The Risk of Using Biometrics

Haya Altaleb

Obuda University, Institute of Mechatronics and Vehicle Engineering (MSc)

haya7atem@gmail.com

Sinan Kocak

Obuda University, Doctoral School on Safety and Security Sciences

sinan.kocak@bgk.uni-obuda.hu

Abstract: Biometric is an advanced technique that provides excellent benefits in access privilege and authentication. This security technology has become an integral part of a variety of sectors, regardless of its type, governmental or private. The growth of proprietary data is becoming increasingly important for excellent authentication solutions that enhance mobile security. The security of information is necessary to protect the property of institutions that may fall into the hands of competitors or hackers and cyber-terrorists. This paper shows the hidden risks of biometric techniques and how to avoid them.

Keywords: biometrics, technologies, risk of biometrics

1 Introduction

Biometrics is a science that studies physical and behavioral properties that can distinguish people from each other. The term biometric comes from two Greek words “bio” meaning life and “metric” meaning to measure [1].The application of biometric systems with their simple conditions actually comes from ancient times. Relevant sources have reported that people who lived thousands of years ago identified each other with characteristics that were easily measured, such as eye colour, skin colour, and height [2].

The 19th century scientist Henry Faulds proposed a paper in a “Nature” magazine about fingerprints, it recommended the use of fingerprints as a definition system, including the scientific definition of criminals [3]. Before the 21st century, there were time losses in the military and commercial sectors because of the lack of

automatic recognition. In the early 21st century this problem got acceleration, computer technology included fingerprint recognition sensors on laptops and applied to other intelligent devices [4].

In 1964, scientists Woodrow Bledsoe, Helen Chan, and Charles Bisson began working on face recognition project. This project was called the man-machine, and the face images of people were compared with the technology of that era RAND tablets. The algorithm was designed to measure pupils, eye edges, forehead lines, and 20 parameters such as mouth width, eye width, and pupil distance [5].

Today's technology has reached a stage of maturity that enables us to reveal our identity through fingerprints, voice, iris, or even through our brain print - quickly, simply, safely, without error, and in an inexpensive way [6]. Information plays a vital role in the success of very organizations, the biometric information is like bits any other digital information, modern security industries and individuals looking for biometrics as an ideal solution [7]. However, it can be stolen, altered even held for ransom. It is subject to all data breaches and other offences that may affect bank information or school records. Biometrics become an interesting research area in recent years, the physiological or behavioural characteristic can be used if it has these properties:

- Unique: It must be different from person to person until the twin brothers.
- Universal: It must be universal and not exist in a specific category of people.
- Durable: It should not be affected by age and be permanent.
- Measurable: Must be measurable with simple technical tools.
- Easy to use: It should be easy and convenient to measure.

The community is not clearly understood about the risks of privacy and security in biometrics. Everyone knows that biological traits can be used to identify people. The technology has enabled a large number of new biometric identification systems that use fingerprints, iris scans, wrist veins scanning, voice recognition and facial recognition [8]. However, when it comes to potential invasion of privacy, these different methods are not equal. All biometric systems capture biometric data, enter that data into a database, and capture new data to run against the database looking for a match. They all work well to identify individuals using computer analysis of various body parts. It is difficult to capture most biometric data, ıt usually requires permission or explicit knowledge to capture fingerprints, iris, vein, and other biometric data [9]. For instance, your bowels or veins may not have been checked once.

2 Selected Biometrics Technologies

Biometric behaviour solutions offer less risk than the huge misuse of physical biometric techniques. Biometric behaviour techniques are currently not widely used and, therefore, will not be discussed in this document. Behavioral biometric information is also much more likely collected without the user's knowledge of the system, and thus may present more legal and Organizational issues of business. This paper covers the basic concept of selected biometric methods for identification and authentication, included:

- Fingerprint
- Facial recognition

There are other Technologies not covered in this paper, included:

- DNA.
- Gait.
- Ear shape.
- Vein patterns.
- Fingernail bed.
- Foot dynamics.
- Retinal matching.
- Skin luminescence.
- Brain wave pattern
- Footprint recognition.
- Facial thermography.

Figure 1. Classification of Biometrics

Technologies (source: [10])

2.1 Fingerprint

Automatic matching of fingerprints is among the oldest biometric techniques. Currently, fingerprint recognition is the most widely used method of biometric authentication and one of the most cost-effective methods. However, there are differences in how to read fingerprints, with some effective reading techniques under the surface of the outer skin, making them more reliable under a variety of operational scenarios. We have seen fingerprint readers integrated into laptops and handheld devices, and this trend is likely to continue, especially in the world of smart phones and Tablet PC. Independent fingerprint readers are manufactured easily and may use a variety of operational techniques and connectivity options [11]. Moreover, there are devices that enable multiple fingerprint collection at the same time. These are of obvious importance to law enforcement and border control agencies. Fingerprint reader is an electronic device that records a digital

fingerprint image. The captured image is known as the direct scan, which is digitally processed. Distinctive features are extracted and a biometric fingerprint template is created. This biometric template is stored and will be used in the matching process later [12].

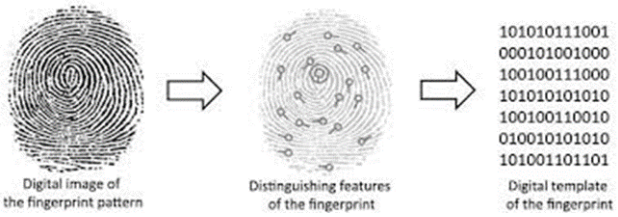

Figure 2. Illustration of fingerprint reader (source: [13])

2.2 Facial recognition

Facial recognition was a revolution in the biometric technology. Especially, in the last 10 years it become a popular topic. Since 2001 September 11, there has been a strong movement to integrate the face Recognition techniques in national security plans [14]. This technology can be used in monitoring activities, it has the ability to access large databases of images obtained during identification processing.

This technology can be considered an easy to implement. Most of the cameras included in laptops and other portable devices are capable, with the right software, of capturing a passable facial image. Face recognition algorithms are varied, like PCA (Principal Component Analysis), ICA (Independent Component Analysis), LDA (Linear Discriminant Analysis), EP (Evolutionary Pursuit), EBGM (Elastic Bunch Graph Matching), Trace Transform Radon, Hidden Markov Model, Eigenfaces Model, Fisher Model, AAM (Active Appearance Model), Artificial Neural Networks, 3D Morphable Model, 3D Face Recognition are frequently used algorithms. Recently, face recognition algorithms have been developed by using machine learning [15].

In 2D facial recognition techniques take recordings with a single camera and convert it to numerical value by using the algorithm that it uses [16]. However, this may even be affected by the user's facial expressions, environmental light and the face. Some algorithms implement the colour and the light normalization, but this process can extend the time for verifying the identity of the user, also increasing false negatives and false positives. Receiving more than one reference face information for a user can also fill the storage area. In addition, 2-dimensional validations can be fooled easily with a passport photo. [17].

In 3D face recognition, optical scanners mapped the surface it scans. Because it requires more than one camera, it increases the cost. On the other hand, colour, light and perspective have no effect in 3D techniques [18]. Because it performs

multiple 2-dimensional analysis, it provides a more accurate authentication than a single two-dimensional image.

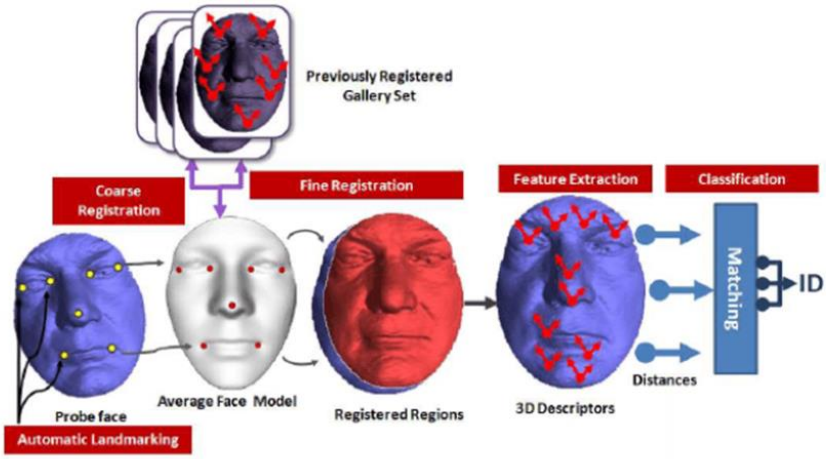

Figure 3. Overall pipeline of a typical 3D face recognition system (source: [19])

The effectiveness of all these systems can be measured. FAR (False Acceptance Rate) is the rate of false detections caused by the system's mapping of information to a person who is not present in the database and matching it to another person in the database. False Rejection Rate (FRR) is the rate at which the system cannot find the existing person in the database [20]. The smaller the FAR and FRR values, the closer the system is to the ideal. There is an inverse ratio between FAR and FRR. Where the FAR and FRR are equal or (the area under which the FAR and FRR curves are equal) is called EER (Equal Error Rate). The lower the EER value, the better the system [21].

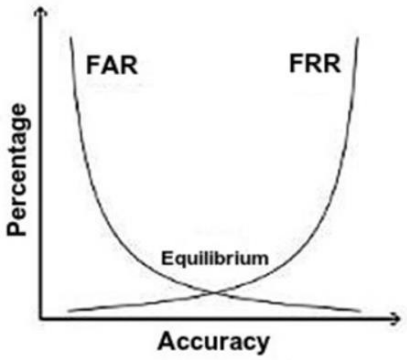

Figure 4. FAR and FRR equilibrium (source: [22])

3 Risk Factors Associated with Biometric Identification

Most of the biometrics systems store the user's data without any encryption or hashing in order to be able to access them quickly. Furthermore, those systems can be rendered ineffective due to problems caused by it, or by intentional attacks, such as a product with a high FAR due to the poor quality of the parts used can verify the wrong person or a manipulation to the sensor or database, can add a person who should not be verified. At the same time, a data of a user previously registered to the system may be copied and presented to the system in different ways. Like using the passport-size photograph of the person in 2-dimensional face recognition.

Due to problems with the Face ID technology of new iPhone devices, there have been instances where the phone can be opened by children or twins. Where physical access to the device is possible, malicious users may modify the sensor to authenticate it. In the channels that provide communication between the system components, it can be performed covertly, the data can be manipulated by Man-in-the-middle attacks, brute-force attacks can be performed, the captured data can be authenticated using again and also artificial data can be generated for matching [23].

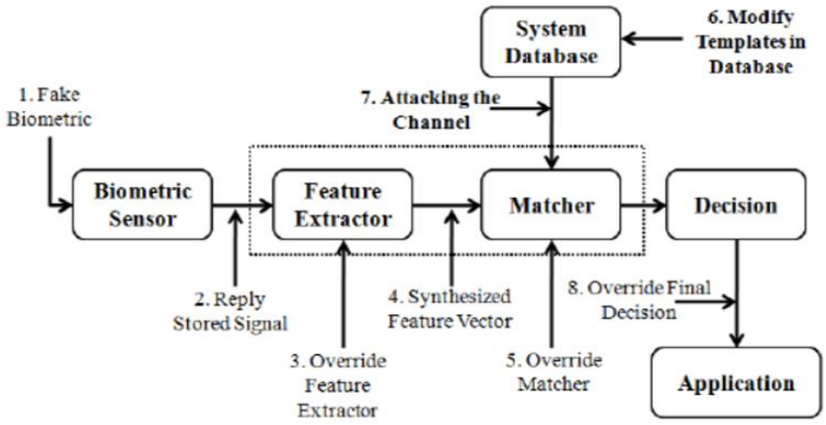

Figure 5 Attacks on Biometric System (source: [24])

In the case of access to the database, the confidentiality and integrity of the data in particular are compromised. Reading unencrypted data can also mean access to personal data. Similarly, the attacker can read the data, access the templates, add his own information, or change data for someone else. By altering the link between identity and biometric, it can lead to an inability to authenticate. If access to decision and matching mechanisms is available, the degree of matching of the entered value can be changed, the previously entered value can be entered again or match results can be tested and brute attack attacks can be carried out. In addition,

biometric identification systems with automatic and unattended registration are always open and misleading identity. Any incorrect information to be entered at the time of registration may result in misuse or may be matched with an accurate biometric, false identification.

Despite these attacks, the first important security measure is to ensure the physical security of the system. At the same time, the information in the database must be stored or encrypted. In order to solve the problems in the channels, it should be preferred that the inter-component traffic flows. Unfortunately, all these features will interfere with the performance of the device (or system). Each encryption processing can extend the time during authentication, even at machine speed. However, such measures should be taken where security and identity certainty are necessary. In addition, it is recommended that biometric verification should be used as a secondary method rather than alone, because of such problems in biometric authentication.

4 Risk Assessment and Reduction Methods

In any technological intelligent systems, the risk assessment is extremely important in order to solve problems. The purpose of the risk assessment is to minimize the potential risks by calculating the probability and severity. In biometric systems, threat sources are adversarial (hackers) and non-adversarial (human errors, structural failures, or natural disasters). It is possible to determine the probability and severity of the potential attacks by considering the result of figure 5.

The risk of the given process should be known correctly to make a reliable decision. In Pokoradi article, a study on fuzzy logic based risk assessment is presented which can be used in the modern complex engineering system. In the article, the author classified the risk possibilities into two categories according to their severity (catastrophic, critical, moderate, and negligible) and probability (frequent, likely, occasional, seldom, unlikely). Table 1 shows the level of risk determination from the article [25].

Table 1. Risk Assessment Matrix

Threat Event Occurs And Results in Adverse Impact	Frequent	Likely	Occasional	Seldom	Unlikely
Catastrophic	Extra High	Extra High	High	High	Medium
Critical	Extra High	High	High	Medium	Low
Moderate	High	Medium	Medium	Low	Low
Negligible	Medium	Low	Low	Low	Low

Many methods can be followed to ensure using biometrics effectively and minimize the risk of using it.

The first method, encrypt templates stored in databases and protect them from attackers. Therefore, digital scales can be used as a key to encrypt data until they are used.

The security and authentication can be performed using the watermark method, which adds some additional information to the security object. This extra bits addition provides security to the source object. On the other hand, the source object also causes some distortion. The watermarking method includes more information to the database (data source, data destination etc.) within the data itself (image, sound etc.) this inclusion may be apparent or invisible. The purpose of using the watermark in biometrics is to confirm the data source plus detection of any change may occur.

The combination of several models, several sensors and multiple biotechnologies such as fingerprints and iris can significantly reduce risks. In addition, the use of more than one biometric image sample will minimize the validation process by doing more calculations.

Conclusions

In this paper, the authors present a brief overview of the hidden risks of biometric techniques, some risk reduction methods and two of the most popular biometric technology fingerprint and face recognition technologies are discussed.

Biometric systems face many security challenges such as system security itself, integrity, and reliability. There is a need for an information security research that addresses the specific problems of biometric systems, such as prevention of attacks based on the provision of false biometrics, reuse of previously captured biometric samples and the development of technologies.

References

[1] Rashid, Rozeha A., Nur Hija Mahalin, Mohd Adib Sarijari, and Ahmad Aizuddin Abdul Aziz: Security system using biometric technology: Design and implementation of Voice Recognition System (VRS), In Computer and Communication Engineering, 2008, ICCCE 2008, International Conference on, IEEE, 2008, pp. 898-902.

[2] A Jain, Anil K., Arun Ross, and Salil Prabhakar: An introduction to biometric recognition, IEEE Transactions on circuits and systems for video technology, Jan 4, 2004, pp. 4-20.

[3] Yager, Neil, and Adnan Amin: Fingerprint verification based on minutiae features: a review, Apr 1, 2004, pp. 94-113.

[4] Maltoni, Davide, Dario Maio, Anil K. Jain, and Salil Prabhaka: Handbook of fingerprint recognition, Springer Science & Business Media, Apr 21, 2009.

[5] Ballantyne, Michael, Robert S. Boyer, and Larry Hines: Woody bledsoe: His life and legacy, AI magazine, Mar 15, 1996, pp. 7-7.

[6] Jain, Anil K., and Ajay Kumar: Biometric recognition: an overview, in Second generation biometrics: The ethical, legal and social context, Springer, 2012, pp. 49-79.

[7] Jain, Anil K., Arun Ross, and Sharath Pankanti: Biometrics: a tool for information security, IEEE transactions on information forensics and security, 2006, pp. 125-143.

[8] El-Bakry, Hazem M., and Nikos Mastoraki: Personal identification through biometric technology, in 9th WSEAS International Conference on Applied Informatics and Communications (AIC09), Moscow, Russia, Aug 20, 2009, pp. 325-340.

[9] Sun, Yunlian, Man Zhang, Zhenan Sun, and Tieniu Tan: Demographic analysis from biometric data: Achievements, challenges, and new frontiers, IEEE transactions on pattern analysis and machine intelligence, Feb 1, 2018, pp. 332-351.

[10] "Assured enterprises: Biometric technology cybersecurity," Biometric Technology Now at Assured, 2018. [Online]. Available: https://www.assured.enterprises/cyber-products/biometric-technology-cybersecurity/. [Accessed 11 12 2018].

[11] T Hupperich, Thomas, Davide Maiorca, Marc Kuhrer, Thorsten Holz, and Giorgio Giacinto: On the robustness of mobile device fingerprinting: Can mobile users escape modern web-tracking mechanisms?, in Proceedings of the

31st Annual Computer Security Applications Conference, ACM, Dec 7, 2015, pp. 191-200.

[12] Garrett, Peter, and Paul Regen: Hand-held electronics device for aggregation of and management of personal electronic data, Google Patents, Jan 3, 2017.

[13] D. Thakkar, "bayometric," Fingerprint Reader Technology Comparison: Optical Fingerprint Scanner; Capacitive-based Fingerprint Reader and Multispectral Imaging Sensor, [Online]. Available: https://www.bayometric.com/fingerprint-reader-technology-comparison/.

[14] Lyon, David: Surveillance after september 11, 2003, pp. 16-25.

[15] Jaiswal, Sushma, Sarita Singh Bhadauria, Rakesh Singh Jadon, and Tarun Kumar Divakar: Brief description of image based 3D face recognition methods, 3D Research, Dec 1, 2010, p. 2.

[16] Raghavendra, Ramachandra, Kiran B. Raja, and Christoph Busch: Presentation attack detection for face recognition using light field camera, IEEE Transactions on Image Processing, Mar 24, 2015, pp. 1060-1075.

[17] Asaad, Aras, and Sabah Jassim: Topological Data Analysis for image tampering detection, in International Workshop on Digital Watermarking, Springer,aug 23, 2017, pp. 136-146.

[18] Preim, Bernhard, Alexandra Baer, Douglas Cunningham, Tobias Isenberg, and Timo Ropinski: A survey of perceptually motivated 3d visualization of medical image data, in Computer Graphics Forum, Wiley Online Library, June, 2016, pp. 501-525.

[19] Petrovska-Delacretaz, Dijana, Chollet, Gerard, Dorizzi, Bernadette: Guide to biometric reference systems and performance evaluation, Springer, Berlin, Mar 10, 2009.

[20] Beritelli, Francesco, and Grazia Lo Sciuto: Performance evaluation of multimodal biometric systems based on mathematical models and probabilistic neural networks, in The International Symposium for Young Scientists in Technology, Engineering and Mathematics, Catania, Italy, 2016, pp. 40-46.

[21] Souza, Luiz, Luciano Oliveira, Mauricio Pamplona, and Joao Papa: How far did we get in face spoofing detection?, Engineering Applications of Artificial Intelligence, June 30, 2018, pp. 386-381.

[22] D. THAKKAR, "False Acceptance Rate (FAR) and False Recognition Rate (FRR) in Biometrics," BIOMETRIC TERMINOLOGY, [Online]. Available: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/. [Accessed 12 10 2018].

[23] Bhagavatula, Rasekhar, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides: Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption, 2015.

[24] Thanki, R. M., and K. R. Borisagar: Discrete wavelet transform and compressive sensing based multibiometric watermarking—A novel approach to embed watermark into biometrie, in Emerging Technology Trends in Electronics, Communication and Networking (ET2ECN), 2014 2nd International Conference on, IEEE, Dec 26, 2014, pp. 1-6.

[25] Pokoradi, Laszlo: Fuzzy logic-based risk assessment, AARMS, Academic and Applied Research in Military Science, Mar 1, 2002, pp. 63-73.

[26] Pfitzmann, Andreas: Biometrics–how to put to use and how not at all?, in International Conference on Trust, Privacy and Security in Digital Business, Springer, Berlin, Heidelberg, Sep 4, 2008, pp. 1-7.