Chapter 7

Evaluation of Biometric Systems

Mohamad El-Abed and Christophe Charrier

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/52084

1. Introduction

Biometrics is considered as a promising solution among traditional methods based on "what we own" (such as a key) or "what we know" (such as a password). It is based on "what we are" and "how we behave". Few people know that biometrics have been used for ages for identification or signature purposes. In 1928 for example, fingerprints were used for women clerical employees of Los Angeles police department as depicted in Figure 1. Fingerprints were also already used as a signature for commercial exchanges in Babylon (-3000 before JC). Alphonse Bertillon proposed in 1879 to use anthropometric information for police investigation. Nowadays, all police forces in the world use this kind of information to resolve crimes. The first prototypes of terminals providing an automatic processing of the voice and digital fingerprints have been defined in the middle of the years 1970. Nowadays, biometric authentication systems have many applications [1]: border control, e-commerce, *etc*. The main benefits of this technology are to provide a better security, and to facilitate the authentication process for a user. Also, it is usually difficult to copy the biometric characteristics of an individual than most of other authentication methods such as passwords.

Despite the obvious advantages of biometric systems, their proliferation was not as much as attended. The main drawback is the uncertainty of the verification result. By contrast to password checking, the verification of biometric raw data is subject to errors and represented by a similarity percentage (100% is never reached). Others drawbacks related to vulnerabilities and usability issues exist. In addition, in order to be used in an industrial context, the quality of a biometric system must be precisely quantified. We need a reliable evaluation methodology in order to put into obviousness the benefit of a new biometric system. Moreover, many questions remain: Shall we be confident in this technology? What kind of biometric modalities can be used? What are the trends in this domain? The objective of this chapter is to answer these questions, by presenting an evaluation methodology of biometric systems.

Figure 1. Women clerical employees of Los Angeles Police Department getting fingerprinted and photographed in 1928 (source [2]).

The outline of the chapter is defined as follows: In Section 2, we present the general concepts of biometric systems as well as their limitations. We then present in Section 3 the evaluation aspects of biometric systems related to 1) data quality, 2) usability and 3) security. In Section 4, we focus on emerging trends in this research field. They mainly have for objective to define efficient biometric systems that respect the privacy of an individual and permit a good usability. A conclusion of the chapter is then given in Section 5.

2. Concepts and definitions

2.1. Biometrics

The term biometrics is originally Greek, "bios" and "metron", literally meaning "measurement of life". In its first meaning, it was defined as a *Part of biological science which applies statistical methods and probabilistic formulas to living beings*. In computer security, biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.

2.2. Biometric modalities

Each biometric information that can discriminate individuals is considered as a biometric modality. An example of biometric modalities is presented in Figure 2. An ideal biometric information should respect the following properties:

- Universality: all individuals must be characterized by this information.
- Uniqueness: this information must be as dissimilar as possible for two different individuals.
- Permanency: it should be present during the whole life of an individual.
- Collectability: it can be measured in an easy manner.
- Acceptability: it concerns the possibility of a real use by users.

http://dx.doi.org/10.5772/52084

Table 1 presents a comparison study of biometric modalities in terms of universality, uniqueness, permanency, collectability and acceptability. From this table, we can deduce that none biometric information satisfies simultaneously all these properties. As for example, DNA analysis is one of the most efficient techniques to verify the identity of an individual or to identify him/her. Nevertheless, it cannot be used for logical or physical access control not only for time computation reasons, but also because nobody would be ready to give some blood to make the verification. Hence, important attention should be done when choosing a specific modality for a specific application and a target population.

Figure 2. An example of biometric modalities. From left to right, top to bottom, face, fingerprint, gait, keystroke dynamics, DNA, iris, finger knuckle and hand veins information.

Information	U	N	P	C	A	E
DNA	Yes	Yes	Yes	Poor	Poor	*****
Gait	Yes	No	Poor	Yes	Yes	***
Keystroke dynamics	Yes	Yes	Poor	Yes	Yes	****
Voice	Yes	Yes	Poor	Yes	Yes	****
Iris	Yes	Yes	Yes	Yes	Poor	*****
Face	Yes	No	Poor	Yes	Yes	****
Hand geometry	Yes	No	Yes	Yes	Yes	****
Fingerprint	Yes	Yes	Yes	Yes	Fair	****

Table 1. Comparison study of biometric modalities in terms of universality (U), uniqueness (N), permanency (P), collectability (C), acceptability (A) and performance (E). For the performance, the number of stars is related to the modality's performance (i.e., EER) in the literature [3].

2.3. The general scheme of a biometric system

The biometric authentication process is divided into three main functionalities:

- **Enrolment**
  It constitutes the initial process of collecting biometric data samples from a person and subsequently creates a reference template representing a user's identity to be used for later comparison. An example of users' templates of different modalities is given in Figure 3.

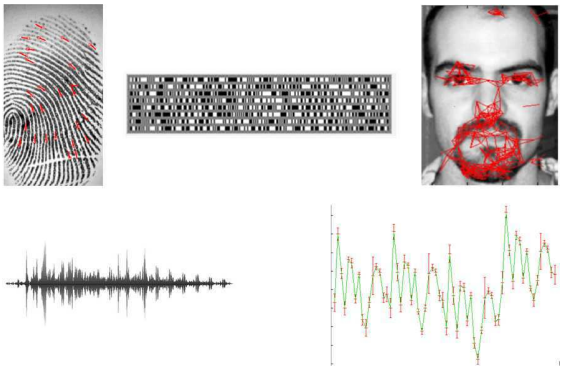

Figure 3. An example of biometric templates. From left to right, top to bottom, extracted minutia from a fingerprint, iris code, facial-based graph using keypoints, vocal and keystroke dynamics signals.

- **Verification**
  It provides a matching score between the biometric sample provided by the user and his/her template. The matching score is defined between 0% and 100% (100% is quite impossible to be reached).
- **Identification**
  It consists of determining the identity of an unknown individual from a database of individuals. In this case, the system can then either attribute the identity corresponding to the most similar profile found in the database to the unknown individual (or a list of the most similar profiles), or reject the individual.

2.4. Architecture of a biometric system

The generic architecture of a biometric system consists of five main modules as depicted in Figure 4:

- Capture 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 previously 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.

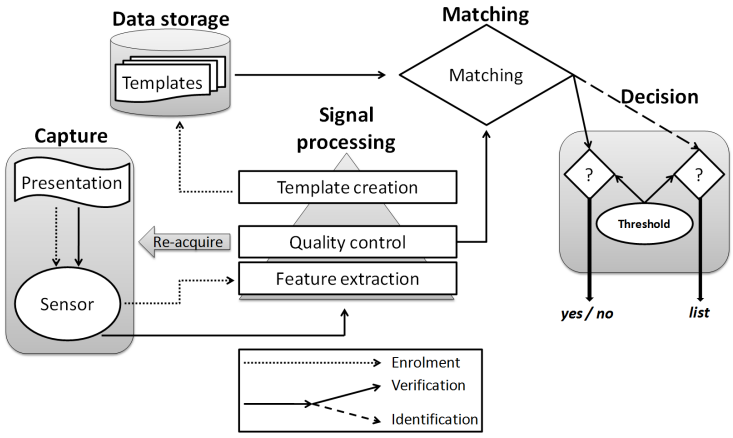

Figure 4. Generic architecture of a biometric system (source [4]).

2.5. Biometric systems limitations

Despite the advantages of biometric systems in terms of easy to use and to provide a better security comparing to traditional solutions, their use is limited to specific kind of applications (such as e-passport). These systems suffer from several limitations which may significantly decrease their widespread of use such as:

- Performance limitation: By contrast to password checking, the verification of biometric raw data is subject to errors and represented by a similarity percentage (100% is never reached). Verification errors are due to many reasons such as the variations of human characteristics (*e.g.*, occlusions [5]), environmental factors (*e.g.*, illuminations [6]) and cross-device matching [7]. This kind of acquisition artifacts may deeply affect the performance of biometric systems and hence, decrease their use in real life applications.
- Acceptability limitations: The use of biometric systems is related its perceived acceptability and satisfaction. Table 1 shows that not all the biometric modalities are accepted. However, the acceptability is also related to its context of use and the target population. Jain et al. (2004) [1] categorize the fundamental barriers in biometrics into three main categories: 1) accuracy in terms of errors, 2) scale or size of the database and 3) usability in terms of easiness to use, acceptability, *etc*. One government can decide that an individual would be identified through a biometric data embedded in the passport. For logical or physical access control in a company, it is more difficult to impose a system that would be not accepted by users.

- Architecture limitations: Several existing works [8–11] show the vulnerability of biometric systems. Ratha *et al.* have identified eight locations of possible attacks in a generic biometric system as depicted in Figure 5. Maltoni *et al.* present several drawbacks of biometric systems related to circumvention, repudiation, contamination, collusion and coercion threats. In addition to these presented threats, several works (such as [11]) present attacks on biometric systems related to the identified points presented in Figure 5. An example of type-1 attacks (*i.e.*, sensor) is given in Figure 6.

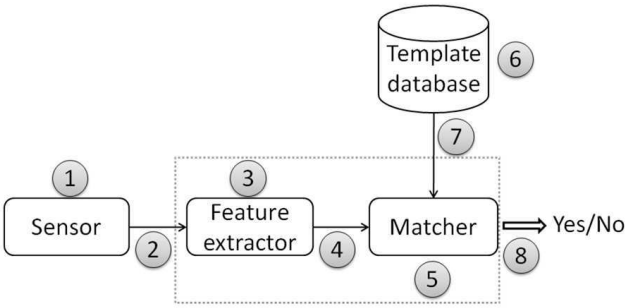

Figure 5. Possible attack points in a generic biometric system: Ratha *et al.* model.

Figure 6. A prosthetic finger created out of latex at the GREYC research laboratory.

3. Evaluation of biometric systems

As shown in the previous section, biometric systems have several limitations which may significantly decrease their use in real life applications. Therefore, the evaluation of biometric systems is carefully considered in the literature. Such kind of evaluation can be categorized into three main categories as depicted in Figure 7: 1) data quality, 2) usability and 3) security. In this section, we present these evaluation aspects followed by a discussion.

3.1. Data quality

The quality assessment of biometric raw data is receiving more and more attention since it is considered as one of the main factors affecting the overall performance of biometric systems. This is mainly due to the acquisition artefacts such as illumination. Therefore, controlling the quality of the biometric raw data is absolutely necessary. Using the quality information, poor quality samples can be removed during the enrollment phase or rejected during the

http://dx.doi.org/10.5772/52084

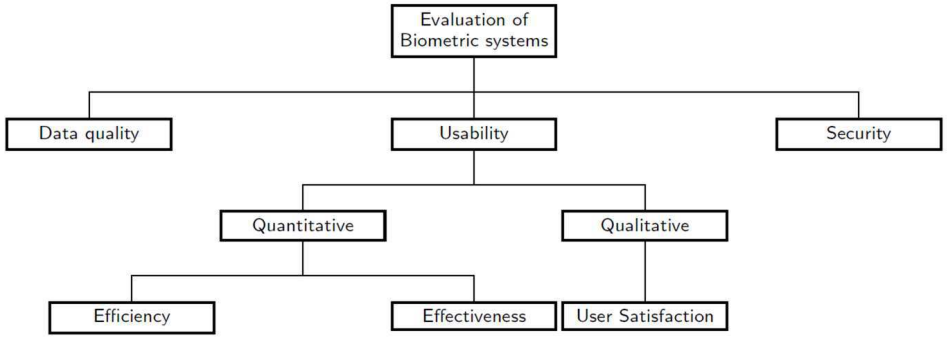

Figure 7. Evaluation aspects of biometric systems: data quality, usability and security.

verification. Such information could be also used for soft biometrics and multimodal approaches [12, 13].

According to the International Organization for Standardization [14], the quality assessment of biometric raw data is divided into three points of view as illustrated in Figure 8:

- Character: refers to the quality of the physical features of the individual.
- Fidelity: refers to the degree of similarity between a biometric sample and its source.
- Utility: refers to the impact of the individual biometric sample on the overall performance of a biometric system.

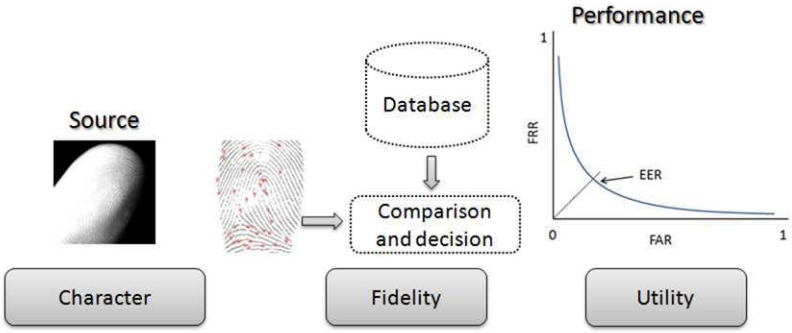

Figure 8. Quality assessment of biometric raw data: character, fidelity and utility.

In biometrics, there is an international consensus on the fact that the quality of a biometric sample should be related to its recognition performance [15]. Therefore, we present in this section an overview of the existing morphological-based quality metrics related to the *utility* point of view.

Alonso-Fernandez et al. (2007) [16] present an overview of existing fingerprint quality metrics. The authors show the impact of bad quality samples on the performance of biometric systems. Many other fingerprint quality algorithms exist [17–19]. The presented methods

have shown their efficiency in predicting the quality of fingerprints images. An example of these metrics is the NIST Fingerprint Image Quality metric (NFIQ) [20] proposed by the NIST. NFIQ metric is dedicated to fingerprint quality evaluation.

Krichen et al. (2007) [5] present a probabilistic iris quality measure based on a Gaussian Mixture Model (GMM). The authors compared the efficiency of their metric with existing ones according two types of alterations (occlusions and blurring) which may significantly decrease the performance of iris recognition systems. Other iris quality metrics are presented in [21, 22].

He et al. (2008) [23] present a hierarchical model to compute the biometric sample quality at three levels: database, class and image quality levels. The method is based on the quantiles of genuine and impostor matching score distributions.

Zhang & Wang (2009) [6] present an asymmetry-based quality assessment method of face images. The method uses SIFT descriptor for quality assessment. The presented method has shown its robustness against illumination and pose variations. Another asymmetry-based method is presented in [24, 25].

Abed, Giot, Hemery, Charrier & Rosenberger (2011) [26] present a quality assessment method based on the use of two types of information: 1) image quality and 2) pattern-based quality using the SIFT descriptor. The presented metric has the advantages of being multimodal (face, fingerprint and hand veins), and independent from the used authentication system.

3.2. Usability

According to ISO 13407:1999 (1999), usability is defined as "*The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use*".

- Efficiency which means that users must be able to accomplish the tasks easily and in a timely manner. It is generally measured as a task time.
- Effectiveness which means that users are able to complete the desired tasks without too much effort. It is generally measured by common metrics including completion rate and number of errors such failure-to-enroll rate (FTE).
- User satisfaction which measures users' acceptance and satisfaction regarding the system. It is generally measured by studying several properties such as easiness to use, trust, *etc.*

We present in Section 3.2.1 the existing works related to performance (Efficiency and Effectiveness), whereas in Section 3.2.2 the acceptance and users' satisfaction aspect.

3.2.1. Performance

As shown in Section 2.5, biometric systems are subject to several kinds of errors. We present in this section an overview of the most used performance metrics [4, 28] in the literature, followed by a presentation of the existing evaluation competitions and platforms.

http://dx.doi.org/10.5772/52084

3.2.1.1 Metrics

1. Fundamental performance metrics
   - Failure-to-enroll rate (FTE): proportion of the user population for whom the biometric system fails to capture or extract usable information from the biometric sample.
   - Failure-to-acquire rate (FTA): proportion of verification or identification attempts for which a biometric system is unable to capture a sample or locate an image or signal of sufficient quality.
   - False-match-rate (FMR): the rate for incorrect positive matches by the matching algorithm for single template comparison attempts.
   - False-non-match rate (FNMR): the rate for incorrect negative matches by the matching algorithm for single template comparison attempts.

   In addition to these error metrics, other performance metrics are used in order to ensure the operational use of biometric systems such as: 1) average enrollment time, 2) average verification time, 3) average and maximum template size and 4) maximum amount of memory allocated.
2. Verification system performance metrics
   - False rejection rate (FRR): proportion of authentic users that are incorrectly denied. If a verification transaction consists of a single attempt, the false reject rate would be given by:

$$FRR(\tau) = FTA + FNMR(\tau) * (1 - FTA) \tag{1}$$

   - False acceptation rate (FAR): proportion of impostors that are accepted by the biometric system. If a verification transaction consists of a single attempt, the false accept rate would be given by:

$$FAR(\tau) = FMR(\tau) * (1 - FTA) \tag{2}$$

   - Receiver operating characteristic curve (ROC): plot of the rate of FMR as well as FAR (*i.e.*, accepted impostor attempts) on the x-axis against the corresponding rate of FNMR as well as FRR (*i.e.*, rejected genuine attempts) on the y-axis plotted parametrically as a function of the decision threshold. An illustration of a ROC curve is presented in Figure 9.
   - Equal Error Rate (EER): this error rate corresponds to the point at which the FAR and FRR cross (compromise between FAR and FRR). It is widely used to evaluate and to compare biometric authentication systems. More the EER is near to 0%, better is the performance of the target system.
3. Identification system performance metrics
   - Identification rate (IR): the identification rate at rate r is defined as the proportion of identification transactions by users enrolled in the system in which the user's correct identifier is among those returned.

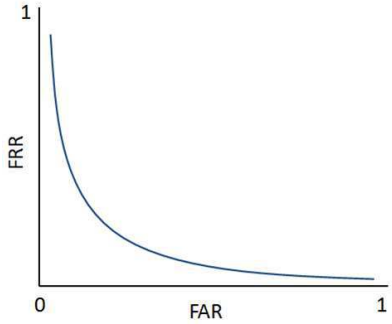

Figure 9. Example of a ROC curve: FAR against FRR.

- False-negative identification-error rate (FNIR): proportion of identification transactions by users enrolled in the system in which the user's correct identifier is not among those returned. For an identification transaction consisting of one attempt against a database of size N, it is defined as:

$$FNIR(\tau) = FTA + (1 - FTA) * FNMR(\tau) \tag{3}$$

- False-positive identification-error rate (FPIR): proportion of identification transactions by users not enrolled in the system, where an identifier is returned. For an identification transaction consisting of one attempt against a database of size N, it is defined as:

$$FPIR = (1 - FTA) * (1 - (1 - FMR)^N) \tag{4}$$

- Cumulative match characteristic curve (CMC): graphical presentation of results of an identification task test, plotting rank values on the x-axis and the probability of correct identification at or below that rank on the y-axis. Examples of CMC curves are given in Figure 10.

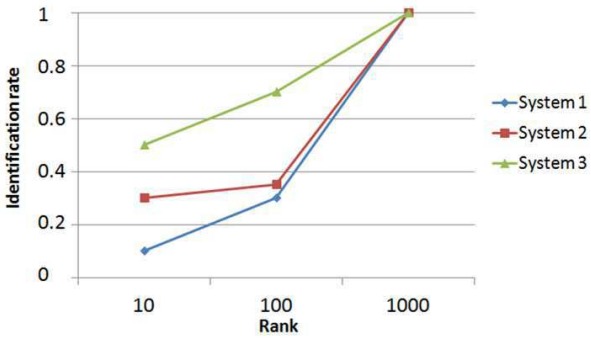

Figure 10. Examples of CMC curves of three biometric systems.

http://dx.doi.org/10.5772/52084

3.2.1.2 Competitions

Several biometric competitions are done in order to compare the performance of biometric systems and are divided into two categories: 1) monomodal and 2) multimodal competitions.

1. Monomodal competitions
   - Signature Verification Competition (SVC) [29]: It is a dynamic signature-based competition organized with the International Conference on Biometric Authentication (ICBA) in 2004. The EER is used as a performance metric.
   - Fingerpint Verification Competition (FVC): It consists of a series of fingerprint-based competitions (http://bias.csr.unibo.it/fvc2006/) organized in 2000, 2002, 2004 and 2006. The participants have tested their algorithms by providing both executables corresponding to the *enrollment* and *verification* phases. Four databases, three real and one synthetic using *SFinGe* software, are used during FVC2006 competition. Different performance metrics are used such as: the distribution of genuine and impostor scores, average and maximum template size, average enrollment and verification time, FTE and ROC curves.
   - Face Recognition Vendor Test (FRVT) and Iris Challenge Evaluation (ICE): both competitions were organized by the National Institute of Standards and Technology (NIST). The ROC curves are used as a performance metric.
   - Speaker Recognition Evaluation (SRE): It consists of a series of voice-based competitions organized by the NIST (http://www.itl.nist.gov/iad/mig/tests/sre/).
2. Multimodal competitions
   - BioSecure Multimodal Evaluation Campaign (BMEC): It is a competition organized by BioSecure (http://biosecure.it-sudparis.eu) in 2007. The BioSecure multimodal database [30] is used within the competition. The used experimental protocol and the results are detailed by by Mayoue et al. (2009) [31].
   - Multiple Biometric Grand Challenge (MBGC) [32]: It is a multimodal competition organized by the NIST in 2009. The main goal of this competition is to enhance the performance of face and iris-based systems over several acquisition conditions. It also consists of evaluating multimodal algorithms (image and score levels) of both modalities.

3.2.1.3 Platforms

- BioSecure Reference and Evaluation framework: BioSecure presents in [33] an evaluation framework based on open-source reference systems, publicly available databases, evaluation protocols and benchmarking results. The framework is available at http://svnext.it-sudparis.eu/svnview2-eph/ref_syst/ and has been used for the first time during the BioSecure Multimodal Evaluation Campaign (BMEC) in 2007. ROC curves and their corresponding EERs are used as a performance indicator.
- GREYC-Keystroke: It is a keystroke-based evaluation platform [34] developed at the GREYC research laboratory. GREYC-Keystroke software is also used to create keystroke databases in order to compare keystroke dynamics algorithms in the literature. Several performance metrics are used such as: the distribution of genuine and impostor scores, ROC curves and the FTA rate.

- Fingerprint Verification Competition-onGoing (FVC-onGoing): FVC-onGoing is an online fingerprint-based evaluation tool accessible at https://biolab.csr.unibo.it/FVCOnGoing. It is the evolution of the series of FVC competitions presented in the previous section. The used performance metrics are: acquisition errors (FTE and FTA), FNMR for a fixed FMR and vice-versa, average enrollment and verification time, maximum template size, genuine and impostor scores distribution, ROC curves and their corresponding EERs.

3.2.2. Users' acceptance and satisfaction

Traditional evaluation methods have worked well to evaluate emerging technologies, new biometric modalities, and algorithm revisions. Many databases have been collected (such as ENSIB face database [35]), many competitions and platforms have been proposed whose objective is mainly to compare enrollment and verification/identification algorithms in the literature. Many metrics have been defined by the International Organization for Standardization ISO/IEC 19795-1 (2006) [4] in terms of error computations, time computation, memory allocations, *etc*. These statistical measures allow in general a precise performance characterization of a biometric system. Nevertheless, these works are dedicated to quantify the system performance (algorithms, processing time, *etc.*) without taking into account user' view within the evaluation process. However, the biometric process is considered as a two-way interaction, between the user and the system. Therefore, taking into account user's view when designing biometric systems is considered as a crucial requirement to the widespread of use of this technology.

According to Smith (2003) [36], some members of the human-computer interaction (HCI) community believe that interfaces of security systems do not reflect good thinking in terms of creating a system that is easy to use, while maintaining an acceptable level of security. Nowadays, several studies have been done to quantify users' acceptability and satisfaction of biometric systems such as:

- The Opinion Research Corporation International ORC (2002) [37] presents the results of a phone survey conducted on 2001 and 2002. The survey has been conducted among national probability samples of 1017 and 1046 adults, respectively, living in United States. The 2001 study showed that 77% of individuals feel that finger-imaging protects individuals against fraud. For privacy issues, 87% in 2001 and 88% in 2002 are worried for the misuse of personal information. The study indicates a good percentage of acceptance, more than 75%, for U.S. law enforcement authorities requiring fingerprint scans to verify identity for passports, at airport check-ins and to obtain a driver license (see [37] for more details).
- The National Institute of Standards and Technology (NIST) has performed a usability test on fingerprints [38]. The survey was conducted on 300 adults recruited from a pool of 10,000 people. There were 151 women and 149 men ranging in ages from 18 to over 65 years. 77% of participants were in favor to provide fingerprint images as a mean of establishing identity for passport purposes. 2% of participants have expressed concerns about the cleanliness of the devices with which they would have physical contact. Another study has been done by NIST to examine the impact on fingerprint capture performance of angling the fingerprint scanners (flat, 10, 20 and 30 degrees) on the existing counter heights (99, 114.3 and 124.5 cm) is presented in in Theofanos et al. (2008) [39].

http://dx.doi.org/10.5772/52084

- Abed *et al.* [40] present a modality-independent evaluation methodology to study users' acceptance and satisfaction of biometric systems. It uses a survey questionnaire for data collection, and some data mining tools for their analysis. Three factors are identified as possible factors influencing respondents' acceptance and satisfaction: 1) the robustness of a systems against attacks, 2) its easiness to use and 3) the computation time during the verification phase. The authors then argue that even if the performance of a biometric system outperformed another one, it will not necessarily mean that it will be more operational or acceptable.
- Other studies presented in [41–48] have highlighted several points about biometric systems such as:
  - Acceptance is linked to the number of uses of the biometrics in general, and information provided by the biometric device can also improve user acceptance.
  - There is a potential concern about the misuse of personal data (*i.e.*, templates) which is seen as violating users' privacy and civil liberties. Another important concern is the probability that criminals may perpetrate heinous acts to gain access. This could include stalking or assaulting individuals to steal their biometric information.
  - Individuals complain that once the biometric template is stolen, it is compromised forever. There are also concerns about hygiene with touching such devices and health risks for more advanced technologies such as iris or retina.

3.3. Security

As shown in Section 2.5, biometric systems present several drawbacks which may significantly decrease their use in a an accurate way. Therefore, it is important that biometric systems be designed to withstand the presented threats when employed in security-critical applications and to achieve an end to end security. Despite the vulnerabilities of biometric systems, few are the works exist in comparison to the performance and quality aspects. Here is an overview of the works related to the security issue of biometric systems.

The International Organization for Standardization ISO/IEC FCD 19792 [49] presents a list of several threats and vulnerabilities of biometric systems. The standard also addresses privacy concerns when dealing with biometric systems. The standard does not present a security evaluation of biometric systems. It aims to guide the evaluators by giving suggestions and recommendations that should be taken into account during the evaluation process.

The Common Criteria Biometric Evaluation Working Group [50] presents a list of threats that may need to be considered when evaluating biometric systems.

Dimitriadis & Polemi (2004) [51] present a security comparison study of several biometric technologies in order to be used as an access control system for stadiums. The presented method can be used easily in comparing biometric systems since it is a quantitative-based method.

Attack tree technique introduced by [52], provides a structure tree to conduct security analysis of protocols, applications and networks. However, attack trees are dependent from the intended system and its context of use. Therefore, it is infeasible to be used for a generic evaluation purpose. An example of its use for the security evaluation of fingerprint recognition systems is presented by [53].

Matyás & Ríha (2002) [54] propose a security classification of biometric systems. Their proposal classifies biometric systems into four categories according to their security level. However, their model could not be considered as discriminative to compare the security level of biometric systems.

Abed et al. (2012) [55] present an on-line platform (*Security EvaBio*) to the security evaluation of biometric systems available at: http://www.epaymentbiometrics.ensicaen.fr/securityEvaBio/. A snapshot of the on-line platform is given in Figure 11. The platform implements a quantitative-based security assessment method based on the notion of risk factors, to allow easily the evaluation and comparison of biometric systems. It also contains a database of common threats and vulnerabilities of biometric systems which may be used by other researchers to quantify their developed systems in a quantitative or qualitative way.

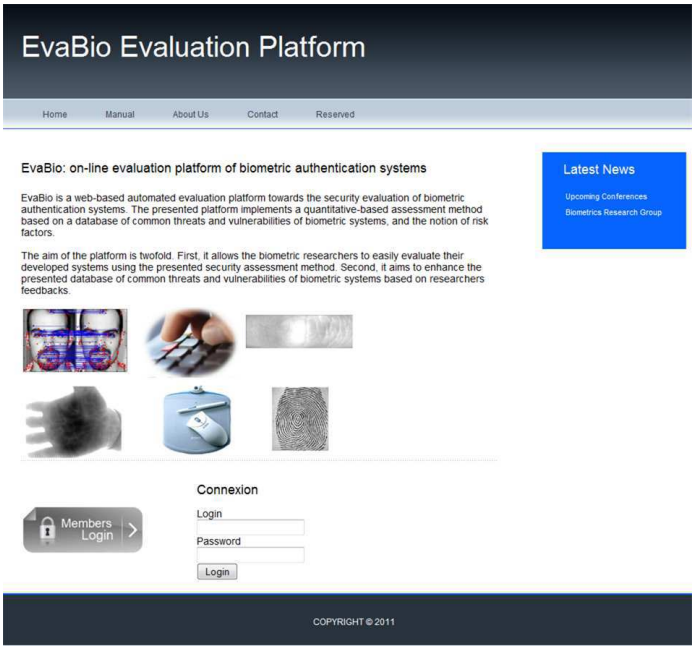

Figure 11. A snapshot of the Security EvaBio platform [55] developed at the GREYC research laboratory.

3.4. Discussion

Biometric systems are shown as a promising solution to authenticate individuals. However, their proliferation is not as much as attended. In this chapter, we see that biometric technology presents several drawbacks which may decrease their widespread of use in real life applications. Therefore, the evaluation of such systems is considered as a key challenge in this research field. Despite this, few are the works that address the evaluation aspects in comparison to recognition algorithms. More generally speaking, most of the existing

http://dx.doi.org/10.5772/52084

works aim to present a better recognition algorithm in terms of performance (*e.g.*, using the EER) without taking into account the other evaluation aspects in terms of data quality, users' acceptance and security. From the presented evaluation works, we can put into obvious these points:

- For the quality aspect, we see that most of the existing quality metrics are modality-dependent (such as NFIQ metric). A step forward is presented by Abed *et al.* which present a multimodal quality metric to evaluate the quality of biometric raw data. However, the presented quality metric do not detect luminance alteration which is considered as an important alteration especially in a facial-based modality. In addition, we believe that more works are required to be done in this evaluation aspect to ensure the accuracy of applications using **only one** biometric information as a reference (*e.g.*, one facial image in e-passport).
- For the security aspect, we see also that most of the existing works aim to present scenarios of attacks (such as hill-climbing attacks) on biometric systems. Few are the works dedicated to the security evaluation of such systems. We believe that more works should be done in this research area in order to ensure the accuracy of biometric systems.

Finally, we believe that taking into account simultaneously the presented evaluation aspects is important when evaluating and comparing biometric systems. In other words, a biometric systems providing 0% errors but not easy to use is not really important (such as DNA-based authentication systems).

4. Future trends

In this section, we present some future trends in biometrics research field. We focus only on those related to the evaluation of biometric systems.

4.1. Evaluation of multimodal-based biometric systems

In order to increase the performance of biometric systems, it is possible to combine different information for the decision making [56]. Different alternatives are available such as combining two different biometric systems (*e.g.*, face and fingerprint), using two sensors of the same modality (optical and sweeping fingerprint sensors), using two different algorithms given a single capture, exploiting different representations of a single biometric modality (2D and 3D face information) . . . Of course, the combination of the decision results given by these multiple biometric sensors can be realized by different techniques from the easiest way based on a logical combination (conjunction) to more complicated methods such as those based on fuzzy logic [57].

Even if the global performance of multi-modal biometric systems is improved, two main drawbacks make this solution rarely used in our daily life. The first one is due to the cost that is, of course, increased as many sensors are necessary. The second one concerns the usability for users that have to make many operations to be authenticated.

4.2. Evaluation of privacy by design biometric systems

One of the main drawbacks of biometrics is the impossibility to revoke the biometric data of a user if they are compromised [58]. Another problem, which is related to the acceptance by the users, is the respect of privacy: how can people be sure that their personal data collected during the enrollment will not be stolen or diverted and used for other purposes?

Over the last decade, a new innovative research field has emerged, trying to protect biometric templates. Nowadays, several protection schemes exist, but unfortunately not yet mature for large scale deployment. Examples of such schemes are fuzzy commitment [59], fuzzy vault scheme [60], and the BioHashing principle presented in several works by [61] and [62].

4.3. Quality assessment of 3D-based face data

In comparison to the 2D-based face recognition, 3D technology is considered as a promising solution to enhance the performance of biometric systems [63]. We believe also that this technology is an efficient solution to detect type-1 fakes (*e.g.*, presentation of a face image of good quality to the sensor). Moreover, quality assessment is required nowadays especially after the growing of this technology (such as 3D films like Avatar, *etc.*).

Despite the advantages of 3D technology in comparison to the 2D, none of the works exist to assess the quality of 3D biometric raw data. In addition, very few are the works addressing the quality assessment of 3D images/videos content. We can cite paired comparison is one of the standardized test methodologies toward the quality assessment of 3D images/videos. We can cite also a recent method toward the 3D quality assessment presented by [64].

5. Conclusion

Biometric systems are increasingly used in our daily life to manage the access of several resources. Several biometric technologies exist toward this goal, going from physiological-based features (such as face) to behavioral-based features (such as keystroke dynamics). However, a key issue to be considered is the evaluation of such systems. This is mainly important to ensure efficient biometric systems that respect the privacy of an individual, and to permit a good usability. In this chapter, we have presented an overview of the existing evaluation aspects of biometric systems based on: 1) **Data quality** which ensures that the quality of the acquired biometric raw data is of sufficient quality. This is mainly important for applications using only one biometric information as a reference (*e.g.*, e-passport); 2) **Usability** which ensures the operational use of the biometric system in terms of users' acceptability and satisfaction; and 3) **Security** which ensures the use of the system in an accurate way by avoiding well known attacks (such as a dummy finger). We have seen in this chapter the limitations of biometric systems, which constitute a main drawback to its proliferation. We have seen also that the existing evaluation works related to the data quality and security aspects are very few in comparison to the performance ones. Therefore, it is important to take more attention to these both evaluation aspects (data quality and security). Finally, we believe that the three evaluation aspects should be take into account simultaneously when evaluating and comparing biometric systems.

Acknowledgment

The authors would like to thank the French Research Ministry for their financial support of this work.

Author details

Mohamad El-Abed[1],
Christophe Charrier[2] and Christophe Rosenberger[2]

1 College of Science & Information Systems, Rafic Hariri University, Meshref Lebanon
2 Université de Caen Basse-Normandie, Caen, France

References

[1] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross. Biometrics: A grand challenge. *International Conference on Pattern Recognition (ICPR)*, 2:935–942, 2004.

[2] Women clerks –california–los angeles county. digital2.library.ucla.edu, 1928.

[3] J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo. Biometric authentication. *Encyclopedia of Information Science and Technology*, pages 346–354, 2008.

[4] ISO/IEC 19795-1. Information technology – biometric performance testing and reporting – part 1: Principles and framework, 2006.

[5] E. Krichen, S. Garcia Salicetti, and B. Dorizzi. A new probabilistic iris quality measure for comprehensive noise detection. In *IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS)*, pages 1–6, 2007.

[6] G. Zhang and Y. Wang. Asymmetry-based quality assessment of face images. In *Proceedings of the 5th International Symposium on Advances in Visual Computing (ISVC)*, volume 5876, pages 499–508, 2009.

[7] N. Poh, J.V. Kittler, and T. Bourlai. Quality-based score normalization with device qualitative information for multimodal biometric fusion. *IEEE Transactions on Systems, Man, and Cybernetics*, 40:539–554, 2010.

[8] N. K. Ratha, J. H. Connell, and R. M. Bolle. An analysis of minutiae matching strength. In *Audio- and Video-Based Biometric Person Authentication*, pages 223–228, 2001.

[9] T. V. der Putte and J. Keuning. Biometrical fingerprint recognition: Don't get your fingers burned. In *Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications*, volume 31, pages 289–306, 2000.

[10] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer-Verlag, 2003.

[11] U. Uludag and A. K. Jain. Attacks on biometric systems: A case study in fingerprints. In *Proc. SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI*, volume 5306, pages 622–633, 2004.

[12] N. Poh, T. Bourlai, and J. Kittler. A multimodal biometric test bed for quality-dependent, cost-sensitive and client-specific score-level fusion algorithms. *Pattern Recognition*, pages 1094–1105, 2010.

[13] N. Poh, T. Bourlai, J. Kittler, L. Allano, F. Alonso-Fernandez, O. Ambekar, J. Baker, B. Dorizzi, O. Fatukasi, J. Fierrez, H. Ganster, J. Ortega-Garcia, D. Maurer, A. A. Salah, T. Scheidat, and C. Vielhauer. Benchmarking quality-dependent and cost-sensitive score-level multimodal biometric fusion algorithms. *Transactions on Information Forensics and Security*, 4(4):849–866, 2009.

[14] ISO/IEC 29794-1. Biometric quality framework standard, first ed. jtc1/sc37/working group 3, 2006.

[15] P. Grother and E. Tabassi. Performance of biometric quality measures. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29:531–543, 2007.

[16] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun. A comparative study of fingerprint image-quality estimation methods. *IEEE Transactions on Information Forensics and Security*, 2:734–743, 2007.

[17] L. Shen, A. C. Kot, and W. M. Koo. Quality measures of fingerprint images. In *Proceedings of the 3rd International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 266–271, 2001.

[18] Y. Chen, S. C. Dass, and A. K. Jain. Fingerprint quality indices for predicting authentication performance. In *5th International Conference Audio- and Video-Based Biometric Person Authentication (AVBPA)*, volume 3546, pages 160–170, 2005.

[19] S. Lee, C. Lee, and J. Kim. Model-based quality estimation of fingerprint images. In *IAPR/IEEE International Conference on Biometrics (ICB'06)*, pages 229–235, 2006.

[20] E. Tabassi and C.L. Wilson. A novel approach to fingerprint image quality. In *International Conference on Image Processing (ICIP)*, pages 37–40, 2005.

[21] Y. Chen, S.C. Dass, and A.K. Jain. Localized iris image quality using 2-d wavelets. In *International Conference on Biometrics (ICB)*, 2006.

[22] N. D. Kalka, J. Zuo, N. A. Schmid, and B. Cukic. Image quality assessment for iris biometric. In *Proc. SPIE 6202*, 2006.

[23] Q. He, Z.A. Sun, T.N. Tan, and Y. Zou. A hierarchical model for the evaluation of biometric sample quality. In *International Conference on Pattern Recognition (ICPR)*, pages 1–4, 2008.

[24] X.F. Gao, S.Z. Li, R. Liu, and P.R. Zhang. Standardization of face image sample quality. In *International Conference on Biometrics (ICB'07)*, pages 242–251, 2007.

[25] J. Sang, Z. Lei, and S. Z. Li. Face image quality evaluation for ISO/IEC standards 19794-5 and 29794-5. In *Proceedings of the Third International Conference on Advances in Biometrics (ICB)*, pages 229–238, 2009.

[26] M. El Abed, R. Giot, B. Hemery, C. Charrier, and C. Rosenberger. A SVM-based model for the evaluation of biometric sample quality. In *IEEE International Workshop on Computational Intelligence in Biometrics and Identity Management*, pages 115–122, 2011.

[27] ISO 13407:1999. Human centred design process for interactive systems, 1999.

[28] James P. Egan. Signal detection theory and ROC-analysis. by Academic Press, New York, 1975.

[29] D.Y. Yeung, H. Chang, Y.M. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll. SVC2004: First International Signature Verification Competition. In *International Conference on Biometric Authentication (ICBA'04)*, pages 16 – 22, 2004.

[30] BIOSECURE. Biosecure Multimodal Biometric Database. http://www.biosecure.info/, 2008.

[31] A. Mayoue, B. Dorizzi, L. Allano, G. Chollet, J. Hennebert, D. Petrovska-Delacrétaz, and F. Verdet. *Guide to biometric reference systems and performance evaluation*, chapter The BioSecure multimodal evaluation campaign 2007 (BMEC'2007), pages 327–372. 2009.

[32] P. J. Phillips, P. J. Flynn, J. R. Beveridge, W. T. Scruggs, A. J. O'Toole, D. S. Bolme, K. W. Bowyer, B. A. Draper, G. H. Givens, Y. M. Lui, H. Sahibzada, J. A. Scallan, and S. Weimer. Overview of the multiple biometrics grand challenge. In *International Conference on Biometrics (ICB'09)*, pages 705 – 714, 2009.

[33] D. Petrovska and A. Mayoue. Description and documentation of the biosecure software library. Technical report, BioSecure, 2007.

[34] R. Giot, M. El Abed, and C. Rosenberger. Greyc keystroke : a benchmark for keystroke dynamics biometric systems. In *IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS)*, pages 1–6, 2009.

[35] B. Hemery, C. Rosenberger, and H. Laurent. The ENSIB database : a benchmark for face recognition. In *International Symposium on Signal Processing and its Applications (ISSPA), special session "Performance Evaluation and Benchmarking of Image and Video Processing"*, 2007.

[36] S. Smith. Humans in the loop: Human computer interaction and security. *IEEE Security & Privacy*, 3:75–79, 2003.

[37] ORC. Public Attitudes Toward the Uses of Biometric Identification Technologiesby Government and the Private Sector. Technical report, Opinion Research Corporation International (ORC), 2002.

[38] M. Theofanos, B. Stanton, S. Orandi, R. Micheals, and N.F. Zhang. Usability testing of ten-print fingerprint capture. Technical report, National Institute of Standards and Technology (NIST), 2007.

[39] M. Theofanos, B. Stanton, C. Sheppard, R. Micheals, N. Zhang, J. Wydler, L. Nadel, and W. Rubin. Usability testing of height and angles of ten-print fingerprint capture. Technical report, National Institute of Standards and Technology (NIST), 2008.

[40] M. El Abed, R. Giot, B. Hemery, and C. Rosenberger. Evaluation of biometric systems: A study of users' acceptance and satisfaction. *Inderscience International Journal of Biometrics*, pages 1–26, 2011.

[41] F. Deane, K. Barrelle, R. Henderson, and D. Mahar. Perceived acceptability of biometric security systems. *Computers & Security*, 14:225–231, 1995.

[42] L. Coventry, A. De Angeli, and G. Johnson. Honest it's me! self service verification. In *The ACM Conference on Human Factors in Computing Systems (CHI)*, pages 1–4, 2003.

[43] J. Moody. Public perceptions of biometric devices: The effect of misinformation on acceptance and use. In *the Informing Science and Information Technology Education*, volume 1, pages 753–761, 2004.

[44] L. A. Jones, A. I. Antón, and J. B. Earp. Towards understanding user perceptions of authentication technologies. In *ACM Workshop on Privacy in the Electronic Society*, pages 91–98, 2007.

[45] S. J. Elliott, S. A. Massie, and M. J. Sutton. The perception of biometric technology: A survey. *Automatic Identification Advanced Technologies*, pages 259–264, 2007.

[46] A. P. Pons and P. Polak. Understanding user perspectives on biometric technology. *Communications of the Association for Computing Machinery (ACM)*, 51(9):115–118, 2008.

[47] R. Giot, M. El Abed, and C. Rosenberger. Keystroke dynamics authentication for collaborative systems. *Collaborative Technologies and Systems, International Symposium*, pages 172–179, 2009.

[48] M. El Abed, R. Giot, B. Hemery, and C. Rosenberger. A study of users' acceptance and satisfaction of biometric systems. In *International Carnahan Conference on Security Technology (ICCST)*, pages 170–178, 2010.

[49] ISO/IEC FCD 19792. Information technology – security techniques – security evaluation of biometrics, 2008.

[50] Common criteria for information technology security evaluation. Technical report, 1999.

[51] C. Dimitriadis and D. Polemi. Application of multi-criteria analysis for the creation of a risk assessment knowledgebase for biometric systems. In *international conference on biometric authentication (ICB)*, volume 3072, pages 724–730, 2004.

[52] B. Schneier. Attack trees. *Dr. Dobb's Journ. of Softw. Tools*, 1999.

[53] O. Henniger, D. Scheuermann, and T. Kniess. On security evaluation of fingerprint recognition systems. In *Internation Biometric Performance Testing Conference (IBPC)*, pages 1–10, 2010.

[54] V. Matyás and Z. Ríha. Biometric authentication - security and usability. In *Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security*, pages 227–239, 2002.

[55] M. El Abed, P. Lacharme, and C. Rosenberger. Security evabio: An analysis tool for the security evaluation of biometric authentication systems. In *the 5th IAPR/IEEE International Conference on Biometrics (ICB)*, pages 1–6, 2012.

[56] A. Ross, K. Nandakumar, , and A.K. Jain. *Handbook of Multibiometrics*. Springer, 2006.

[57] A. Azzini, S. Marrara, R. Sassi, and F. Scotti. A fuzzy approach to multimodal biometric authentication. In *Knowledge-Based Intelligent Information and Engineering Systems*, number 8, pages 801–808, 2007.

[58] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008:1–17, 2007.

[59] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *ACM Conference on Computer and Communication Security*, pages 28–36, 1999.

[60] A. Juels and M. Sudan. A fuzzy vault scheme. In *IEEE International Symposium on Information Theory*, pages 237–257, 2001.

[61] A. Goh and C. Ngo. *Computation of Cryptographic Keys from Face Biometrics*. Lecture Notes in Computer Science. Springer, Berlin, 2003.

[62] R. Belguechi, C. Rosenberger, and S.A. Aoudia. Biohashing for securing minutia template. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR'10)*, pages 1168–1171, 2010.

[63] S. Berretti, A. D. Bimbo, P. Pala, B. B. Amor, and M. Daoudi. A set of selected sift features for 3D facial expression recognition. In *Proceedings of the 20th International Conference on Pattern Recognition (ICPR)*, pages 4125–4128, 2010.

[64] J. Lee, L. Goldman, and T. Ebrahimi. A new analysis method for paired comparison and its application to 3d quality assessment. In *Proceedings of the 19th ACM International Conference on Multimedia*, pages 1281–1284, 2011.