Chapter 1

General introduction

Martin Drahanský[1] *and Svetlana Yanushkevich*[2]

1.1 Introduction

It is not necessary to discuss the biometrics, because this is well known not only in research area but nearly the whole population uses it. From the pioneer electro-mechanical systems moved the biometrics to digital world. At the beginning, we still have to present our physical biometric characteristics to the biometric system; however, the acquirement is immediately done into digital representation, i.e., we work with digital data. In most cases, biometric recognition is realized on image or video data.

On our body, we have many possibilities for biometric recognition. Of course, not all of our body parts are suitable for this task. When we neglect behavioral biometric characteristics, we can find two very important areas on our body, which offer a lot of biometric characteristics—these two areas are hand and head. On our hands we can use fingerprints, palmprints, 2D and 3D hand geometry, thermal image of the hand, finger veins, hand veins and nail structure. This topic will be discussed in the scope of this whole book. Considering our head, we can recognize 2D and 3D face, thermal image of the face, eye iris, eye retina, ear shape, lips movement and dental information. All these biometric characteristics predestine these areas to a really very important part of our body, because some of the abovementioned characteristics surely belong to the mostly used, including biometric travel documents (e-passports), where fingerprint, face and eye iris appear. The discussion is opened for other possible technologies, which are suitable for biometric travel documents; however, these are on hand or on head.

1.2 Hand physiology and its suitability for biometrics

As mentioned in the introductory part of this chapter, *hand* is really very interesting, because of having a lot of unique features, which could be extracted and used for comparison of people. Our hands are unique—this has been proven in the whole

[1]Faculty of Information Technology, Centre of Excellence IT4Innovations, Brno University of Technology, Czech Republic
[2]Faculty of Electrical and Computer Engineering, University of Calgary, Canada

year in which the biometric characteristics from hand are in use. It is essential that the human hand features are different for identical twins. The trouble arises especially for faces—identical twins have so similar faces that these cannot be distinguished from each other. Nevertheless, the most of other biometric characteristics on our body are not based only on DNA structure and similarity with our twin but are based on preterm development in the mother's womb. The position of fetus, inner pressure and other factors inside the mother's womb play an important role for building the structure of our cells. These factors influence nearly all of our biometric characteristics on hand. Only the hand geometry (especially in 2D) could be very similar to the twin ones. Fingerprints, veins structure, etc. are very unique for every person on the planet.

The inner hand physiology is discussed in the second chapter, the outer hand physiology in the third chapter and nail structure in the fourth chapter of this book. The *inner hand physiology* covers bones, tendons, muscles, cardiovascular system, etc. The most important diseases appearing in the inner hand structure, having influence on biometric characteristics, are discussed in the second chapter as well. The inner hand structure influences 2D and 3D hand geometry, hand thermal image, finger and hand veins structure. All these biometric characteristics could be influenced by the diseases appearing inside the hand. In many cases, the disease just slightly changes the structure, i.e., we nearly cannot detect any change, however sometimes (e.g., just simple edema) can make the biometric characteristics unusable for biometric recognition purposes.

When we speak about *outer hand physiology*, we mean especially skin. In the third chapter, there is discussed skin structure and dermatologic diseases as well. These diseases could be divided into three main categories [1,2]—(a) histopathologic changes, (b) color change and (c) combination of histopathologic and color changes. Just color change has a slight influence to just optical scanning technology, but no influence to other scanning technologies. On the other hand, the histopathologic changes cause change of the structure of ridges, which are crucial for fingerprint and palmprint recognition. The change of ridge structure could be caused by medicaments [3] as well; the medical drugs based on capecitabine are responsible for finger ridge structure disappearance. Luckily, after the use of this medicament is stopped, the finger ridge structure will be recovered. Unluckily, the patients who use capecitabine-based medicaments cannot use fingerprint recognition technology during the medical treatment.

The *nail* structure belongs to the outer hand physiology; however, this is such specific biometric feature that we devoted a separate chapter space to this topic, concretely the fourth chapter. The nail structure and diseases connected to nail are discussed. Nail structure is not used in biometrics, because there are many factors making this technology not very popular, especially troubles during scanning [the finger nail has to be placed into a chamber where camera and light source are placed in a certain position, the influence of surrounding light has to be blocked, the uniqueness (biometric entropy) of nail is not very high, some diseases influence the nail structure and the nail lacquer or artificial nails are totally making this technology unusable]. On the other hand, during scanning the

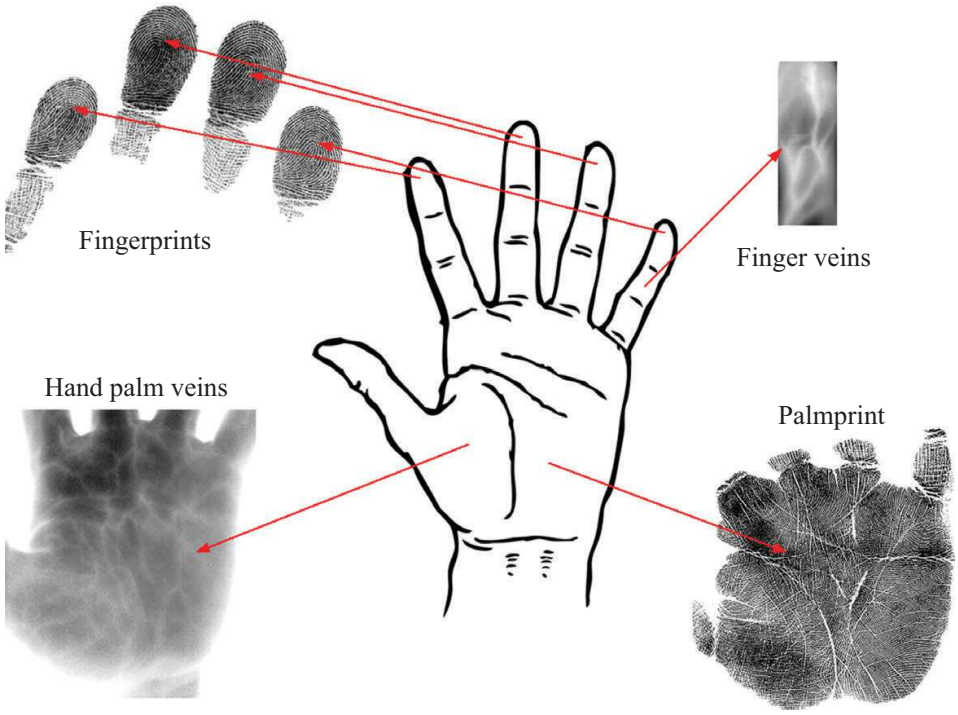

Figure 1.1 Biometric characteristics on hand palm

hand back, we can get a very nice nail structure, which is suitable for biometric recognition.

When we look on our hand palm, we can acquire and use the following biometric characteristics (see Figure 1.1):

- Fingerprint
- Palmprint (sometimes fingerprints are visible in the complete palmprint)
- Hand palm veins (under infrared illumination)
- Finger veins (under infrared illumination)
- Thermal image of the hand palm and fingers (will be discussed in the part of hand back)

Fingerprints are the mostly used biometric characteristic from the hand. In this book, you can find the introduction to the state of the art in Chapter 5. The basic information about fingerprint acquirement, (pre)processing and recognition are summarized here. Sometimes, the users have a connection of fingerprints with criminal police (they search for latent fingerprints on a crime scene); however, most people do not have any problem with the use of their fingerprints for biometric purposes. A good question is what happens with all fingerprints that are stored in large-scale national databases, because they are stored there forever and in some cases of lightly protected databases these fingerprints could be misused. Anyway, we will come to this topic later on. Because these large-scale databases include millions of fingerprints, it is necessary to speed up the process of recognition and search in these databases. This topic is covered in the sixth chapter. Furthermore, the troubles with fingerprints (the same could be applied to palmprint) have to be

discussed, because they are very prone to be influenced by dermatologic diseases. This topic is covered in the seventh chapter. Our team invested a lot of time into getting a unique database with annotated diseased fingerprints by a dermatologist. At the moment, we use these diseased fingerprints for analysis. However, this topic includes injuries, dirtiness on finger or scanner surface and other troubles, which can cause an end effect their inapplicability for automatic processing and recognition.

As mentioned in the previous paragraph, if an attacker or generally an impostor gets an unauthorized access to the database with fingerprints, he/she can misuse this stolen data. It is not necessary to copy the images of fingerprints (in most cases, they are not stored in the databases, just only extracted features); just a template with extracted features is suitable for production of a synthetic fingerprint with minutiae points on correct positions, with correct types and angles. This fingerprint has a different pattern and run of ridges, what we can observe by a naked eye immediately; however, for the algorithms based on minutiae recognition, the global pattern (fingerprint class) is unimportant, because they are searching just only for minutiae positions, types and angles. The description of generation of synthetic fingerprints could be found in Chapter 8. This chapter covers not only the generation of a synthetic fingerprint in the nice black and white representation, followed by how could be this image changed into the real world representation. Some of the works related to this chapter, e.g., [4,5], describe the use of simulation techniques for putting the skin diseases or other disturbing artifacts into synthetic fingerprints. Indeed, in the connection with synthetic fingerprints, we should not neglect the use of spoofs. The trouble is if we can generate a synthetic fingerprint that very closely simulates the real finger, or in the worst case, we can get a real fingerprint in a good quality, the creation of finger(print) spoof is not so difficult. This topic is described in Chapter 15. Of course, the spoof created using nearly the same materials could be applied on the whole hand, especially on characteristics based on outer hand physiology. The antispoofing techniques are discussed in Chapters 14 and 16.

Palmprint is, generally speaking, a very big fingerprint. In the case when we use a complete scan of the hand, we get fingerprints together with the palmprint scan (see Figure 1.2). Therefore, all the positive and negative aspects discussed in the previous paragraphs could be applied to palmprint. Palmprint technology is not so often used in the praxis, because the scanner area is too big and the processing time and memory requirements are higher in comparison with fingerprint recognition. Palmprint is of interest for criminal police, because if the offender did not use gloves, he would very probably leave some part or even the whole palmprint, which is very representative for a concrete person. There could be found a big amount of minutiae points and moreover the run of lines of life is very representative as well. The palmprint is covered in Chapter 12. At the moment, the mobile devices (phones and tables) have so high resolution that they could be used for acquirement of palmprint and fingerprints. The quality is really so good that the ridges are visible and usable for the automatic processing. This can cause troubles, because if we post our photos on webpages or social networks, the full structure of our finger and palm ridges could be seen.

Figure 1.2 Palmprint with fingerprints [6]

If we speak about *hand palm veins*, we can apply the same for *hand back veins*. Just in the praxis, the use of hand back veins is rare. Most technologies are oriented on hand palm veins, because the user just positions his/her hand above the device and the scanner can acquire this biometric characteristic. Hand veins belong to the inner hand physiology and have a big advantage—it is very difficult to change their structure. In general, it is possible, however so difficult, that probably no one will take this surgery into account. Because the veins are inside our hands, we need an infrared illumination to make them visible. The illumination belongs to the near infrared (due to ISO 20473 scheme); however, the concrete wavelength plays an important role. If we are closer to red (above 650 nm), we can see better oxygenated blood, i.e., arteries. If we come closer to 950 nm, we can acquire better deoxygenated blood, i.e., veins. This principle is used in medical oximeters [7]. The arteries and veins on hand palm or back are very nicely visible and thick enough to be acquired without any big trouble. The surrounding light could be filtered out; just only fluorescent lamps can cause troubles, because they produce a strong

infrared illumination, which can have an impact to the acquirement process. These devices use infrared filters to filter out the surrounding light, and only a selected wavelength(s) can pass, but if the light source produces radiation on the same wavelength, this can bring a lot of problems. The hand palm vein topic is discussed in Chapter 10.

Finger vein recognition is comparable with hand vein recognition. The illumination principle is the same. The pulse oximeters are used on fingers—they can measure not only the heart pulse but also the oxygenation of blood as well. A small disadvantage arises here—the arteries and vein structure in fingers is not intertwined enough, i.e., the amount of information (biometric entropy) is low. On the other hand, if we acquire a video and the user rotates the finger around (e.g., from one side to the another one), we can get a very precise space structure of the finger veins, i.e., the amount of information (biometric entropy) will be very high, and furthermore, we can avoid the use of finger veins spoofs, because to construct a 3D finger vein structure is not simple, especially if we consider the use of both wavelengths to make visible oxygenated and deoxygenated blood. In that case, just a 3D model printed from an appropriate material (e.g., metal powder) on a 3D printer will be not enough, because this will represent only the deoxygenated blood, anyway the oxygenated scan will be empty. The finger vein recognition is covered in Chapters 9 and 11.

Now we come to the hand back. Here we can acquire and use the following biometric characteristics (see Figure 1.3):

- Thermal image of the hand palm and fingers
- 2D hand geometry
- 3D hand geometry
- Finger nail
- Hand back veins (were discussed in the previous part)
- Finger veins (were discussed in the previous part)

Using a thermal imaging camera, we can get a *thermal image* of our *hand palm* or *hand back*. There are two drawbacks in using this technology—a thermal imaging camera with a good resolution (more than 240×180 pixel) is very expensive. A thermal imaging camera with resolution 640×480 pixel costs above approx. 15,000 EUR. Such devices are not suitable for a common biometric market. The second drawback is the usability of the thermal scan of the hand for biometric recognition. There is very low amount of thermobars [areas with the same temperature building stains with the same color, because each color on the image represents a concrete corresponding temperature (if the emission coefficient was set to the appropriate material)], which represents our hands. Furthermore, these thermobars are strongly influenced by environment (temperature and humidity) and if the person smokes. Smoking causes the narrowing of blood vessels that causes the change of the hand temperature in general. Therefore, this biometric characteristic is not used for biometric recognition of people. Thermal images of fingers are not usable for any form of biometric recognition, because they do not include sufficient amount of information and are totally strongly influenced by surrounding

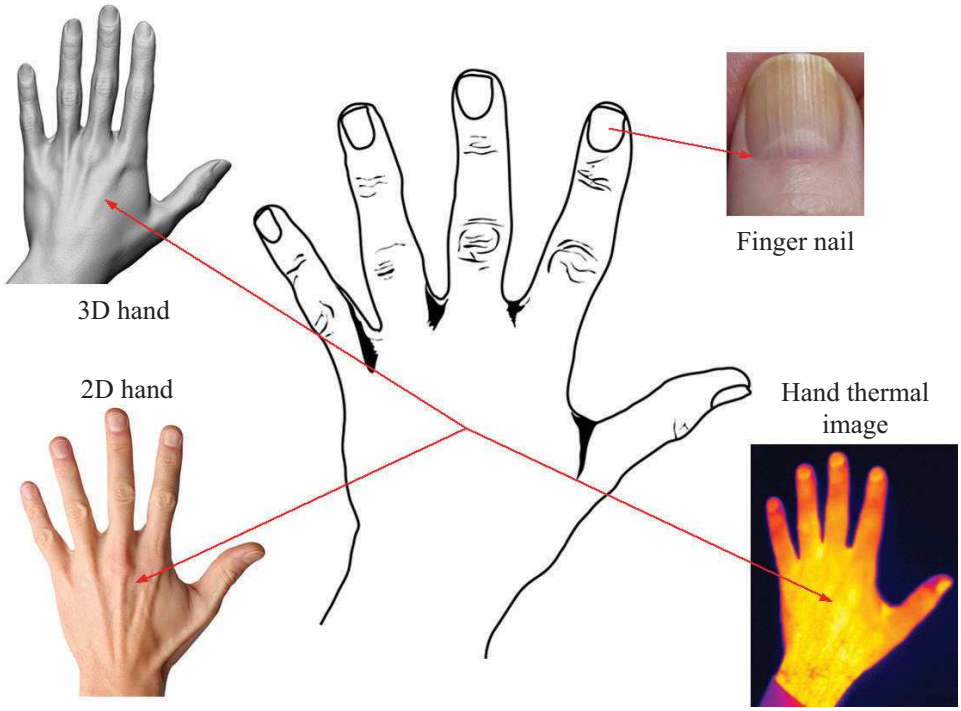

Figure 1.3 Biometric characteristics on hand back

environment and smoking. From this reason, the technology is very shortly mentioned in Chapter 14.

By using a 2D classic camera or line scan camera, we are able to scan and process the *2D hand geometry* (shape). The hand shape could be acquired in two main scenarios—hand is placed on a pad or is scanned moving above the camera. The first scheme brings the hand into a concrete position, and if a fixation pins for fixing the fingers into concrete positions are used as well; we get a very nice images which could be very quickly and automatically processed. In this case, the orthogonal scanning is used, where we acquire the shape of hand from above, but from side as well. The second approach scans the moving hand. In this case, a 2D camera with high framerate or line scan camera could be used. The reason is that the hand is moving and if we use a camera with low framerate, the images will be blurred, i.e., unsuitable for automatic processing and extraction of 2D hand features. However, this second approach enables the use of the technology "on the fly," i.e., where users just only pass the biometric scanning station and do not need to stop and place the hand to a scanner surface. This "on the fly" technology is applicable on fingerprints as well; however, other biometric characteristics are not very suitable for scanning in this style of use. In comparison to 3D hand geometry, 2D hand includes lower amount of information (biometric entropy) that is suitable for smaller groups of people. This 2D hand geometry (shape) technology is discussed in Chapter 12.

If we use any 3D scanning technology (structured light, time of flight or any technology producing depth map or point cloud), we are able to scan and process the *3D hand geometry* (shape). We can select from a big amount of devices on the market, starting by low-cost devices, going through middle class till very expensive

scanners. One exception, pretty new on the market, is the use of 3D line scan camera. All these cameras are suitable for "on the fly" scenario. Many of these cameras enable to get not only the point cloud (3D surface) but also the texture information (images of a real hand surface) as well. This texture information could be used as an additional biometric characteristic, especially if we scan hand palm, e.g., the 3D line scan camera is so precise that we can see ridges structure. It is surprising that this technology is still in research form, and no professional devices are on the market. The 2D technology has dominated the market for a very long time. The introduction and explanation of the 3D hand geometry technology could be found in Chapters 12 and 13.

As mentioned in the beginning of this chapter, the *nail structure* is interesting; however, no devices for this technology are available on the market and the research is not very spread in this area. Just fragments in the literature could be found, e.g., [8–10]. Therefore, no space in this book is devoted to this research area, because it will be very difficult to prepare a chapter that covers such topic. Anyway, the abovementioned sources cover this topic and could be used for further study in this biometric recognition area.

At the end of this subsection, we have discussed troubles with *spoofs* and *antispoofing* methods. In some cases, it is not difficult to produce a working spoof. Especially for fingerprints and palmprints, there could be found a lot of articles and webpages, which describe the style of creation of such spoofs. This topic is very interesting for criminal police as well. If an offender leaves spoofed fingerprints in a crime scene, this can lead to arrest of a wrong person. Spoofs of 2D or 3D hand geometry are known as well—the casting of a hand is possible and is not expensive, or the 3D print using a 3D printer is possible as well. The quality of a low-cost 3D printer is sufficient for fooling the biometric system in 2D and 3D version. The vein structure in 2D version could be cheated as well; just only a metallic powder is sufficient to reconstruct the paths of veins. However, if the oxygenated blood (arteries) is taken into account, the production of such a fake mixture of oxygenated and deoxygenated blood is very difficult and nearly impossible. The spoof of finger nail is unknown and could not be found in literature. However, a very precise casting of the nail structure could be useful. The last technology using a thermal imaging camera is very easy to be cheated. Our research group did trials on making the spoof of thermal face image, which is more demanding, and we were successful. Therefore, the production of a hand or finger spoof is very easy, effective and cheap. The spoofs are discussed in Chapter 15. The methods against these spoofs are called antispoofing or liveness detection. These methods are based on various mechanisms, which are connected to a living human body, e.g., pulse, skin properties and perspiration. In the past, there were successful attacks (spoofs) on nearly every antispoofing technology. The most promising technology is the multispectral one, which is based on illumination of living human skin using ultraviolet, visible and infrared light. The skin reflects, absorbs and scatters the incoming illumination. If the skin is dead or any other material is used, the reaction of the skin differs from a live skin. Therefore, this method is very reliable. For fingerprint recognition, an optical tomography or ultrasound technology could be used—these two

technologies cannot be overcome easily, i.e., they are promising for the future as well. The antispoofing methods are summarized in Chapters 14 and 16, whereas Chapter 14 is oriented also on optical skin properties.

The last very important property of each of the above-discussed biometric characteristics is its interclass and intraclass variation [11,12]. These measures represent the changes inside my own biometric samples (*intraclass variation*) and among my biometric samples and all other samples not belonging to my person (*interclass variation*). We wish to have very low intraclass variation, i.e., that all acquired biometric samples from our one biometric characteristic are very similar, nearly the same, and otherwise, we want to have the interclass variation so high as possible, i.e., that all biometric samples of the same biometric characteristic, but from various users, differ a lot. Very low intraclass variation has especially biometric characteristics belonging to the inner hand physiology (hand and finger veins); all other hand-based biometric characteristics have a middle one. Regarding the interclass variation, the highest is for fingerprints and palmprints; hand veins, nail and 3D hand geometry have the middle one; and 2D hand shape, thermal hand image and finger veins have the lowest one. The highest biometric entropy (amount of information) could be found in palmprint, fingerprint and 3D hand geometry; middle in 2D hand geometry, hand veins and nail; the lowest in thermal hand image and finger veins. However, it strongly depends on the end application, where the concrete biometric characteristic will be used. If we expect just only a small group of users, all of these technologies could be used. If we expect a high security and a big group of users, just only those biometric characteristics could be used, which have high amount of information (biometric entropy), low intraclass variation and high interclass variation.

1.3 Use of biometrics for ABC systems—watchlists

In this section, we will discuss one very interesting topic, which is connected to every biometric technology, especially those biometric characteristics, which are suitable for electronic travel documents (e-passports)—watchlist for e-boarders.

Biometric-enabled watchlist itself as well as watchlist check procedure are the specific security technologies which include various aspects of profiling of person of interest in both physical and virtual world. It is related to the performance of distributed databases, acquisition of biometric traits, risk assessment of watchlist check errors, manifestation, correction, updating and respective public responses to the watchlist mismatch. Moreover, watchlist technology is a part of national and international security infrastructure that dictates various application constraints. For simplification, we follow the above-specified requirements (time constraints and reliability of decisions) to the biometric-enabled watchlists in mass-transit systems. Based on this understanding, we provide below the analysis of the publications in this area, as the synergy of research efforts in the following directions:

- *Impact of quality of biometric traits on performance:* Effects of real-world biometric databases for e-passport holders are studied in [13,14]. The study

[15] addresses the problem of degraded biometric traits, typical for watchlist, as well as recognition of unconstrained facial images. The watchlist technology includes the age estimation, age progression and template aging tools, as well as detectors of factors that impact the quality and performance including rare features. Intensive integration of forensic experience is urgent trend in biometric-enabled watchlist technology. It is well documented in forensics that errors can occur in profiling, searching, matching and identification using biometric traits [16]. Ideally, the watchlist should contain synthetic facial images of persons of interest constructed by composite machines.

- *Impersonation phenomenon:* Impersonation is the key problem of border passage from ancient time including contemporary e-borders based on biometric-enabled tools. It is well understood that phenomenon of impersonation (or passive, or zero-effort attack) experimentally detected in speech recognition by Doddington *et al.* [17] can be also detected in other biometric modalities. In design of biometric systems, Doddington phenomenon should be taken in account. Unfortunately, not only passive attacks are an inherent property of watchlist technology, impersonation from social networks can affect the watchlist reliability. Impersonation can be mitigated via multibiometrics. For example, this approach has been implemented in [18] (face and fingerprints), as well as in other pioneering project by the Department of Homeland Security (DHS). Particular interest in watchlist technology is mitigating effects of plastic surgery and makeup, as well as spoofing detection [19].
- *Profiling and risk-assessment technologies* [20], including simulation and modeling, aiming to optimize and harmonize logistic of transit hubs, potential threats, throughput and requirements to supporting IT infrastructure (surveillance, authentication, early warning, risk assessment) [21], as well as via situational awareness. Because of high complexity, various proving grounds are created, such as DHS testing areas.
- *Breakthrough approaches:* Recognition at a distance and on the move [22] including detection of the health-relating features and mobile distributed systems. One of the goals is the acquisition of biometric traits through the interview [23]. The state of the art of the contemporary e-border technologies is given in overviews [24,25].

Definition 1: *The e-border infrastructure is a networking tool for traveler authentication and risk assessment*. The automated border control tasks include checking the document for authenticity and verifying the biometric templates stored in the traveler's e-passport/ID against the probe photo or fingerprint taken at the console. The proper technology must account for age progression, in particular, and ensure certainty of traveler biometric appearance (individual can change his/her evidence using plastic surgery, color lenses or/and make-up).

Definition 2: *Given the traveler, his/her risk assessment is defined via evidence accumulation paradigm which results in a certain security indicator for making decision at acceptable level of reliability and credibility under specified time*

constraints. One of the elements of such evidence accumulation process is the check of the trustworthiness of the Advanced Passenger Information which is provided by the traveler about him/herself. The crucial phase of risk assessment of this data is the watchlist check. Watchlist is defined as a mandatory component of e-borders. It enables identification of individuals of interest using the biometric traits and related contextual information. No biometric-enabled watchlist technology can be 100% effective—there is always a chance that the watchlist may be compromised. Compromising watchlist may, however, require higher amounts of equipment and management resources relative to disabling the watchlist. Thus, the question becomes not "Is the watchlist technology effective?" but "Is watchlist technology A more effective than watchlist technology B?"

Definition 3: *Watchlist check known also as screening, or negative identification, establishes whether a traveler is not on the watchlist. It is characterized by false negative (FN) (miss-match, or miss-identification) errors and false positive (FP), or false alarm (false detection, or impersonation)*. The corresponding error rates are called an FN Rate and an FP Rate. In general terms, and in positive identification, those are called false rejection rate (FRR) and false acceptance rate. An FP results in convenience problem, as an innocent traveler is denied access and need to be manually checked or examined to get access.

Definition 4: *Watchlist architecture is defined as a distributed infrastructure for (a) collection (capture biometric and related contextual data from real and virtual world for the purpose of matching), (b) matching (identifying or verifying the identity of an individual), (c) storing (enrolling, maintaining and updating biometric related contextual data) and (d) sharing (exchange biometric and related contextual data, as well as match results among government agencies accordance with national regulations) of personal data of individuals of interest*. Sharing unclassified biometric data with other agencies having a counter terrorism mission is a high priority task. In e-borders, misidentification may not only offend or hurt travelers (wrongly suspected as terrorists) but can also create a bottleneck situation favorable for terrorist attacks. As a result of the watchlist screening process, the travelers may complain that they were adversely affected and seek relief. In such mass-application as e-borders, government agencies involved in watchlist screening have a certain redress process to resolve the complaint and respond to the complainant.

Definition 5: *The redress complaint disposition (RCD) metric is defined as a traveler's complaint that indicates that he/she was adversely affected and seeks a relief. In the RCD-metric, the traveler can be in one of the following states [21]: (a) nonrelated, (b) positive match or (c) misidentified.* Face, fingerprints and iris are the most suitable for watchlist biometric modalities. For fingerprint recognition in the identification mode, the false nonmatch rate is calculated as a proportion of samples from genuine attempts that cannot be matched against enrolled templates of genuine users. For face recognition in verification mode, the FRR is defined in a scenario when a genuine user is incorrectly rejected.

FRR determines the manual workload since such users will most likely complain and will have to be handled manually. For example, one fingerprint is not acceptable for identification mode but can be accepted for verification. However, a single fingerprint together with face leads to a better performance in terms of accuracy. In addition, useful statistics on face recognition in authentication gates is provided in [26].

Definition 6: *Performance of the watchlist is defined as a quantifiable indicator used to assess how well the watchlist is achieving its desired objectives.* The number of transactions per day is a system characteristic for a watchlist. For example, DHS managed over 160,000 search queries a day (for visa, visitors, naturalization, etc.) due to Government Accountability Office of Department of Defence. In addition to the known RCD measures of watchlist efficiency, we defined the following performance metrics: the throughput (the number of served travelers per hour), operational reject rate [expressed as "one in *N* travelers (1:*N*) is wrongly directed to special control"] and life-cycle performance assessment which combines theoretical (algorithmic limit), predicted (vendor-reported) and operational (real) false reject and accept rate or accuracy. The main focus is on estimation of risk of a miss when searching for a wanted person, as well as a mismatch of an innocent traveler against someone on a watchlist.

Definition 7: *Social embedding addresses the mapping of the watchlist technology onto social infrastructure, including privacy issues. The depth of social embedding is the key criterion for development the watchlist technology*. Example of a deep embedding watchlist technology is DHS's ADVISE that aims at finding and tracking relationships in data available about the traveler. Searches and evidence accumulation result to as semantic graphs which help to detect activities that threaten the United States by facilitating the analysis of large amounts of structured data (such as information in a database) and unstructured data (such as e-mail texts, reports and news articles). The information is then analyzed and used to monitor social threats such as community-forming, terrorism, political organizing or crime.

Definition 8: *Watchlist inference is defined as a mechanism for traveler risk assessment using a watchlist components such as biometric traits and relevant records or metadata*. Currently, no commonly agreed set of factors exist upon which to base an evaluation, regardless of the watchlist purpose or requirements. We propose the comprehensive criteria and taxonomy for watchlists and focus on the most vulnerability in border crossing biometrics known as impersonation.

Definition 9: *A model of a watchlist technology for traveler risk assessment in e-borders includes technical part (databases, mechanism for searching, collecting, filtering and identification) and management part (logistics, redress code, sharing and privacy policy)*.

Definition 10: *The performance of the watchlist is defined as a quantifiable indicator used to assess how well the watchlist is achieving its desired objectives*. The number of transactions per day is a system characteristic for a watchlist.

For example, DHS managed over 160,000 search queries a day (for visa, visitors, naturalization, etc.) due to Government Accountability Office of Department of Defence. In addition to the known RCD measures of watchlist efficiency, we defined the following performance metrics: the throughput (the number of served traveler per/hour), operational reject rate (expressed as "one in *N* travelers (1:*N*) is wrongly directed to special control") and life-cycle performance assessment which combines theoretical (algorithmic limit), predicted (vendor-reported) and operational (real) ones.

Definition 11: *Doddington metric is defined as the four type classification of recognition process*:

- *Category I ("sheep"), recognized normally;*
- *Category II ("goats"), hard to recognize;*
- *Category III ("wolves"), good at impersonating; and*
- *Category IV ("lambs"), easy to impersonate.*

Typical examples of the watchlist check in Doddington metric are given in Figure 1.4: left pair of images results the effect of misidentification and the right pair images addresses the impersonation effect. Our experiments concern the following scenarios of the border crossing passage:

- Scenario 1: The traveler is a person of interest, he/she belongs to the class of "goats" and, thus, poses a risk of not being matched against the watchlist, and, consequently, passing the border control.
- Scenario 2: The traveler is not a person of interest, he/she belongs to the class of "lambs" (and "wolves" in the symmetric matcher) and, thus, might match against someone on the watchlist and generate a false alert and the likely RCD procedure.
- Scenario 3: The traveler is a person of interest, he/she belongs to the class of "wolves" and may create a lot of matches against the watchlist, thus creating logistic problems; therefore, the case, however, may not be what the attacker intends as this event will still alert border control.

Figure 1.4 Images of subjects in Doddington metric: (a) and (b) are "goat" subject; (c) an image of a "wolf/lamb" subject that looks similar to subject (d) (images are from the LFW database [27])

Our previous studies [28,29] and actually running study address the risks of future generation of automated watchlist check in mass-transit systems, such as e-borders. We consider risks of biometric-enabled technology under the following critical constraints: (a) limited operating time (few minutes) and (b) impersonation phenomenon when using face traits of person of interest. These operating conditions are radically different from Entry–Exit systems such as US VISIT in the United States and Smart Borders in EU in which information about the visitor is available in advance.

In contemporary border crossing automation, only alphanumeric data from e-passport/ID are used in traveler risk assessment via watchlist. It is understood that nonbiometric traveler documents can be forged, stolen or even worst; they can be genuine but issued using the false borne certificates. In practice, this drawback means that authentication and risk-assessment machine cannot identify such persons of interest.

It is well documented that vulnerability of recognition process using biometric traits can be measured using Doddington metric. Similar to human, recognition algorithm can mistake one person for another due to resemblance or poor light conditions. In practice of border crossing, this means that machine can identify terrorist as innocent person and vice versa. It is possible to mitigate and even suppress these effects by multibiometrics. For example, in Entry–Exit systems for visitors traveling on visa, high-quality fingerprints are used in addition to high-quality face biometric in database. In mass-transit systems, which operate under time constraints and deal with unknown traveler, the Entry–Exit paradigm cannot be applied directly. In this application, fast and reliable watchlist check is the core of traveler risk assessment. This leads to the need of embedding of this technology into social infrastructure, in particular, via bridging the gap between the watchlist technology and forensics.

However, in practice of e-borders, any extension of biometric modalities in traveler authentication and risk assessment requires creation of a costly supporting infrastructure. Facial biometric is the privilege of most documents and government databases for creation of watchlists. Weakness of facial biometric can be alleviated by fingerprint traits acquired at distance. Motivated by this fact, our study leads to the following key conclusions:

1. Application of Doddington detector in watchlist check provides additional information of critical importance. We showed using Doddington metric that there are always risk of impostors among persons of interest. In terms of security, this means that machine may mistakenly provide border crossing passage to a wanted terrorist.
2. Application of the evidence accumulating paradigm can be considered useful in detection of persons of interest who are hard to recognize, thus increasing the likelihood of detecting a wanted person; this may, however, add few innocent travelers to the pool of suspects.
3. It is in agreement with the reported studies that "Wolves/Lambs" category is the most sensitive Doddington class. Our study confirms that the proposed two-phase watchlist inference is inefficient to identify the subject of interest who

can easily impersonate, compared with the results of using solely the cooperative traveler's biometrics.

The general conclusion is that the proposed watchlist inference is an efficient extension of watchlist technology. The accumulated evidence paradigm allows for bridging the gap between forensics and biometric-enabled watchlists for e-border applications.

The future steps will involve mitigating the effects caused by high variability of Doddington categories. For this, we are investigating Dempster–Shafer measures of uncertainty to be used for the watchlist inference. We also experiment with other biometric modalities, suitable for two-phase evidence accumulation.

1.4 Conclusion

This chapter includes the overview of all described technologies in this whole book. At the beginning, we address medical point of view to the hand, i.e., inner and outer hand physiology, including nail structure. We continue with very well-known fingerprint recognition, continued by palmprint recognition, recognition of hand and finger veins and finished by 2D and 3D hand geometry recognition. Because of lack of interest and availability, we neglect nail structure recognition for biometric purposes and recognition of thermal images of hand and finger. However, we discuss a very important topic, which is liveness detection, i.e., spoofing and antispoofing methods for various hand-based biometric characteristics, especially fingerprints.

ABC systems, watchlists for e-boarders and use of electronic travel documents (e-passports) play an important role for biometric systems based on recognition of hand features, especially for fingerprints because they are used in biometric e-passports. This topic is discussed in the second section of this chapter.

Acknowledgment

This work was supported by The Ministry of Education, Youth and Sports of the Czech Republic from the National Programme of Sustainability (NPU II); project IT4Innovations excellence in science—LQ1602 and by the BUT project "Secure and Reliable Computer Systems" FIT-S-17-4014.

References

[1] Doležel M., Drahanský M., Urbánek J., Březinová E. and Kim T.H. *Influence of Skin Diseases on Fingerprint Quality and Recognition*. New Trends and Developments in Biometrics. Rijeka: InTech – Open Access Publisher, 2012, pp. 275–303. ISBN 9789535108597.

[2] Drahanský M., Březinová E., Lodrová D. and Orság F. *Fingerprint Recognition Influenced by Skin Diseases*. International Journal of Bio-Science and Bio-Technology, 2010, Vol. 3, No. 4, pp. 11–22. ISSN 1976-118X.

[3] Chavarri-Guerra Y. and Soto-Perez-de-Celis E. *Loss of Fingerprints*. New England Journal of Medicine, 2015, Vol. 372, No. 16, p. 22.
[4] Bárta M. and Drahanský M. *Generation of Skin Diseases into Synthetic Fingerprints*. International Journal of Image Processing, 2016, Vol. 10, No. 5, pp. 229–248. ISSN 1985-2304.
[5] Kanich O. and Drahanský M. *Simulation of Synthetic Fingerprint Generation Using Petri Nets*. IET Biometrics, 2017, Vol. 6, No. 6, pp. 402–408. ISSN 2047-4938.
[6] Web page: http://academyofhandanalysis.org/tag/hand-printing/page/2/.
[7] Sinex J.E. *Pulse Oximetry: Principles and Limitations*. The American Journal of Emergency Medicine, 1999, Vol. 17, No. 1, pp. 59–66.
[8] Kumar A., Garg S. and Hanmandlu M. *Biometric Authentication Using Finger Nail Plates*. Expert Systems with Applications, 2014, Vol. 41, No. 2, pp. 373–386.
[9] Premakumari L.T. and Jothi A.S. *Multimodal Biometric Endorsement for Secure Internet Banking using Skin Spectroscopy, Knuckles Texture and Finger Nail Recognition*. International Research Journal of Engineering and Technology, 2016, Vol. 3, No. 2, pp. 1086–1090.
[10] *Automated identification through analysis of optical birefringence within nail beds*, U.S. patent US 6631199 B1, 1998, available on https://www.google.com/patents/US6631199.
[11] Ross A. and Jain A.K. *Multimodal biometrics: An overview*, Signal Processing Conference, 2004 12th European. IEEE, 2004, pp. 1221–1224.
[12] Li S.Z. and Jain A.K. *Encyclopedia of Biometrics*. Springer Publishing Company, Incorporated, 2015, ISBN 1489974873.
[13] Butt M., Marti S., Nouak A., Koplin J., Raghavendra R. and Li G. *Towards e-passport duplicate enrollment check in the European Union*, Proc. European Intelligence and Security Informatics Conf., 2013, pp. 247–251.
[14] DeCann B. and Ross A. *Has This Person Been Encountered Before? Modeling an Anonymous Identification System*, Proc. IEEE Workshop on Biometrics at the Computer Vision and Pattern Recognition Conf., 2012, pp. 89–96.
[15] Bourlai T., Ross A. and Jain A.K. *Restoring Degraded Face Images: A Case Study in Matching Faxed, Printed, and Scanned Photos*. IEEE Transactions on Information Forensics and Security, 2011, Vol. 6, No. 2, pp. 371–384.
[16] Cowell R.G. *FINEX: A Probabilistic Expert System for Forensic Identification*. Forensic Science International, 2003, Vol. 134, No. 1, pp. 196–206.
[17] Doddington G., Liggett W., Martin A., Przybocki M. and Reynolds D. *Sheep, goats, lambs and wolves a statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation*, Proc. Int. Conf. Spoken Language Processing, 1998.
[18] Cantarero D.C., Herrero D.A.P. and Mendez F.M. *A multi-modal biometric fusion implementation for ABC systems*, Proc. IEEE European Intell. and Security Informatics Conf., 2013, pp. 277–280.

[19] Menotti D., Chiachia G., Pinto A., *et al*. *Deep Representations for Iris, Face, and Fingerprint Spoofing Detection*. IEEE Transactions on Information Forensics and Security, 2015, Vol. 10, No. 4, pp. 864–879.

[20] Easley D. and Kleinberg J. *Networks, Crowds, and Markets: Reasoning About a Highly Connected World*, Cambridge University Press, New York, NY, 2010.

[21] Lee A.J. and Jacobson S.H. *The Impact of Aviation Checkpoint Queues on Optimizing Security Screening Effectiveness*. Reliability Engineering and System Safety, 2011, Vol. 96, No. 8, pp. 900–911.

[22] Tistarelli M., Li S.Z. and Chellappa R. *Handbook of Remote Biometrics*. Advances in Pattern Recognition, Springer, New York, NY, 2009.

[23] Nunamaker J.F., Derrick D.C., Elkins A.C., Burgoon J.K. and Patton M.W. *Embodied Conversational Agent-based Kiosk for Automated Interviewing*. Journal of Management Information Systems, 2011, Vol. 28, No. 1, pp. 17–48.

[24] Eastwood S.C., Shmerko V.P., Yanushkevich S.N. *et al*. *Biometric-enabled Authentication Machines: A Survey of Open-set Real-world Applications*. IEEE Transactions on Human-Machine Systems, 2016, Vol. 46, No. 2, pp. 231–242.

[25] Labati R.D., Genovese A., Muñoz E., Piuri V., Scotti F. and Sforza G. *Biometric Recognition in Automated Border Control: A Survey*, ACM Computing Surveys, 2016, Vol. 49, No. 2, pp. A:1–A:39.

[26] Spreeuwers L.J., Hendrikse A.J. and Gerritsen K.J. *Evaluation of automatic face recognition for automatic border control on actual data recorded of travelers at Schiphol Airport*, Proc. of the Int. Conf. Biometrics Special Interest Group (BIOSIG), 2012, pp. 99–110.

[27] Huang G.B., Ramesh M., Berg T. and Learned-Miller E. *Labeled Faces in the Wild: A Database for Studying Face Recognition in Unconstrained Environments*, University of Massachusetts, Amherst, Technical Report 07-49, October 2007.

[28] Lai K., Kanich O., Dvořák M., Drahanský M., Yanushkevich S. and Shmerko V.P. *Biometric-Enabled Watchlists Technology*. IET Biometrics, 2017, Vol. 6, No. 6, pp. 1–10. ISSN 2047-4938.

[29] Eastwood S.C., Shmerko V.P., Yanushkevich S., Drahanský M. and Gorodnichy D. *Biometric-Enabled Authentication Machines: A Survey of Open-Set Real-World Applications*. IEEE Transactions on Human-Machine Systems, 2016, Vol. 46, No. 2, pp. 2168–2291. ISSN 2168-2291.