ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 1, 191-200 (2020)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

Biometric System Vulnerabilities: A Typology of Metadata

Abdou-Aziz Sobabe*, Tahirou Djara, Antoine Vianou

Laboratoire d'Electronique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC) Université d'Abomey-Calavi, Benin, Institut d'Innovation Technologique (IITECH) Abomey-Calavi, Bénin

ARTICLE INFO

Article history:
Received: 19 September, 2019
Accepted: 13 January, 2020
Online: 22 January, 2020

Keywords:
Biometric vulnerabilities
Metadata
Area Under the Curve (AUC)

ABSTRACT

This study presents a root cause analysis of biometric vulnerabilities and provides a comprehensive typology of metadata in biometric adaptation. Although they are more reliable and secure than traditional authentication methods, biometric techniques are subject to vulnerabilities that pose challenges. Faced with the proliferation of cases of identity theft and fraud, biometrics is increasingly used to protect assets and people in several areas such as commercial, forensic and government applications. As a first step, a metadata analysis was performed. A focus has then been placed on their role in the fight against biometric vulnerabilities. Thus, the vulnerabilities studied have been classified into two main categories: intrinsic limits and adverse attacks. Finally, one of the scenarios considered was implemented, particularly the case of the combination of skin color with facial recognition. The implementation resulted in encouraging results with an Area Under the Curve (AUC) of 0.826 for the face system and 0.908 for the multimodal system.

1. Introduction

The fast-growing digital transformation is a process of fully integrating digital technologies into all of an organization's activities. In this digital world, the authentication stage is often considered as the weak link in computer security, because of the large number of identity theft cases. User authentication is an important challenge in securing assets. In reference to computer security, biometrics refers to the use of morphological, behavioral or biochemical characteristics to determine or verify the identity of a user.

Security is about "protecting" "assets" against all forms of "threats" [1]. Threat is the type of action that may be harmful in the absolute, while vulnerability (sometimes called a gap or breach) represents the level of exposure to the threat in a particular context. Finally, the countermeasure is the set of actions implemented to prevent the threat. The countermeasures to be implemented are not only technical solutions but also training and awareness measures for users, as well as a set of clearly defined rules. From the notions of threat, vulnerability and countermeasures, we can define the notion of risk as a danger that can be sustained at any time. The risk in terms of security is generally characterized by the following equation:

$$Risk = \frac{Threat * Vulnerabilities}{Countermeasures}$$

The security procedure can be represented by Figure 1 below.

As we can see, vulnerabilities are at the heart of the security procedure. Biometric authentication systems are positioned as the means of countermeasure put in place to ensure the protection of assets. But these systems face a number of challenges and vulnerabilities. Among the solutions to these challenges and vulnerability, the use of metadata figures prominently. In the following sections, we present an overview of biometrics metadata before addressing their role in addressing identified vulnerabilities.

2. Overview of some Non-Current Biometric Features

Biometric features are more reliable and secure for person recognition than traditional methods based on knowledge or possession. They can be morphological (palmprint, palm vein, (DNA, odor) or bioelectrical (electrocardiogram, electromyogram) [2–5].

2.1. Morphological Features

2.1.1. Hand and Finger Geometry

The human hand has some relatively stable features (e.g., length of fingers) which are peculiar (although not very distinctive) to an individual. They can therefore be used for biometric recognition purposes. The "measurement" of the hand is made up of several measures such as finger dimensions, joint

*Corresponding Author: Abdou-Aziz Sobabe, Email: azizsobabe@yahoo.fr

characteristics, palm and hand shape. Such an identification system studies on average 90 lines of the hand to recognize an individual. The first step of authentication is that of the scan. To do so, the person must put his hand on a platinum. The fingers must be properly placed. etc.), behavioral (voice, signature, gait, keystroke), biochemical. An infrared camera then takes an image from two different angles to obtain a three-dimensional reproduction of the hand. It normally takes no more than three seconds to read. The hand geometry systems have large physical size, so they cannot be easily embedded in existing security systems [6,7]. The hand geometry technology is used for applications such as access control, where one is cocerned about an individual trying to gain access by using someone else's card or PIN. In terms of advantages, the hand geometry authentication technique seems less intrusive than fingerprint registration. In addition, it requires the retention of smaller files compared to a database for comparing fingerprints. For example, scanning an image of a hand is only a space of about 15 bytes while the image of the fingerprint represents a file size of around 500 bytes or more. Finally, external factors such as the moisture of the skin and dirt on the hand do not prevent a good measurement. The same is true for burns and minor cuts. Compared to the fingerprint, this technique has a high rate of false positives. This means that family members with significant physical similarities can easily deceive the system. In addition, the shape of the hands is likely to change due to diseases related to old age, such as arthritis. Furthermore, the geometry of the hand requires a larger scanner than a fingerprint reader. As a result, its use becomes embarrassing when it comes to securing a small object such as a computer [8].

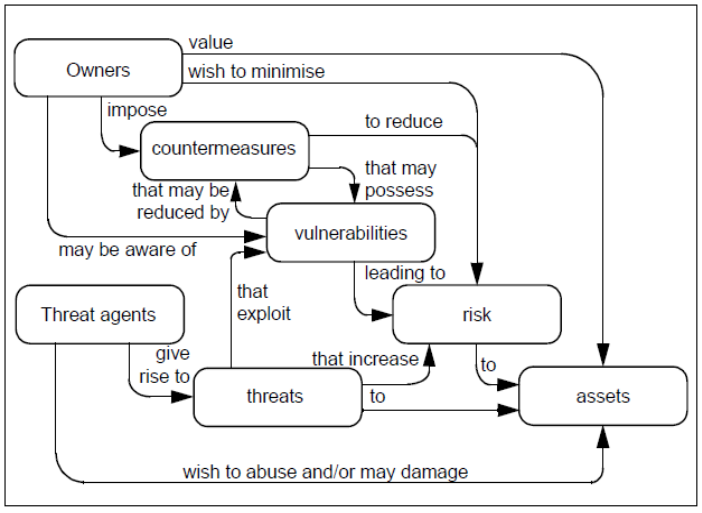

Figure 1: Security procedure [1]

2.1.2. Iris

Iris scan technology is one of the most reliable biometric recognition systems developed recently. The recognition of the iris is a biometric technique to recognize an individual by the observation of his iris. The iris is located in the aqueous humor, it is surrounded by the white of the eye, the pupil is located in its center, the cornea is in front of him and the crystalline behind. The iris corresponds to the colored part of the eye and it is this part that is used in biometrics. Indeed, the texture of the iris (i.e. the pattern of the iris), includes many features. Those most often used in biometrics are stripes, pits, and furrows. These elements of the iris remain fixed, they vary only very little during a lifetime. Each pattern determined by the chaotic processes during embryonic development is stable and unique (the probability of similarity is 1 in 10 power 72) [8,7]. In addition, the pattern of the iris is not genetic in contrast to the color of the eyes. So, two individuals, even if they are parents, can have the same iris color but never the same motive. That's why the iris makes it possible to distinguish the identical twins. Iris-based systems have a very low False Accept Rate (FAR) compared to other biometric traits. Nevertheless, it is important to note that iris systems have a high False Reject Rate (FRR) [6,9]. Iiris sample images quality have an impact on the accuracy of Visible Wavelength iris recognition systems. To deal with this problem, several iris image quality enhancement methods have been developed by researchers. Liu and Charrier [10] evaluated the performance of nine image enhancement approaches on Visible Wavelength iris biometric images. Experimental results showed that three of them (CLAHE, MEDIAN, and UNSHARP) can highly improve the system performance. In contrast, two other methods (SSR and WIENER) have a lower level of performance improvement.

2.1.3. Retina

The retina is the sensory membrane that lines the inner surface of the back of the eyeball. It's composed of several layers, including one that contains specialized cells called photoreceptors (https://www.allaboutvision.com/resources/retina.htm). The elements that distinguish two retinas are the veins that line them. The arrangement of these veins is stable and unique from one individual to another (from one eye to another). And the models that come from inherit the stability of this disposition. The difficulties involved in capturing the image of a retina are as much psychological as medical and technical. To obtain an image of a retina, it is necessary to illuminate the back of the eyeball by means of a light beam. This beam is of very low intensity so as not to disturb the user; it is safe and of lower intensity than on ophthalmic devices. A very precise camera system then comes to recover the image of the retina. Retina readers are available, and provide a very high level of security. After capturing an image of the retina, the reading device software cuts a ring around the fovea. In this ring, it locates the veins and their orientation. It then creates an "eye signature" that is used for retinal recognition. The operation itself is quite simple to describe but the algorithms remain relatively complex.

Retinal biometry provides a high level of recognition. This technology is well suited for high security applications (military sites, safes, etc.). The arrangement of the veins of the retina ensures a good reliability and a high barrier against fraud. [11].

2.1.4. Palmprint

Several authors have researched palm-based biometric recognition. These include [12,11,13]. Palm print recognition is a biometric authentication method based on the unique patterns of various characteristics in the palms of people's hands. It is a relatively new biometric when compared to other biometric systems such as face, fingerprint and iris recognition systems. Palmprint is concerned with the inner surface of a hand. A palm is covered with the same kind of skin as the fingertips and it is larger

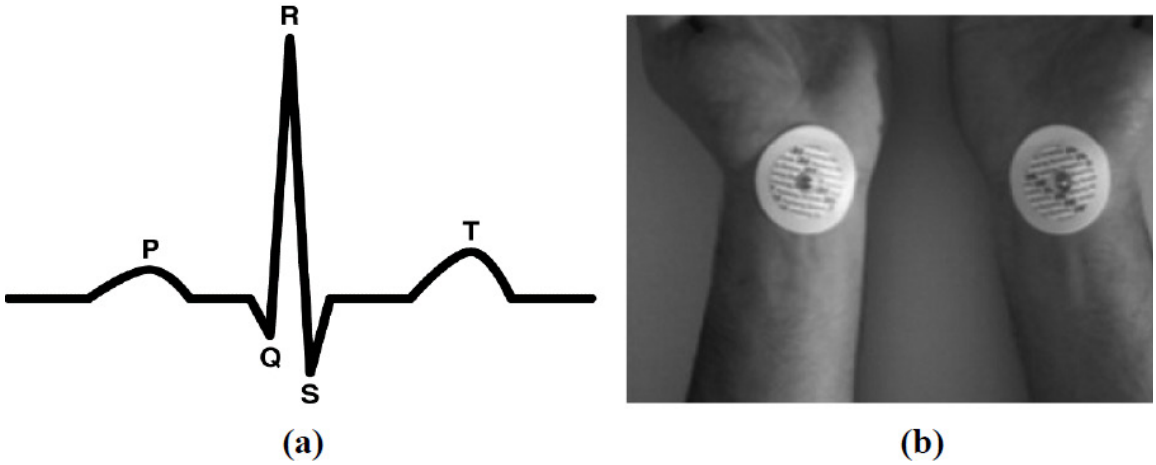

Figure 2: ECG biometrics: (a) ECG signal with regular rhythm (b) positioning of the electrodes on the forearms for ECG capture [14]

than a fingertip in size. Five features of a palmprint are usually used to uniquely identify a person. It is: (a) Geometry Features (such as width, length and area); (b) Principal Line Features (both location and form of principal lines); (c) Wrinkle Features (the thinner and more irregular lines); (d) Delta Point Features (the center of a delta-like region in the palmprint, usually located in the finger-root region) and (e) Minutiae Features (see fingerprint).

Other morphological traits are often used in biometric recognition. Those systems include Palm Vein, Ear and Facial Thermogram. More information can be found in [12,4].

2.2. Behavioral Features

2.2.1. Gait

Gait refers to the way a person walks, and is one of the few biometric traits that can be used to recognize people at a distance. Therefore, this trait is very appropriate in surveillance scenarios where the identity of an individual can be surreptitiously established [11]. Gait-based systems also offer the possibility of tracking an individual over an extended period of time. However, the gait of an individual is affected by several factors including the choice of footwear, nature of clothing, affliction of the legs, walking surface, etc. [9]. This type of biometric recognition system identifies individuals by their posture and the way they walk through unique characteristics that are perceivable at a low resolution, hard to conceal and non-invasive. [8].

2.2.2. Keystroke

Keystroke is a biometric solution "Software Only". It is applied to the password, which becomes much more difficult to "imitate". During the implementation of this technique, the user is asked to enter his password a dozen times in a row. Using an algorithm that exploits the support time on each key and the time between each key, the ten input is "averaged" to build a "typing profile" of the user that will serve as a reference. At the following accesses, the password entry will be coupled to a keying profile that will be compared to the reference profile. The access right is then granted according to the level of similarity of this profile with the reference. Depending on the degree of filtering that an administrator will have defined, this access will be more or less difficult. Whether additional security to an application, a Single Sign On, Intranet or Internet, in addition to security to a personal smart card, it is a solution, reliable, easy to implement and very competitive because without hardware. Its main advantages are related to rapid implementation for many users. It also significantly reduces the need for password changes and solicitation of IT services. As a major drawback, you must be in good condition before using the system at the risk of having your own password refused [8,11].

2.3. Bioelectrical Features or Hidden Features

2.3.1. Electrocardiogram

An electrocardiogram (ECG) is a test that studies how the heart works by measuring its electrical activity. At each heartbeat, an electrical pulse (or "wave") passes through the heart. This wave causes the heart muscle to contract so that it expels the blood from the heart [5]. The ECG is mainly used in clinical applications to diagnose cardiovascular disease. The ECG signal is characterized by the shape of its beats consisting of five typical waves, namely P, Q, R, S, and T or sometimes the U wave (Figure 2) [14]. ECG biometrics has been the subject of a number of studies [15–17]. The use of ECG in biometrics is relatively new. In fact, there are several biometric methods based on the ECG. There are approaches that are based on ECG analysis [18]. Others rely on the integration of analytic and appearance features extracted from ECG signals [19]. Several research studies confirm that the cardiac profile is specific to each individual and does not vary with age or even if the rhythm of the heart is racing after an effort or an emotion. Compared with other biometric modalities, the ECG is more universal and difficult to forge [20].

2.3.2. Electromyogram

Electromyogram (EMG) signals are bioelectrical signals recorded in the muscles. They provide various information on the state of the peripheral nerves. The EMG signal has several clinical applications. Its use as a hidden biometric modality can be particularly interesting. In this context, some recent experiments have been carried out [21,22,19]. In particular, this work has focused on the analysis of surface electromyography (SEMG) signals [23]. When acquiring these signals, individuals are encouraged to apply manual pressure of a constant intensity to a force probe for several seconds (Figure 3) [14]. The signal thus

obtained is analyzed in the spectral domain. Then, parameters are extracted such as the signal strength, the average frequency, the flattening coefficient and the asymmetry coefficient. Indeed, these parameters provide a device vector that we can use to characterize individuals.

In addition, it should be noted that magnetic resonance imaging (MRI) and X-rays are part of the hidden biometric techniques used for the authentication and identification of individuals [24].

3. Applications of Biometrics

The requirements related to the level of development of humanity and the security constraints require a rapid and reliable user authentication. Biometrics is an emerging field where technology improves man ability to identify a person [25]. The applications of biometrics can be divided into three main groups [26,13,27]:

- Commercial applications involve computer network access, electronic data security, e-commerce, Internet access, credit card, physical access control, cell phone, medical records management, remote study, etc One of the most popular technologies for ECG-based biometrics is the HeartID developed by researcher Foteini Agrafioti of the Canadian University of Toronto. This technology can be integrated into any electronic device, starting with smartphones, tablets or game consoles. The idea is to offer both an identification system to secure this type of device, but also to share them by activating user profiles opening on specific settings and contents. The sensors can be implanted so that the user only has to hold the terminal so that his heart rate is analyzed by the recognition algorithm, the identification taking about 1.2 seconds. A preliminary learning phase is necessary to record the electrocardiogram whose profile can then be stored in the terminal itself or on a database to which it will connect. Only requirement, the user must hold the terminal with both hands so that the signal can be captured because the electrocardiogram results from an electrical activity requiring two reference points on either side of the heart.

Another application of ECG-based biometrics is the Nymi bracelet developed by the Canadian company Bionym. This bracelet is able to detect the electrical signals emitted by the heart to control the identity of the wearer. Once identified, the owner can open his car, unlock his laptop or phone, or make payments such as with a credit card. With each electrical impulse, the heart will contract, and produce regular beats (between 60 and 80 per minute at rest). It is by analyzing this "cardiac signature" that the Nymi bracelet can identify its owner then, through a Bluetooth connection, interact with electronic devices to enter a PIN or unlock a user session.

- Government applications include national identity card, driver's license, social security, border control, passport control, voter registration, etc. For example, the Government of Benin has created a Permanent Electronic Electoral List, the first draft of which was put online in January 2015. Since then, it has served as a basis for the various elections held in the country. The Schiphol Privium device at Amsterdam Airport uses an iris sensor to speed up the process of checking passports and visas.

- Forensic applications include body identification, criminal investigation, terrorist identification, parenthood determination, missing children etc. The Federal Bureau of Investigation (FBI) of the US Department of Justice utilizes the Integrated Automated Fingerprint Identification System (IAFIS), a 10-fingerprint matching system that captures rolled prints. In 2008, the Chinese Police adopted an Integrated Automated Biometric Identification System (IABIS) solution to allow forensic fingerprint examiners the ability to cross check inmate identities for possible matches within the database [28].

4. Typology of Metadata

Metadata or ancillary information is non-biometric data that is either combined with pure biometric data (fingerprint, face, iris, signature, etc.) or exploited by a system that makes biometric adaptation. The goal of adaptation is to provide ways to deal with the challenges of biometric systems.

In general, there are two main methods for adapting biometric systems, the first link to the user (soft biometrics) and the second link to the acquisition system. In the first case, there are a multitude of traits from the user that can be extracted and combined with pure biometric modalities. Jain et al. were among the first to explore this area. They did experiments on the following traits: Height, gender, ethnicity. Later, Dantcheva et al. [29] conducted a study on several soft biometric traits such as: age, skin color, hair color, eye color, marks, etc.

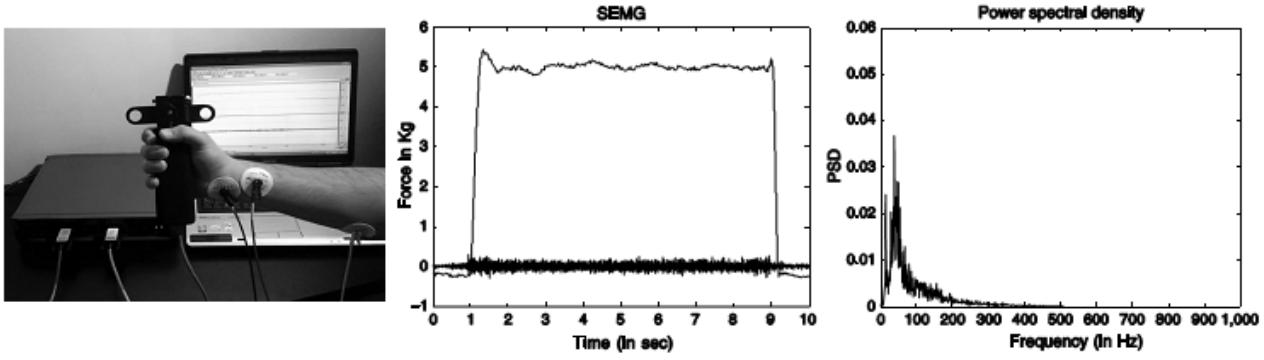

Figure 3: EMG biometrics: (a) Acquisition of an EMG signal (b) The intensity applied by the user and the relative EMG (c) EMG periodogram [14]

It should be noted that depending on the authors, certain traits are classified either as pure biometric modalities or as soft biometrics. This is the case of the gait which is sometimes considered as a behavioral modality [8] and sometimes as a trait of soft biometrics [29].

At the level of the acquisition system, adaptation can be done on the one hand at the sensor (volume, flash, etc.) and on the other hand taking into account the context of implementation (brightness, noise, etc.). Here, the metadata are not directly merged with the pure biometric data. The consideration is made at two levels. Either the system administrator makes adjustments to the various parameters such as volume, ambient brightness, flash, etc. On the other hand, the acquisition device is pre-sized to ensure automatic control of these different parameters. Such a device will be smart enough not to trigger for example a facial image when the brightness is not at a minimum required.

Several studies have focused on the role of metadata in improving biometric performance. In [30], the authors show the benefits of using gender, ethnicity and height information of the user in addition to fingerprint. The use of these soft biometric data leads to an improvement of approximately 5% over the main biometric system. [29] spoke of similar results which reduced the total error rate to 1.5% from 3.9% when body weight score is fused with fingerprint score. The table 1 below presents a typology of metadata in the biometric adaptation.

In the next section, special emphasis will be placed on the effect of metadata in the fight against biometric vulnerabilities.

5. Role of Metadata in Facing Biometric Challenges and Vulnerabilities

The challenges of biometric systems are essentially at the level of limits in terms of performance and acceptability. In addition, biometric authentication faces vulnerabilities that have been identified at eight levels on a generic biometric architecture [31]. Figure 4 shows the eight possible locations of attacks in a generic biometric system. [32] then listed a total of four different levels of biometric system vulnerabilities. These are intrinsic failure, administration issues, non-secure infrastructure, and biometric overtness. The last three levels have been grouped into adversary attacks from outside the system. These four levels of vulnerability were synthesized through a fish-bone model (see Figure 5).

5.1. Intrinsic Failure

An intrinsic failure is a biometric system security failure that generates an incorrect decision taken in a native way ie without without the intervention of an external element. It can occur even in the absence of an explicit effort by an attacker to bypass the system. This type of failure is also known as "zero-effort-attack". A biometric verification system can make two types of errors in decision making. These are false acceptances and false rejections. In the first case, false acceptances are usually caused by a lack of uniqueness in the biometric trait, which can lead to a great similarity between the characteristics of different users. At this level, adding metadata can be effective in combating this problem. Among the most probable cases, there are those of two identical twins or brothers who have a perfect similarity of the face for example. Taking into account soft biometric data such as marks and make-up will make it possible to distinguish between two individuals even if they have exactly the same face because the face recognition algorithms do not take into account these accessory data.

A legitimate user may be falsely rejected by the biometric system because of the large differences between the user's stored model and the input biometric feature sets. These intra-user variations may be due to an incorrect interaction of the user with the biometric system. This is the case, for example, of the effect of twists on a fingerprint image or the effect of the changes of pauses on a face image. Metadata do not provide a specific solution for these cases of intra-user variations. But increasingly, the biometric verification algorithms take into account these issues. [33] have proposed a contactless fingerprint recognition algorithm that addresses this issue. On another level, it should be noted that the false rejections can be due to noise introduced at the sensor such as, for example, the residual traces left on a fingerprint sensor. Metadata does not provide a solution to this limit. Multimodal

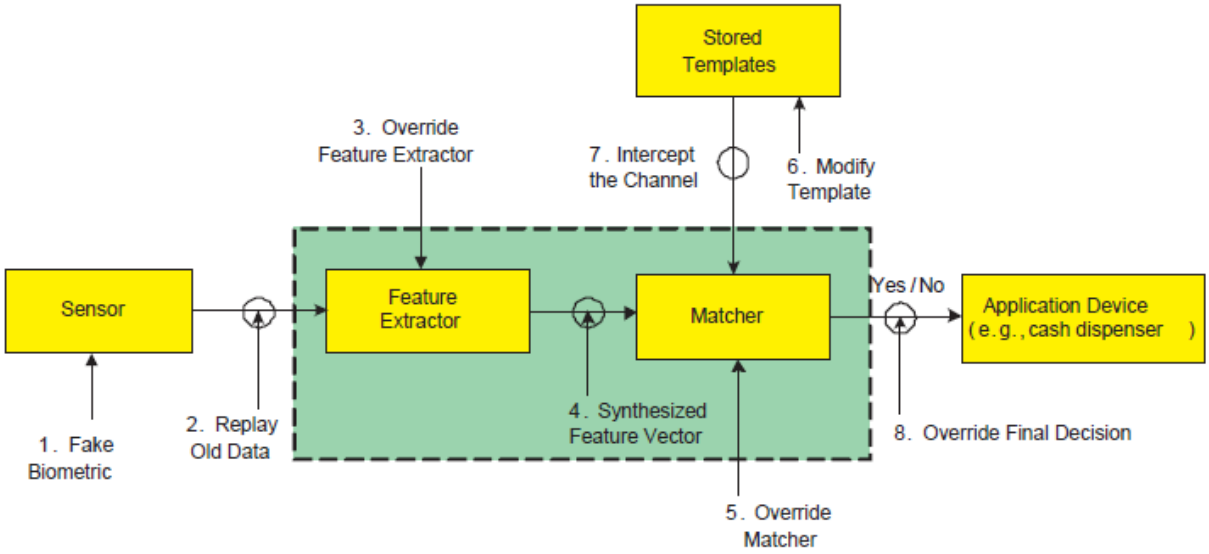

Figure 4: Possible locations of attacks in a generic biometric system [32]

biometrics offers an alternative to false rejects. Indeed, when one of the modalities is affected of noise, the system is able to ignore it and pass to the following modality.

For the limits related to the detection technology, the exploited metadata can be the volume (case of the voice modality) or the flash (case of the face, the contactless fingerprint, etc.). Finally talking about limits in the context of implementation, parameters such as brightness, noise, and temperature are used as metadata to deal with intrinsic errors.

5.2. Adversary Attacks

An adversary intentionally launch an attack on the biometric system by exploiting a multitude of loopholes in the system design. The three possible forms of attack are: Administration attacks, non-secure infrastructure attacks, and biometric overtness attacks.

5.2.1. Administration Attack

This attack is still called insider attack. It usually comes from malicious, familiar people who exploit vulnerabilities created by poor biometric system administration. These include (i) the integrity of the registration process (for example, the validity of credentials submitted during registration), (ii) collusion (or coercion) between the opponent and the system administrator or a legitimate user and (iii) abuse of exception handling procedures. Under these conditions, the use of metadata will not provide a response to this type of attack in the absolute. On the other hand, the additional use of soft biometric traits can make the system more complex and require more effort on the part of the attacker.

5.2.2. Non-Secure Infrastructure

The infrastructure of a biometric system includes the hardware, software and communication channels between the different modules. An opponent can manipulate the biometric infrastructure in several ways, which can lead to eight security breaches as described below.

First level:

Falsified biometric data: A reproduction of the biometric data used will be presented to the biometric sensor. In the case of authentication by the fingerprint, the attacker can present a false finger facing a contact-based sensor or just have the image of a finger facing a contactless sensor. It should already be noted that this form of attack is more common with the fingerprint which is a widely used modality with a high discriminatory power. On the other hand with other modalities such as face, retina, and signature, it is more difficult to present a falsified data. Moreover, if the biometric system integrates a soft biometric feature to be combined with pure biometric modality, this form of attack becomes more complicated to implement. Take for example a case of fingerprint authentication associated with the height of the user. Even if the fingerprint is falsified, the impostor will be stucked during the enrollment of the height. Considering another case of face authentication combined with the skin color automatically extracted from the facial image, an impostor will have a hard time tampering with a face while taking into account the specificities and requirements related to the detection of the skin color.

Second level:

Transmission of intercepted biometric data: Here, the attacker plays back an old biometric data stored in the system without passing through the biometric sensor. This is the case with the presentation of an old copy of the fingerprint image. Since the attacker bypasses the biometric sensor by providing the system with an old recorded data, the metadata will have no effect against this form of attack.

Third level:

Attack on the feature extraction module: This module could be replaced by a Trojan horse so as to produce information chosen by the attacker. The legitimate user does not realize that this module has been corrupted and provided information in accordance with the hacker's instructions. The feature extraction module being compromised by the hacker, the metadata will not be effective against this kind of attack.

Fourth level:

Alteration of extracted features: After data is obtained by the feature Extraction Module, it is altered or even replaced by other data defined by the attacker. For non-secure infrastructure attacks, from the second level of attack to the eighth level, we are in situations where the biometric system is corrupted and will only provide responses according to the intent of the hacker. Metadata will not be effective in these contexts.

Fifth level:

The matching module is replaced by a malicious module: This module could be replaced by a Trojan horse to artificially produce high or low scores.

Sixth level:

Database corruption: The database of biometric templates is available locally, remotely or distributed on multiple servers. In this type of attack, the attacker modifies one or more models to allow an impostor or even to prevent a legitimate user from accessing it.

Table 1: Typology of metadata in biometric adaptation

Level of adaptation	User	Acquisition system	
Type of adaptation	Soft biometric	Sensor	Context
Example	Marks; Make-up; Age; Weight	Volume (microphone); Flash (camera)	Brightness, noise, temperature
Exploited data	Metadata		
Training need	Without training (immutable)		After training

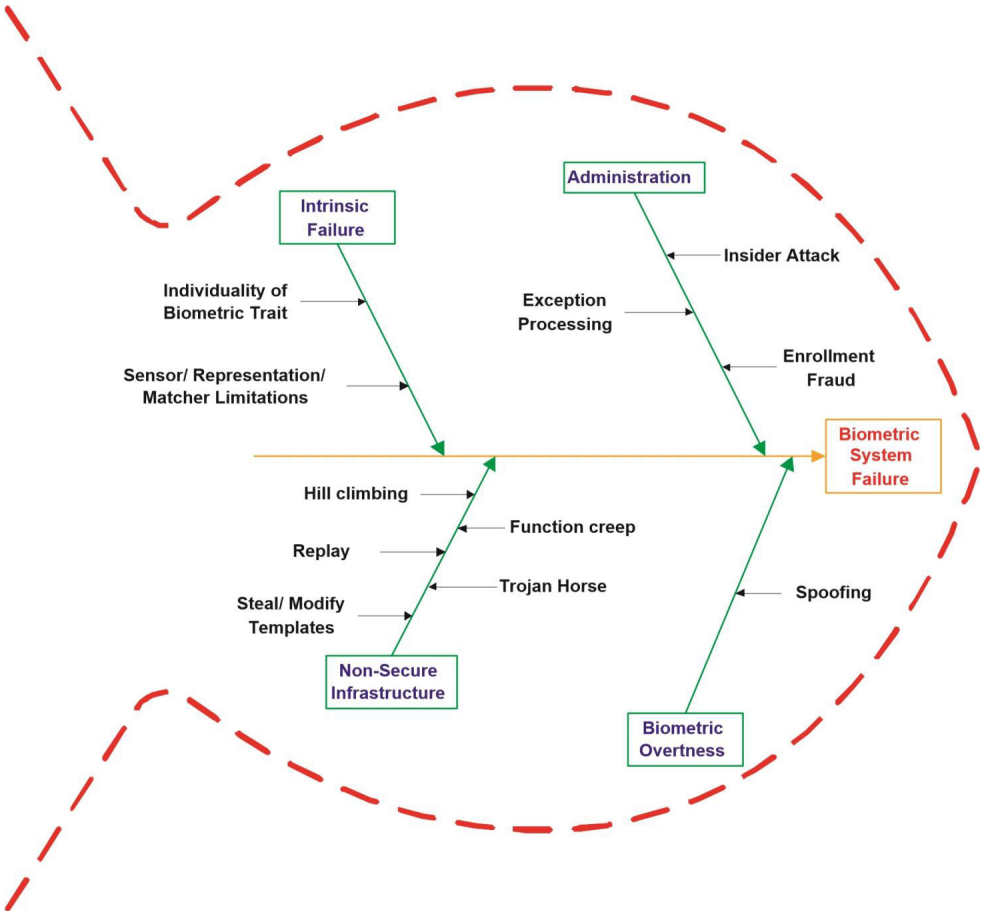

Figure 5: Fish-bone model for categorizing biometric system vulnerabilities [32]

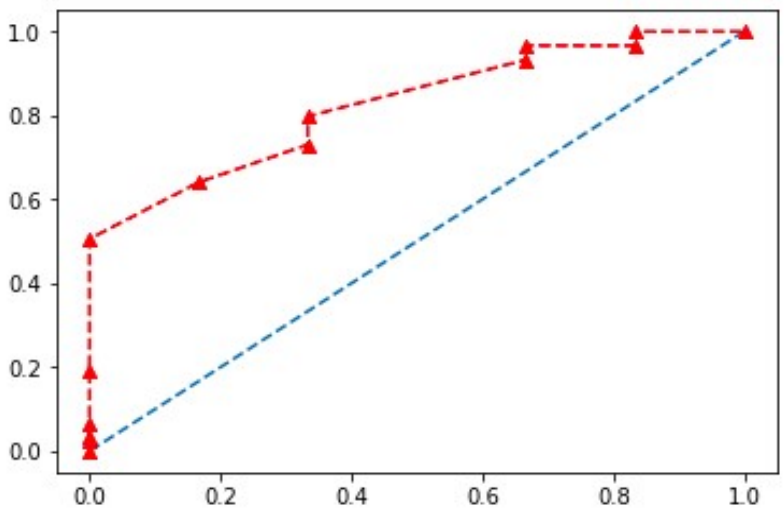

Figure 6: ROC curve with AUC: 0.826

Seventh level:

Attack on the channel between the database and the matching module: In this type of attack, the models are altered on the transmission link connecting the model base and the matching module.

Eighth level:

Alteration of decisions (accepted or rejected): This type of attack alters the boolean decision (yes or no) made by the decision module. The danger of this attack is high because even if the system is robust in terms of performance, it was rendered useless by this type of attack.

5.2.3. Biometric Overtness

An attacker may discreetly acquire the biometric characteristics of a legitimate user and use them to create an artificial production of the biometric feature (fingerprints taken from the surface of a contact-based sensor). Therefore, if the biometric system is not able to distinguish between a live biometric presentation and an artificial parody, an opponent can circumvent the system by presenting falsified traits. This case perfectly matches the first level of attack on non-secure infrastructure. The analysis performed at this level is also valid here. It should be noted that soft biometrics represents a response to this form of attack for two reasons. Indeed, the user is obliged to appear in person in front of the data acquisition device or this data is automatically extracted from a pure biometric modality having a number of characteristics hardly respectable by the artificial productions.

The table 2 below summarizes for each vulnerability category the existence of effects as well as the possible actions of the metadata. Examples of usable metadata have been listed at different levels in order to provide more probable scenarios of integration of multi-biometric metadata using a variety of disparate fusions of traits.

6. Skin Color as a Solution to Overtness in Face Authentication

6.1. Materials and Methods

The objective of this section is to present a practical case of adding metadata to a pure biometric modality in order to fight against certain vulnerabilities. The materials and methods used are among the most recent technologies in progress. The implementation of the proposed system was carried out under Python framework with the OpenCV package (https://sourceforge.net/projects/opencvlibrary/). Two stages are to be considered in accordance with the two modalities that are the face and the skin color (of the face). First, we performed face recognition using the LBPH (Local Binary Pattern Histogram) algorithm [34]. Then, for authentication by skin color, the Haar Cascade algorithm [34] made it possible to detect the face, while the extraction of the dominant skin colors was carried out automatically using the algorithm of the K-means [35]. Only one database was used; it is the Caltech faces database (http://www.vision.caltech.edu/html-files/archive.html). This database contains 450 images of faces of size 896x592 in JPEG format for 27 unique people with a variable number of images. For experimental purposes, we have resized the database to 19 people with 17 images each. 12 images were used to form the model and 5 images were used for the tests.

6.2. Experimental Results

After implementing these two modalities, the matching scores obtained were merged using the weighted sum method. A weight of 0.9 was assigned to the modality of pure biometrics (face) while the modality of soft biometrics (skin color) received a weight of 0.1. The experimental results are satisfactory with a performance of 82.6% for the facial system and 90.8% for the multimodal system. Figures 6 and 7 respectively show the results (ROC curve) of the face alone and of the face combined with the skin color.

6.3. Discussion

The inclusion of metadata in face authentication allows on the one hand to improve recognition performance and on the other hand to make the system less vulnerable. The calculation of the processing time for the two modalities gave the following results. For the face, the average processing time (for 15 images) is 1.24 s. The average time for skin color is 7.21 s. The fusion of the facial and skin color scores takes an average time of 1.52 s (always for the 15 images). It should be noted that the total processing time of the multimodal system increases due to two factors, namely the extraction time of the skin color and the time taken to merge the two scores. This confirms once again that each biometric authentication system has its advantages and limits. These are the application cases and the implementation conditions which generally determine the choices to be made.

7. Conclusion and Future Work

This paper presented a detailed typology of metadata on multi-biometric system vulnerabilities. We have provided an overview of some non-current biometric sensing systems before dealing with the applications and privacy issues. Furthermore, we discussed the categorization of biometric metadata, namely user level (ie soft

Table 2: Typology of metadata on biometric system vulnerabilities

Vulnerability category	Intrinsic failure	Adversary attacks		
		Administration Attack	Non-secure infrastructure	Biometric overtness
Existence of metadata effect	Yes (except the case of false rejects)	Partial	Yes (1 case out of 8)	Yes
Possible actions	1- Reduce false acceptances 2- Limit FTE and FTA	Make the system harder to attack	Prevent attack by presenting falsified biometric data	Prevent attack by presenting falsified biometric data
Example of metadata	1- Marks (tattoos, scars, etc.); make-up 2- Volume, flash; Brightness, noise, temperature	Weight, body shapes, etc.	Height, eye color, etc.	Gait, gender, skin color, etc.

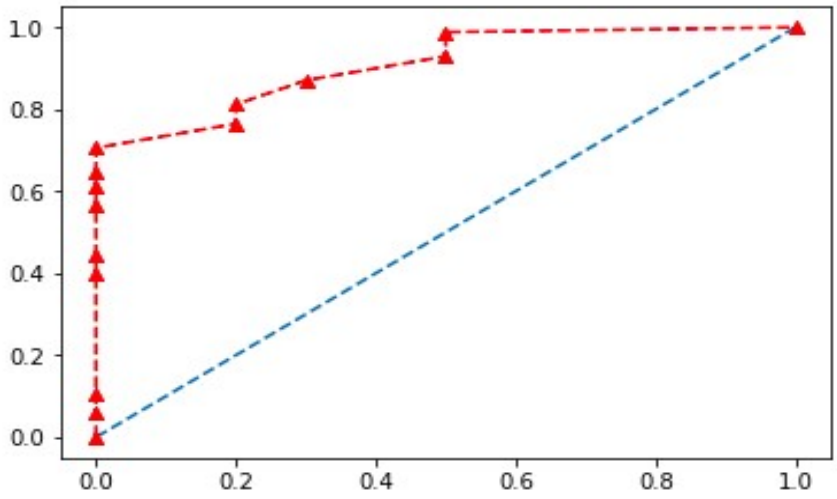

Figure 7: ROC curve with AUC: 0.908

biometric) and acquisition system level (ie sensor and acquisition context). To finish, a practical case of adding metadata to a pure biometric modality have been presented in order to fight against face recognition vulnerabilities.

Contactless fingerprint authentication [33] is a promising technique but one that is potentially vulnerable on several levels. For future work, we will explore the role of metadata in addressing contactless fingerprint vulnerabilities.

References

[1] [Common Criteria, 2012] Common Criteria for Information Technology Security Evaluation ; Part 1: Introduction and general model ; September 2012 ; Version 3.1 ; Revision 4

[2] M. Nageshkumar, P.K. Mahesh, and M.N. Shanmukha Swamy, "An efficient secure multimodal biometric fusion using palmprint and face image," International Journal of Computer Science Issues, Vol. 2, pp 49-53, 2009, arXiv:0909.2373v1.

[3] A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," Elsevier, Pattern Recognition 38, pp 2270-2285, 2005, DOI:10.1016/j.patcog.2005.01.012.

[4] R. Gad, A. El-Sayed, N. El-Fishawy, and M. Zorkany, "Multi-biometric systems: A state of the art survey and research directions," International Journal of Advanced Computer Science and Applications, Vol. 6, No. 6, pp. 128-138, 2015, DOI : 10.14569/IJACSA.2015.060618.

[5] S. N. Abbas, M. Abo–Zahhad, S. M. Ahmed, M. Farrag, "Heart-ID: human identity recognition using heart sounds based on modifying melfrequency cepstral features," © The Institution of Engineering and Technology, IET Biom., Vol. 5, Iss. 4, pp. 284-296, 2016, doi: 10.1049/iet-bmt.2015.0033.

[6] A.K. Jain and A. Kumar, "Biometric recognition: An overview," Chapter 3, © Springer Science + Business Media B.V., pp 49-79, 2012, DOI 10.1007/978-94-007-3892-8_3.

[7] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, © Springer-Verlag London Limited, 2009.

[8] M. O. Oloyede and G.P. Hancke, "Unimodal and multimodal biometric sensing systems: A review," IEEE Access, Volume 4, pp 7532-7555, 2016, Digital Object Identifier: 10.1109/ACCESS.2016.2614720.

[9] A. Ross, K. Nandakumar, and A.K. Jain, Handbook of Multibiometrics, Springer, New York, USA, 1st edition, 2006.

[10] X. Liu and C. Charrier, "Can image quality enhancement methods improve the performance of biometric systems for degraded visible wavelength iris images?," BioSMART 2019 Proceedings, 3rd International Conference on Bio-engineering for Smart Technologies, Paris, 24th-26th April pp. 119-122, 2019, 978-1-7281-3578-6/19/$31.00 ©2019 IEEE.

[11] H. AlMahafzah and M.Z. AlRwashdeh, "A survey of multibiometric systems," International Journal of Computer Application, volume 43 No 15 April, pp 36-43, 2012, DOI : 10.5120/6182-8612.

[12] D. Cherifi, R. Kaddari, H. Zair, and A. Nait-Ali, "Infrared face recognition using neural networks and HOG-SVM," BioSMART 2019 Proceedings, 3rd International Conference on Bio-engineering for Smart Technologies, Paris, 24th-26th April, pp. 132-136, 2019, ©2019 IEEE, 978-1-7281-3578-6/19/$31.00.

[13] A.K. Jain, P.J. Flynn, and A. Ross, Handbook of Biometrics, © Springer Science + Business Media, LLC, 2008.

[14] H. Toufik, "Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne," Ph.D Thesis, Badji Mokhtar University-Annaba, 2016.

[15] Q. Zhang, "Wavelets networks: The radial structure and an efficient initialization procedure," Technical Report of Linköping University, 1992, LITH-ISY-I-1423.

[16] J. Sjöberg , Q. Zhang, L. Ljung, A. Benveniste, B. Deylon, P.Y. Glorennec, H. Hjalmarson, and A. Juditsky, "Nonlinear black-box modeling in system identification: Unified overview," Automatica, Vol.31, no.12, pp.1691-1724, 1995.

[17] A. Juditsky, "Wavelet estimators: Adapting to unknown smoothness," Technical Report IRISA, June 1994.

[18] Q. Zhang, "Using Wavelet Network in Nonparametric Estimation," Publication Interne 833, IRISA, June 1994.

[19] Q. H. Zhang, "Using Wavelet Network in Nonparametric Estimation," IEEE Trans.Neural Networks, Vol.8, pp.227-236, 1997.

[20] S. Chantaf, "Biométrie par signaux physiologiques," Ph.D Thesis, Université Paris-Est, 2011.

[21] J. Zhang, G. G. Walter, Y. Miao, and W. N. W .Lee, "Wavelet Neural Networks for function learning" IEEE Trans. signal process, Vol.43, No.6, pp.1485-1497, June 1995.

[22] S. Mallat, "A theory for multiresolution signal decomposition: The wavelet transform," IEEE Trans. Pattern Anal. Machine Intell., Vol.11, pp.674-693, July 1989.

[23] N. Draper and H. Smith, "Applied regression analysis, Series in Probability and Mathematical Statistics," Wiley, 1981, Second edition.

[24] A. Nait-ali, "Hidden biometrics: towards using biosignals and biomedical images for security applications," 7th international Workshop on Systems, Signal Processing and their Applications, Invited paper, Tipaza, pp. 352–356, 2011, DOI: 10.1109/WOSSPA.2011.5931509.

[25] L. Allano, La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles, PhD thesis, Institut National des Télécommunications dans le cadre de l'école doctorale SITEVRY en co-accréditation avec l'Université d'Evry-Val d'Essonne, 2009.

[26] A.K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on circuits and systems for video technology, vol. 14, no. 1, January, pp 4-20, 2004, DOI: 10.1109/TCSVT.2003.818349.

[27] S. Guerfi, "Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D," PhD thesis, Université d'Evry-Val d'Essonne, 2008.

[28] T. K. Ho, J. J. Hull, and S. N. Srihari, "Decision combination in multiple classifier systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, 16(1), January 1994, pp 66–75, DOI: 10.1109/34.273716.

[29] A. Dantcheva, C. Velardo, A. D'Angelo, J. L. Dugelay, Bag of Soft Biometrics for Person Identication : New trends and challenges, Multimed Tools Appl 51, © Springer Science+Business Media, LLC 2010, pp. 739–777, 2011, https://doi.org/10.1007/s11042-010-0635-7.

[30] A.K. Jain, K. Nandakumar, X. Lu, U. Park, "Integrating faces, fingerprints, and soft biometric traits for user recognition," Proceedings of Biometric Authentication Workshop, LNCS 3087, Prague, pp. 259-269, May 2004, DOI:10.1007/978-3-540-25976-3_24.

[31] M. El-Abed, C. Charrier, "Evaluation of biometric systems," chapter 7. In: New Trends and Developments in Biometrics, pp. 149–169, 2012, https://doi.org/10.5772/52084.

[32] A.K. Jain, K. Nandakumar, A. Nagar, "Biometric template security," in EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, pp 1-20, January 2008, DOI:10.1155/2008/579416.

[33] T. Djara, M.K. Assogba, and A. Vianou, "A contactless fingerprint verification method using a minutiae matching technique," International Journal of Computer Vision and Image Processing, Volume 6, Issue 1, pp 12-27, January-June 2016, DOI: 10.4018/IJCVIP.2016010102.

[34] L. Dinalankara, "Face detection and face recognition using open computer vision classifiers", Robotic Visual Perception and Autonomy, Faculty of Science and Engineering, Plymouth University, august 4, 2017.

[35] C. C. Aggarwal, C. K. Reddy, Data clustering : algorithms and applications, Taylor & Francis Group LLC, 2014.