, we discuss the results of the study and give a conclusion in section VI.

II. Related works

The operational testing of a fingerprint system is realized by using a dataset collected for the purpose of the test or an existing one. The second case makes sense only if the testing dataset is well known with good confidence it has not been used during the training of the recognition algorithm. However, due to the fact that most of the tested biometric systems are tested as black boxes, it is not easy to say how it is fair and unbiased to use a public existing dataset. For this reason, most of the testing methodologies use a dataset collected for a single product. Thus, taking into account certain parameters would be an excellent way of averaging if not minimizing bias for biometric systems. We list all capture parameters influencing the performance of fingerprint systems:

- **Demography**: It has been demonstrated that demography is a key factor of bias not only for face recognition but also for other biometrics. From a study conducted on Malaysian groups, authors in [3] conclude that fingerprint patterns could be inherited genetically. They also found that some ethnicities are more likely to have a certain pattern. The same goes for gender and occupation. In [4], authors conducted a study on groups of Caucasian males, Caucasian women, Black males, and Black women using two fingerprint matching algorithms and quality measurement. Their study allows them to conclude that most observed demographic differentials

can be explained by the poor quality of some fingerprint images and the high accuracy of the used matching algorithm make them less sensitive to demographic bias. Age is also an important factor especially for children and old people as they are more subject to skin transformation [5]. Therefore, they are big contributors to the False Non-Match rate and the Failure-to-Acquire rate in performance assessment studies.

- **User**: User's anatomy has always been known as a source of perturbation in a recognition task for a biometric system. Indeed, beards, mustaches [6], and baldness can lead to bad recognition scores particularly if the state of that factor was different during the enrolment. This is known as template aging and is applicable to fingerprints. Harvey et *al.* [7] studied this phenomenon over seven years with the same group of people. They propose a methodology that can be used to isolate the effect of biometric template aging. Lanitis [8] gives a complete survey of the effects of aging on biometric identity verification with different biometric modalities. Other things such as the subject's motivation, familiarity, behavior [9], and appearance (fingernails can impact the positioning), fingerprint condition [5] (depth and spacing ridges, dry, cracked or damp), ... are known to a source of quality variation during the capture of fingerprint data.

- **Environment**: The environmental conditions are known to have impacts on the recognition process. In [2], authors conducted a study with different acquisition conditions and show that quality and recognition performance across two matching algorithms are impacted by the acquisition conditions. Solutions based on biometric template updating [10] have been proposed to solve this issue. Other studies can be found in the state-of-the-art [11, 12, 13]. Authors in [14] studied this on a fingerprint anti-spoofing system.

- **Capture system**: The capture system is the object of this study. The sensor quality is the main source of image quality variations. As pointed out by Marasco [15], the quality variation between different sensors is a big challenge for the operability of biometric systems. There are works that proposed solutions to overcome this issue [16] [17].

We propose in this paper to focus on this last aspect and estimate any biases related to the capture (sensor or captured sample).

III. Experimental protocol

We present in this section the experimental protocol.

A. Dataset

For this work, we use a fingerprint dataset generated using Synthetic Fingerprint Generator SFinGe [18]. SFinGe [18] (Synthetic Fingerprint Generator) is one the first and most well-known fingerprint generator models. It has been proposed by researchers from the University of Bologna[1] in 2004 and is based on the mathematical modeling of fingerprint characteristics. The fingerprints generation using SFinGe can be summarized as follows:

- Directional map generation,
- Density map generation,
- Ridge pattern generation,
- Noising and Rendering.

The main shape of the fingerprint is elliptical segments. SFinGe applies a mathematical ridge-flow model from Sherlock and Monro [19] to the positions of the singularities to generate a directional map. Filters similar to the Gabor filters are applied to a white image with random points. The orientation and frequency filters are locally adjusted according to the directional and density maps which makes appear realistic minutiae. Other effects such as dilatation, erosion, and noise are added to make the generated fingerprint look more realistic. Figure 1 gives a visual representation of these steps.

Using SFinGe 4.1, we generated a dataset imitating capacitive and optical sensors. For each sensing technology, we use the integrated quality indicator to control the quality of the generated data. These different quality sets are simulating the quality of the fingerprint sample. Thus, we generated five different groups of images with different qualities:

- **High quality**: Fingerprints with almost no translation and rotation, most ridge patterns of very high quality, with almost no skin distortion or other perturbations.
- **Medium quality**: Fingerprints with almost no translation and rotation, ridge patterns of medium/high quality, with limited skin distortion and perturbations.
- **Low quality**: Fingerprints with almost no translation and rotation, ridge patterns of low quality, with limited skin distortion and perturbations.
- **Very low quality**: Fingerprints with almost no translation and rotation, ridge patterns of very low quality, with various perturbations.
- **Varying quality**: Fingerprints with varying quality and perturbations: most ridge patterns of medium quality, but some of low or very low quality.

In the proposed methodology, we generated 200 unique fingers for each set with 5 impressions per finger. The images have a resolution of 1000 dpi and a size 832x1120 pixels. Examples of the generated data are shown in Fig. 2.

B. Evaluation methodology

To validate the impact of acquisition conditions on biometric systems, different metrics, and methods are used. We consider two types: 1) fingerprint quality assessment, and 2) performance.

[1] http://biolab.csr.unibo.it/sfinge.html

(a) Singularities (b) Directional map (c) Ridge pattern (d) Denoising (e) Final

Fig. 1: Different steps of SFinGe generation: in (a) and (b) a Directional map is generated, a ridge pattern is created in (c) and Denoised in (d) to give the final image in (e).

(a) Capacitive image of high quality (b) Capacitive image of medium quality (c) Capacitive image of low quality (d) Capacitive image of very low quality

(e) Optical image of high quality (f) Optical image of medium quality (g) Optical image of low quality (h) Optical image of very low quality

Fig. 2: Examples of images from the data generated with SFinGe: First-row images are from a capacitive sensor and second-row images are from an optical one.

1) Quality assessment: The quality of a fingerprint is an indicator of the capability of recognition associated with a particular user. In recent years, efforts have been made to harmonize the quality measurement of fingerprints [20]. The NFIQ2.0 is widely adopted as metric of quality. However, other alternatives have been proposed in the literature [21], [22], [23]. The metric we use in this work is the NFIQ2.0 (NIST Fingerprint Image Quality) tool [24]. NFIQ gives

an overall score based on the usability and features of a fingerprint image. Scores go from 0 to 100 (0 bad and 100 good). It is used here to see an overview of the usability of the fingerprint image.

2) Fingerprint matching: We use two fingerprint matching algorithms from minutiae templates: NIST Bozorth3 [25] and the MCC matching algorithm [26].

3) Performance evaluation: The performance evaluation of biometric systems is generally measured using two metrics: the AUC (Area Under the Curve) and the EER (Equal Error Rate). AUC (Area Under the roc Curve) value can be viewed as a ranking measure that is very useful and is based on pairwise comparisons between classifications of two classes. In other words, the AUC value is equal to the probability that a classifier will rank a randomly chosen positive instance higher than a randomly chosen negative one: Given two randomly chosen users, one being a legitimate user and the other an impostor, the AUC represents the probability $P(S^{leg} > S^{imp})$ (i.e. probability of a good assignment):

$$AUC = \frac{\sum_{p=1}^{n_g} \sum_{q=1}^{n_i} I(S_p^{leg}, S_q^{imp})}{n_g n_i} \quad (1)$$

where n_g and n_i are respectively number of legitimate users and impostors.

$$I(S_p^{leg}, S_q^{imp}) = \begin{cases} 1 \textit{ if } S_p^{leg} > S_q^{imp} \\ 0 \textit{ otherwise} \end{cases} \quad (2)$$

That way, AUC can be considered as a global criterion of performance. The higher the AUC is, the better the performance.

The EER value is when the False Acceptance Rate (FAR) is equal to the False Rejection Rate (FRR). It can be seen as a compromise between usability and security. The goal of a matcher is to minimize this value. Both AUC and EER are computed after a bootstrap of 1000 draws and are given within a confidence interval with 95% of confidence.

IV. Experimental results

In order to identify any bias in the fingerprint capture, we consider the quality of samples and the associated performance.

A. Quality analysis

We observe the quality variation over the generation parameters. We compute the average value and standard deviation of the NFIQ2.0 scores. Tables I and II show the statistical indicators (mean and standard deviation) of the dataset. Fig. 3 and Fig. 4 show the data profiles of the NFIQ2.0 scores for each set of quality. They also give the range of data points between the 10th and 90th percentile (shaded area), as well as the average value and the standard deviation.

Considering NFIQ2 values, we can understand that the intrinsic quality of the generator may differ from a pure fingerprint quality metric. Indeed, one may expect High-quality generation samples to have higher statistics than other generation settings. This may be due to the fact that if we consider for example the set with "varying quality", it may cover a wider range of quality scores and contain higher scores than the "high-quality" setting which has high-quality samples but is confined to a narrow range.

	Capacitive with no option (%)	Scratches (%)
High Quality	40.97 ±4.1	40.92 ±4.0
Medium Quality	43.50 ±3.6	43.47 ±3.7
Low Quality	40.52 ±5.0	40.94±4.8
Very Low Quality	34.36 ±6.1	35.23±6.0
Varying Quality	42.3 ±4.2	42.37 ±4.5

TABLE I: NFIQ2.0 statistical figures of the capacitive dataset

	Optical with no option (%)	Scratches (%)
High Quality	42.49 ±3.5	42.47 ±3.5
Medium Quality	43.84 ±3.8	43.87 ±3.8
Low Quality	40.11 ±3.6	40.65±4.1
Very Low Quality	32.03 ±6.5	33.24±6.7
Varying Quality	42.77 ±4.1	42.73 ±3.9

TABLE II: NFIQ2.0 statistical figures of the Optical dataset

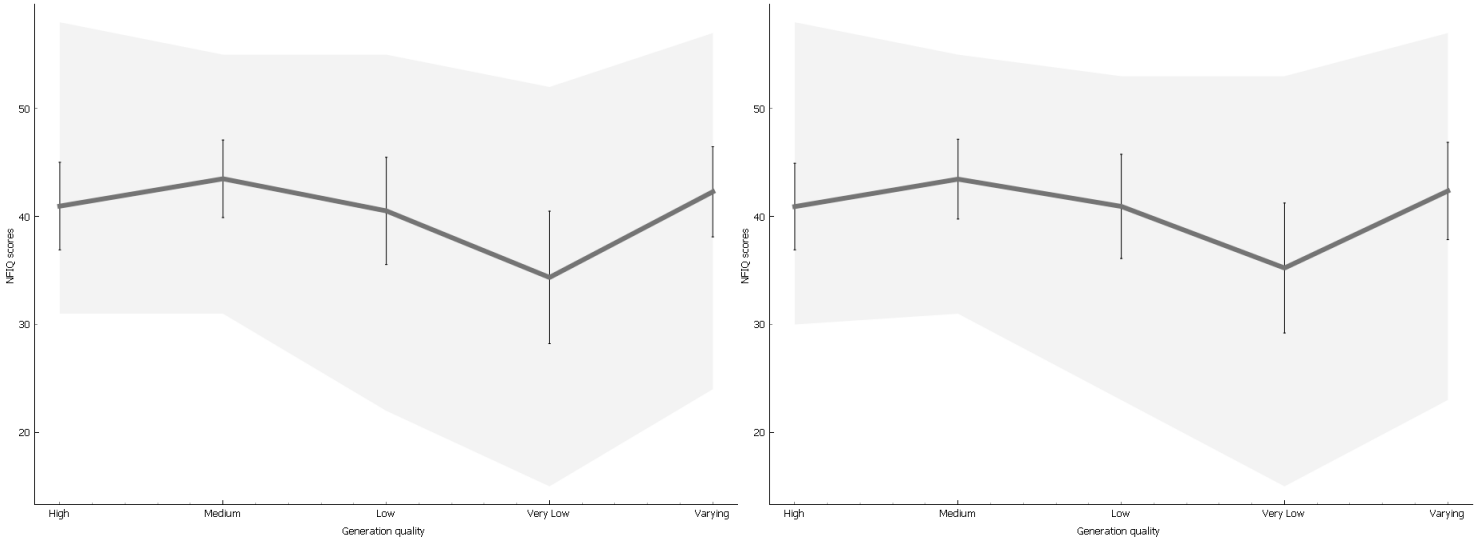
B. Performance

In this part, we evaluate the performance of the generated dataset considering the metrics (AUC and EER) detailed in the previous section using two matching algorithms. Images from SFinGe have been generated with fingerprint templates respecting ISO/IEC 19794:2 format which can be directly used with MCC for comparison tasks. We also extract minutiae from fingerprint samples with NIST *mindct* [25] for Bozorth3. For each matching algorithm, we compare the AUC and the EER values.

Tables III and IV show the AUC and EER computed with the NIST Bozorth3 matcher for the capacitive sensor and optical sensor. We can observe that the scratches do not introduce a high decrease in the AUC or EER values. The actual difference in performance comes mainly from the acquisition quality. Despite the scratches, the inherent generation quality is the only factor that seems to be very important here when we consider a single capture technology and the same matching algorithm. The same observation applies to the MCC matcher for which the performance is shown in TablesV and VI.

V. Discussion

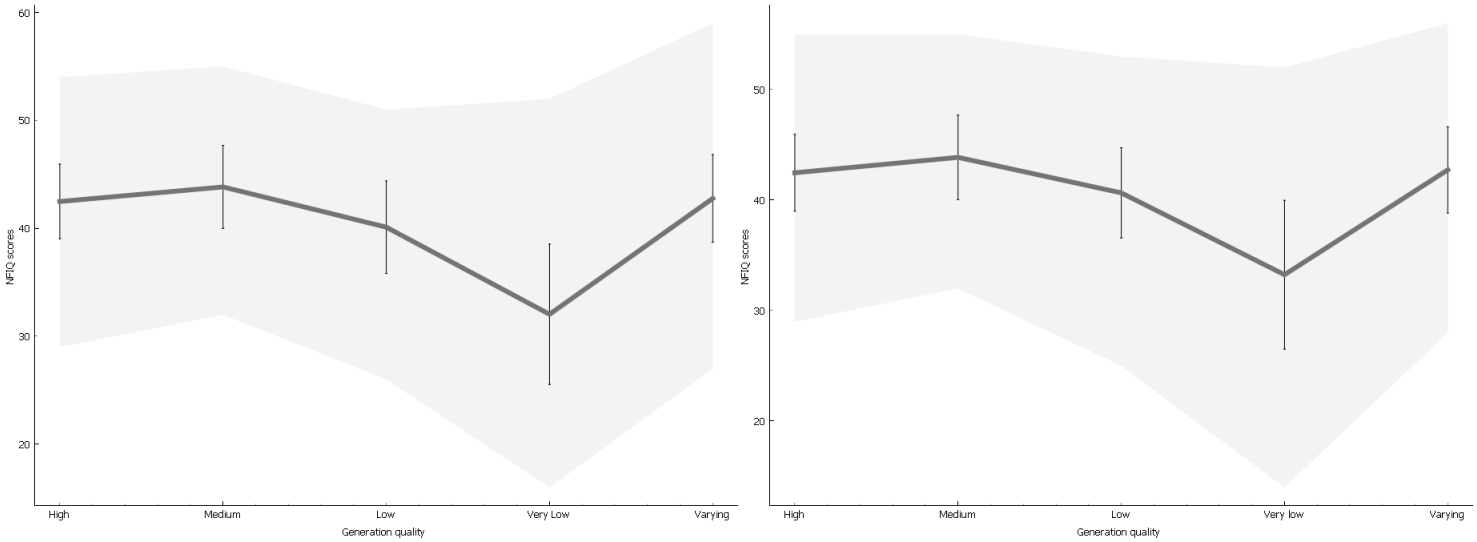
This study focuses on the bias introduced by the acquisition system. Different sets of fingerprint images have been created, from very low-quality images to high-quality images with a set of varying-quality images, with two capturing technologies and the presence or no of scratches. The quality scores reveal no significant variation introduced by the scratches within the same capturing quality group. The "varying" quality generation parameter serves here as a reference as it is the most likely capturing quality one can find in the market and



(a) No option (b) Scratches

Fig. 3: Visualization of data profiles of the NFIQ2.0 quality scores from the capacitive images

.



(a) No option (b) Scratches

Fig. 4: Visualization of data profiles of the NFIQ2.0 quality scores from the optical images

.

	Capacitive with no options		Capacitive with Scratches	
Generation quality	AUC (No option)	EER (No option)	AUC (Scratches)	EER (Scratches)
High	81.1314 $\pm 1.4981e-14$	0.27258 $\pm 4.1308e-17$	80.5505 $\pm 2.3793e-14$	0.27908 $\pm 4.8193e-17$
Medium	89.0779 $\pm 3.525e-15$	0.1805 $\pm 6.1962e-17$	89.0546 $\pm 5.2874e-15$	0.17883 $\pm 1.2048e-17$
Low	79.907 $\pm 1.8506e-14$	0.30119 $\pm 1.0327e-17$	79.9247 $\pm 6.1687e-15$	0.27194 $\pm 4.1308e-17$
VeryLow	67.1891 $\pm 7.0499e-15$	0.3942 ± 0	67.4475 $\pm 3.525e-15$	0.38437 $\pm 6.1962e-17$
Varying	86.5812 $\pm 1.3219e-14$	0.21417 $\pm 2.2375e-17$	86.1737 $\pm 2.6437e-14$	0.21369 $\pm 6.3683e-17$

TABLE III: Performance of Bozoth3 on the capacitive dataset

the most representative of what we may observe in a real-life fingerprint collection. So, we compute the relative NFIQ2.0 score variation to the average value of the ”varying” quality set. Results are shown in Fig. 5. We can see that with respect to our reference, the variation of NFIQ2.0 scores can be clearly significant. This is an indication of the quality gap

	Optical with no options		Optical with Scratches	
Generation quality	AUC (No option)	EER (No option)	AUC (Scratches)	EER (Scratches)
High	84.8549 $\pm 2.115e-14$	0.16339 $\pm 2.4096e-17$	84.6644 $\pm 1.6744e-14$	0.16488 $\pm 8.6058e-18$
Medium	81.9144 $\pm 4.4062e-15$	0.19922 $\pm 6.8847e-17$	82.323 $\pm 2.6437e-15$	0.19497 $\pm 6.8847e-17$
Low	73.6108 $\pm 2.7318e-14$	0.33473 $\pm 8.9501e-17$	73.7676 $\pm 1.7625e-15$	0.31858 $\pm 3.7866e-17$
VeryLow	65.0311 $\pm 4.4062e-15$	0.40782 $\pm 1.3425e-16$	65.7977 ± 0	0.39931 $\pm 7.5731e-17$
Varying	87.2199 $\pm 2.6437e-14$	0.19555 $\pm 4.6472e-17$	86.0072 $\pm 1.0575e-14$	0.17967 $\pm 3.0981e-17$

TABLE IV: Performance of Bozorth3 on the optical dataset

	Capacitive with no options		Capacitive with Scratches	
Generation quality	AUC (No option)	EER (No option)	AUC (Scratches)	EER (Scratches)
High	100 ± 0	0 ± 0	100 ± 0	0 ± 0
Medium	100 $\pm 1.078e-07$	2.5025e-06 $\pm 2.6951e-07$	100 $\pm 1.057e-07$	2.3618e-06 $\pm 2.6425e-07$
Low	99.2677 ± 0.016163	0.010583 ± 0.00018142	99.2364 ± 0.0168	0.0094371 ± 0.00016929
VeryLow	99.206 ± 0.016697	0.0088748 ± 0.00019145	99.2459 ± 0.016929	0.009172 ± 0.000169
Varying	99.7168 ± 0.010108	0.0046938 ± 0.00012898	99.6998 ± 0.010504	0.0054811 ± 0.00012706

TABLE V: Performance of MCC on the capacitive dataset

	Optical with no options		Optical with Scratches	
Generation quality	AUC (No option)	EER (No option)	AUC (Scratches)	EER (Scratches)
High	100 ± 0	0 ± 0	100 ± 0	0 ± 0
Low	99.2654 ± 0.016659	0.010627 ± 0.00018694	99.2217 ± 0.016867	0.0096432 ± 0.0001709
Medium	100 $\pm 1.0852e-07$	2.5528e-06 $\pm 2.7129e-07$	100 $\pm 1.0677e-07$	2.4322e-06 $\pm 2.6693e-07$
Varying	99.7109 ± 0.0099345	0.0047217 ± 0.00012742	99.6982 ± 0.010712	0.0054164 ± 0.00012792
VeryLow	99.1992 ± 0.016722	0.0089747 ± 0.00019379	99.2344 ± 0.017533	0.0092891 ± 0.00017349

TABLE VI: Performance of MCC on the optical dataset

we may observe between an average sensor in the market and very distinctive sensors. The quality is an indicator of the usability of a fingerprint as a biometric sample, a decrease in quality can lead to a poor recognition capacity and a bad user experience as a good biometric system should be able to recognize people equally. This variation is more important considering the optical technology. Fig. 6 and Fig. 7 show the relative variation of the AUC of each set against the reference set (e.g "varying") respectively with Bozorth3 and MCC. We can observe that the relative variation of Bozorth is similar to the NFIQ2 score (Fig. 5). From an operational perspective, this means that this matching algorithm is highly sensitive to the quality of the fingerprints. Moreover, considering the same type of sensor, we can see a change depending on its quality. For the MCC algorithm, given a type of sensor, the AUC seems to be stable regardless of the quality of the sensor. It is visible with its AUC variable close to 0% for 3 datasets and stays stable for the last set. This can be explained by the good performance it achieves which makes the algorithm able to handle samples of various qualities.

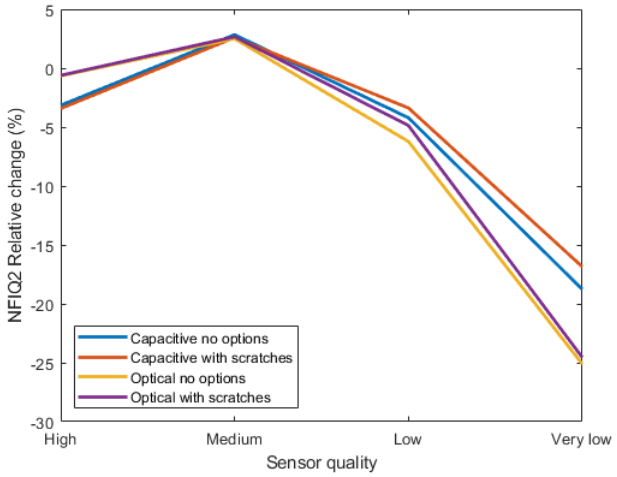


Fig. 5: Relative change of the NFIQ: the value of each group is computed against the average score of the "varying" set of that category.

VI. Conclusion and perspectives

In this study, we created different datasets using the fingerprint generator SFinGe to simulate different capturing technologies and sensors of different quality. The tested algorithms show that the main challenge for the performance comes from the algorithm. Indeed, even if for Bozorth3 the sensor technology and sensor quality are sources of variations in the performance, the MCC allows us to conclude that recognition algorithms with very high accuracy are less sensitive to sensing technology and more likely to be used with sensors of different quality. The advantage of this work is the controlling of the generation and the quantification of the impact of each parameter. Future works will include the study of other parameters such as the resolution of the sensor and the pressure.

VII. Acknowledgement

This work is supported by Fime SAS and the French National Association for Research and Technology (ANRT) as part of doctoral research between Fime SAS and the GREYC Laboratory.

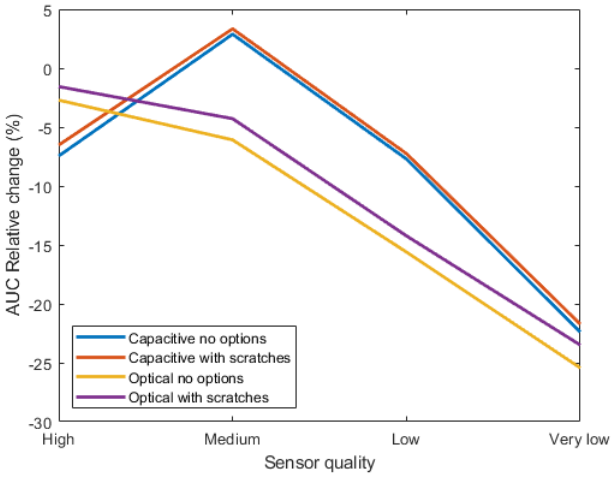


Fig. 6: Relative change of the AUC of the Bozorth3 fingerprint matching algorithm: the value of each group is computed against the AUC of the "varying" set of that category obtained with the same matcher.

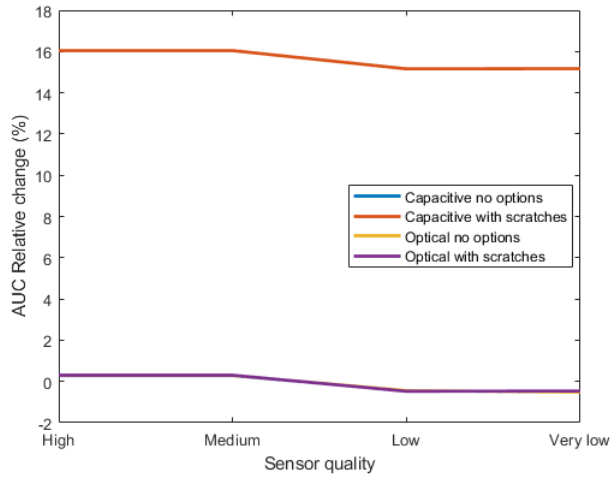


Fig. 7: Relative change of the AUC of the MCC fingerprint matching algorithm: the value of each group is computed against the AUC of the "varying" set of that category obtained with the same matcher. The 3 groups of images have almost equal relative change.

References

[1] "ISO/IEC 19795-2: 2021 Biometric performance testing and reporting — Part 2: Testing methodologies for technology and scenario evaluation," vol. 2021, 2021.

[2] A. Wone, J. Di Manno, C. Charrier, and C. Rosenberger, "Impact of environmental conditions on fingerprint systems performance," in *2021 18th International Conference on Privacy, Security and Trust (PST)*, pp. 1–5, IEEE, 2021.

[3] G. S. Heng, N. A. Ismail, Z. A. A. Rahman, and A. Anan, "Distribution of fingerprint patterns among young adults and siblings in malaysia," *Int. J. Med. Sci*, vol. 3, no. 1, pp. 11–7, 2018.

[4] A. Godbole, S. A. Grosz, K. Nandakumar, and A. K. Jain, "On demographic bias in fingerprint recognition," in *2022 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–10, 2022.

[5] "ISO/IEC 19795-1: 2021 Biometric performance testing and reporting — Part 1: Principles and framework," vol. 2021, 2021.

[6] A. Pentland, B. Moghaddam, T. Starner, *et al.*, "View-based and modular eigenspaces for face recognition," 1994.

[7] J. Harvey, J. Campbell, and A. Adler, "Characterization of biometric template aging in a multiyear, multivendor longitudinal fingerprint matching study," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 4, pp. 1071–1079, 2019.

[8] A. Lanitis, "A survey of the effects of aging on biometric identity verification," *International Journal of Biometrics*, vol. 2, no. 1, pp. 34–52, 2010.

[9] E. P. Kukula, C. R. Blomeke, S. K. Modi, and S. J. Elliott, "Effect of human-biometric sensor interaction on fingerprint matching performance, image quality and minutiae count," *International Journal of Computer Applications in Technology*, vol. 34, no. 4, pp. 270–277, 2009.

[10] U. Uludag, A. Ross, and A. Jain, "Biometric template selection and update: a case study in fingerprints," *Pattern recognition*, vol. 37, no. 7, pp. 1533–1542, 2004.

[11] H. Kang, B. Lee, H. Kim, D. Shin, and J. Kim, "A study on performance evaluation of fingerprint sensors," in *Audio-and Video-Based Biometric Person Authentication: 4th International Conference, AVBPA 2003 Guildford, UK, June 9–11, 2003 Proceedings 4*, pp. 574–583, Springer, 2003.

[12] P. Krishnasamy, S. Belongie, and D. Kriegman, "Wet fingerprint recognition: Challenges and opportunities," in *2011 International Joint Conference on Biometrics (IJCB)*, pp. 1–7, IEEE, 2011.

[13] D. Pathak and S. Tiwari, "A survey of wet and wrinkled fingerprint recognition techniques," *International Journal of Engineering Research and Technologies IJERT, ISSN*, pp. 2278–0181.

[14] B. Tan, A. Lewicke, D. Yambay, and S. Schuckers, "The effect of environmental conditions and novel spoofing methods on fingerprint anti-spoofing algorithms," in *2010 IEEE International Workshop on Information Forensics and Security*, pp. 1–6, IEEE, 2010.

[15] E. Marasco, "Biases in fingerprint recognition systems: Where are we at?," in *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–5, 2019.

[16] H. Alshehri, M. Hussain, H. A. Aboalsamh, and M. A. Al Zuair, "Cross-sensor fingerprint matching method based on orientation, gradient, and gabor-hog descriptors with score level fusion," *IEEE Access*, vol. 6, pp. 28951–28968, 2018.

[17] A. K. Jain and A. Kumar, "Biometrics of next generation: An overview," *Second generation biometrics*, vol. 12, no. 1, pp. 2–3, 2010.

[18] C. Raffaele, M. Dario, M. Davide, *et al.*, "Sfinge (synthetic fingerprint generator)," 2004.

[19] B. G. Sherlock and D. M. Monro, "A model for interpreting fingerprint topology," *Pattern recognition*, vol. 26, no. 7, pp. 1047–1055, 1993.

[20] 2016, title = 29794-1:2016: 2016 Information technology — Biometric sample quality — Part 1: Framework, volume = 2016, institution = International Organization for Standardization.

[21] Z. Yao, J.-M. Le Bars, C. Charrier, and C. Rosenberger, "Literature review of fingerprint quality assessment and its evaluation," *Iet Biometrics*, vol. 5, no. 3, pp. 243–251, 2016.

[22] Z. Yao, J. Le bars, C. Charrier, and C. Rosenberger, "Quality assessment of fingerprints with minutiae delaunay triangulation," in *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 315–321, 2015.

[23] M. El Abed, A. Ninassi, C. Charrier, and C. Rosenberger, "Fingerprint quality assessment using a no-reference image quality metric," in *21st European Signal Processing Conference (EUSIPCO 2013)*, pp. 1–5, IEEE, 2013.

[24] O. Bausinger and E. Tabassi, "Fingerprint sample quality metric nfiq 2.0," in *BIOSIG*, 2011.

[25] W. J. S. Ko Kenneth, "User's guide to nist biometric image software (nbis)," tech. rep., 2007.

[26] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, pp. 2128–41, 12 2010.