International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 8, No.5 (Sep-2019)
http://dx.doi.org/10.12785/ijcds/080504

On the Security of Face Recognition Terminals at Modern Airports

Chouaib Moujahdi[1] and Noureddine Assad[2]

[1] *Scientific Institute of Rabat, Mohammed V University in Rabat, Morocco*
[2] *Laboratory of Information Technologies, National School of Applied Sciences University of Chouaib Doukkali, El Jadida, Morocco*

Received 29 Mar. 2019, Revised 3 Jul. 2019, Accepted 25 Aug. 2019, Published 1 Sep. 2019

Abstract: The inability of airports to absorb the increasing numbers of passengers year after year, makes the use of e-gates and face recognition terminals a promising solution to enhance the quality of service and security. Thus, over the past few years, many airports around the world have adopted facial recognition technology to facilitate verification and identification of passengers, for example for surveillance systems, and recently for face recognition terminals. We believe that there are still many challenges and questions about face recognition in the context of these huge security applications, concerning performance, security and privacy. We believe that these concerns must be deeply discussed. In this paper, we discuss the potential vulnerabilities of facial recognition, then we present and discuss the result of an adopted attack against security applications that compare the live face of a passenger with his/her stored face image in passport or visa. Our experimental results illustrate the ability of the presented trick attack to be a serious threat for such modern security applications.

Keywords: Security Applications, Verification, Identification, Face Recognition Terminals; Surveillance Systems; E-gates; Privacy.

1. INTRODUCTION

We will begin this paper with a symbolic event, in the context of this discussion, that took place on March 29th 2008. Indeed, the same day that the British authorities decided to make the control of the biometric data of passengers mandatory in their airports, a group of hackers, called "Chaos Computer Club (CCC)", decided to warn the government, in its own way, that biometric systems are not really secure. The CCC group published in the number 92 of its magazine, called *Die Datenschleuder* [1], not only a tutorial on the forgery of fingerprints, but a copy of a fingerprint belonging to the German Ministry of the Interior at that time, which strongly defends the use of this new technology for security applications. In addition, they also published a list of several hacked politicians, including the German Chancellor. This action of the CCC Group is a sign of protest against the use of biometric data in electronic passports, and its objective is to open up a serious debate on the issues of the security and confidentiality of biometric systems. What can be learned from this event is that at a time when policy makers, encouraged by community of industry, are moving towards the use of biometric technology in an irresponsible hasty manner, many academic and professional voices are never stop to spread awareness about the unthinking use of this technology, especially for huge security applications. This work is a part of this context of awareness.

Over the past few years, many airports around the world have adopted facial recognition technology to facilitate passenger verification and identification (e.g., e-gates and recently face recognition terminals, see Figure 1). According to airports managers, our faces will turn into an important alternative document or tool that we can use for several tasks, for example we can be authenticated rapidly at the airport before joining or leaving flights (i.e., check-in and check-out), and we can be identified as not a threat as well by authorities (i.e., unauthorized person or not a wanted terrorist / criminal). Face can be used as well to track passengers to provide better and more personalized services, such as enabling airline staff at the airport to locate and assist late passengers who may miss their flights. In addition, authorities can use our faces as well to arrest those who seek to enter countries using someone else's identity.

E-mail: chouaib.moujahdi@um5.ac.ma, assad.n@ucd.ac.ma

The supporters of such new procedures claim that today around 4 billion passengers a year are traveling around the world, and this number is expected to double over the next 20 years. They claim, therefore, that the inability of airports to absorb these numbers of travelers makes the use of e-gates and face recognition terminals as a must to enhance the service quality and security. All these claims are supported as well by the majority of travelers who accept relatively today these biometric systems since they are familiar with them in all recent modern smartphones (i.e., face and fingerprint sensors).

Figure 1. (top): Example of an e-gate used by the first author of this paper at Los Angeles Airport USA on November 24th 2018. (Bottom): Example of a face recognition terminals at Atlanta's Hartsfield–Jackson Airport USA.

We believe, and several other authors [2][3], that there are still many challenges / questions (concerning performance and security) about face recognition in the context of these huge security applications. It is also still not clear how these applications can work or collaborate with the classical airport monitoring systems. Indeed, many questions can be asked: can face recognition ensure high performance (especially in the identification scenario with a large number of identities)? Can face recognition ensure security in all scenario of attacks? Will face recognition terminals be optional for users, so those who do not want to scan their faces can avoid this and follow traditional procedures within the airport, or these new biometric applications will be compulsory?

In this paper, we discuss the scenario where the traveler will use his face and also the face image stored in his issued passport / visa to deal with the face recognition terminals. It should be noted that the stored face images must respect several photometric requirements to be accepted by the authorities of a country before printing a visa or passport [4]. Every country has his own policy to take these pictures for passports and visas, either by taking live photos of individuals using high quality digital camera, or by asking them to provide a printed face ID picture. We discuss here the scenario where the passports and visas are issued using a printed face ID picture. We will present in this paper how we can use a printed face ID photo to attack modern face recognition terminals or e-gates.

The objective of the presented attack is to use someone else's identity to have an unauthorized access over these modern biometric applications.

The rest of the paper is organized as follows. In Section 2, we review the vulnerabilities of face recognition systems. We present the trick of attack and the used tools to make it in Section 3. Our experimental validation is presented in Section 4. Our conclusion is provided in Section 5.

2. LITERATURE REVIEW

The increasing use of biometrics for security applications has sparked an extensive interest to search and explore new adapted methodologies to attack biometric systems. These researches have shown that biometric systems are vulnerable to several attacks [2-5]. The main purpose of this section is to present a general view of biometric systems vulnerabilities while paying a particular attention to the attack scenario discussed in this paper.

A. Levels of attack against a biometric system

In the context of an application of security that uses biometric technology, a hostile attack presents the possibility that an opponent (enrolled or not in the system database) to circumvent a system without any awareness of administrators or designers of the application. In general, any biometric system consists of four main modules: the sensor module, feature extraction module, database module and classification module (Figure 2). Opponents can exploit this architecture to launch specific attacks on one or more modules of the system. In literature, vulnerabilities and attacks against a biometric system have been presented following different viewpoints [5-11]. We present here, briefly, the four attack categories of Jain et al. [11]:

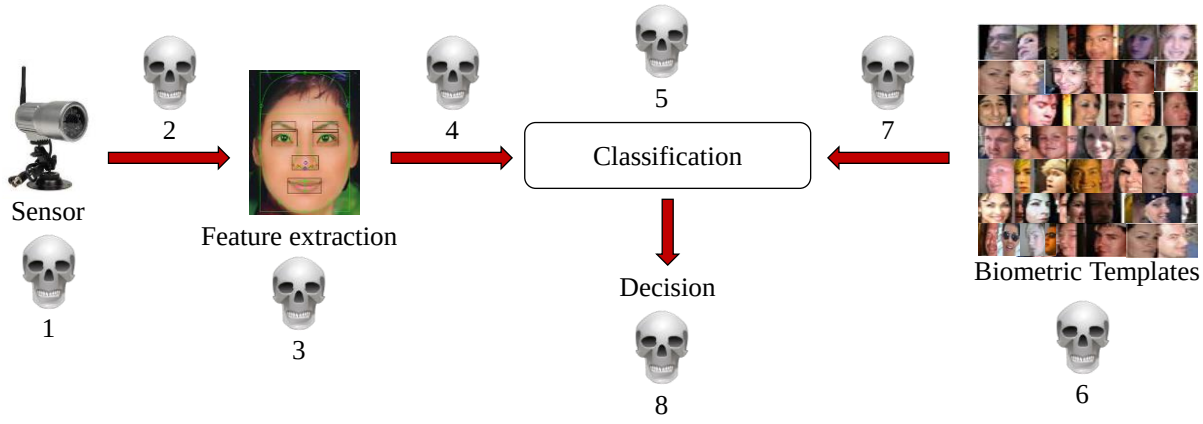

Figure 2. The eight levels of attack in a face recognition system.

- Direct attacks on the system sensor [12][13] (level 1 of Figure 2). For example, the sensor can be physically destroyed (e.g., denial of service attack). An opponent may present as well falsified biometric features to the system during enrollment or recognition task (e.g., spoofing or mimicry attack).
- Attacks on the interface between the modules of system [8][14] (levels 2, 4, 7 and 8 of Figure 2). Indeed, the modules of a biometric system are linked by communication channels in order to transfer the necessary information to perform the recognition task. Several types of attacks can be launched at these channels: between the sensor and feature extractor, between the feature extractor and the classifier, between the database and the classifier, and between the classifier and the decision application. For example, an adversary may destroy or disrupt these channels, or simply just intercept and / or modify the data transferred in the channels (e.g., replay attacks and hill climbing attacks).
- Attacks on the software module using virus and Trojan-horse programs to return the suitable values for the opponent [15][16] (levels 3 and 5 of Figure 2). For example, at the feature extraction module, the opponent can develop an algorithm to generate synthetic test images that resemble to images of the used sensor. This program can then send the images to the feature extraction module while surpassing the sensor. Thus, the system may be unable to distinguish whether the images come from its sensor or the opponent's malware.
- Attacks against the system database [17][18] (level 6 of Figure 2). For example, storage can be modified by adding, modifying or deleting biometric templates in order to have unauthorized access to the system. This attack could be launched during enrollment or authentication, or at any time directly on the database.

It should be noted that, depending on the used biometric trait and the adopted architecture, some of these attack categories may be possible in one system, but not in another. In the following subsection / sections, we will present the most relevant threats to face recognition terminals and we will discuss the concepts of security, integrity and privacy in the context of this biometric security application.

B. Face recognition terminals and their potential vulnerabilities

With the spread of illegal immigration attempts and terrorist incidents around the world, various international airports have begun to take innovative measures to protect their countries and travelers by adopting face recognition terminals or kiosks (Figure 1). To use this terminals, face of a passenger will be scanned, then the image will be compared with the stored reference image of the customs and border protection of the host country. Reference images can be the photos used to issue passport and visa and / or the photos of a wanted list.

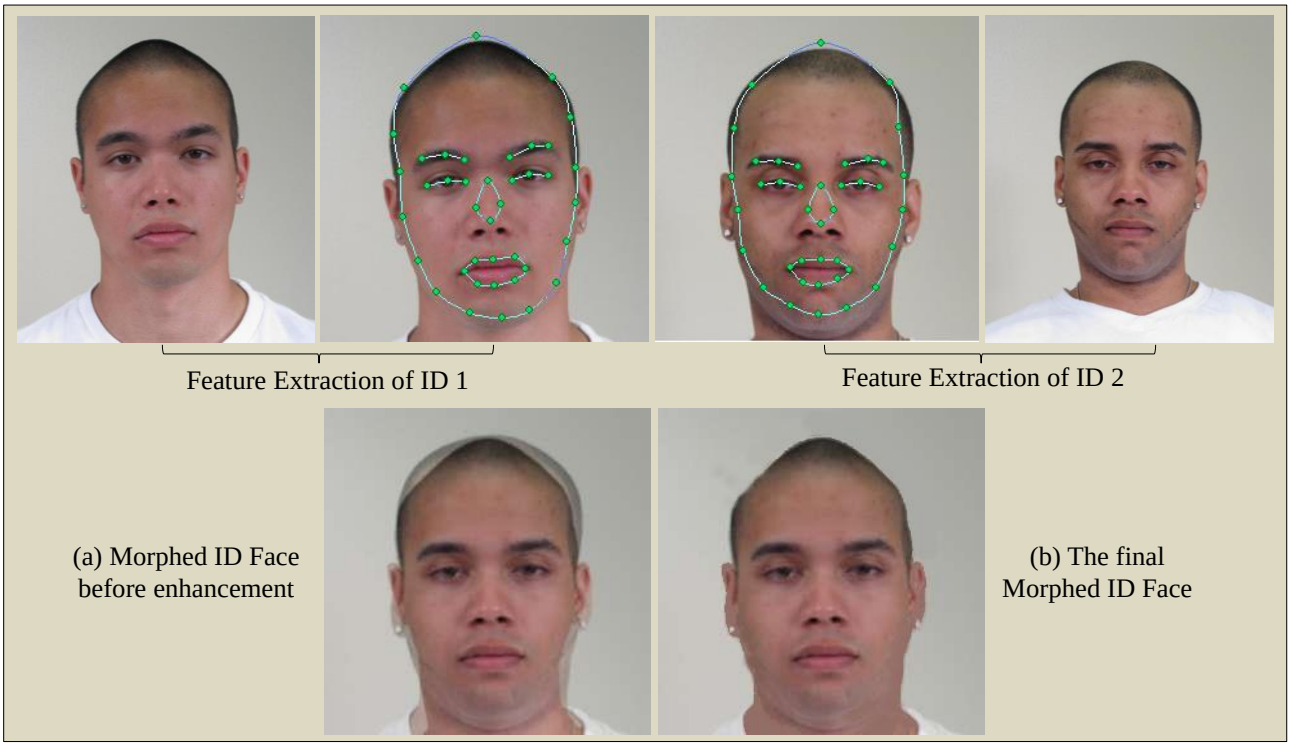

Figure 3. The construction and enhancement of the morphed ID face image.

We believe that it is difficult to lunch one of the attack categories of the pervious subsection against a face terminal. For example, an opponent, inside a well secured airport, has no chance to add any changes to the database of reference images, the only way to do that is via the intervention of a person working inside the database module. It is also very difficult to use a falsified face or a mask, such spoofing attack may compromise the sensor of a terminal only if this last do not contain high level technologies of liveness detection methods [19], things that is not possible for a well-equipped international airport. However, we believe that an opponent can exploit a simple trick to have unauthorized access from a face terminal. We know that some countries and consulates ask citizens to provide just a printed face ID picture to deliver passports and visas. An opponent, with the help of an assistant, that has no criminal record, can make a morphed ID face image that will be applied to the authorities to have a passport and then a visa. The issued document will be original, legal and able to circumvent face terminals. We will give more detail about the described trick in the following section.

3. TRICK OF ATTACK

The main idea of the proposed attack against face terminals is to create a morphed face image of two individuals (the opponent and his assistant). In general, we can define the morphing of two images as the process of going through smooth transition (or cross-dissolves) from the first image to the second one [20]. Thus, if we apply the morphing on two face ID photos, one of the intermediate transition frames can be chosen as the

morphed image, that we can enhanced later by some manual retouching to create the final face ID photo to be applied for authorities.

First, to morph face images, we have used the v2.51 of the free software called FaceMorpher [21]. Some face features (i.e., points) are extracted using this tool: eyes, noise, mouth, and the contour of segmented face. In general, these features, especially eyes location, are used to superimpose the two ID face images and then apply an alignment (Figure 3(a)). Second, for the manual enhancement, we have used the free GNU Image Manipulation Program [22] v2.10 (Figure 3(b)). Please see Figure 4 to visualize some other examples using ID face images of two women and also for man with a woman. Indeed, Figure 4 show as well some examples of morphed ID faces and test images that we will use in our experimental validation.

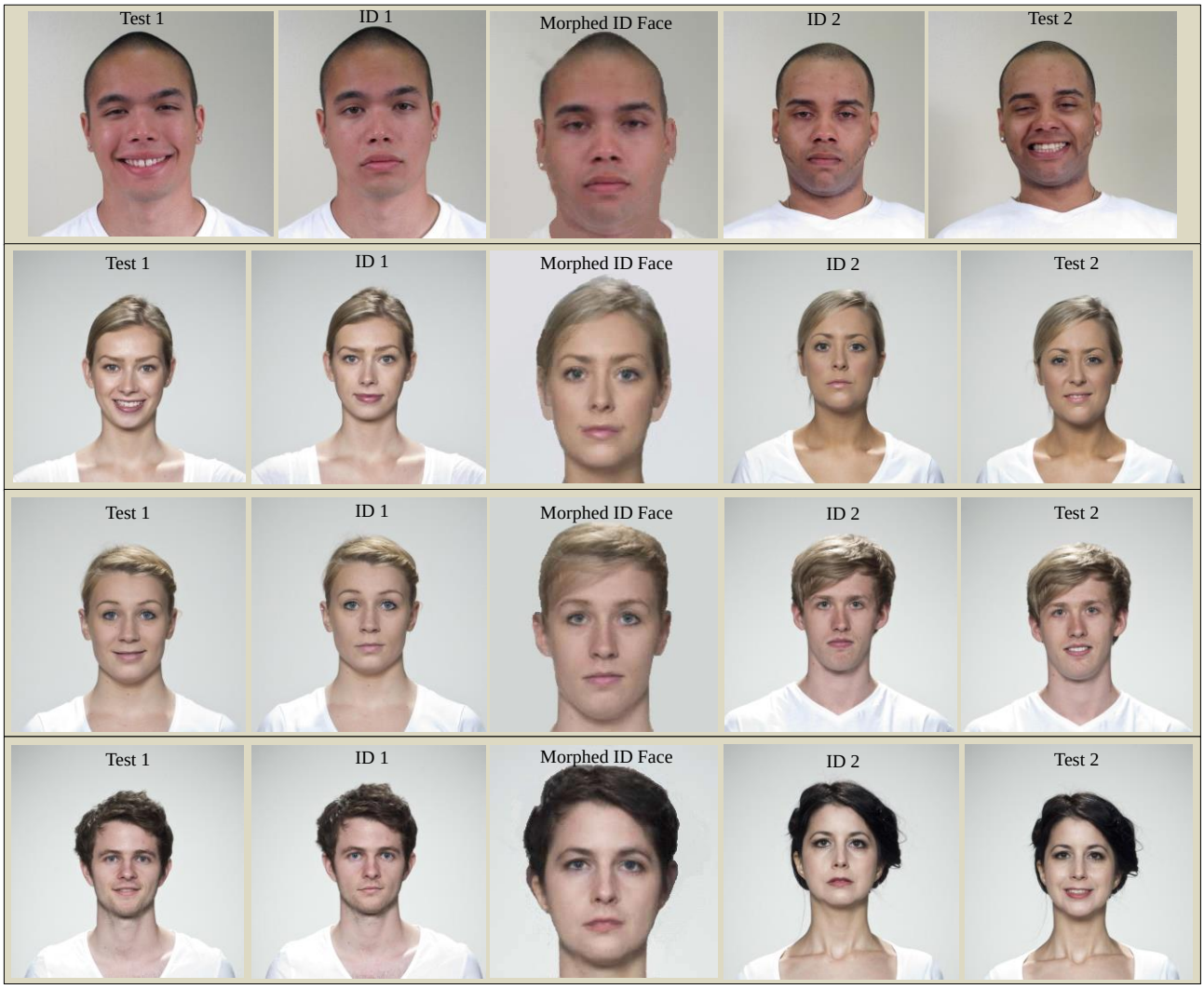

Figure 4. Examples of several possible combinations to construct morphed ID face images.

It should be noted that the presence of similarity in facial features and morphology between the two identities to be used to create a morphed ID face will make the process easier. In addition, we have to mention that an expert graphic designer can make our final morphed ID face more natural to circumvent human eyes / brain. However, we confirm that our created images already respect all photometric requirements [4] and they achieve all the necessary matching score to be accepted by the system (i.e., at least false accept rate of 0.001% according to ISO/IEC 19794-5:2011 [23]). We will present these results in the following section.

4. EXPERIMENTAL VALIDATION

In this section, we evaluate the verification accuracy using the trial version 10.0 of the commercial software Neurotechnology Face Verification SDK [24]. This solution is proving high performance / security in several

verification / identification scenarios, and it was used in several works of the state of the art [17][25][26][27]. In addition to the verification task, we have also used it for several other detection types: gender, age, emotion and expression detection. For the security level, we have applied a high level, than the recommended one, by fixing the False Accept Rate (i.e., FAR) at 0.0001%. The FAR reflects the probability of incorrectly acceptation or, in other words, the ability to reject an impostor correctly. According to the European Border and Coast Guard Agency [28], the designer of a face verification system must ensure at least a security level, in terms of the False Accept Rate (FAR), of 0.001% or less. The False Rejected Rate (i.e., FRR) is not very important here since we will not discuss the quality of service (i.e., precision of recognition) for legitimate users. According to the Developer's Guide of the Neurotechnology Face Verification SDK [24], matching threshold is determined regarding the fixed FAR value. In our case, since we have fixed the FAR at 0.0001%, the verification score of the created morphed ID images must be upper to a threshold value equal to 70 to be accepted by the system.

Figure 5. The verification match scores of the same identities of Figure 4 using Face Verification SDK.

The OSU Compound Facial Expressions of Emotion Database [29] is used in our experiments. This last contains 5060 face images, of various expressions, from 230 distinct identities (i.e., each person is represented by 22 images). We have construct using this database: 10 morphed ID faces by using two images of male identities, 10 morphed ID faces for female identities and 5 ID faces are constructed by morphing one male image with one female image.

Figure 5 present the scores of verification using the same ID face images of Figure 4, all attacks took place successfully. In addition, all the remaining 21 ID Face images of attack were used successfully to circumvent the system with a match score upper to 70 with a FAR fixed

at 0.0001%. Through this preliminary series of experiments, it is clear that this simple trick of attack might be able to threat the security system of airports based on face recognition terminals. Thus, any official permanent use of this new technology must be done carefully and followed by an extensive study of vulnerabilities and possible adversary attacks.

As temporary solutions for this simple attack: first, the authorities must require live photos of applicants, using high quality cameras, to issue passports and visas. Second, facial recognition terminals, e-gates, surveillance systems and all other biometric security applications should be equipped with the necessary techniques to detect passports / visas that contains morphed ID face images like [30]. However, we believe that the most effective solution, in the long term, is to subject any new large uses of biometrics to in-depth studies to be able to make system resources unchanged, modified, or manipulated to ensure the integrity of the system. Then, we have to use them in a gradual manner without completely eliminating the traditional procedures.

We would like to mention here some other drawbacks and ideas, that we cannot validate experimentally. If we imagine a world with a ubiquitous biometrics, absolutely citizenship remains limited only to the person who proves the safety of all members of his body. In addition, we think that privacy summarizes the ability of a user to use and control their identity without being tracked, stolen or compromised, despite the fact that their personal information is revealed during enrollment, use, storage, modification, transfer and suppression. Thus, in a world with a ubiquitous biometrics, talking about users privacy might be useless.

We want to emphasize at the end of this section that for sure absolute security does not exist. It is also perhaps very important that we simply understand that no identity recognition system is ideal (including those that are based on biometrics), and it may never exist. However, we think that we can trust the security of biometric recognition systems if they are used gradually, with wisdom and in conjunction with other protection techniques

5. CONCLUSION

In this paper, we present the potential vulnerabilities of facial recognition, then we discuss the result of an adopted attack against security applications that compare the live face of a passenger with his/her stored face image in passport or visa. Indeed, an opponent, with the help of an assistant that has no criminal record, can make a morphed ID face image that can be applied to the authorities to have a passport and then a visa. The issued document will be original, legal and able to circumvent facial security applications. We have used two commercial software to create morphed ID face images and then we have tested the possibility to lunch the presented attack successfully using a commercial verification system. Our experimental validation indicates that the proposed trick might be able to threat the security system of airports based on face recognition terminals. In this context, our recommendations include to require live photos of applicants, using high quality cameras, to issue passports and visas, and to enhance biometric security applications with the necessary techniques to detect passports / visas that contains morphed ID face images. For the long term solution, we believe that community of security must open up a serious debate on the issues of the security and confidentiality of biometric systems, especially for huge applications, before any widespread use.

REFERENCES

[1] Die Datenschleuder magazine web site: https://ds.ccc.de/

[2] P. Campisi. Security and privacy in biometrics. Springer Publishing Company, Incorporated, 2013.

[3] A.K. Jain, K. Nandakumar and A. Ross. 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters. vol. 79, pp. 80–105, 2016

[4] International Civil Aviation Organization web site: https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[5] N.K. Ratha, J.H. Connell and R.M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal. vol. 40, pp. 614–634, 2001.

[6] N.K. Ratha, J.H. Connell and R.M. Bolle. Biometrics break-ins and band-aids. Pattern Recognition Letters. vol. 24, pp. 2105 – 2113, 2003.

[7] B. Cukic and N. Bartlow. Biometric System Threats and Countermeasures: A Risk Based Approach. In Biometric Consortium Conference, 2005.

[8] A. Adler. Vulnerabilities in Biometric Encryption Systems. In Audio- and Video-Based Biometric Person Authentication, Springer Berlin Heidelberg. vol 3546, pp. 1100–1109, 2005.

[9] A.K. Jain, A. Ross and S. Pankanti. Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security. vol. 1, pp. 125–143, 2006.

[10] C. Roberts. Biometric attack vectors and defenses. Computers & Security. vol. 26, pp. 14–25, 2007.

[11] A.K. Jain, K. Nandakumar and A. Nagar. Biometric Template Security. EURASIP Journal on Advances in Signal Processing. pp. 1–17, 2008.

[12] J. Galbally, R. Cappelli, A. Lumini, G. Gonzalez de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia and D. Maio. An Evaluation of Direct Attacks Using Fake Fingers Generated from ISO Templates. Pattern Recognition Letters. vol. 31, 725–732, 2010.

[13] K. Sooyeon, Y. Sunjin, K. Kwangtaek, B. Yuseok and L. Sangyoun. Face liveness detection using variable focusing. International Conference on Biometrics (ICB). pp. 1–6, 2013

[14] A. Juels, D. Molnar and D. Wagner. Security and Privacy Issues in Epassports. First International Conference on Security and Privacy for Emerging Areas in Communications Networks. pp. 74–88, 2005.

[15] D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar. Handbook of fingerprint recognition. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[16] P. Grother, W. Salamon, C. Watson, M. Indovina and P. Flanagan. Performance of Fingerprint Match-on-Card Algorithms Phase II / III Report. NIST Interagency Report 7477 (Revision I), 2009.

[17] C. Moujahdi, G. Bebis, S. Ghouzali and M. Rziza. Fingerprint shell: Secure representation of fingerprint template. Pattern Recognition Letters. vol. 45, 189 – 196, 2014.

[18] C. Moujahdi, G. Bebis, S. Ghouzali, M. Mikram and M. Rziza. Biometric Template Protection Using Spiral Cube: Performance and Security Analysis. International Journal on Artificial Intelligence Tools. vol. 25, 1550027, 2016

[19] J. Hernandez-Ortega, J. Fiérrez, A. Morales and J. Galbally. Introduction to Face Presentation Attack Detection. Handbook of Biometric Anti-Spoofing. pp. 187-206. 2019

[20] P.J. Benson. Morph transformation of the facial image. Image and Vision Computing. vol 12, pp. 691-696, 1994.

[21] FaceMoepher software web site: http://www.facemorpher.com/

[22] GNU Image Manipulation Program Web Site : https://www.gimp.org/

[23] Information technology -- Biometric data interchange formats -- Part 5: Face image data. Web site : https://www.iso.org/standard/50867.html

[24] Neurotechnology Face Verification SDK web site : https://www.neurotechnology.com/

[25] F.K. Brendan and A.K. Jain. Face recognition: Impostor-based measures of uniqueness and quality. IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS). pp. 237-244, 2012.

[26] P. Wild, P. Radu, L. Chen and J. Ferryman. Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. Pattern Recognition. vol. 50, pp. 17-25, 2016.

[27] M. Azimi and A. Pacut. The effect of gender-specific facial expressions on face recognition system's reliability. IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR). pp. 1-4, 2018.

[28] European Border and Coast Guard Agency web site: https://europa.eu/european-union/about-eu/agencies /frontex_en

[29] S. Du, Y. Tao and A.M. Martinez. Compound facial expressions of emotion. Proceedings of the National Academy of Sciences. 111(15), E1454-E1462, 2014.

[30] R. Raghavendra; S. Venkatesh; K. Raja and C. Busch. Towards making Morphing Attack Detection robust using hybrid Scale-Space Colour Texture Features. 5th International Conference on Identity, Security and Behaviour Analysis. Hyderabad, IN, January 22-24., 2019

Chouaib Moujahdi is an Assistant Professor at the Scientific Institute of Mohammed V University in Rabat, Morocco. He received both the Master's and the Ph.D. degrees in Computer Science and Telecommunications from Mohammed V University. He was a Fulbright visiting student at University of Nevada - Reno between 2012 and 2014. His research interests include Biometrics and Pattern Recognition. Current work focuses on Biometric Security Protection.

Noureddine Assad is an Assistant Professor at the National School of Applied Sciences of University of Chouaib Doukkali, El Jadida, Morocco. He received both the Master's and the Ph.D. degrees in Computer Science and Telecommunications from Mohammed V University. His research interests are: sensor nodes deployment quality in wireless sensor networks and network coverage / connectivity.