INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
ISSN 1841-9836, 11(3):315-330, June 2016.

Biometrics Systems and Technologies: A survey

I. Buciu, A. Gacsadi

Ioan Buciu*, Alexandru Gacsadi
Department of Electronics and Telecommunications
Faculty of Electrical Engineering and Information Technology
University of Oradea, 410087, Romania
*Corresponding author: ibuciu@uoradea.ro

Abstract: In a nutshell, a biometric security system requires a user to provide some biometric features which are then verified against some stored biometric templates. Nowadays, the traditional password based authentication method tends to be replaced by advanced biometrics technologies. Biometric based authentication is becoming increasingly appealing and common for most of the human-computer interaction devices. To give only one recent example, *Microsoft* augmented its brand new Windows 10 OS version with the capability of supporting face recognition when the user login in. This chapter does not intend to cover a comprehensive and detailed list of biometric techniques. The chapter rather aims at briefly discussing biometric related items, including principles, definitions, biometric modalities and technologies along with their advantages, disadvantages or limitations, and biometric standards, targeting unfamiliar readers. It also mentions the attributes of a biometric system as well as attacks on biometrics. Important reference sources are pointed out so that the interested reader may gain deeper in-depth knowledge by consulting them.
Keywords: biometric modalities, biometric attacks, biometric standards.

1 Biometrics - Introduction

Let us begin with a simple scenario. Let us assume a user wants to remotely access a tele-presence group with secured and restricted credentials. The access is done by launching a verification application requiring a password and user ID. Unfortunately, for some reasons, the user does not remember the password. In this case, the application or system provides a link for *Forgot Password*. The user needs then to type his e-mail address to which a new temporary password is sent by the verification system. The user enters his e-mail account, copies the temporary password and the system asks the user to change again the temporary password with a new more meaningful password. Moreover, the brand new password must be re-typed to avoid any typo mistake. The whole process may take several minutes and requires the use of the keyboard for several times, not mentioning memorizing or writing down the brand new password. The action may become very frustrating and inconvenient for the user who might become angry soon. Let us now consider there is another application which can get the user access easily and very fast without requiring any typing and with a minimum user interaction or effort. Such applications already exist and they are based on user's biometric features.

A biometric feature can be defined as a physiological (face, fingerprints, iris, etc.) or behavioural (gait, voice, signature, etc.) attribute of a human being that can discriminate one individual from another. Nowadays, the great interest for biometric recognition systems can be justified due to increased demand for security. The goal of a biometric based recognition system is either automatic identification or verification of identities, given input data comprising images, speech or videos. Unlike the traditional ways, such as password, biometric traits have some advantages: they cannot be stolen (although spoof attacks may exist to tamper the biometric system), lost or forget. However, to be reliable, biometric traits should be unique and persistent

over time. Some other criteria should be met such as user convenience and acceptability (mainly due to privacy reasons). Biometric recognition is usually performed by extracting a biometric template in query from the input device and compare it against some enrolled biometric templates. The comparison is processed using of the two modes: a) verification (or authentication) and b) identification (or recognition). *Verification* is an one-to-one process where the query face is compared against the user claiming his genuine identity to verify his claimed ID. The output is binary, either accept or reject, based on a matching procedure. We should note here that a biometric authentication technology may be used in conjunction with traditional authentication methods such as password, passports, PIN, smart cards, access tokens, etc, employed as second factor authentication. *Identification* is one-to-many process where the query is compared against each enrolled biometric template (multiple templates) from the database to search for the identity of the query. Identification is a bit more complex than verification as the system serves as both identifier and authenticator. A biometric based recognition system needs an *enrollment* procedure which allows the registration of persons in a biometric database that may be later used for identification or verification. The acquired initial data may undergo some pre-processing steps depending on the biometric modality. For instance, in the case of images, histogram equalization may help when the image suffers from illumination imbalance. For audio data, voice separation from the background may be also a pre-processing step. Biometric features are constructed by feature extraction step resulting a biometric template, further stored in the database. After a person is enrolled, the person's biometrics are scanned and matched against the enrolled biometric templates. *Matching* is a complex pattern recognition problem between the enrolled samples and the test one. A *matching score* is computed to reflect the similarity between two biometric templates. Overall, the person's recognition process is challenging because the representation of the same biometric is basically taken either by different sensors or, more often, at two or multiple different points in time, so that the acquisition conditions between the enroll and test samples may greatly vary due to various factors: noise, change in illumination, partial occlusion, different resolution, etc. This issue translates in a matching score lower than its optimum value. A *threshold level* is next setup for a final decision. A matching score higher than the threshold would give a match and consequently an accept, while a lower score would lead to rejection.

The associated risks for any biometric system are *false accept* (when an unauthorized person is wrongly accepted), represented by *False Acceptance Rate* (FAR) and *false reject* (when an authorized person is incorrectly denied for access), represented by *False Rejection Rate* (FRR). An ideal biometric system should have both FAR = FRR = 0. In real life, no such biometric system or technology exists. While connected to the threshold level, FAR and FRR are inversely proportional. More precisely, a low threshold level would decrease FRR and increase FAR. This situation is preferred for applications where the level of security is not critical. However, for applications demanding high security level, the threshold is set to a very high value to favour low FAR in detriment of high (possible disturbing) FRR. One such applications is the authorized and secure remote access for telepresence requiring very strict authorization. When FRR equals FAR we have Equal Error Rate (EER), a measure that is often reported when the performance of a biometric system or technology is addressed.

Biometric systems or technologies can be categorized based on several classifications: a) physiological versus behavioural; b) cooperative versus non-cooperative; c) mono-modal versus multimodal biometric systems; d) contact versus touchless versus "at distance" (or remote) technology, e) server based versus mobile based biometric technology; f) human versus no human monitoring for data acquisition. The appropriateness of each classification is highly depending on the application type. For instance, a biometric based surveillance technology may operate with full a) category (face as physiological and gait as behavioural) using non-cooperative user interaction, remote sensors and server based processing (involving large video data), while the

contact based biometric type is fully absent. Similarly, a biometric authorization based access for telepresence application might also require either contact or contactless sensing technology, but no human monitoring is typically involved at the sensory remote spot.

2 Physiological versus Behavioural Biometrics

Physiological biometrics addresses direct measurement from parts of the human body, while behavioural biometrics relates to measurements derived from human actions. In terms of acquisition, behavioural biometrics need measurements acquired over a certain period of time which is an important factor.

2.1 Physiological Biometrics

The majority of commercial biometrics technologies involve physiological measurements which are considered to remain steady over relatively large time interval. Such measurements may include the following modalities:

- face recognition
- facial thermography
- fingerprint recognition
- hand geometry based recognition
- ear geometry based recognition
- iris recognition
- retina recognition
- vascular pattern recognition

The above biometric modalities have, more or less, reached maturity. However, the performance of such technologies are greatly dependent of application class. If, for a controlled acquisition environment (high image resolution, good quality light, occlusion free and steady images - a process preferable under external human monitoring) a face recognition technology may easily acquire a very high matching score for an genuine individual, the matching score may significantly degrade for different environmental conditions in the absence of a watching guard compensating the ideal conditions. This case is specific for surveillance applications or, more generally, when the remote biometric sensor is separated by the processing module location. Moreover, in the absence of any preventive or detective control, an attacker can get access by attacking the system with stolen biometric data (a printed photo of the genuine's face, fingerprint, video record, etc.). The scenario is closely related to *network authentication* such as telepresence, automated teller machine access, internet banking, mobile based biometrics, cloud technology. For a centralized biometric network, authentication the user who needs to be authenticated is physically present at the same site with the sensor while the recognition process takes place on a general - purpose computer or server, located some distance away from the sensor. The remote access is granted or rejected based on server decision which communicates with the sensor.

Face Recognition

Face identification and verification dates back to 60's when the computer vision community has started to address the problem. While the face recognition technology is somehow inferior as performance compared to other biometric modalities (such as iris recognition for example), it is more accepted due to its major advantage: it is the only physiological biometric that can be reliable measured at distance and, moreover, the authentication of the users can happen without their explicit interaction with the sensor or their knowledge. The performance of face recognition systems can vary considerable depending upon the context and various factors. The modifications of facial features are caused by both long-term and short-term changes. Long-terms changes refer to aging where prominent and wrinkles may appear upon the face and permanently change the facial texture. In this case, periodic enrollment is necessary to update the biometric template. Short - term changes may refer to weight loss or gain. Other factors affecting the system's accuracy are partial occlusions (growing beard or moustache, glasses, hat, scarf) or various environment conditions (distance from camera, varying lighting conditions, noise, motion blur, etc). Another factor is given by face position. While the enrollment is usually taken in frontal pose, the matching process may suffer from non-frontal pose acquisition, where pose estimation might be needed.

The face recognition systems and technologies are based either on 2D or 3D representation of the face appearance. The 2D based face biometrics systems are pose variant and rely on the information conveyed in the gray level structure of the facial image (2D face texture), while the 3D approaches are pose invariant and involve the volumetric structure of the face along with its depth map. The 3D image acquisition technologies come with different cost and approaches. The most cost-effective solution called stereo acquisition is to use several calibrated 2D cameras to acquire images simultaneously followed by 3D reconstruction. While the acquisition is fast, this approach is highly light sensitive. Changes in illumination can lead to image artifacts compromising the performance of the 3D face recognition system. An alternative is to project a structured light pattern on the facial surface during acquisition. A third solution relies on active sensing where a laser beam is scanning the face surface generating a reflected facial pattern. Once the facial data are acquired, either as 2D or 3D, an automatic landmarking process is necessary to detect facial interest points such as eyes, eyebrows, mouth contour, nose, chin, etc. These landmarks are further used for face registration so that facial features (landmarks) are localized at the same position (geometrical coordinates) across multiple face images. The process continues with feature extraction and matching. For feature extraction, various techniques were proposed, including subspace methods (principal component analysis, linear discriminant analysis, independent component analysis), filtering approaches (different implementation of Gabor wavelets) or statistical approaches (including vacuous versions of local binary patterns). For the last step, matching, methods starting from distance based classifiers (Euclidean distance, cosine similarity measure) up to complex classifiers (neural networks or support vector machines) were implemented. The literature presents an abundant source of methods and it is impossible to provide references for all representative proposed techniques. The reader my consult the most recent edited or authored face recognition books such as [1], [2], [3], [4], [5], [6], where all related aspects and techniques are presented in great details.

Facial Thermography

A very challenging issue for conventional face recognition systems is when they are operating under low illumination environment. Off-the-shell methods to cope with this issue exist, but their outcome is typically very noisy and the overall performance of this biometric system is slightly improved. One solution is to shift from visible spectrum to infrared (IR) or near infrared

(NIR) range that requires dedicated sensors. For long-wave IR (8 - 14 μm) the human body is a light source emitting heat due to the blood flow under the skin and the resulting thermal patterns can be collected in total darkness [7], [8], [9]. While an external light is not necessary, these sensors are completely useless when the system operates in daylight, as usually happens. This is because the body thermal patterns strongly interferes with the surrounding temperature coming from artificial light or sunlight. Alternatively, less heat sensitive near infrared spectrum - NIR (0.8 - 2.5 μm) can also be used. For a reliable functioning, the NIR sensor need an ambient light. Studies have reported, however, modest performances of somewhere between 84% and 93% [10], [11]. This is due to the fact that many facial texture patterns that are clearly distinctive in the visible spectrum are absent in the IR or even NIR facial imagery, thus lowering the discriminant capability of facial thermography based biometrics systems. Facial thermography is affected by medical conditions such as, for example, fever.

Fingerprint Recognition

The fingerprint recognition is perhaps the most used biometric having applications in both law enforcement and computer systems, having a mature and widely accepted technology. The technology is implemented on various platforms and devices, including laptops, mobile phones or personal digital assistants. Conventional fingerprint systems belong to touch-based sensing technology and require touching or rolling a finger onto a rigid surface with a live-scan device. One disadvantage is the usability aspect as the system depends on the finger placement, finger scarfs or skin conditions (dirt, sweat, moisture). To make them robust against skin conditions, touchless fingerprint technologies are emerging. Two classes exist: reflection - based touchless finger imaging (RTFI) and transmission-based touchless finger imaging (TTFI). In the case of RTFI there are 2 light sources illuminating the fingerprint [12]. The finger must absorb only a small portion of the incident light, while the majority of light is reflected back to the optical detector. The device must be designed to allow different light quantity absorbed by the fingerprint's valleys compared to the light absorbed by the ridges to assure a good contrast. The other parameters such as the depth-of-focus and field-of-view of the camera, the irradiation and the frequency of the light sources are also crucial for reliable performance when the skin condition changes from dry to wet. The light sources has to be placed as close as possible to detector to minimize the shadowing effect and the emitted light should be in the blue spectrum (around 500 nm wavelength). The design is very complex and acquiring an optimum image contrast is not an easy task, leading to expensive devices compared to the touch-based fingerprint devices. The other approach, TTFI is similar to the optical coherence tomography principle where the light is transmitting through the finger [13] and the light that is back-scattered from the skin tissue is captured. The finger is placed between the light source and detector so that the light illuminates the nails side of the finger while the opposite finger part is oriented towards the detector. A red light with wavelength of 660 nm is used here because this wavelength corresponds to the maximum transmittance ratio to the skin tissue. The light penetrate the finger and then collected by the detector. Apart from high cost for the touchless fingerprint recognition technology, the curvature of the finger represents another limitation of this technology resulting in a relatively low interest for commercial adoption. The latter issue can be solved by employing a multi-vision system consisting of several cameras located on a semicircle and pointing out to the center of the finger. Such device may contain five cameras along with a set of green LED arrays to illuminate the finger [14]. Once the finger is in the correct position, each LED array is set to a specific light intensity and the five cameras start capturing a picture of the finger simultaneously. Using five cameras a enlarged (180 degree) field-of-view is obtained and the views are combined together to form a 3D finger reconstruction.

Hand Geometry based Recognition

Hand geometry based recognition systems consider the measurement of length, width, thickness, and surface area of the fingers and hand [15]. This biometric offers low security level because it is not scalable, i.e. those measurements do not tend to be unique for large-scale identification systems [16]. One important inconvenient is that such biometric systems require complex hardware to capture the hand image and may not be appropriate for computer-based login [17].

Iris Recognition

Iris recognition is the most reliable type of biometric identification. It is considered to be the ideal biometric in terms of uniqueness and stability (its features do not vary over time) leading to massive deployment for large-scale systems that proved to be very effective [18]. The iris is the colored portion of the eye surrounding the pupil and the biometric system searches for its specific intricate patterns composed of many furrows and ridges. The basic steps are: image acquisition, iris localization using landmark features and segmentation, biometric template generation and biometric template matching. The acquisition factors are resolution, signal/noise ratio, contrast and illumination wavelength. Once the iris is segmented, it may suffer a pseudo-polar coordinate transformation operation to take into account variations in pupil size. To capture the iris image, the conventional iris recognition technology requires a very short focal length, increasing the intrusiveness of this approach. However, iris recognition systems where the iris image is captured at longer distance exist nowadays. While for short focal length the image resolution is not an issue, this becomes very challenging with increasing distance, leading to significant drop in accuracy. Iris biometric technologies operating at long distance (beyond 1 m) are developed by various vendors. For instance, AOptix has implemented a system able to operate within a range of 1.5 - 2.5 m [19]. They have also developed a system having onboard coaxial imaging and adaptive optics to facilitate the capture of iris image at up to 18 m. Another vendor, Honeywell [20] has designed a combined face and iris recognition system that is capable of acquiring face and iris images at distances from 1 m and beyond 4 m. Carnegie Mellon University's CyLab Biometrics Center have been developing an iris recognition solution for the past several years that can successfully identify subjects from up to 12 meters away [21]. However, regardless of technology, one important aspect with the iris recognition systems is that the approach is not applicable when the user has contact lens.

Retina Recognition

In order to obtain retinal images, an infrared camera is used to capture the unique pattern of veins located at the back of the eye. Similarly to iris recognition, this modality also suffers from the problem of user inconvenience, which is even more inconvenient as the user is asked to carefully present their eyes to the camera at very close proximity. Another inconvenient is that this approach requires complex and expensive dedicated hardware, making such solution to be limited to applications with very high security demands [22]. On a positive side, unlike face, iris or fingerprint biometrics, retina based patterns are very difficult to spoof.

Vascular Pattern Recognition

This approach uses the subcutaneous vascular network on the back of the hand for specific individual patterns which are distinctive even for identical twins. A near-infrared light is emitted toward the back or palm of the hand. The reflected light prints an image on the sensor, image representing the encoded absorbance of blood vessels [23]. Due to the hemoglobin presented

in the blood, the veins appear as dark areas pattern and clearly delimited. The image is next digitized and specific features including vessel branching points, thickness, or branching angles are extracted as distinct features.

2.2 Behavioural Biometrics

The behavioural biometrics typically measures the behaviour of the user over time. This biometric type usually does not explicitly ask the user to be cooperative and thus, it is more transparent, user-friendly, less intrusive and more convenient than their physiological counterparts. On the downside, the behavioural biometrics suffers from low level of uniqueness and permanence, compared to the physical biometrics. Moreover, their accuracy for authentication is lower and are rather more suitable for verification. The approaches can be split into the following classes:

- gait recognition
- keystroke analysis based authentication
- mouse dynamics
- speaker recognition

Gait recognition

Analyzing the way an individual walks is the key issue for the gait recognition systems. The main advantage is the fact that this approach has no physical contact being ideal for acquiring data at long distance with low resolution. The fine details are not crucial here, rather the movement time patterns are considered. Such systems are influenced by external factors such as footwear walking surface or clothing. The gait recognition systems can be classified either as model based or appearance based [24]. Model based approaches fit a model representing time pattern of the human anatomy against video data then extracting and analyzing its parameters. Appearance model based approaches analyze the silhouette shape and motion of an individual and the way this vary in time. The images are recorded while the individual walks in a plane normal to the camera view. The performance of these biometric systems are highly dependent on the camera viewpoint. A change in the walking direction can negatively influence their performance. By using geometric cues, some systems improve viewpoint invariance when dealing with 2D imagery. Another alternative is to use 3D human figure capturing to have viewpoint independence. Both 2D and 3D approaches are described in great details in [24].

Keystroke analysis based authentication

Keystroke analysis based authentication is defined as the process of recognizing an individual from his typing characteristics. The verification can be performed either static (text-dependent) or dynamic (text-independent) mode. The characteristics are typically composed of the time between successive keystrokes, more precisely the inter-stroke latency, time durations between the keystrokes, dwell times (i.e. the time a key is pressed down), overall typing speed, frequency of errors (use of backspace), use of numpad, etc. For a large scale application, these characteristics are not unique amongst too many users. Therefore this analysis cannot be reliable used as recognition feature (although some report indicate this could also be possible [25]), but they can be suitable for verification systems. Aside from relative low accuracy, the enrollment procedure is the major drawback of such behavioural biometric systems. To generate representative biometric

templates the user might be asked to repeat the enroll procedure by providing a username, password or a specific text for a large number of times. An interesting application is presented in [26] where the keystroke dynamics based authentication has been analyzed in the context of collaborative systems.

Mouse dynamics

A behavioural profile can be also constructed using mouse actions performed by an user. Mouse derived features are easy to handle without user's knowledge. The mouse authentication involves registration phase and login phase. A template is built using the mouse features captured at the time of registration. The same template is compared with login details which are captured by the mouse task. In case of laptop, touchpad helps to extract the mouse features. The mouse's sensitivity affects the performance. The mouse features include general movement, drag and drop, stillness, point and click (single or double) actions, [27], [28].

Speaker recognition

Speaker recognition is the most researched behavioural biometric. Although the voice production considers the physical aspects of the mouth, nose and throat, this biometric is considered as behavioural type because the pronunciation and the manner of speech is intrinsically behavioural. The specific voice features refer to various analysis such as amplitude spectrum, localization of spectral peaks related to the vocal tract shape or pitch striations related to the user's glottal source. Similar to keystroke analysis, the speaker recognition can be performed either in static (text-dependent) or dynamic mode (text-independent) mode [29]. In the text-dependent mode the use is asked by the biometric system to pronounce a particular phrase, while, in the case of the text-independent mode the user is free to speak any phrase. In the latter case the verification accuracy usually improves as the text length increases. In between, a pseudo-dynamic mode exists where the user is requested to say two numbers randomly previously enrolled in a database. As principle, the normalized amplitude of the input signal is decomposed into several band-pass frequency channels with the purpose of feature extraction. The type of the extracted feature may vary. Typical features are the Fourier transform of the voice signal for each channel, along with some extra information consisting in pith, tone, cadence or shape of the larynx. Amongst behavioral biometric systems, the speaker recognition is the most accurate behavioral approach. Nevertheless, the voice might be perturbed by various factors such as illness, emotional or mental state or even age, conducting to inaccurate results.

3 Mobile and Web-based Biometrics Technology

According to Acuity Market Intelligence, the mobile biometric market will technically explode from $1.6 billion in 2014 to $34.6 billion in 2020 [30]. This prediction is foreseen for all biometric sensors (modalities) embedded in smart mobile devices (smart phones, tablets, and intelligent wearables. Another mobile biometrics considered also refer to biometric applications offered by vendors or mobile service providers, including retailers, payment procedures or banks. A third identified biometric sector is given by payment or non-payment transactions using secure web (cloud)-based services augmented with biometric authentication option. The report claimed that 100% of smart mobile devices will include embedded biometric sensors as a standard feature by 2020. According to the report, each year, more than 800 billion transactions requiring different level of biometric authentication will be processed, while more than 5.5 billion biometric applications are foreseen to be downloaded.

The aforementioned statistics come with no surprise. Millions of internet users experience a malware or hacker attack each year. The situation is even more critical with the use of mobile access where losses to fraud or identity theft are measured in the hundred of billions of dollars. Thus, implementing more authentication modalities by replacing the conventional ways with biometrics for mobile devices seems to be a reliable solution. Mobile biometrics solutions are implemented by device manufacturers as well as independent vendors as third-parties which offer software solutions. Intel Security Division has developed a biometric authentication application relying either on face or fingerprint named $TrueKey^{TM}$ [31], application available for various platforms either server-based or mobile. Another company, Sensory, released an authentication application named $TrulySecure^{TM}$ that combines voice and vision (face-based) authentication for mobile phones, tablets, and PCs [32]. Fingerprints, face, iris palm print or voice biometric authentication and verification solutions are developed by Neurotechnology [33].

Mobile technology also incorporates various biometric modalities. Devices with built-in fingerprint sensors exist on the market. One example is TouchID fingerprint technology developed for iPhone 5S by Apple, that incorporates a fingerprint module. Samsung also came up with fingerprint solution for its Samsung's Galaxy Tab S model as well as Samsung Galaxy S6 model. Vision based authentication solutions are allowed by all smartphones which integrate high resolution cameras into their hardware, facilitating third-parties to easily develop such software based authentication options. Other mobile or web-based biometric technology vendors include Applied Recognition with Ver-ID for various applications [34]. Notable, a facial biometric application has been recently released by IsItYou augmented with a unique anti-spoofing mechanism [35].

To address the interoperability among authentication devices a Fast IDentity Online (FIDO) Alliance was formed in 2012 [36], including powerful partners such as Google, Paypal, Miscrofsot, MasterCard, GitHub or DropBox. The alliance works towards creating secure interfaces between FIDO-enabled biometric devices and cloud-based website by developing dedicated plugins. FIDO is very active in defining web-based related biometric standards and a great impact is foreseen for macroeconomic application. Recently (November 2015), FIDO submitted to the World Wide Web Consortium three technical specifications with the purpose of defining a web-based API to be integrated into all web browsers and platform to facilitate a strong and secure authentication option.

4 Biometrics Attack

Similar to hacking a conventional authentication modality (password, token, etc), efforts have been made to hack or break a biometric authentication systems. A potential attack against a biometric system is possible for any component of the system. The network distributed (web-based) systems are more vulnerable to the attacks compared to the stand-alone biometric systems. This is due to the fact that, for a stand-alone biometric system, all processes are performed into a single processing unit. On the contrary, for physically disparate biometric systems, the attack may also occur in the transmission path, or any server performing the authentication.

The most common attack is the one against the sensor. When the samples acquisition process is fully automated (i.e. no watching guard exists to monitor the acquisition process) an impostor can easily bypass the system by simply presenting a copy of biometric data of a legitimate user in front of the sensor. The attempt of breaking the biometric system using such method is named spoofing attack. To date, there is no commercial biometric technology that is robust against such attacks.

The copy may come in various formats, depending on the biometric modality. In the case of facial biometric, the impostor may present a still image, video sequence playback, or even a 3D silica or rubber mask of the genuine user. A demonstration carried out by the Security

and Vulnerability Research Team of the University of Hanoi drawn attention regarding this issue by bringing evidence on how easy is to bypass the biometric systems namely Lenovo's Veriface III, Asus' SmartLogon V1.0.0005, or Toshibas Face Recognition version 2.0.2.32 - each set to its highest security level, using fake facial images of the valid user and thus gaining illegitimate access to the laptops [37]. This vulnerability was also tested in the spoofing challenge competition organized as special session at ICB 2013 [38]. These examples clearly point out the weaknesses of such systems and emphasize the necessity of incorporating reliable anti-spoofing mechanisms into the FA systems. Hence, not surprisingly, many research works were devoted to find robust solutions for detecting spoofing attacks. Within the same framework, a competition on counter measures to 2D facial spoofing attacks was also settled at ICB 2013 where anti-spoofing methods were evaluated [39]. The spoofing attack issue for various biometrics (face, iris, fingerprint, gait, etc) is a theme for the FP7 funded project TABULA RASA, where the topic was intensively and specifically addressed and analyzed [40]. Various solutions have been proposed to detect spoofing attacks. The spoof detection approaches may fall into four categories: a) challenge response based methods requiring user interaction, b) behavioral involuntary movements detection for parts of the face and head, c) data - driven characterization, and d) presence of special anti-spoofing devices. Google proposed a blinking based antispoofing mechanism [41].

The fingerprint modality can also be easily spoofed, as fingerprints are left behind on many objects the user touches. An impostor can use the same approach deployed by law enforcement agencies for lifting the fingerprints. Once lifted, a duplicate can be easily constructed from silicon or gelatin material. By so doing, in 2002, Matsumoto successfully fooled eleven different commercial fingerprint readers, with both optical and capacitive sensors, and some with live finger detection option, with a rate of success of 80% [42]. Matsumoto created a copy of a live finger as well as an artificial finger using a latent fingerprint left on a glass also accepted as genuine. Eleven years later (i.e. 2013), a biometrics hacking team of the Chaos Computer Club (CCC) has successfully bypassed the biometric security of Apple's TouchID implemented on iPhone 5S and Samsung Galaxy S5 [43]. Regarding Samsung's S5 biometric authentication system, the team claimed that not only it was possible to spoof the fingerprint authentication system, even after the device has been turned off, but the system also allows for seemingly unlimited authentication attempts without ever requiring a password, which was unacceptable. Two more years later, the vulnerability remains as it was reported at the Blackhat hacking conference in Las Vegas by Zhang et al. [44]. Similar to facial spoofing challenge competition, an iris and fingerprint based live detection competition is open [45]. The most recent report (2015) confirms the issue is still not solved, although some improvements exist [46].

Spoofing a real iris with a good quality image is also possible. Gupta et al. [47] used a commercial SDK, VeriEye [48] and successfully spoofed the system with printed images of iris.

Finally, voice impersonation can be applied to trick both automated and human verification for voice authentication systems [49]. A legitime user's voice can be recorded in various ways, including close proximity between the attacker and user, throughout a spam call or searching for audio-video recordings over the Internet. With the help of a voice morphing program, the attacker may synthesize the user's voice by using just a few samples. The cloned voice "borrowed" the features of the authentic voice and the authors successfully fooled the speaker authentication system that was based on the Bob Spear Speaker Verification System [50]. Their findings were alarming, i.e. the system was able to reject only 20 % of fake voices.

5 Attributes of Biometric Technology

The biometric systems and technologies is expected to posses several characteristics to be practically usable, as follows:

- Universality. This is the ability for a specific biometric system to be applied to a whole population of users. This is directly connected to Failure to Enroll (FTE) condition that refers to the case when a part of the population may not be enrolled for whatever reason. On particular reason is when the individual does not have the required biometric, leading to Failure to Enroll (FTA) error. A person suffering from mutism can not be enrolled with a speaker recognition technology; a fingerprint system can not be used for persons with missing fingers, etc.

- Uniqueness. The ability to successfully discriminate people. The biometric features must be as distinct as possible from one individual to another. The biometric features must convey large differences between individuals (large inter-class variability) while having small difference between samples taken from the same individual (small intra-class variability).

- Permanence. The ability of biometric features not to change over time. Some features do not change (iris, fingerprint patterns, vascular system, etc.) while others do (facial features). For time varying features a periodic biometric update is required.

- Collectibility. The ability of the system to perform the acquisition for any occasion (regardless of environment change, such as change in illumination, etc). There are cases where the acquisition process can not be performed for the same individual previously enrolled. For example, if the person suffers some skin condition destroying the epidermis or gets a serious scar on his finger, the fingerprint biometric authentication system will more likely output a false reject due to significant difference between the enroll and test biometric features. Similar scenario is possible for people suffering from cataract when tested with an iris authentication system, or people undergoing facial plastic surgery recovering from accidents or facial injury, when tested against a facial biometric system.

- Simplicity. Recording and transmission should be easy to use and not error-prone.

- Cost-efficiency. The whole process should be cost-efficient.

- Acceptability. The degree to which a biometric technology is found acceptable by the society. Typically, gross invasive biometric technologies (such as retina based systems) are tend to be less acceptable than those using non-invasive approaches (such as vision based or touchless sensors). Another aspect to be considered is the access to privacy.

- Scalability. This attribute refers to the ability of the system to accommodate a large number of enrollment individuals while providing a reasonable accuracy. The degree of scalability is application dependent. For instance, when using a biometric-based lock option for a mobile device with the intent to lock some specific applications inside the device, only one (device's owner) or a few individuals (perhaps family's members) would enroll. The matching is then either one-to-one or one-to-few type and the scalability is not an issue. On the contrary, for a network distributed system (such as bank application or decision systems) the number of enrolled individuals might easily reach millions and the system should cope with this overwhelming data. For such large-scale biometric application its performance (accuracy, FRR and FAR) is more critical. More exactly, one false rejection a month might be acceptable, but hundreds false rejection a day would be disastrous. The same rationale applies to FAR. Just to give a simple example, let us suppose a biometric system is 99.9% accurate. That is, if someone is an attacker, there is a 1-in-1000 chance that the biometric system fails to detect the attacker (outputs a false accept), while the same chance would be for a legitimate user to be denied as false attacker.

- Resilience. The ability of the system to handle exceptions. An example would be an individual whose biometric features might not be easily acquired. If a user has a broken arm, he may need human intervention to use a hand or fingerprint based biometric system.
- Circumventable. The ability of the system to detect attacks. An important role has the sensor that should be tamper-proof.

6 Biometric Standards

As noted throughout the chapter, a network distributed biometric technology involves several components, including the sensor, the communication channel, the web-based decisional server, components that rely on different hardware architecture. Not only the hardware is different but also the integrated software is different for each hardware configuration. Moreover, a fully operational system working on a specific operating system is not compatible with another operating system. Another representative example is provided by the multi-modal biometric systems relying on two or multiple biometric modalities (face, fingerprint, voice, as an example) that yield individual scores which are finally fused to output a single matching score. Without a common format that has to be shared among these modalities, the multi-modal biometric system can not operate. Finding mechanisms for each component of the biometric system to communicate has leaded to standardization. There are several working groups concerning biometric standards. At international level, the International Standard Organisation (ISO) and International Electrotechnical Commission (IEC) play a significant role. ISO and IEC have established a Joint Technical Committee 1 JTC 1/SC 37 [51] to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of formal international biometric standards. There are several aspects to consider, including Data Interchange Formats, Data Structure Standard and Technical Interface Standards.

- *Data Interchange Format* represents the lowest level of interoperability between systems using the same modality and addresses the actual representation of the biometric data itself. The number and type of features can vary considerable depending upon the matching algorithm. There is a need to format these features so that the other components of the system may properly interpret the transmitted information.
- Once the data is formatted it needs to be transmitted. *Data Structure Standard* addresses this by providing the necessary wrapper around the biometric data within the so called *Common Biometric Exchange File Format* to facilitate interoperability between different systems or system components, forward compatibility for technology improvement, and software hardware integration. Data Interchange Format Standards provide the mechanism for extraction, matching and decision modules of the biometric system. The main component of this standard is the *Biometric Information Record* composed of three parts. The first part named the *Standard Biometric Header* contains information to an application regarding the format of and other properties of the next part named the *Biometric Data Block* that contains the biometric data conforming to a defined format. The third part named the *Security Block* provides information related to the encryption protocol and the integrity of the Biometric Information Record.
- *Technical Interface Standards* provide an Application Programming Interface (API) by defining the format for the Biometric Information Record so that components can understand and interpret records. A representative standard is BioAPI [52] that defines

a framework for installing the components, making them compliant with plug-and-play concept. BioAPI tries to hide as much as of unique attributes of individual biometric technologies, vendor implementations, products and devices. A *Biometric Service Provider* could then plug the components throughout a *Service Provider Interface*. An application can use biometric services using two fundamental ways: either through primitive functions or through abstract functions. Primitive functions are the most basic functions and relates to $BioAPI\_Capture$, $BioAPI\_Process$, $BioAPI\_VerifyMatch$ and $BioAPI\_IdentifyMatch$. The abstract functions are defined by $BioAPI\_Enroll$, $BioAPI\_Verify$ and $BioAPI\_Identify$.

The standardization of biometric technology leaded to proper interoperability between and within biometric systems, ensuring a cost-effective technology implementation.

7 Conclusions

This paper only briefly touches the main issues of biometric systems and technologies, pointing out their differences, modalities, open problems and standardization. Their performance greatly vary upon the operating and external conditions as no universal biometric technology exists. The best performance is obtained where the technology is designed for strict controlled conditions and where data acquisition is accomplished under human supervision. Not mentioning a possible accuracy drop, when no human guard is present, a biometric system can be easily attacked and spoofed, a critical open issue yet to be solved. Intensive work is still undergoing to improve their performance while protecting them against various attacks.

Bibliography

[1] S. K. Zhou, R. Chellappa, Ramalingam, W. Zhao (2006), *Unconstrained Face Recognition*, Springer.

[2] K. Delac, M. Grgic (Eds.) (2007), *Face Recognition*, I-Tech Education and Publishing, Vienna, Austria.

[3] K. Delac, M. Grgic, M. S. Bartlett (Eds.) (2008), *Recent Advances in Face Recognition*, IN-TECH, Vienna, Austria.

[4] M. Tistarelli, S. Z. Li, R. Chellappa (Eds.)(2009), *Handbook of Remote Biometrics for Surveillance and Security*, Springer.

[5] S. Z. Li, Stan, A. Jain (Eds.)(2011), *Handbook of Face Recognition*, Springer.

[6] M. D. Marsico, M. Nappi, M. Tistarelli (Eds.)(2014), *Face Recognition in Adverse Conditions*, IGI-Global.

[7] X. Chen, P. J. Flynn, K. W. Bowyer (2005), IR and Visible Light Face Recognition, *Computer Image and Vision Understanding*, 99(3): 332–358.

[8] S. G. Kong, J. Heo, B. R. Abidi, J. K. Paik, M. A. Abidi (2005), Recent Advances in Visual and Infrared Face Recognition: A Review, *Computer Image and Vision Understanding*, 97(1): 103–135.

[9] D. Socolinsky, L. Wolff, J. Neuheisel, C. Eveland (2001), Illumination Invariant Face Recognition Using Thermal Infrared Imagery, *Proc. of 2001 IEEE Conf. on Computer Vision and Pattern Recognition*, 1: 527-534.

[10] D. Socolinsky, A. Salgian, J. D. Neuheisel (2003), Face recogniton with visible and thermal infrared imagery, *Computer Image and Vision Understanding*, 91(1): 72–114.

[11] D. Socolinsky, A. Selinger (2004), Thermal face recognition in an operational scenario, *Proc. of 2004 IEEE Conf. on Computer Vision and Pattern Recognition*, 1012-1019.

[12] Y. Song, C. Lee, J. Kim (2004), A New Scheme for Touchless Fingerprint Recognition System, *Proc. of 2004 Intl Symposium on Intelligent Signal Processing and Communication Systems*, 524-527.

[13] E. Sano, T. Maeda, T. Nakamura, M. Shikai, M. Sakata, M. Matshusita, K. Sasakawa (2006), Fingerprint Authentication Device Based on Optical Characteristics Inside a Finger, *Proc. of 2004 IEEE Conf. on Computer Vision and Pattern Recognition Workshop*, DOI:10.1109/CVPRW.2006.83.

[14] G. Parziale, E. Diaz-Santana, R. Hauke (2006), The surround Imager: a multi-camera touchless device to acquire 3d rolled-equivalent fingerprints, *Proc. of the 2006 Intl Conf. on Advances in Biometrics*, 244-250.

[15] R. Smith (2002), *Authentication: From Passwords to Public Keys*, Addison and Wesley, Boston.

[16] J. Ashbourn (2000), *Biometrics: Advanced Identity Verification: The Complete Guide*, Springer, London.

[17] `http://us.allegion.com/Products/biometrics/Pages/default.aspx`

[18] J. Daugman (1994), *Biometric personal identification system based on Iris Recognition*, U.S. Patent 5,291,560.

[19] M. J. Northcott, J. E. Graves (2008), *Iris Imaging Using Reflection from the Eyes*, U.S. Patent Application 200800002863.

[20] G. Geterman, V. Jacobsen, J. Jelinek, T. Phinney, R. Jmza, T. Ahrens, G. Kilgore, R. Whillock, S. Bedros (2008), *Combined Face and Iris Recognition*, U.S. Patent Application 20080075334.

[21] `http://www.cmu-biometrics.org/`

[22] R. Das (2014), *Biometric Technology: Authentication, Biocryptography, and Cloud-Based Architecture*, CRC Press.

[23] N. Miura, A. Nagasaka, T. Miyatake (2004), Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, *Machine Vision and Applications*, 15(4): 194-203.

[24] R. D. Seely , M. Goffredo, J. N. Carter, M. S. Nixon (2009), View Invariant Gait Recognition, *Handbook of Remote Biometrics for Surveillance and Security*, 61-81.

[25] J. Ilonen (2003), Keystroke dynamics, `http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/Ilonen.pdf`.

[26] R. Giot, M. El-Abed, C. Rosenberger (2009), Keystroke dynamics authentication for collaborative systems, *Intl. Symposium on Collaborative Technologies and Systems*, 172-179.

[27] P. Bours (2012), Continuous keystroke dynamics: A different perspective towards biometric evaluation, *Information Security Techn. Report Volume* 17(1-2): 36-43.

[28] C. Shen, Z. Cai, X. Guan, Y. Du, T. Yu (2013), User Authentication Through Mouse Dynamics, *IEEE Trans. on Information Forensics and Security* 8(1): 16-30.

[29] Z. Saquib, N. Salam, R. P. Nair, N. Pandey, A. Joshi (2010), A Survey on Automatic Speaker Recognition Systems, *Signal Processing and Multimedia*,134-145.

[30] The Global Biometrics and Mobility Report: The Convergence of Commerce and Privacy Market Analysis and Forecasts 2014 to 2020, Available at: http://www.acuity-mi.com/GBMR_Report.php, Accessed on 12 Dec. 2015.

[31] `https://www.truekey.com/` Accessed on 14 Dec. 2015.

[32] `http://www.sensory.com/products/technologies/trulysecure/`, Accessed on 14 Dec. 2015.

[33] `http://www.neurotechnology.com/`

[34] `http://appliedrec.com/`

[35] `http://www.isityou.biz/`

[36] `https://fidoalliance.org/`

[37] N. M. Duc and B. Q. Minh (2009), Your face is NOT your password, *Black Hat Conference*.

[38] `http://www.tabularasa-euproject.org/evaluations/tabula-rasa-spoofing-challenge-2013/`

[39] `http://www.biometrics-center.ch/testing/tabula-rasa-spoofing-challenge-2013`

[40] `http://www.tabularasa-euproject.org/`

[41] `http://www.google.com/patents/US8437513`, Accessed on 17 Dec. 2015.

[42] T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino (2002), Impact of Artificial Gummy Fingers on Fingerprint Systems, *Proc. of SPIE*, Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

[43] `https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid`

[44] Y. Zhang,Z. Chen, H. Xue, T. Wei (2015), Fingerprints On Mobile Devices: Abusing and Leaking, *Black Hat Conference*.

[45] `http://livdet.org/`

[46] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay, S. A. Schuckers (2015), LivDet 2015 Fingerprint Liveness Detection Competition 2015, Available at: `http://livdet.org/reports.php`

[47] P. Gupta, S. Behera, M. Vatsa, R. Singh (2014), On Iris Spoofing Using Print Attack, *Proc. of the 2014 22nd Intl Conf. on Pattern Recognition*, 1681-1686.

[48] VeriEye, Iris recognition software, http://www.neurotechnology.com/verieye.html

[49] D. Mukhopadhyay, M. Shirvanian and N. Saxena (2015), All Your Voices Are Belong to Us: Stealing Voices to Fool Humans and Machines, *European Symposium on Research in Computer Security.*

[50] E. Khoury, L. El Shafey, S. Marcel (2014), Spear: An open source toolbox for speaker recognition based on Bob, *IEEE Intl. Conf. on Acoustics, Speech and Signal Processing (ICASSP).*

[51] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on

[52] http://www.iso.org/iso/catalogue_detail.htm?csnumber=33922