Incorporating Metadata in Multibiometric Score-Level Fusion: an Optimized Architecture

Tahirou Djara, Abdou-Aziz Sobabe, Antoine Vianou

This manuscript presents a review on multibiometrics using ancillary information, in addition to the main biometric data. The proposed method involves taking non-biometric information into account in the biometric recognition process to improve system performance. This ancillary information can come from the user (the skin color), the sensor (the camera flash, etc.) or the operating environment (the ambient noise). Moreover, the paper presents an extension of the adapted sequential fusion framework through a complete description of the method used for the score-level fusion architecture presented at the IEEE BioSmart 2019 Proceedings. An optimized score-level fusion architecture is proposed. An introduction of new concepts (namely "biochemical features" and "multi origin biometrics") is also made. The first part of the paper highlights the various biometric systems developed up to now, their architecture and characteristics. Then, the manuscript discussed about multibiometrics through its advantages, its diversity and the different levels of fusion. An attention was paid to the score-level fusion before addressing the consideration of ancillary information (or metadata) in multibiometrics. Dealing with the affective computing, the influence of emotion on the performance of biometric systems is explored. Finally, a typology of biometric adaptation is discussed. As an application, the proposed methodology will implement a multibiometric system using the face, contactless fingerprint and skin color. A single sensor will be used (a camera) with two shots while the skin color will be extracted automatically from the facial image.

Keywords **:** ***Authentication, Biometrics, Biometric Adaptation Typology, Multi Origin Biometrics.***

I. INTRODUCTION

There are two traditional ways to verify the identity of an individual. The first method is knowledge-based. This knowledge corresponds, for example, to the password used for accessing a secured WiFi network or at the start of a Windows session, the PIN (Personal Identification Number) code for unlocking a Smartphone. The second method is based on a possession (possession-based). It can be an ID card, a key, a badge, etc. [1], [2]. These two modes of authentication can be used in a complementary manner to obtain an increased safety (e.g. a credit card). However, they have their respective weakness. In the first case, the password can be forgotten by its user or guessed by another person. In the second case, the badge (or ID card or key) may be lost or stolen. Table-I below shows the limits of traditional authentication systems. To overcome the problems of traditional methods, biometrics has been introduced as an alternative method for person authentication. It consists of determining or verifying an individual's identity basing on his physiological or behavioral features (https://www.biometrie-online.net/biometrie/c-est-quoi-la-biometrie) [3], [4].

Table- I: The limits of traditional authentication systems

Authentication systems	Copy	Theft	Forgetting	Loss
Key	✓	✓	✓	✓
Badge	-	✓	✓	✓
ID Card	-	-	✓	✓
Password or PIN Code	✓	-	✓	-

These features, whether innate like fingerprints or acquired as keystroke, are attached to each individual and therefore do not suffer from any weakness of the traditional methods. Thus, biometric recognition is based on what we are or how we behave (being-based or behavior-based) [1]. Etymologically, the word biometrics means "measure + life" or "measure of life", and designates in a very broad sense the quantitative study of living beings [2]. El-Abed and Charrier [5] assert that biometrics is originally Greek, "bios" and "metron", literally meaning "measurement of life". The emergence of biometrics dates to the 19th century (http://www.dagnelie.be/docpub/dagnelie-1988a.pdf).

II. Overview of the Different Biometric Features

Biometric features can be physiological (face, facial thermogram, fingerprint, DNA, retina, iris, hand venous network, hand geometry, odor, ear shape, Electro Cardiogram -ECG-, etc.) or behavioral (voice, signature, gait, keystroke) [3], [4], [6]. The physiological traits can be divided into two kinds namely morphological (face, facial thermogram, fingerprint, retina, iris, hand venous network, hand geometry, ear shape, etc.) and biological (e.g DNA, odor, ECG) [7]. Since odor is more a chemical modality, we suggest talking about biochemical modalities. Some features are considered to be in the middle of morphology and behavior. This is for example voice and gait [8], [2]. Somme common biometric features are shown in Fig. 1, classified into three categories.

Revised Manuscript Received on November 08, 2019.

***** Correspondence Author

Tahirou DJARA, Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC). Institut d'Innovation Technologique (IITECH), Email: csm.djara@gmail.com

Abdou-Aziz Sobabe*, Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC). Institut d'Innovation Technologique (IITECH), Email: azizsobabe@yahoo.fr

Antoine VIANOU, Laboratoire d'Electrotechnique de Télécommunication et d'Informatique Appliquée (LETIA/EPAC), Université d'Abomey-Calavi (UAC). Institut d'Innovation Technologique (IITECH), Email : avianou@yahoo.fr

These morphological, behavioral and biochemical characteristics that identify an individual are referred to as traits, features, indicators, identifiers or modalities.

A. Morphological features

1) Face

Naturally, the first modality used by individuals to identify themselves is the face [8], [2]. Thus, automatic face recognition methods have been introduced and are among the most used in biometrics today. Guerfi conducted a study on face authentication [9]. She claimed that Automatic Face Recognition is performed in three main steps: (1) face detection, (2) extraction and normalization of facial features, (3) identification and / or verification. Several research works have led to the development of a multitude of techniques ranging from simple face detection, to the precise location of the characteristic regions of the face, such as the eyes, the nose, the nostrils, the eyebrows, the mouth, lips, ears, etc. Extraction of features such as eyes, nose, mouth is a pre-treatment step required for facial recognition [10]. We can distinguish two different practices: the first is based on the extraction of entire regions of the face; it is often implemented with a global approach to face recognition. The second practice extracts particular points from different characteristic areas of the face, such as the corners of the eyes, mouth and nose. Jain et al. have made a review of several face recognition algorithms. More recently, Chihaoui et al. [11] have presented a survey of 2D face recognition techniques. These different authors classified the face recognition algorithms into two broad categories: feature-based methods and appearance-based methods. Popular algorithms such as Eigenfaces or PCA (Principal Components Analysis), Fisherfaces or LDA (Linear Discriminant Analysis), ICA (Independent Components Analysis), LFA (Local Feature Analysis), Correlation Filters, Manifolds and Tensorfaces are based on the appearance of the face. However, EBGM (Elastic Bunch Graph Matching), NN (Neural Network) and SVM are based on face features. The main difficulties of face recognition are at two levels. These are inter-subject and intra-subject variations.

The traditional 2D image acquisition mode can work from a distance and not require significant user cooperation. But this technic has some imagery problems such as pose and lighting variation. To overcome these problems, 3D face recognition has gained attention in the face recognition community. Compared to a traditional classification scheme, 3D-based face recognition systems make it possible to improve the classification performance [8]. To avoid illumination change problems in face recognition, the infrared face recognition is more and more studied. Cherifi et al. [12] developed an infrared face recognition system using two methods. The first method used Histogram of Gradient (HOG) for feature extraction and SVM for classification while the second method used a neural networks algorithm, namely the Backpropagation algorithm. Experimentations showed that Backpropagation could classify the test set with 100% accuracy using only a few data. HOG-SVM method is also able to classify with a high accuracy.

Nowadays, one of the most reliable face recognizer is the Local Binary Patterns Histograms(LBPH) [13]. It introduces precision with the data and lucidity in identifying the correct face.

2) Fingerprint

The fingerprint-based human identification technique is the oldest of the recognition methods. It is also the most efficient and most used for more than a century, due among other things to its uniqueness and consistency overtime. [14],10]. Fingerprint matching techniques can be classified into three categories, namely minutiae-based matching, image-based matching and hybrid matching technique [15]. Minutiae-based matching essentially consists of finding the alignment between the pre-registered template and the input minutiae trait sets that result in the maximum number of minutiae pairings. Image-based matching system is used to compare two fingerprint images by superimposing the images.

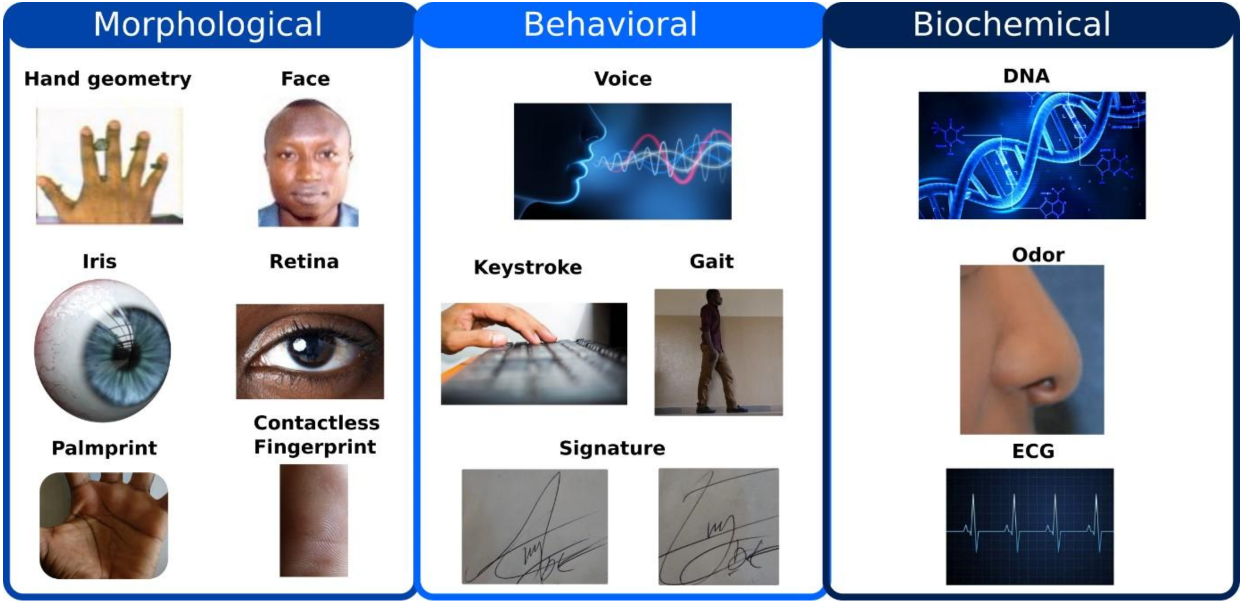

Fig. 1: Some common biometric modalities

The global pattern of ridges and valleys of a fingerprint are the main focus in this algorithm, where the grey-level information of the image is directly used [16]. Traditional contact-based are also source of hygiene problems (spread of epidemics) and safety (risk of chemical attacks). For all these reasons, contactless 2D [15] and contactless 3D [17] fingerprint acquisition systems were introduced recently.

B. Behavioral features

1) Voice

Voice identification is considered by users as one of the most normal forms of biometric technology because it is not intrusive and requires no physical contact with the sensor. Voice analysis technology (also called speaker analysis) is successfully applied where other technologies are difficult to use. It is used in areas such as call centers, banking, access to accounts, on home PCs, for access to a network or for legal applications. The fact that an authentic voice can be recorded and used by an imposter for unauthorized authentication is an important disadvantage of the voice recognition system. Despite all these difficulties, the voice remains an interesting biometric means to exploit because convenient and available via the telephone network, unlike other biometric features [14].

2) Signature

A signature is a handwritten name or nickname, a draw or any mark that is stylized to be unique to an individual. This type of biometrics is currently little used but its defenders hope to impose it quickly enough for specific applications (electronic documents, reports, contracts ...). The process is usually combined with a graphic palette (or equivalent) provided with a pen. This device will measure several characteristics during the signature, such as speed, order of strikes, pressure and accelerations, total time, etc. In short, everything that can identify a person in the most secure way possible when using data as changing as the signature. We have two classes of signature verification methods, according to the input signature information: on-line and off-line. On-line method refers to the use of the time functions of the dynamic signing process (e.g., position trajectories, or pressure versus time), which are obtained using acquisition devices like touch screens or digitizing tablets. Off-line method refers to the use of the static image of the signature. [2].

C. Biochemical features

1) DNA

Deoxyribonucleic acid or DNA is a biological macromolecule present in all cells. It can be used as a very stable biometric feature for human identification and authentication. Jain and Kumar assert that the DNA structure of every human is unique, except from identical twins, and is composed of genes that determine physical characteristics such as eye or hair color [10]. Profiles can be generated from buccal swab, biological stains or cells, typically stains of blood, saliva, urine or semen, from hairs (with roots) and from skin cells (left by mere contact e.g. such as a finger mark). Bioinformatics involves the manipulation, search and exploration of biological data, which includes DNA sequences. The development of techniques for storing and searching for DNA sequences has led to advances in computer science widely used elsewhere, particularly with regard to sub-string search algorithms, machine learning and database theory. To cap it all, the DNA matching process is expensive, time consuming and therefore not yet suitable for large scale biometrics applications for civilian usage.

2) Odor

The odor of individuals contains unique chemical compositions that can be used for authentication purpose [18]. Odor can be detected by using a “chemical sensor” such as those based on metal-oxide technology. Such sensors detect the odorants by detecting the tiny amounts of molecules that are evaporated from materials that have odor. The human odor has the advantage of being impossible to replicate. In 2014, Inbavalli and Nandhini created a model system that authenticates people based on their body odor. Their experimental results show that this biometric identifier has the lowest error rate (15%) in comparison to other biometric identifiers such as face, fingerprints and iris recognition. It should be noted that the effect of ambient and auxiliary odors on human odor is variously appreciated by the authors. Indeed, [14] assert that it is not certain if the invariance in the body odor can be detected if there is the presence of deodorant or chemical composition of the surrounding environment. On the other hand, Inbavalli and Nandhini (2014) conclude after a study that even deodorants and perfumes cannot mask the basic human odor. These artificial scents do not eliminate the organic compounds present in the odor.

III. PROPERTY OF A BIOMETRIC FEATURE

To be practical and reliable a biometric system should meet some specific properties [2], [6], [5]. In this work, we put a focus on eight desirable properties for a biometric characteristic. Table- II shows the performance of the various biometric sensing systems.

- Universality or availability: Means that the entire population must possess this modality.
- Distinctiveness or uniqueness: Means that any two persons should sufficiently have different traits.
- Permanence or stability: The biometric characteristics should be invariant over time. Biometrics, to serve as a means of authentication, must be relatively stable over time and, above all, must be stable for a person regardless of the circumstances of the acquisition (external conditions, emotional conditions of the person, etc.);
- Collectability: Means that the biometric characteristics should be measurable with some (practical) sensing device.
- Accuracy: Describes how accurate a biometric system performs. Biometric accuracy is based on several verifying criteria including the identification rate, error rates, and additional biometric system standards.
- Acceptability: Means that a user and the public in general should have no (strong) objections to the measuring of the biometric traits.
- Resistance to circumvention: Refers to the degree of difficulty required to defeat or bypass the system.
    - Cost: It is the costs necessary to implement the systems.

Table- II: Performance of the various biometric sensing systems (adapted from [14], [6], [5], [19])

Biometric Characteristics	Universality	Distinctiveness	Permanence	Collectability	Accuracy	Acceptability	Circumvention	Cost
Morphological characteristics								
Face	H	L	M	H	L	H	H	M
Fingerprint	M	H	H	M	H	M	M	L
Hand Geometry	M	M	M	H	M	M	M	M
Iris	H	H	H	M	H	L	L	H
Retina	H	H	M	L	H	L	L	H
Palm Print	M	H	H	M	H	M	M	H
Facial Thermogram	H	H	L	H	M	H	L	H
Ear	M	M	H	M	H	H	M	H
Hand Vein	M	M	M	M	H	M	L	H
Behavioral characteristics								
Voice	M	L	L	M	M	H	H	H
Signature	L	L	L	H	M	H	H	L
Gait	M	L	L	H	H	H	M	H
Keystroke	L	L	L	M	L	M	M	L
Biochemical characteristics								
DNA	H	H	H	L	H	L	L	H
Odor	H	H	H	L	L	M	L	H

H: High; M: Medium; L: Low

IV. ARCHITECTURE OF A BIOMETRIC SYSTEM

The generic architecture of a biometric system consists of five main modules as depicted in Fig. 2 [5], [2].

- Sensor module: It consists of capturing the biometric raw data in order to extract a numerical representation. This representation is then used for enrollment, verification or identification.
- Signal processing module: It allows the reduction of the extracted numerical representation in order to optimize the quantity of data to store during the enrollment phase, or to facilitate the processing time during the verification and identification phases. This module can have a quality test to control the captured biometric data.
- Storage module: It is used to store biometric individuals' templates.
- Matching module: It is used to compare the extracted biometric raw data to one or more pre-stored biometric templates. The module therefore determines the degree of similarity (or of divergence) between two biometric vectors.
- Decision module: It is used to determine if the returned index of similarity is sufficient to determine the identity of an individual.

V. TYPE OF MATCHING

There are two types of matching in biometrics: authentication (or verification) and identification. The both types are known as recognition. In the case of authentication, the identity (non-biometric part) of a person is proclaimed and a comparison is made with the sample of the database corresponding to this identity ie a single comparison (one-to-one or 1:1). However, in the case of identification, no identity is proclaimed. This leads to a comparison between the biometric sample taken and all the samples in the database (one-to-many or 1: n) [2]. Moreover, in the case of specific applications such as access control, there is no clear distinction between authentication and identification meaning that techniques developed in one application scenario can be applied to another [20]. Authentication is to answer the question: are you the one you claim to be? On the other hand, identifying comes down to answering the question: who are you? A biometric system can operate either in authentication mode or in identification mode depending in the application context. In most common uses of biometrics, authentication mode is used. Identification is often used in forensic operations such as criminal investigations and autopsies.

VI. MODE OF RECOGNITION [21], [19]

Depending on the considered application, a biometric system may operate in a positive or negative recognition mode.

- Positive recognition: in this mode, the system determines whether the person is who he claims to be. The goal of positive recognition is to prevent many people from using the same identity. This is for example the case where a single person is allowed to access a secure resource. If the system succeeds in matching the registered signature of this person to the signature extracted from the acquired biometry, this corresponds to an acceptance, and if not a rejection.
- Negative recognition: this kind of system is used to determine if the person is what they deny. In this case, the purpose of the recognition is to prevent a single person from using multiple identities. This corresponds, for example, to an application of social benefits where the system records in its database the persons who have already received benefits. If a person wants to fraudulently receive the benefits a second time by claiming to be a third person, the system must check if he corresponds to one of the beneficiaries registered in the database. In the case where the system manages to match the signature extracted from the acquired biometry of this person with one of the signatures of the database,

this corresponds to a rejection, and if not an acceptance.

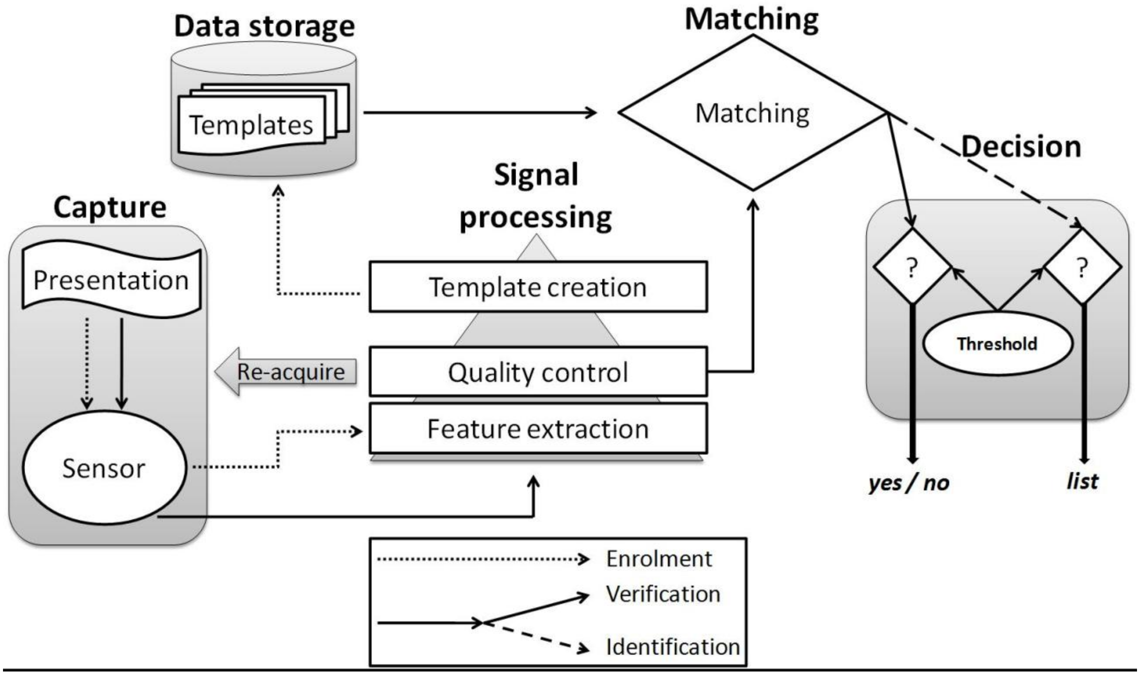

Fig. 2: Generic architecture of a biometric system [5]

VII. CHALLENGES IN BIOMETRIC SYSTEMS [8], [14], [5]

Biometric systems face three main challenges. These are the limitations in terms of performance, acceptability and architecture:

- Performance limitation: Human characteristics are subject to variation and these changes negatively impact performance in biometric recognition. Verification errors are due to many reasons such as occlusions, environmental factors (e.g., illumination, noise) and cross-device matching.
- Acceptability limitations: Three main factors contribute to the complexity of biometric system in terms of acceptability: 1) accuracy in terms of errors, 2) scale or size of the database and 3) usability in terms of easiness to use, security and privacy.
- Architecture limitations: Eight vulnerable points have been identified in a generic biometric system as depicted in Fig. 3 below. Security holes have been identified in all biometric systems. Reference [22] have listed the vulnerabilities in the form of fish-bone (see Fig. 4).

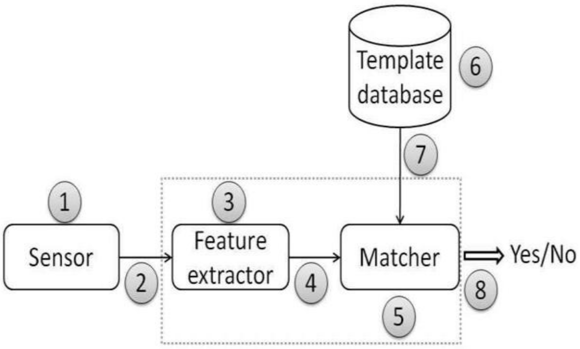

Fig. 3. Possible attack points in a generic biometric system [5]

In the field of biometric template protection, Zannou et al. [23] proposed an algorithm to secure a fingerprint model stored in a database. They used the center of mass technique combined with the modified Hausdorff distance to construct a spiral curve. Experimental results showed a significant improvement in the value of FAR compared to the Fingerprint Shell technique.

VIII. MODE OF BIOMETRIC IDENTIFICATION

There are two modes of biometric identification, i.e. the Open set identification and the Closed set identification [12]. In the open set mode, there is no possibility that the subject presented to the biometric system has previously been enrolled in the database. This is the case of a watch list identification from surveillance cameras which involves a continuous check of a list of people as against streaming videos. On the other hand, the closed set identification deals with the situation where the person of interest is likely to be present in the biometric database and in such case the biometric system does not return an empty candidate list.

IX. CLASSIFICATION OF BIOMETRIC SYSTEMS

There are two systems of biometrics, namely Unimodal and Multibiometrics.

A. Unimodal biometrics

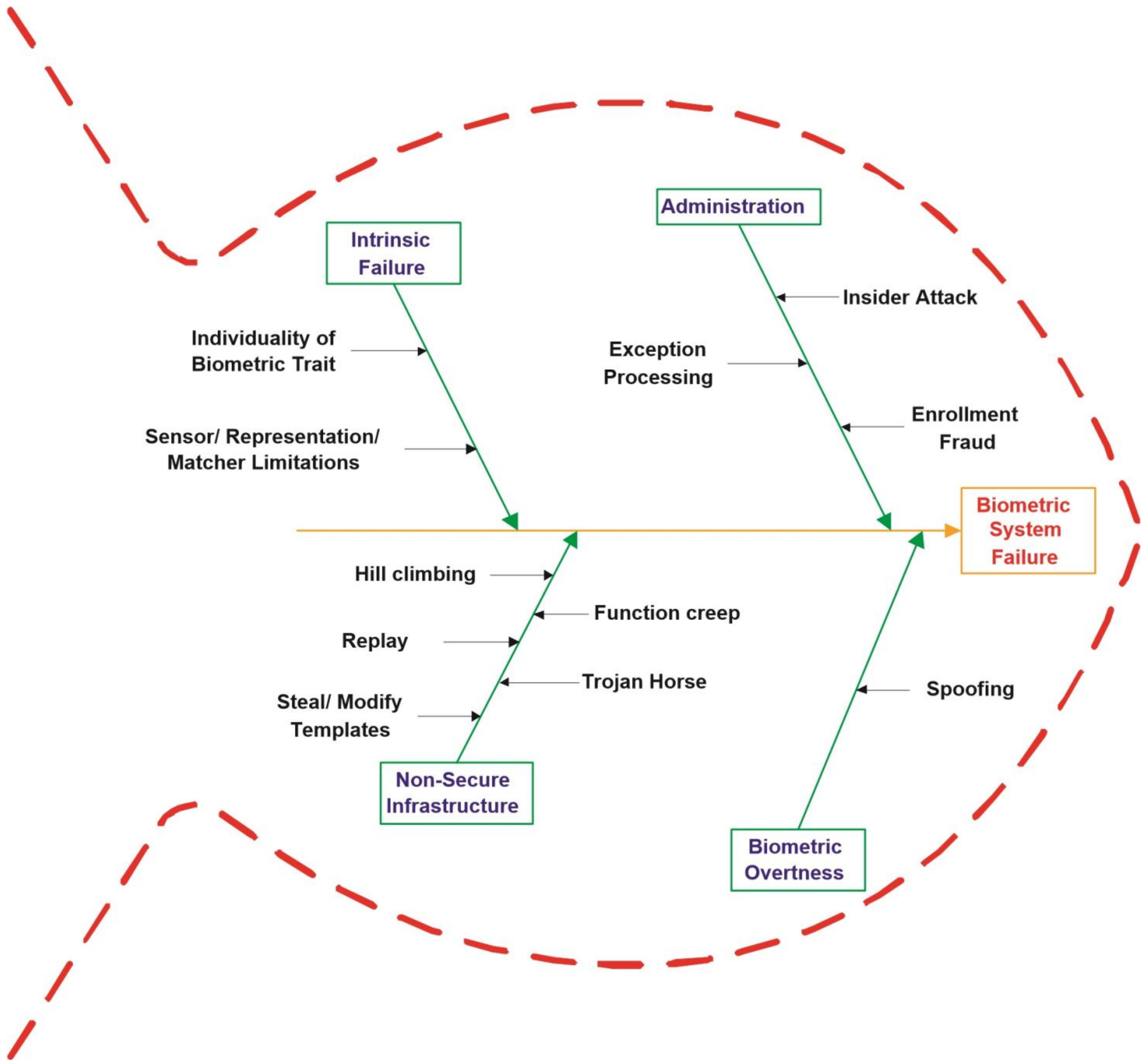

Fig. 4: Fish-bone model for categorizing biometric system vulnerabilities [11]

These systems rely on the evidence of a single source of information for authentication (e.g., single fingerprint, face). They have to contend with a variety of problems such as: (i) Noise in sensed data; (ii) Intra-class variations; (iii) Inter-class similarities; (iv) Non-universality and (v) Spoof attacks [2].

B. Multibiometrics

Multibiometrics denotes the fusion of different types of information. This type of biometrics reduces the constraints of unimodal biometrics by combining several systems. References [6], [24] differentiate six types of multibiometric systems according to their nature. They are called:

- Multi-sensors when they associate several sensors to acquire the same modality, for example an optical sensor and a capacitive sensor for acquiring the fingerprint.
- Multi-instances when they associate several instances of the same biometry, for example the acquisition of several face images with changes in pose, expression or illumination.
- Multi-algorithms when several algorithms process the same acquired image, this multiplicity of algorithms can intervene in the extraction module by considering several sets of characteristics and/or in the comparison module using several comparison algorithms.
- Multi-samples when they combine several different samples of the same modality, for example two different fingerprints or two irises. In this case the data are processed by the same algorithm but require different references to the record, in contrast to multi-instances systems that require only one reference.
- Multi-modal when considering several different modalities, for example face and fingerprint.
- Hybrid system when they combine these different types of associations, for example the use of the face and the fingerprint, but using several fingers.

Jain et al. [25] presented a multibiometric system that combines primary biometric features (e.g. hand-geometry, voice, iris, retina, etc.) with soft biometric traits (such as skin color, age or hair color). We suggest calling this type of multibiometrics a Multi-origin system (see section 12 below). Fig. 5 presents different sources of information for biometric fusion.

C. Levels of fusion

According to Sanderson and Paliwal, the combination of several biometric systems can be done at five different levels [26]: data (or sensor) level, feature level, score level, rank level and decision level.

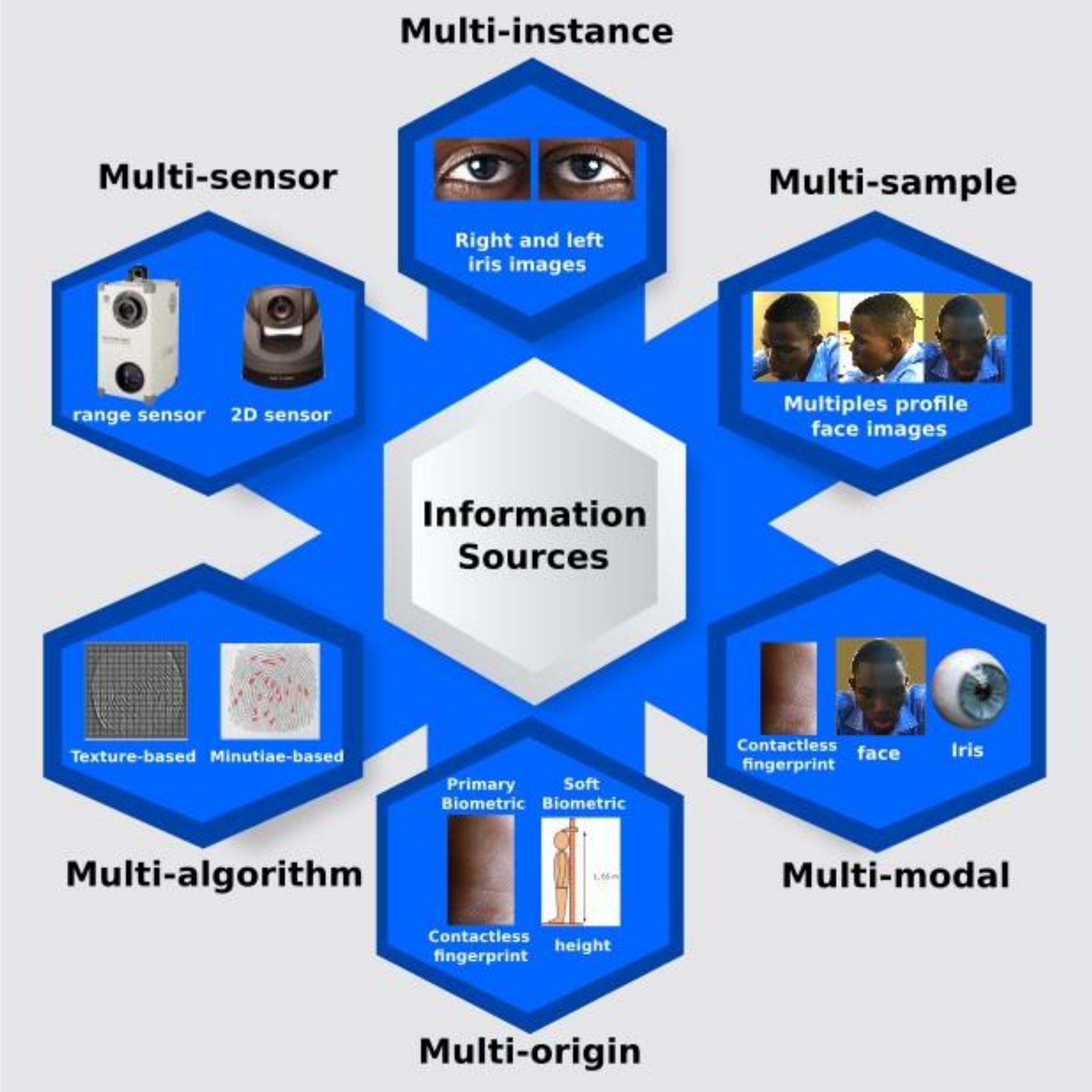

Fig. 5: Sources of information for biometric fusion

These five levels of fusion can be classified into two subsets: the pre-classification fusion (before matching) and the post-classification fusion (after matching). The pre-classification fusion corresponds to the fusion of the information coming from several biometric data at the sensor (raw images) or at the level of the characteristics extracted by the extraction module. Pre-classification fusion methods are on the one hand, rarely used because they pose a number of constraints that can only be met in some very specific applications. On the other hand, post-classification fusion is very studied by researchers. This fusion can be done at the level of the scores coming from the matching modules, at the rank [27] or the decision level. Gad et al. [6] present the hybrid level fusion that aims at making the system faster and significantly reduce the error rate. Bisogni and Nappi [28] proposed a fast score-level fusion method in multibiometrics. The method used optimization and training to generate the total score of multibiometric system. They reach an accuracy of 87% with 100 samples in experiments.

D. Advantage, weakness and solutions to the challenges of multimodal biometrics [14]

1) Advantages

Multimodal biometrics has addressed some issue related to unimodal such as noise, inflexibility, intra-class distinctions, high error rates, spoof attacks, and non-universality. In terms of intra-class distinctions, a multimodal system utilizes several biometrics traits and thus the fusion allows more data points to be initialized providing a better classification of data points.

2) Drawbacks

The implementation of a multimodal biometric system requires many preliminary challenges to overcome. Kumar and Farik (A review of multimodal biometric authentication systems) have identified in 2016 the four following challenges: (1) multimodal systems are difficult to design, (2) user acceptance is quite low, (3) requires higher level of investment and (4) the performance trade-off. Multimodal system design needs to consider various questions such as what number of factors to be used, which factors to be used, which architecture to develop, which level of fusion to consider, how to initialize an appropriate threshold for all the factors to ensure acceptable levels of False Reject Rate and False Accept Rate? The answer to all these questions require significant research and experimentation.

3) Solutions to the challenges

Compared to unimodal biometrics, multimodal systems offer many advantages but at the same time they face challenges. To benefit from these advantages, it is necessary to propose solutions to these challenges. One of the solutions proposed by Kumar and Farik (2016) lies in the development of Integrated Development Environments (IDEs). We suggest other possible solutions, such as (1) the design of systems capable of extracting several different characteristics from a single acquisition, (2) the design of sensor capable of acquiring data from several different modalities. These solutions can significantly reduce the cost of implementation of multibiometric systems.

E. Focus on the scores fusion in biometric systems [28], [29], [30], [31]

1) Multimodal systems fusion architecture

Multimodal systems combine several biometric systems and thus require the acquisition and processing of several data in three modes namely serial (incremental or cascade), parallel (or global) and hierarchical. In the serial mode, the acquisition and processing are done successively and a similarity score is obtained at the end of each acquisition while in the parallel mode the processing is done simultaneously and the final score is obtained after all the processing's. In the hierarchical mode, individual classifiers are joint together in a hierarchy-tree-like-structure. This mode is preferred when dealing with many classifiers. In fact, the acquisition of the biometric data is generally sequential for practical reasons. The architecture is thus generally linked to the processing and particularly to the decision. The parallel architecture (Fig. 6) is the most used because it allows to use all available information and therefore to improve the performance of the system. On the other hand, the acquisition and processing of many biometric data is costly in terms of time and equipment, and reduces ease of use. Therefore, the serial architecture (Fig. 7) may be preferred in some applications; for example, if multimodality is used to provide an alternative for people unable to use the fingerprint.

To improve fusion performance, Allano [31] has proposed the sequential fusion mode (Fig. 8). This mode is derived from that in series with the particularity of having two decision thresholds instead of a single threshold in the serial mode.

2) Methods of score combination

The methods of score combination are very simple methods whose objective is to obtain a final score S from the N available scores S_i for $i = 1$ to N from N systems. The most commonly used methods are the mean, the product, the minimum, the maximum or the median. Combining the scores by the mean consists in computing S such that

$$S = \frac{1}{N}\sum_{i=1}^{N} S_i \qquad (1)$$

Combining the scores by the *product* involves computing S such that

$$S = \prod_{i=1}^{N} S_i \qquad (2)$$

Combining the scores with the *minimum* consists in computing S such that

$$S = \min\,(S_i) \qquad (3)$$

Combining the scores by the *maximum* consists in computing S such that

$$S = max\,(S_i)$$

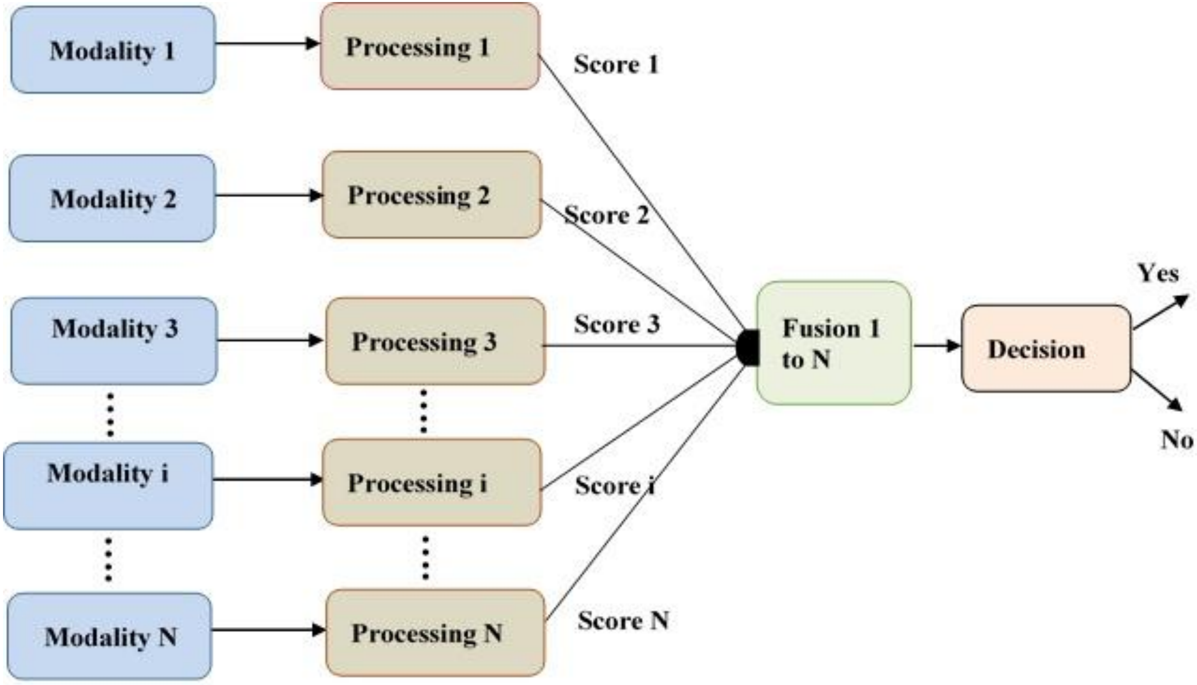

Fig. 6: Parallel fusion system architecture

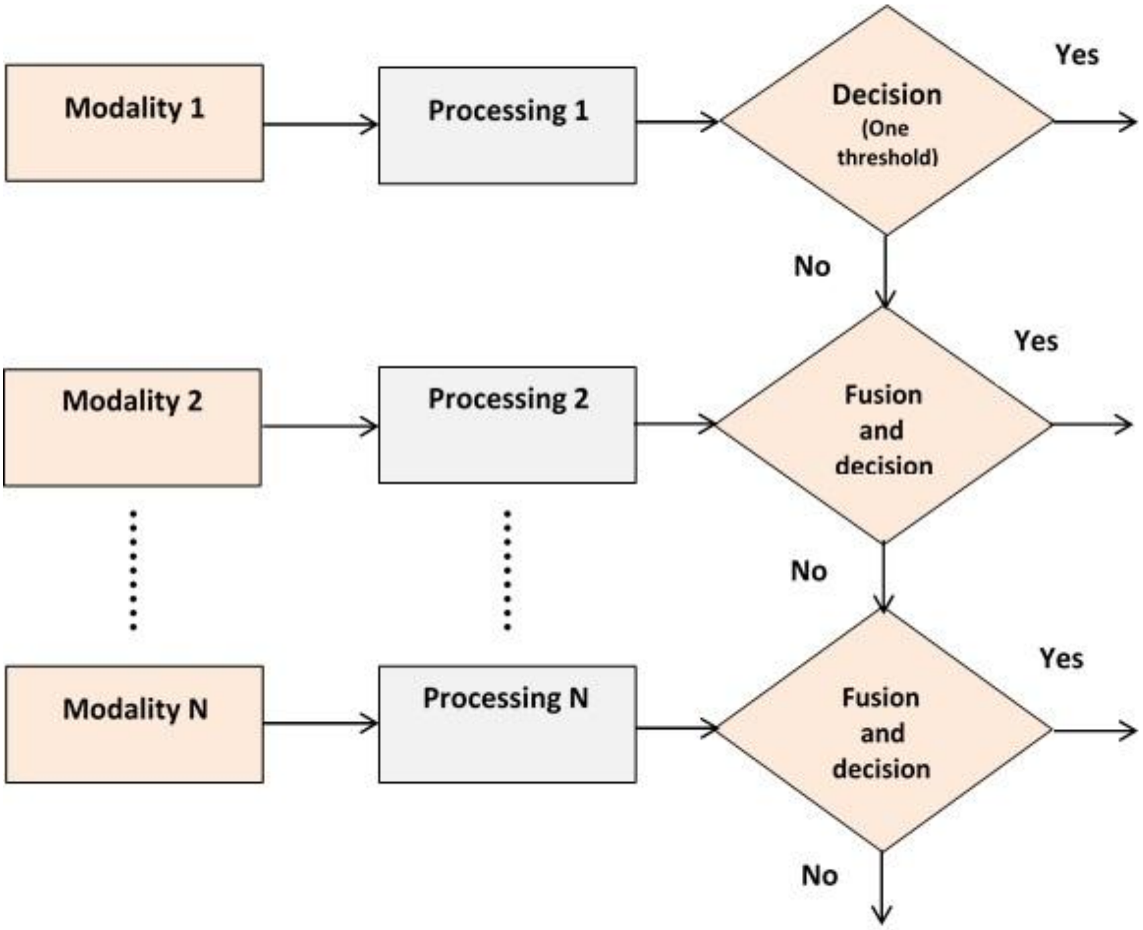

Fig. 7: Serial fusion system architecture

Combining scores by the *median* consists of computing S such that

$$S = \text{med}\ (S_i)$$

All these methods are simple methods that require no adaptation. There are also some more advanced combining methods that require setting parameters such as the *weighted sum*:

$$S = \sum_{i=1}^{N} \omega_i S_i$$

The *weighted sum* makes it possible to give different weights ω_i to each of the subsystems according to their individual performance or their interest in the multimodal system. However, all these combination methods can only be used if all the scores from the subsystems are homogeneous. For this, the methods of combining scores require a prior step of normalization of the scores.

3) Methods of score normalization

The methods of normalizing scores aim at individually transforming each of the scores from the subsystems to make them homogeneous before combining them. Indeed, the scores from each subsystem may be different in nature. Some systems produce similarity scores (the higher the score, the more the reference looks like the test, so the user is a customer), others produce distances (the lower the distance, the closer the reference and the test, the more the user is a client). Moreover, each subsystem can have intervals of variation of the different scores, for example for a system the scores vary between 0 and 1 and for another the scores vary between 0 and 100. Hence the need to normalize the scores before to combine them with the methods cited above. In [4], authors examine the effect of different score normalization techniques on the performance of a multimodal biometric system. They compared seven normalization techniques on the basis of robustness and efficiency.

X. Privacy issues

Biometric data is personal data because it allows to identify a person. For most of them, they have the particularity of being unique and permanent, allowing, in fact, the generalized tracing of individuals. The generalization of human tracking systems raises many questions. With video surveillance, the use of biometrics applied to humans raises questions of bioethics. Faced with the inexorable development of biometrics and the opening up of the world to nano-technologies, the awareness of individuals on this issue appear necessary because people fear that biometric identifiers could be used for linking personal information across different systems or databases. In terms of fundamental rights and freedoms, biometrics clearly oppose the individual's right to data protection and privacy to the collective security requirement. It therefore calls for a balance between these rights and legitimate interests.

On the positive side, biometrics can be used as a mean for protecting individual privacy by safeguarding identity and integrity. For example, the use of a credit card and the access to medical records can be secured by the verification of a biometric features [19].

XI. INFLUENCE OF EMOTION ON THE PERFORMANCE OF BIOMETRIC SYSTEMS

Affective computing is the study and development of systems and devices that can recognize, interpret, process, and simulate human affects. It is an interdisciplinary field spanning computer science, psychology, and cognitive science (Banafa, 2018, https://www.bbvaopenmind.com/en/what-is-affective-computing/). Affective computing and sentiment analysis are very decisive for the development of Artificial Intelligence and all the research fields that derive from it [32]. Many concepts related to the Affective computing are often used interchangeably in the literature namely affect, feeling, emotion, sentiment and opinion. In the rest of the document we focus on the concept of emotion. Emotion can be generated by multiple sources such as a) the things we think about, b) actions we take, c) the way we react to stimuli [33]. Emotion is a fuzzy notion and difficult to define [34]. Several definitions and roles have been given to emotion. These definitions differ according to the different approaches proposed. However, despite these divergences, most contemporary authors retain a consensual definition of emotional states. They describe emotion as a complex response system that integrates three aspects: (1) the physiological / biological aspect that covers the physiological reactions (cardiac rhythm, respiratory rate, ...), (2) the behavioral aspect that covers the behavioral and expressive reactions, strongly influenced by the personality of the subject and (3) the cognitive aspect that covers cognitive and experiential reactions (internal state / feeling). It should be noted that mood and personality have an influence on emotion. Djara et al. [35] presented the concepts and tools related to this field of study. In another work, Djara et al. [36] proposed a study on multimodal emotional state recognition. They used both the image and signal processing to estimate the emotional state of the user. That work was a state of the art about emotion recognition systems. It gave a general overview on emotions (concepts, representation, characteristics, approach of recognition).

Biometrics intervenes mainly in the phase of detection and recognition of emotion. Emotion has a negative influence on the performance of biometric systems. However, this influence is limited to the level of behavioral characteristics. It has been proven that emotional states are accompanied by physical reactions. This makes possible the characterization of emotion through the measurement of physical characteristics. The most commonly explored biometric measurement of emotions is facial expression recognition (Chandler and Cornes, 2011, “Biometric Measurement of Human Emotions,”). Reference [21] carried out a work on the influence of emotion on the face. He believes that the facial expression of emotion, combined with speech, can produce significant changes in the appearance of the faces. The number of possible configurations is incalculable. The influence of facial expression on recognition is therefore difficult to assess. Since the facial expression affects the geometric shape and the positions of the facial features, it seems logical that the global or hybrid techniques are more robust than most geometric techniques. In the literature review presented by [21], some authors claim that facial expressions do not have a significant influence on recognition algorithms, if they remain reasonable. Contrariwise, extreme cases that cause significant deformations of the mouth (such as crying) and narrowing or closing the eyes severely degrade the performance of automatic recognition.

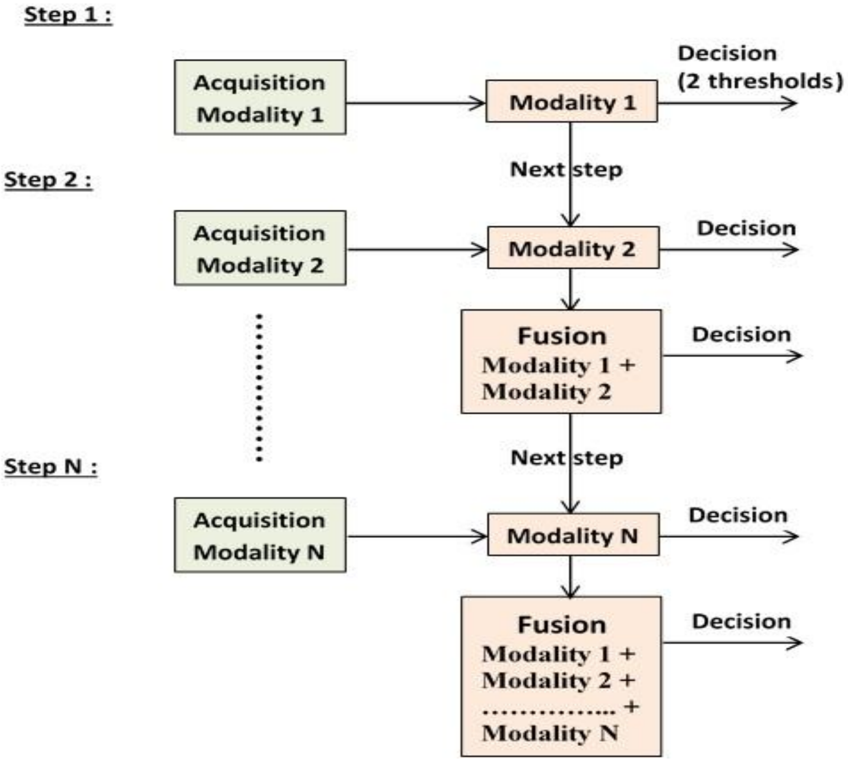

Fig. 8: Sequential Fusion System Architecture (adapted from [30])

XII. BENEFIT OF INCORPORATING METADATA IN THE MULTIBIOMETRIC SCORE-LEVEL FUSION

Jain et al. [25] have presented another multi-modal biometric approach combining traditional biometric attributes (e.g. voice and iris) and soft biometric identifiers (e.g. skin color, age, etc.). Since the same attribute can be shared by many different people, soft biometric characteristics cannot be used to authenticate individuals reliably. On the other hand, a combined use of the soft biometric attributes with the conventional biometric modalities considerably improves the performance of the authentication system. Another advantage of soft biometric attributes is that they facilitate the indexing of large biometric databases by reducing the number of entries to search in the database. In that work, they proposed a framework for integrating soft biometric data with the traditional biometric system. This framework has two subsystems for the biometric recognition system (Fig. 9). The first subsystem based on conventional biometric attributes (signature, voice, DNA, etc.) is called the primary biometric system. It could work based on one or several modalities. The second subsystem is called the secondary biometric system. It is based on soft biometric features (height, eye color, skin color, etc.). Specifically for gender classification, Barra et al. [37] provided an interesting gait analysis proposal. Their work was based on the 2D estimated skeleton points. Experimental results showed that the human gender can be classified just considering the pose information provided by the body pose information.

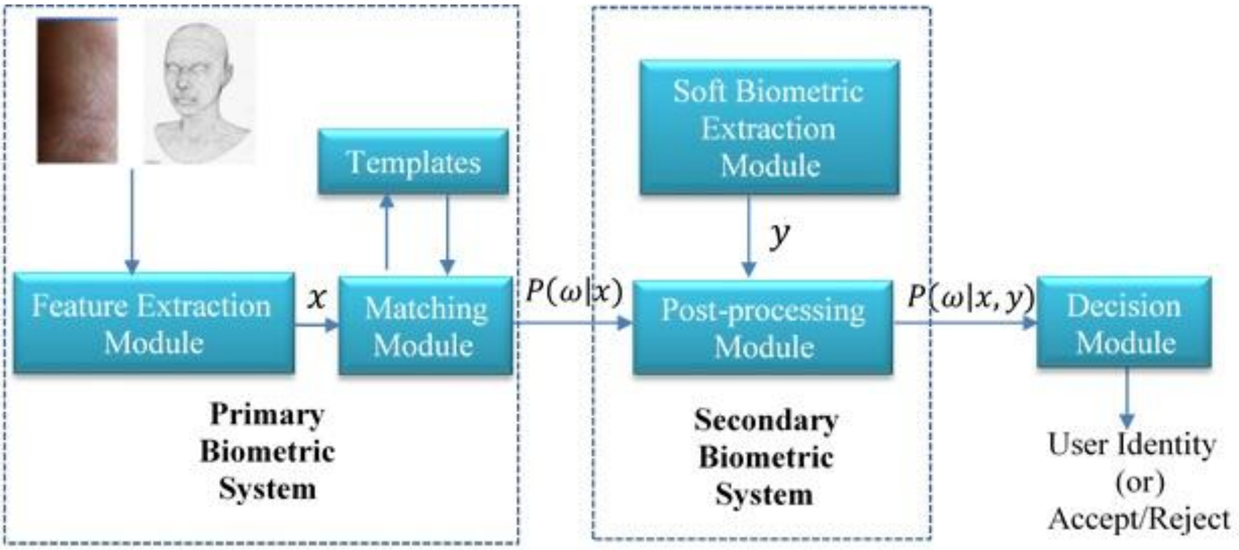

Fig. 9: Integration of Soft Biometric Traits with a Primary Biometric System [30]

We use ancillary information in order to make biometrics adaptation. There are several avenues for adapting biometric systems, one linked to the user and the other to the acquisition system and its environment (context). The monomodal or multimodal biometric systems are generally adjusted according to the application. The adjustments of a system are made at several levels which correspond to the different modules of the structure of a system (Fig. 2). Once the application has been defined and the modalities chosen, the modules to be defined are the extraction of features, the matching, the fusion, the ranking and the decision. The setting of these modules therefore depends on the application and the target population. For example, for the same mass identity verification system for visas, the setting will not necessarily be the same in all countries according to the characteristics of the populations. Some criteria like skin color, the percentage of people with bad fingerprints can vary the settings of the systems to achieve equivalent performance. For applications such as mass identity control, the system must be set for a population as a whole and cannot be specific to each user. On the other hand, for applications with a smaller population, such as access to a secure area with a predefined and limited user number, or personal applications, such as protecting a workstation, we can design systems that are not only optimized for a defined population but also adapted to each user [31]. Several authors have studied the adaptation to the user of biometric systems. We have [1] who introduced adaptation to the user in 2002, and then [38] and [20] in their thesis works.

According to [1], adaptation in multimodal biometrics can be done at two levels: (a) developing a user-specific decision threshold and (b) assigning a weighting coefficient for each biometric feature. Experimental results prove that user-specific thresholds improved system performance by ~ 2%, while user-specific weights improved performance by ~ 3%. The adaptation of the biometric systems to each user is potentially very interesting to improve the performances of the systems because each user is unique. Moreover, for the same user, the settings can vary from one moment to another. Another way of adapting the systems is to consider contextual information (temperature, brightness, noise etc.) or personal information (eye color, age, height, etc.) which are known as metadata [31], [24].

XIII. TYPOLOGY OF BIOMETRIC ADAPTATION

Based on the description of the adaptation of biometric systems made in section 12, it is presented a typology of biometric adaptation. Table- III indicates two possible levels of adaptation i.e user level and acquisition system level. For each level of adaptation, four analysis parameters are defined. These parameters provide details for a better understanding of biometric adaptation. They concern adaptation types, examples per adaptation type, types of data manipulated and training need.

Table- III: Typology of biometric adaptation

Level of adaptation	**User**			**Acquisition system**	
Type of adaptation	Decision threshold	Weighting (based on data quality)	Soft biometric	Sensor	Context
Example	Voice: 0,7 Iris: 0,6	Fingerprint: 0,6 Face: 0,4	Gender; Height; Skin, eye and hair color	Volume (microphone); Flash (camera)	Brightness, noise, temperature
Exploited data	Biometric data (image or signal)		Metadata		
Training need	After training		Without training (immutable)		After training

XIV. EXTENSION OF THE ADAPTED SEQUENTIAL FUSION APPROACH

Sobabe et al. [39] presented a new framework for score-level fusion. The principle developed is presented with more details. It is based on two previous works. The first work is related to the integration of soft biometric attributes with a traditional biometric system in a parallel fusion scheme [25]. Referring to the Bayes rule, the probability of a user's recognition from his primary biometric characteristic and his soft biometric attribute is computed as follows:

$$P(\omega_i|x,y) = \frac{p(y|\omega_i)\,P(\omega_i|x)}{\sum_{i=1}^{n} p(y|\omega_i)P(\omega_i|x)} \tag{7}$$

x is the vector of pure biometric features;
$y = [y_1, y_2, \dots, y_k, y_{k+1}, y_{k+2}, \dots, y_m]$ is the vector of the soft biometric attributes, where y_1 through y_k are continuous variables and y_{k+1} through y_m are discrete variables;
$\omega_1, \omega_2, \dots, \omega_n$ represent the n users registered in the database;
$P(\omega_i \mid x), i = 1,2, \dots, n$ is the probability that the test user is ω_i given the feature vector x.
Assuming that soft biometric variables are independent [25], (7) becomes:

$$P(\omega_i|x,y) = \frac{p(y_1|\omega_i)\dots P(y_k|\omega_i)\,P(y_{k+1}|\omega_i)\dots P(y_m|\omega_i)\,P(\omega_i|x)}{\sum_{i=1}^{n} p(y_1|\omega_i)\dots P(y_k|\omega_i)\,P(y_{k+1}|\omega_i)\dots P(y_m|\omega_i)\,P(\omega_i|x)} \tag{8}$$

In (8), $p(y_j|\omega_i), j = 1, 2, \dots, k$ is evaluated from the conditional density of the variable y_j for the user ω_i. On the other side, the discrete probability $p(y_j|\omega_i), j = k+1, k+2, \dots, m$ represents the probability that the user ω_i be assigned to the class y_j. In order to simplify the problem, we assume that the accuracy of the classification module is independent of the user, based on the biometric indicator y_j.

(18)

Let

$$p(y) = \sum_{i=1}^{n} p(y_1|\omega_i) \dots P(y_k|\omega_i)\,P(y_{k+1}|\omega_i) \dots P(y_m|\omega_i)\,P(\omega_i|x) \tag{9}$$

The logarithm of $P(\omega_i|x,y)$ in (8) can be expressed as follows:

$$\log P(\omega_i|x,y) = \log p(y_1|\omega_i) + \cdots + \log p(y_k|\omega_i) + \log P(y_{k+1}|\omega_i) + \cdots + \log P(y_m|\omega_i) + \log P(\omega_i|x) - \log p(y)$$

Considering the relative importance of the different modalities involved, weights are assigned to them. We obtain the following discrimination function:

$$g_i(x,y) = a_0 \log P(\omega_i|x) + a_1 \log p(y_1|\omega_i) + \cdots + a_k \log p(y_k|\omega_i) + a_{k+1} \log P(y_{k+1}|\omega_i) + \cdots + a_m \log P(y_m|\omega_i) \tag{11}$$

with $\sum_{i=0}^{m} a_i = 1$ and $a_0 >> a_i,\ i = 1, 2, \dots, m$. Note that the coefficients $a_i, i = 1, 2, \dots, m$ represent the weights assigned to the soft biometrics features and that a_0 is the weight assigned to the identifier of pure biometrics. (21)
$a_0 >> a_i$ means that a_0 is very larger than a_i.

(10)

Moreover, five years later, Allano [31] presented the strategy of sequential score-level fusion (see architecture in the Fig. 10). In [39], authors have considered hypothesis H_0 and H_1 and the two species errors α and β are computed as follows:

$$\alpha = FRR \tag{12}$$

and

$$\beta = FAR \tag{13}$$

They defined the Probability Ratio PR as follows:

$$PR = \frac{P(X_n|H_0)}{P(X_n|H_1)} \tag{14}$$

The Sequential Probability Ratio Test (SPRT) defines k_0 and k_1 as the stopping criteria around the k border. The rejection option represents the intermediate zone (uncertainty zone) that leads to the next step $(k+1)$ with the addition of additional data. Thus, in step k, H_0 is accepted if:

$$\frac{P(x_1,\ x_2, \dots, x_k|H_0)}{P(x_1,\ x_2, \dots, x_k|H_1)} \geq k_1 \tag{15}$$

H_0 is rejected (and H_1accepted) if :

$$\frac{P(x_1,\ x_2, \dots, x_k|H_0)}{P(x_1,\ x_2, \dots, x_k|H_1)} \leq k_0 \tag{16}$$

We are in the uncertainty zone if :

$$k_0 < \frac{P(x_1,\ x_2, \dots, x_k|H_0)}{P(x_1,\ x_2, \dots, x_k|H_1)} < k_1$$

In this case, we recalculate the likelihoods ratio after adding data from step $k+1$.
k_0 and k_1 are computed as follows:

$$k_0 = \frac{\alpha}{1-\beta}$$

and

$$k_1 = \frac{1-\alpha}{\beta} \tag{19}$$

Assuming the independence assumption on the test samples [31], the likelihoods ratio is computed as follows:

$$\frac{P(x_1,\ x_2, \dots, x_k|H_0)}{P(x_1,\ x_2, \dots, x_k|H_1)} = \frac{P(x_1,\ x_2, \dots, x_{k-1}|H_0)}{P(x_1,\ x_2, \dots, x_{k-1}|H_1)}\,\frac{P(x_k|H_0)}{P(x_k|H_1)} = \prod_{i=1}^{k} \frac{P(x_i|H_0)}{P(x_i|H_1)}$$

The sequential test can be summarized by the uncertainty zone equation in step k as follows:

$$\log\left(\frac{\alpha}{1-\beta}\right) < \sum_{i=1}^{k} \log\left(\frac{P(x_i|H_0)}{P(x_i|H_1)}\right) < \log\left(\frac{1-\alpha}{\beta}\right) \quad (20)$$

We can make a graphical representation of the SPRT through the Fig. 10 below.

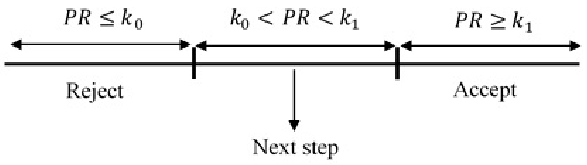

Fig. 10: Graphical representation of the SPRT

The method of sequential fusion of scores implements several modalities of traditional biometrics. It gives better results compared to the traditional method of serial fusion. These better results concern the reduction of time and difficulty use of several biometric systems.

To capitalize on the two principles described above through (7) to (21), we propose a new score-level fusion architecture (see Fig. 11) that we call the *adapted sequential fusion strategy*. On the Fig. 11, BM means Biometric Modality, MD means Metadata, PR means Probability Ratio and ⊕ represents the symbol of fusion.

Let $X_m = (x_1, x_2, \dots, x_m), m > 1$ be a vector of pure biometric features;

let $Y_{mn} = \begin{pmatrix} y_{11} & y_{1k} & y_{1n} \\ y_{l1} & y_{lk} & y_{ln} \\ y_{m1} & y_{mk} & y_{mn} \end{pmatrix}, n \geq 1$ be the matrix of metadata (or soft biometric) characteristics;

for $j = (1, 2, \dots, n)$, let $y_{ij} = (y_{i1}, y_{i2}, \dots, y_{ik}, y_{ik+1}, y_{ik+2}, \dots, y_{in})$ be the set of metadata attributes, where y_{i1} through y_{ik} are continuous variables and y_{ik+1} through y_{in} are discrete variables;

(17) let $\omega_r = (\omega_1, \omega_2, \dots, \omega_q)$ be the enrolled users in the database;

based on the attribute x_i, a user ω_r is recognized by the prior probability expressed as follows: $P(\omega_r|x_i)$;

From (7) and (20), the Probability Ratio is computed as follows:

$$PR = \prod_{i=1}^{m} \prod_{j=1}^{n} \frac{P(x_i, y_{ij}|H_o)}{P(x_i, y_{ij}|H_1)} \quad (22)$$

Considering (21), the sequential test can be summarized by the equation of the uncertainty zone at the stage k as follows:

$$\log\left(\frac{\alpha}{1-\beta}\right) < \sum_{i=1}^{k} \sum_{j=1}^{n} \log\left(\frac{P(x_i, y_{ij}|H_0)}{P(x_i, y_{ij}|H_1)}\right) < \log\left(\frac{1-\alpha}{\beta}\right) \quad (23)$$

With reference to the weighting scheme used in (11), the discrimination function is defined by the following expression:

$$g_{ij}(x_i, y_{ij}) = \sum_{i=1}^{m} \sum_{j=1}^{n} [a_0 \log P(x_i|H_0) - a_0 \log P(x_i|H_1) + a_j \log P(y_{ij}|H_0) - a_j \log P(y_{ij}|H_1)] \quad (24)$$

Remark:

Considering the Fig. 11, it is important to specify that from step 2 ($i = 2$), each first sub-step (i.1) corresponds only to the treatment of the pure biometric modality; thus, the weight $a_0 = 1$ and the obtained score (probability ratio) is noted PR_i (see Fig. 11). The transition to the second sub-steps noted i.2 implies the taking into account of metadata and forces to recalculate the probability ratio of the step i.1 noted PR'_i with $a_0 < 1$.

For a better description of the adapted sequential fusion architecture, a framework has been designed. The algorithm derived from the proposed framework makes it possible to define the input and output variables before the presentation of the instructions on 59 lines [39].

XV. CONCLUSION AND FUTURE WORK

This paper presented an overview of the different biometrics, the multibiometric systems before dealing with the fusion schemes. We then focus on the score-level fusion in multibiometric systems before addressing the influence of the emotion on the performance of biometric systems. Besides, we discussed the taxonomy of multibiometrics. To this end, we have introduced the concept of *multi-origin biometrics* to refer to data from both pure biometric modalities and soft biometric traits. In a world where access control is increasingly becoming a major issue, the adapted sequential fusion architecture will play an important role for multi-biometric authentication.

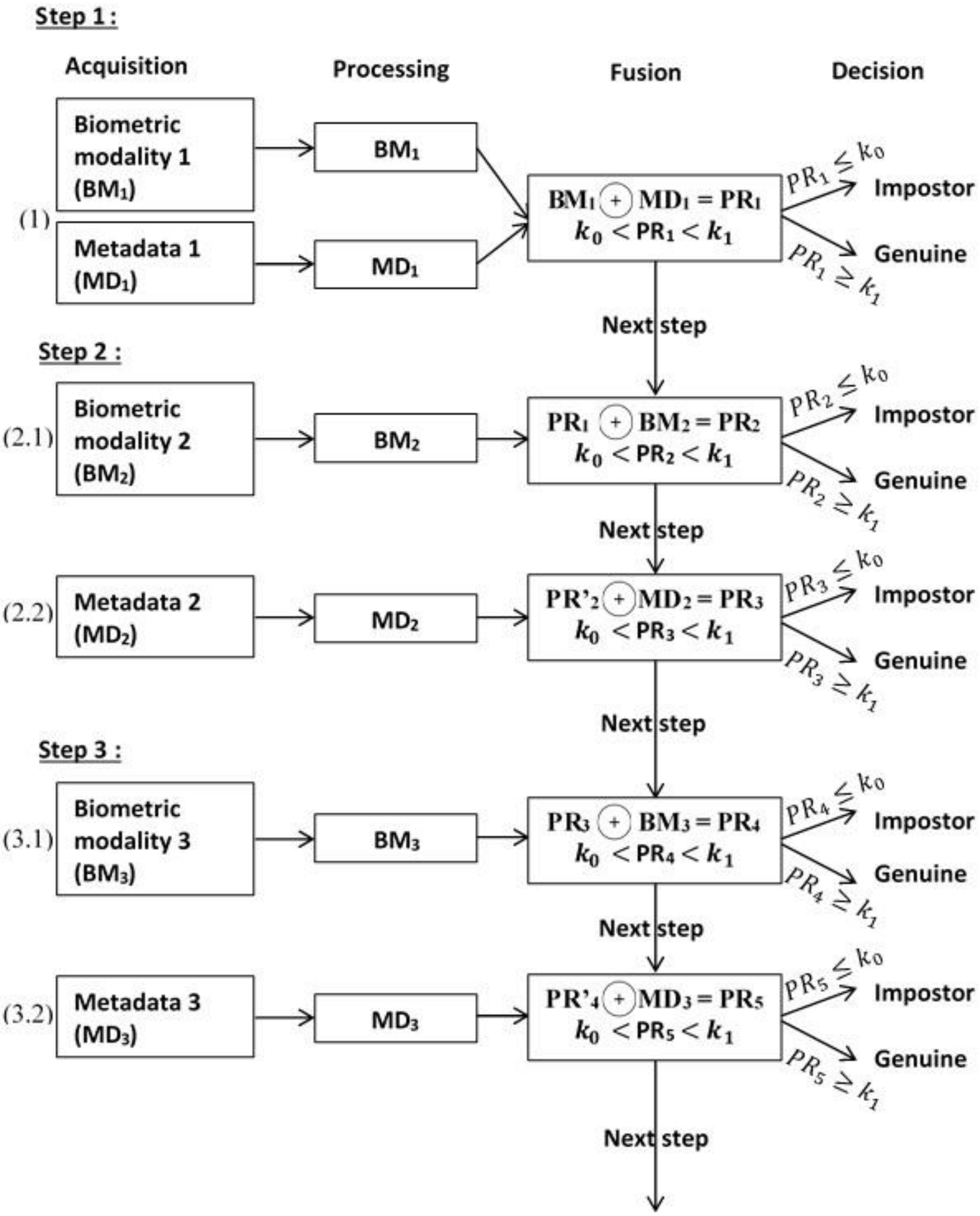

Fig. 11: Adapted sequential fusion architecture

After the designing of the framework, the next step will deal with its implementation in order to evaluate its performance. The implementation will consist of the fusion of scores from the three biometric modalities to implement. This is the face, the color of the skin of the face and the contactless fingerprint. The scores obtained from these three modalities will be merged using our adapted sequential fusion algorithm. The implementation will be under the Python environment. Local Binary Patterns Histograms (LBPH) algorithm will be used for 2D face recognition [13]. The algorithm of the HSV (Hue, Saturation and Value) technique will be used to detect the color regions of the skin. It is based on the pixel technique and uses color spaces to characterize the skin (Abd El Hafeez, 2010, A New System for Extracting and Detecting Skin Color Regions from PDF Documents). For contactless fingerprint verification, the minutiae detection algorithm proposed by Djara et al. [15] will be used.

As perspectives to the works presented in section 11, we also aim at measuring the impact of emotion on the performance of biometric systems. We will experiment based on the emotion expressed through the face.

REFERENCES

1. A. K. Jain and A. Ross, "Learning user-specific parameters in a multibiometric system," Appeared in Proc. International Conference on Image Processing (ICIP), Rochester, New York, September (2002), pp 22-25, DOI: 10.1109/ICIP.2002.1037958.
2. H. AlMahafzah and M. Z. AlRwashdeh, "A survey of multibiometric systems," International Journal of Computer Application, volume 43 No 15 April (2012), pp 36-43, DOI : 10.5120/6182-8612.
3. 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, (2009), pp 49-53, arXiv:0909.2373v1.
4. A. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," Elsevier, Pattern Recognition 38 (2005), pp 2270-2285, DOI:10.1016/j.patcog.2005.01.012.
5. M. El-Abed and C. Charrier, "Evaluation of biometric systems. new trends and developments in biometrics," (2012), pp. 149 - 169, http://dx.doi.org/10.5772/52084. <hal-00990617>
6. 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, (2015), pp 128-138, DOI : 10.14569/IJACSA.2015.060618.
7. T. Djara, A.-A. Sobabe, M. B. Agbomahena, and A. Vianou, "Practical method for evaluating the performance of a biometric algorithm," © ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019, Springer Nature Switzerland AG 2019, AFRICATEK 2018, LNICST 260, (2019), pp. 125–132, https://doi.org/10.1007/978-3-030-05198-3_11.
8. N. Gopal and R. K. Selvakumar, "Multimodal biometric identification system - An overview," International Journal of Engineering Trends and Technology (IJETT) – Volume 33 Number 7- March (2016), pp 351-355, DOI: 10.14445/22315381/IJETT-V33P267.
9. S. Guerfi, Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D. Traitement du signal et de l'image, PhD thesis, Université d'Evry-Val d'Essonne, (2008). <tel-00623243>
10. A. K. Jain and A. Kumar, "Biometric recognition: An overview," Chapter 3, © Springer Science + Business Media B.V. (2012), pp 49-79, DOI 10.1007/978-94-007-3892-8_3.
11. M. Chihaoui, A. Elkefi, W. Bellil, and C. Ben Amar, "A survey of 2D face recognition techniques," Computers 2016, 5, 21, September (2016), doi:10.3390/computers5040021, www.mdpi.com/journal/computers.
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 (2019), ©2019 IEEE, pp. 132-136, 978-1-7281-3578-6/19/$31.00.
13. M. A. Singh, V. Kukreja, "Contemporary study of face recognition systems for attendance autonomous systems," International Journal of Management, Technology And Engineering, Volume 8, Issue XII, Dec 2018, pp. 285-295, DOI:16.10089.IJMTE.2018.V8I12.17.2028.
14. M. O. Oloyede and G. P. Hancke, "Unimodal and multimodal biometric sensing systems: A review," IEEE Access, Volume 4, (2016), pp 7532-7555, Digital Object Identifier: 10.1109/ACCESS.2016.2614720.
15. 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, January-June (2016), pp 12-27, DOI: 10.4018/IJCVIP.2016010102.
16. F. Francis-Lothai and D. B. L. Bong, "A fingerprint matching algorithm using bit-plane extraction method with phase-only correlation," Int. J. Biometrics, Vol. 9, No. 1, (2017) pp.44–66, DOI: 10.1504/IJBM.2017.084135
17. A. Kumar and C. Kwong, "Towards contactless, low-cost and accurate 3D fingerprint identification," IEEE Transactions on pattern analysis and machine intelligence, Vol. 37, No. 3, March (2015), pp 681-696, doi: 10.1109/TPAMI.2014.2339818.
18. C. A. Oyeleye, T. M. Fagbola, R. S. Babatunde, and A. A. Adigun, "An exploratory study of odor biometrics modality for human recognition," International Journal of Engineering Research & Technology (IJERT), Vol. 1 Issue 9, November (2012), pp 1-10, ID: IJERTV1IS9205.
19. 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 (2004), pp 4-20, DOI: 10.1109/TCSVT.2003.818349.
20. N. Poh, Multi-system biometric authentication, PhD thesis, EPFL, Lausanne, (2006).
21. A. Chaari, Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée. Modélisation et simulation. PhD thesis, Université d'Evry-Val d'Essonne, (2009). <tel-00549395>.
22. A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," Published in EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January (2008), pp 1-20, DOI:10.1155/2008/579416.
23. S. B. Zannou, T. Djara, and A. Vianou, "Secured revocable contactless fingerprint template based on center of mass," BioSMART 2019 Proceedings, 3rd International Conference on Bio-engineering for Smart Technologies, Paris, 24th-26th April (2019), 978-1-7281-3578-6/19/$31.00 ©2019 IEEE, pp. 156-159.
24. A. Ross, "An introduction to multibiometrics," Appeared in Proc. of the 15th European Signal Processing Conference (EUSIPCO), (Poznan, Poland), September (2007), DOI: 10.1007/978-0-387-71041-9_14.
25. A. K. Jain, K. Nandakumar, X. Lu, and U. Park, "Integrating faces, fingerprints, and soft biometric traits for user recognition," Proceedings of Biometric Authentication Workshop, LNCS 3087, Prague, May (2004), pp. 259-269, DOI:10.1007/978-3-540-25976-3_24.
26. C. Sanderson and K. K. Paliwal, "Information fusion and person verification using speech and face information," Digital Signal Processing, Vol. 14, No. 5, (2004), pp. 449–480, http://dx.doi.org/10.1016/j.dsp.2004.05.001.
27. 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.
28. C. Bisogni and M. Nappi, "Multibiometric score-level fusion through optimization and training," BioSMART 2019 Proceedings, 3rd International Conference on Bio-engineering for Smart Technologies, Paris, 24th-26th April (2019), ©2019 IEEE, pp. 127-131, 978-1-7281-3578-6/19/$31.00.
29. Y. Faridah, H. Nasir, A. K. Kushsairy, and S. I. Safie, "Multimodal biometric algorithm: A survey," Biotechnology 15 (5), (2016), pp 119.124, DOI: 10.3923/biotech.2016.119.124.
30. L. Allano, S. Garcia-Salicetti, B. Dorizzi, "A low cost incremental biometric fusion strategy for a handheld device," S+SSPR 2008 : Joint IAPR International Workshops on Structural, Syntactic and Statistical Pattern Recognition, Dec 2008, Orlando, United States. pp.842 -851, 10.1007/978-3-540-89689-0_88., hal-01375832.
31. 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).
32. E. Cambria, "Affective computing and sentiment analysis," IEEE Computer Society, (2016), pp 102-107, DOI: 10.1109/MIS.2016.31.
33. M. Soleymani et al., "A survey of multimodal sentiment analysis," Image and Vision Computing (2017), © 2017 Published by Elsevier B.V., pp 1-12, http://dx.doi.org/10.1016/ j.imavis.2017.08.003.
34. A. M. Ousmane, T. Djara, F. J. Zoumarou W., and A. Vianou, "Automatic recognition system of emotions expressed through the face using machine learning : Application to police interrogation simulation," BioSMART 2019 Proceedings, 3rd International Conference on Bio-engineering for Smart Technologies, Paris, 24th-26th April (2019), ©2019 IEEE, pp. 160-163, 978-1-7281-3578-6/19/$31.00.
35. T. Djara, A. M. Ousmane, and A. Vianou, "Mood and personality influence on emotion," © ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2019, Springer Nature Switzerland AG 2019, AFRICATEK 2018, LNICST 260, (2019), pp. 166–174, https://doi.org/10.1007/978-3-030-05198-3_15.
36. T. Djara, A. M. Ousmane, and A. Vianou, " Emotional state recognition using facial expression, voice, and physiological signal," International Journal of Robotics Applications and Technologies, Volume 6, Issue 1, January-June 2018, Copyright © 2018, IGI Global, DOI: 10.4018/IJRAT.2018010101, pp. 1-20.
37. P. Barra, C. Bisogni, M. Nappi, D. Freire-Obregon, and M. Castrillon-Santana, "Gender classification on 2D human skeleton," BioSMART 2019 Proceedings, 3rd International Conference on Bio-engineering for Smart Technologies, Paris, 24th-26th April (2019), ©2019 IEEE, pp. 123-126, 978-1-7281-3578-6/19/$31.00.

38. J. Fierrez-Aguilar, Adapted Fusion Schemes for Multimodal Biometric Authentication, PhD thesis, Universidad Politecnica de Madrid, (2006).
39. A. -A. Sobabe, T. Djara, and A. Vianou, “A framework for combination of sequential architecture and soft biometrics in multibiometric scores fusion,” BioSMART 2019 Proceedings, 3rd International Conference on Bio-engineering for Smart Technologies, Paris, 24th-26th April (2019), ©2019 IEEE, pp. 164-167, 978-1-7281-3578-6/19/$31.00.

AUTHORS PROFILE

Tahirou Djara is a Senior Lecturer at the Polytechnic School of Abomey-Calavi located in the University of Abomey-Calavi, Bénin. His research interests include: biometrics, signal and image processing, computational intelligence, industrial applications and symbolical programming. He is member of the research laboratory: Laboratory of Electronics, Telecommunications and Applied Data Processing Technology (Laboratoire d’Electrotechnique de Télécommunication et d’Informatique Appliquée– LETIA/EPAC). He received the PhD degree in signals and image processing from the University of Abomey-Calavi, in 2013. He is a consultant in quality assurance in higher education and consultant in the field of science and engineering technology.

Abdou-Aziz Sobabe is a PhD student at the Doctoral School of Engineering Sciences located at the University of Abomey-Calavi in Benin. He conducts his research at the Laboratory of Electronics, Telecommunications and Applied Data Processing Technology (Laboratoire d’Electrotechnique de Télécommunication et d’Informatique Appliquée – LETIA/EPAC). His research interests include: biometrics, signal and image processing, affective computing and software engineering. His areas of specialization include multimodal biometrics, contactless biometrics, score fusion and user-specific parameters in biometric systems. In software engineering, he is interested in object-oriented programming and relational databases for applications. In the field of artificial intelligence, he uses Machine Learning methods applied to biometric authentication.

Antoine Vianou is a PhD Engineer in Energy and Electricity sciences. He has been graduated through many universities as the University of Dakar and the University of Evry Val d’Essonne. He is a Full Professor in Engineering Sciences and Technologies (E.S.T.). Pr. VIANOU is currently Chairman of the Sectoral Scientific Committee of E.S.T. of the Scientific Council of UAC in Benin and is also Director of the Laboratory of Thermophysic Characterization of Materials and Energy Mastering. He is the Director of the Doctoral School of Engineering Sciences in UAC. During his academic career, Professor VIANOU taught in several African Universities and in several French ones. He is author of over hundred articles in the fields of Engineering Sciences and Technologies. In addition, he received several honors in recognition for his professional career.