Biometrics of Next Generation: An Overview

Anil K. Jain[1], *Ajay Kumar*[2]

[1]Department of Computer Science and Engineering

Michigan State University, East Lansing, MI 48824-1226, USA

[2]Department of Computing

The Hong Kong Polytechnic University, Hung Hom, Hong Kong

Email: *jain@cse.msu.edu*, *ajaykr@ieee.org*

Abstract

Prevailing methods of human identification based on credentials (identification documents and PIN) are not able to meet the growing demands for stringent security in applications such as national ID cards, border crossings, government benefits, and access control. As a result, biometric recognition, or simply biometrics, which is based on physiological and behavioural characteristics of a person, is being increasingly adopted and mapped to rapidly growing person identification applications. Unlike credentials (documents and PIN), biometric traits (e.g., fingerprint, face, and iris) cannot be lost, stolen, or easily forged; they are also considered to be persistent and unique. Use of biometrics is not new; fingerprints have been successfully used for over one hundred years in law enforcement and forensics to identify and apprehend criminals. But, as biometrics permeates our society, this recognition technology faces new challenges. The design and suitability of biometric technology for person identification depends on the application requirements. These requirements are typically specified in terms of identification accuracy, throughput, user acceptance, system security, robustness, and return on investment. The *next generation biometric technology* must overcome many hurdles and challenges to improve the recognition accuracy. These include ability to handle poor quality and incomplete data, achieve scalability to accommodate hundreds of millions of users, ensure interoperability, and protect user privacy while reducing system cost and enhancing system integrity. This chapter presents an overview of biometrics, some of the emerging biometric technologies and their limitations, and examines future challenges.

1.1 Introduction

Human identification leads to mutual trust that is essential for the proper functioning of society. We have been identifying fellow humans based on their voice, appearance, or gait for thousands of years. However, a systematic and scientific basis for human identification started in the 19th century when Alphonse Bertillon [26] introduced the use of a number of anthropomorphic measurements to identify habitual criminals. The Bertillon system was short-lived: soon after its introduction, the distinctiveness of human fingerprints was established. Since the early 1900s, fingerprints have been an accepted method in forensic investigations to identify suspects and repeat criminals. Now, virtually all law enforcement agencies worldwide use Automatic Fingerprint Identification Systems (AFIS). With growing concerns about terrorist activities, security breaches, and financial fraud, other physiological and behavioral human characteristics have been used for person identification. These distinctive characteristics, or biometric traits, include features such as face, iris, palmprint, and voice. Biometrics [1,2] is now a mature technology that is widely used in a variety of applications ranging from border crossings (e.g., the US-VISIT program) to visiting Walt Disney Parks.

Biometric recognition is based on two fundamental premises about body traits: *distinctiveness* and *permanence* [1]-[2]. The applicability and identification accuracy of a specific biometric trait essentially depends to what extent these two premises hold true for the population at hand. Fingerprints, face, and iris are amongst the most popular physiological characteristics used in commercial biometric systems, with fingerprint alone capturing over 50% of the civilian market share [21]. Distinctiveness as well as the permanence of many of the behavioural characteristics proposed in the literature (such as signature, gait, and keystroke dynamics) is weak. As such, very few operational systems based on these traits have been deployed so far. The choice of a specific biometric modality typically depends on the nature and requirements of the intended identification application. As an example, voice biometric is appropriate in authentication applications involving mobile phones since a sensor for capturing voice (microphone) is already embedded in the phone. Fingerprint is the most popular biometric for accessing laptops, mobile phones and PDAs since low cost, small footprint fingerprint sweep sensors can be easily embedded in these devices. Some of the traits, for example, hand geometry, are more appropriate for verification applications (1:1 matching) whereas others like fingerprint, iris, and face have sufficient discriminating power to be applicable in large-scale identification applications (1:N matching). One of the unique applications of biometrics is in the negative identification, *i.e.*, the person is not the one who has already been registered/enrolled in the system. The negative identification is required to prevent multiple

enrolments of the same person which is critical for large scale biometric applications, *e.g.* claiming social benefits from the government sponsored programs. Therefore, even in verification applications, identification capabilities for the negative identification are necessary. We now briefly introduce some of the popular biometric modalities.

(a) Face: Humans have a remarkable ability to recognize fellow beings based on facial appearance. So, face is a natural human trait for automated biometric recognition. Face recognition systems typically utilize the spatial relationship among the locations of facial features such as eyes, nose, lips, chin, and the global appearance of a face. The forensic and civilian applications of face recognition technologies pose a number of technical challenges both for static mug-shot photograph matching (e.g., for ensuring that the same person is not requesting multiple passports) to unconstrained video streams acquired in visible or near-infrared illumination (e.g., in surveillance). An excellent survey of existing face recognition technologies and challenges is available in [40]. The problems associated with illumination, gesture, facial makeup, occlusion, and pose variations adversely affect the face recognition performance. While face recognition is non-intrusive, has high user acceptance, and provides acceptable levels of recognition performance in controlled environments, robust face recognition in non-ideal situations continues to pose challenges.

(b) Fingerprint: Fingerprint-based recognition has been the longest serving, most successful and popular method for person identification. There are numerous historical accounts which suggest that fingerprints have been used in business transactions as early as 500 B.C. in Babylon [38] and later by Chinese officials to seal the official documents in the 3rd century B.C. [39]. Fingerprints consist of a regular texture pattern composed of ridges and valleys. These ridges are characterized by several landmark points, known as minutiae, which are mostly in the form of ridge endings and ridge bifurcations. The spatial distribution of these minutiae points is claimed to be unique to each finger; it is the collection of minutiae points in a fingerprint that is primarily employed for matching two fingerprints. In addition to minutiae points, there are sweat pores and other details (referred to as extended or level 3 features) which can be acquired in high resolution (1000 ppi) fingerprint images. These extended features are receiving increased attention since forensics experts seem to utilize them particularly for latent and poor quality fingerprint images. Nearly all forensics and law enforcement agencies worldwide utilize Automatic Fingerprint Identification Systems (AFIS). Emergence of low cost and compact fingerprint readers has made fingerprint modality a preferred choice in many civil and commercial applications.

(c) Iris: The iris is the colored annular ring that surrounds the pupil. Iris images acquired under infrared illumination consist of complex texture pattern with numerous individual attributes, *e.g*. stripes, pits, and furrows, which allow for highly reliable personal identification. The iris is a protected internal organ whose texture is stable and distinctive, even among identical twins (similar to fingerprints), and extremely difficult to surgically spoof. An excellent survey on the current iris recognition technologies and future research challenges is available in [41]. First invented by Daugman [72], both the accuracy and matching speed of currently available iris recognition systems is very high. Iris recognition has been integrated in several large-scale personal identification systems (e.g., border crossing system in the United Arab Emirates [88]). Several efforts are also being made to capture iris at a distance [89]-[90]. However, relatively high sensor cost, along with relatively large failure to enrol (FTE) rate reported in some studies, and lack of legacy iris databases may limit its usage in some large-scale government applications.

(d) Palmprint: The image of a human palm consists of palmar friction ridges and flexion creases [42]. Latent palmprint identification is of growing importance [92] in forensic applications since around 30% of the latent prints lifted from crime scenes (from knifes, guns, steering wheels) are of palms rather than of fingers [49]. Similar to fingerprints, latent palmprint systems utilize minutiae and creases for matching. While law enforcement and forensics agencies have always collected fingerprints, it is only in recent years that large palmprint databases are becoming available. Based on the success of fingerprints in civilian applications, some attempts have been made to utilize low resolution palmprint images (about 75 dpi) for access control applications, [108], [115]-[116].These systems utilize texture features which are quite similar to those employed for iris recognition. To our knowledge, palmprint recognition systems have not yet been deployed for civilian applications (e.g., access control), mainly due to their large physical size and the fact that fingerprint identification based on compact and embedded sensors works quite well for such applications.

(e) Hand Geometry: It is claimed that individuals can be discriminated based on the shape of their hands. Person identification using hand geometry utilizes low resolution (~20 ppi) hand images to extract a number of geometrical features such as finger length, width, thickness, perimeter, and finger area. The discriminatory power of these features is quite limited, and therefore hand geometry systems are employed only for verification applications (1:1 matching) in low security access control and time-and-attendance applications. The hand

geometry systems have large physical size, so they cannot be easily embedded in existing security systems.

(f) Voice: Speech or voice-based recognition systems identify a person based on their spoken words. The generation of human voice involves a combination of behavioral and physiological features. The physiological component of voice generation depends on the shape and size of vocal tracts, lips, nasal cavities, and mouth. The movement of lips, jaws, tongue, velum, and larynx constitute the behavioral component of voice which can vary over time due to person's age and medical condition (e.g., common cold). The spectral content of the voice is analyzed to extract its intensity, duration, quality, and pitch information, which is used to build a model (typically the Hidden Markov Model) for speaker recognition. Speaker recognition is highly suitable for applications like tele-banking but it is quite sensitive to background noise and playback spoofing. Again, voice biometric is primarily used in verification mode.

(g) Signature: Signature is a behavioral biometric modality that is used in daily business transactions (e.g., credit card purchase). However, attempts to develop highly accurate signature recognition systems have not been successful. This is primarily due to the large *intra-class variations* in a person's signature over time. Attempts have been made to improve the signature recognition performance by capturing dynamic or online signatures that require pressure-sensitive pen-pad. Dynamic signatures help in acquiring the shape, speed, acceleration, pen pressure, order and speed of strokes, during the actual act of signing. This additional information seems to improve the verification performance (over static signatures) as well as circumvent signature forgeries. Still, very few automatic signature verification systems have been deployed.

(h) DNA: The DNA is an acronym for deoxyribonucleic acid which is present in nucleus of every cell in human body and therefore a highly stable biometric identifier that represents physiological characteristic [130]. The DNA structure of every human is unique, except from identical twins, and is composed of genes that determine physical characteristics (like eye or hair color). Human DNA samples can be acquired from a wide variety of sources; from hair, finger nails, saliva and blood samples. Identification based on DNA requires first isolating from source/samples, amplifying it to create multiple copies of *target sequence,* followed by sequencing that generates a unique DNA profile. The DNA matching is quite popular for forensic and law enforcement applications. However, it requires tangible samples and cannot yet be done in real time. Currently, not all the steps in DNA matching are automated and therefore results can be skewed if the process is not conducted properly or the DNA samples

themselves get contaminated. In summary, the DNA matching process is expensive, time consuming and therefore not yet suitable for large scale biometrics applications for civilian usage.

(i) Hand Veins: The pattern of blood vessels hidden underneath the skin is quite distinct in individuals, even among identical twins and stable over long period of time. The primary function of veins is to carry blood from one part of the body to another and therefore vascular pattern is spread throughout the body. The veins that are present in hands, *i.e*. palm, finger and palm dorsal surface, are easy to acquire (using near infrared illumination) and have been employed for the biometric identification [129]. The vein patterns are generally stable for adults (age of 20-50 years) but begin to shrink later due to decline in strength of bones and muscles. There are several diseases, like diabetes, atherosclerosis, or tumors, which can influence the vein patterns and make them thick or thin. Biometric authentication devices using finger and palm vein imaging are now available for some commercial applications [128].to the best of our knowledge, there is no known large scale vascular biometric system. This could be primarily due to concerns about the system cost and lack of large scale studies on vein individuality and stability. On the plus side, these vascular systems are touchless which often appeals to the user.

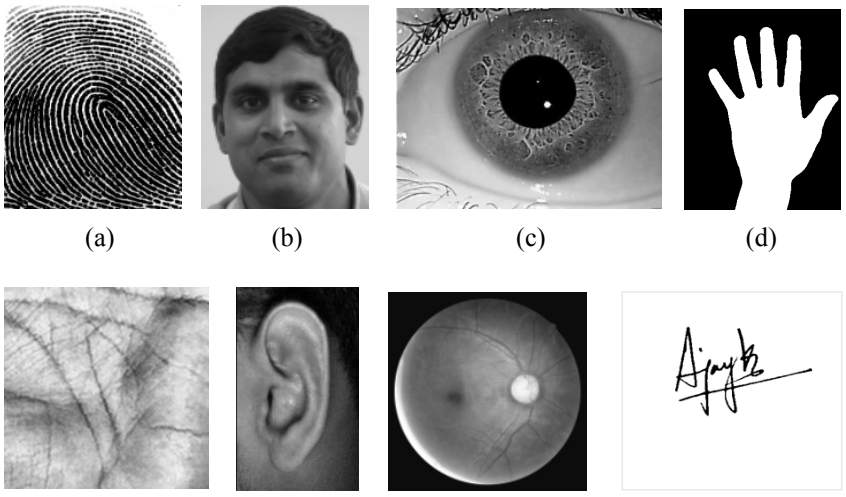


Figure 1: Commonly used biometric traits: (a) fingerprint, (b) face, (c) iris, (d) hand shape, (e) palmprint, (f) ear, (g) retina, and (h) signature.

The recognition accuracy of individual biometric traits outlined above may not be adequate to meet the requirements of some high security applications. The low individuality or uniqueness and lack of adequate quality of individual biometric traits for some users in the target population can also pose problems in large scale applications. The biometric modality

employed for large-scale deployments demands high universality among the user population. It was reported [60] that about 2% of the population does not have usable fingerprints for enrolment in fingerprint identification systems (Note that this figure can vary significantly from one target population to the other). Therefore the combination of different biometric modalities needs to be employed to ensure desired level of security and flexibility in some applications. Another advantage of multimodal systems is that they can potentially offer protection against spoof attacks as it is extremely difficult to spoof multiple modalities simultaneously.

1.2 Expectations from Biometrics Technologies

Increasing requirements for security in many sectors of our society have generated a tremendous interest in biometrics. This has also raised expectations from biometric technologies. These expectations can be summarized into five categories: performance, cost, user convenience, interoperability, and system security.

(i) **Performance**: The recognition performance achievable from a biometric system is of utmost interest in the deployment of biometric systems. A biometric system is prone to numerous errors; failure to enrol (FTE), false accept rate (FAR), and false reject rate (FRR). The system performance is further characterized in terms of transaction time or throughput. The accuracy of a biometric system is not static, but it is data dependent and influenced by several factors: (a) biometric quality, which is related to the quality of sensed signal/image, (b) composition of target user population (e.g., gender, race, age, and profession), (c) size of database (i.e., number of subjects enrolled in the system), (d) time interval between enrolment and verification data, (e) variations in the operating environment (e.g., temperature, humidity, and illumination), (f) distinctiveness of biometric modality, and (g) robustness of employed algorithms (namely, segmentation, feature extraction, and matching algorithms). A biometrics authentication system can make two types of errors: a *false match*, in which the matcher declares a match between images from two different fingers, and a *false non-match*, in which it does not identify images from the same finger as a match. A system's false match rate (FMR) and false non-match rate (FNMR) depend on the operating threshold; a large threshold score leads to a small FMR at the expense of a high FNMR. For a given biometrics system, it is not possible to reduce both these errors simultaneously.

(ii) **Cost**: The cost of deploying a biometric system is often estimated from its direct and indirect components. The direct component includes hardware components (sensor, processor,

memory) and the software modules (GUI and matcher). The sensor should be low cost and it should be easy to embed it in the existing security infrastructure. There are multifaceted components that constitute the indirect cost in the usage of biometric system. These include system installation, training/maintenance requirements, and most importantly, user acceptance. In the end, return on investment or the cost-benefit analysis is critical for making a case for biometric systems in most applications.

(iii) Interoperability: As biometrics systems are being increasingly deployed in a wide range of applications, it is necessary that the system be interoperable among different biometrics technologies (sensors/algorithms/vendors). A biometric system can no longer operate under the assumption that the same sensor, same algorithms, or same operating conditions will always be available during its lifetime. The biometric system should be highly interoperable to authenticate individuals using sensors from different vendors and on varying hardware/software platforms. The system should employ usage/development/deployment of common data exchange facilities and the formats to exchange the biometric data/features between different vendors, from different geographical locations. This would significantly reduce the need for additional software development and bring all the associated advantages (cost savings and efficiency).

(iv) User Convenience: A biometrics system should be user friendly. Any perceived health or hygienic concerns with the continuous usage of biometric sensors can influence user acceptance. Hygiene as well as security has been one of the motivations for developing touchless fingerprint sensors. Some biometric modalities are easier to acquire than others and require less user cooperation during data acquisition. Human factors and ergonomic issues will continue to play a major role in widespread deployment of biometric systems in non-government applications (such as physical and logical access control).

(v) **Security:** Biometric systems are vulnerable to potential security breaches from spoof and malicious attacks. These systems should therefore offer a high degree of protection to various vulnerabilities resulting from intrinsic failures and adversary attacks [48]. One of the major system security concerns deals with biometric template security. The access protocols and the storage of biometric and other user specific data should be provided the highest level of security.

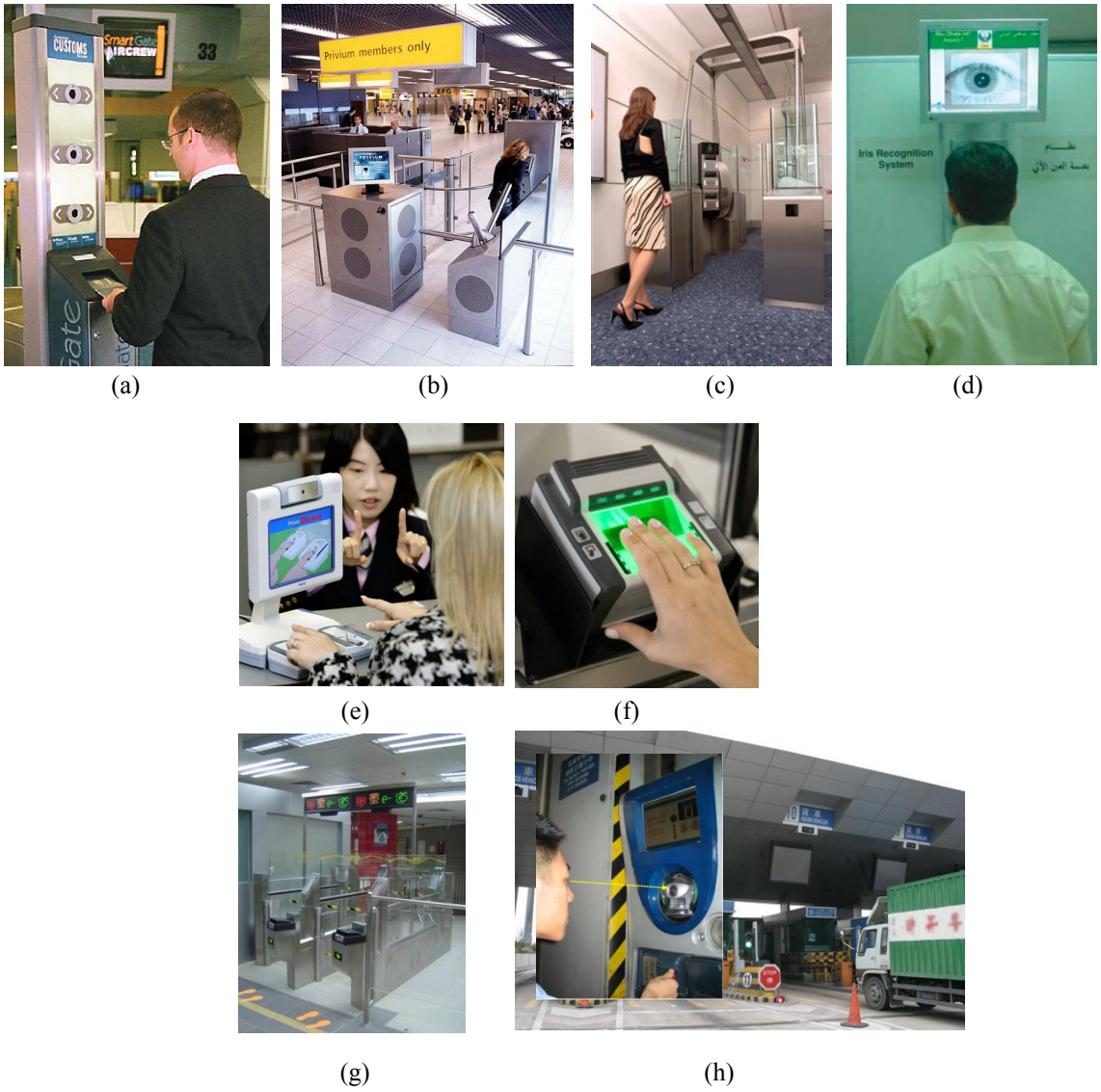
Based on the above considerations, the second generation biometric systems should be easy to use, have low cost, be easy to embed and integrate in the target security application and be robust, secure, and highly accurate in their matching performance.

1.3 First Generation Biometrics

Early applications of biometrics, mainly fingerprints, were primarily in forensics and law enforcement agencies. Even though fingerprints were first used over 100 years ago to convict a criminal [15] the first generation of automatic fingerprint identification systems (AFIS) for law enforcement agencies did not become available until the 1970s. We refer to these systems as the *zeroth generation biometric systems* because of their limited performance and lack of interconnectivity (stand alone). We also place the hand geometry systems which were used in several access control applications, including The Immigration and Naturalization Service Accelerated Service System (INSPASS [94]) in this early generation. The INSPASS system, installed at some of the major airports in the U.S. in mid nineteen nineties, was later abandoned due to its limited user enrollment and weak performance.

We use the term *first generation biometric systems* to describe biometric readers and systems developed and deployed over the last decade. These systems include a variety of fingerprint, iris, and face recognition systems that have found their applications in a wide range of civilian and commercial systems. Some examples include: the US-VISIT system based on fingerprints [94], the Privium system at Amsterdam's Schiphol airport based on iris [95], and the SmartGate system at the Sydney airport [17] based on face. These are examples of major first generation systems used at international border crossings. Other examples include the fingerprint-based system at Walt Disney Parks [97] and face-recognition-based cigarette vending machines installed at some locations in Japan [33]. Continuing advances in the sensing technologies, computational speed, operating environment, and storage capabilities over the past decade have spearheaded the development and deployment of first generation biometric systems. This has helped permeate biometric authentication in our daily lives, as evident from laptops that come embedded with fingerprint sensors. These advances have also tremendously improved the speed and accuracy of fingerprint matching in forensics and law enforcement. As an example, the FBI's IAFIS system has a database of 10 print fingerprint images for about 80 million subjects and handles close to 80,000 searches per day [98]. However, even with this impressive throughput of IAFIS system, it may not be adequate to meet the increasing workload and real-time requirements for several online applications (*e.g.*

for border crossings and law enforcement systems). This problem is even worse for matching latent fingerprints where a substantial amount of human expertise is required both for feature marking and evaluating the matches returned by the system. The ongoing efforts by NIST under MINEX (The Minutiae Interoperability Exchange Test) program are focused at improving the template based interoperability. The recent interoperability test [119] from



(a) (b) (c) (d)

(e) (f)

(g) (h)

Figure 2: Deployment of biometrics systems at border crossings for immigration control; (a) face recognition system (SmartGate) at Sydney airport [17], (b) iris recognition system at Amsterdam Schiphol airport [95], (c) at Manchester airport (UK) [96] and (d) at UAE airport [88]; (e) fingerprint recognition using index fingers at airports in Japan [46]; (g) ten fingerprint acquisition at airports in the United States [94]; (h) fingerprint based immigration clearance for passengers at Hong Kong airport; (i) vehicular clearance using fingerprint and face in Hong Kong [3].

NIST has suggested several limitations of state-of-the-art fingerprint matching algorithms in coping with minutiae interoperability. In addition to poor interoperability, the first generation biometrics systems are vulnerability to spoofing (e.g. [24]) and face increasing challenges in ensuring template security and privacy from sophisticated attacks. In summary, the major limitations of the first generation biometrics system can be summarized as: achievable performance, security, and privacy. This demonstrates the need to develop second generation biometrics system which is described below.

1.4 Second Generation Biometrics

The deployment of first generation biometrics solutions has highlighted several challenges in the management of human identity. The *second generation biometrics systems* must confront these challenges and develop novel techniques for sensing, signal/image representation, and matching. The challenges posed to the second generation biometric technologies can be put in two categories: (i) challenges from *engineering perspective*, which are focused on problems related to security, accuracy, speed, ergonomics, and size of the application; (ii) challenges from the *social perspective*, which include the privacy protection policies, ethical and health related concerns, and cultural biases.

1.4.1 Engineering Perspective

1.4.1.1 Data Acquisition Environment

The performance of matching algorithm critically depends on the quality of biometric data. Sensor design and deployment faces two contradictory requirements: high quality data for improved accuracy vs. flexible data acquisition protocol with the least amount of user cooperation for high user acceptability. We now outline two such challenges facing the second generation biometrics system to improve the data acquisition environment using new sensing technologies.

1.4.1.1.1 Improving User Convenience

Most biometric technologies are able to provide satisfactory matching performance in controlled situations where the user is cooperative and data acquisition conditions and environment can be controlled (e.g., face image captured for passport photos). However, in many applications, biometric data is acquired in less than ideal conditions (figure 3), such as matching latent prints lifted from crime scenes or recognizing faces in surveillance videos. The unsatisfactory performance of biometrics technologies in these relatively uncontrolled situations has limited their deployment; as a result, these applications still heavily rely on human intervention. A significant improvement in recognition performance in less controlled situations is one of the main challenges facing biometric technologies.

There are an increasing number of research and development efforts to expand the scope of personal identification *at-a-distance* and *on-the-move*. Médioni *et al*. [87] have demonstrated the feasibility of non-cooperative personal identification using face images at a distance of 6-9 meters. There have been some efforts to achieve iris identification on-the-move, as well as at-a-distance to enable capture of iris images of sufficient quality while the subjects are moving at a normal walking speed [89], [90], [107]. However, biometric identification at-a-distance and on-the-move is still in the research domain and not yet sufficiently mature [105] for deployment. Human face images are highly pose, view and illumination dependent (figure 3) and the performance evaluation conducted by NIST suggested that the recognition accuracy falls to 47% for the best system in less constrained outdoor conditions [123]. The increased user convenience therefore requires the development of robust matching algorithms and noise elimination techniques that can handle wide range of pose and illumination variations in biometric imaging.

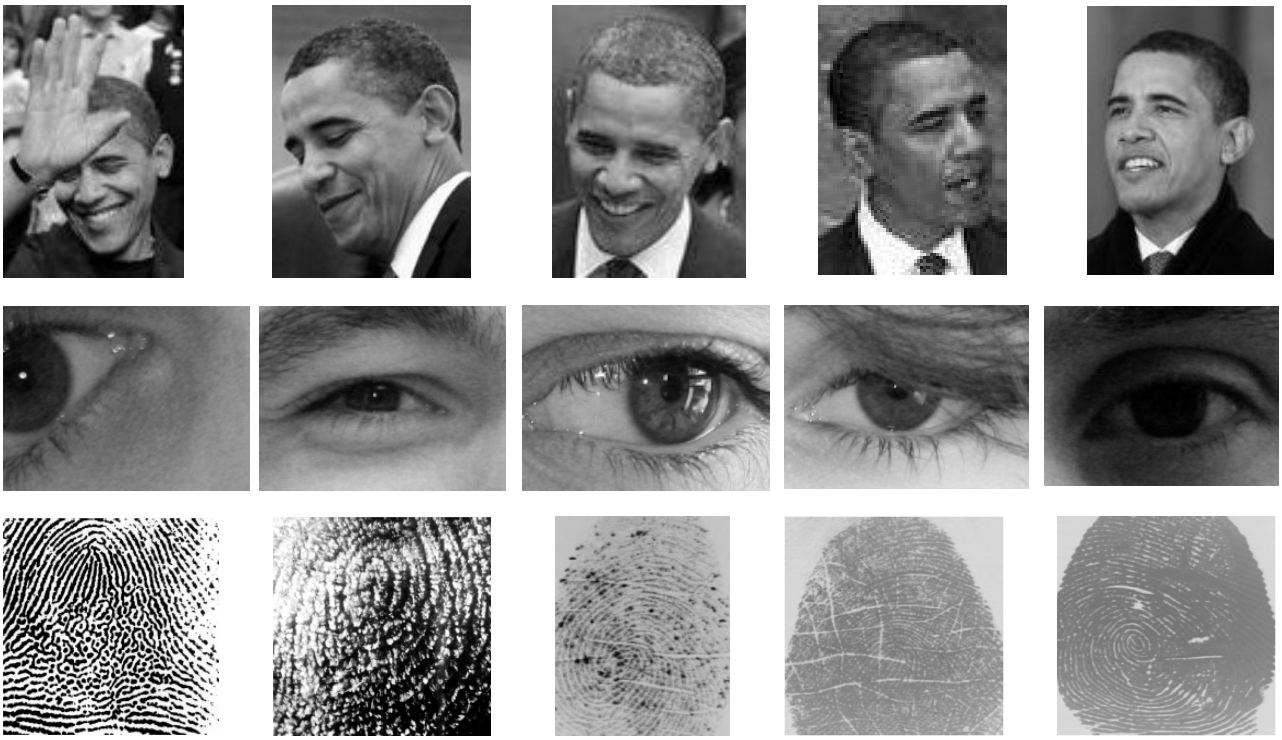


Figure 3: Typical examples of face [125], iris [90] and fingerprint images [124] acquired in less than ideal conditions.

1.4.1.1.2 Improving Data Acquisition Quality

The next generation biometrics sensors that can acquire high quality of biometric data will be required to facilitate the significantly higher level of identification accuracy required in wide range of large scale applications. High resolution fingerprint sensors that can facilitate use of extended features for more accurate identification are being adopted as a standard in law enforcement. Similarly, biometrics sensors that can simultaneously acquire 2D/3D face data can evolve as an essential component of face

recognition applications. The current biometrics systems are predominantly focused on 2D imaging and the use of 3D image acquisition has not delivered its promise due to technological limitations posed by speed, cost, resolution, and size of 3D imagers/scanners as well as the representation and matching issues. Therefore, continued design and development of multimodal biometric sensors that can simultaneously acquire 2D and 3D images is another key challenge in the development of second generation biometric technologies.

1.4.1.2 Handling Poor Quality Data

Consider the case of latent fingerprints that are imaged through a number of techniques ranging from simply photographing the impression to more complex dusting or chemical processing [110]. As latent prints provide important clues for investigating crime scenes and acts of terrorism, matching latents against reference prints (rolled prints) of known persons is routinely performed in law enforcement applications. Compared to plain/rolled fingerprint matching, latent matching is a much more challenging problem because latent prints have complex background, small image area, unclear ridge structure, and large distortion. The accuracy of automatic latent matching is significantly lower than plain/rolled fingerprint matching [111]. As a result, manual intervention is essential in the latent matching process, which leads to low throughput and introduces an element of subjectivity. There has been substantial effort in government, industry, and academia to achieve significant improvement in both the accuracy and degree of automation (*lights out* capability) [111,112,113]. To improve the matching accuracy, extended fingerprint feature set (EFS) has been utilized in addition to minutiae [111]. However, manually marking EFS is very tedious and therefore robust automatic extraction algorithms need to be developed. The increased capabilities to handle poor quality data for biometric identification is not only required for improving latent matching accuracy but is also essential for range of biometric systems employed for commercial applications. The failure to enroll rate (FTE) and the achievable throughput from the deployed biometrics system can also be further improved by imparting new capabilities that can handle poor quality biometric data.

There are a number of applications and scenarios where multiple levels of security and/or throughput are expected in the deployed biometric systems. There have been some efforts [99], [101]-[103] in developing multimodal biometric systems to achieve such dynamic security requirements. However, it is not easy to design adaptive multimodal biometrics systems that are flexible enough to consider user preference for biometric modalities, user constraints, and/or varying biometric image quality. In this context, Nandakumar *et al*. [104] suggested that the likelihood ratio-based fusion can effectively handle the problem of missing biometric modality/data, which could also be perceived as user preference in adaptive multimodal biometric systems.

New user enrolments in a large-scale biometric system will typically require periodic re-training or updating of the matcher. Therefore, another aspect of an adaptive biometric system is *online*

learning, which can periodically update the matcher [109]. A semi-supervised learning approach for adaptive biometric systems is proposed in [103].

1.4.1.3 Biometric System Security

The security ensured by the deployed biometric systems can itself be compromised. A number of studies have analyzed the likelihood of such security breaches and potential approaches [50] to counter these vulnerabilities. The general analysis of a biometric system for vulnerability assessment determines the extent to which an impostor can compromise the security offered by the biometric system. Ratha *et al.* [51] identified the potential points of an adversary attack on the biometric system as shown in figure 4. While many of these attacks are applicable to any information system, the attacks using *fake biometric* and template modification are unique to biometrics systems. We briefly discuss the characteristics of such attacks, which need to be effectively thwarted in second generation biometrics systems.

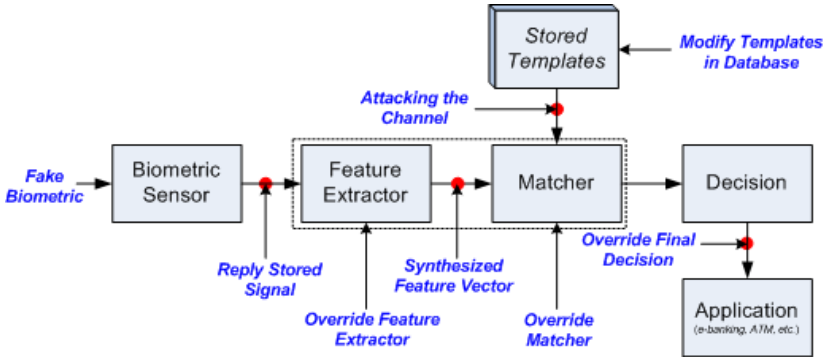


Figure 4: Typical attack points in a biometric system (adapted from [51]).

(i) Sensor level attack: A *fake* biometric sample can be presented at the sensor to gain access. A fake biometric can be generated by covertly acquiring the biometric characteristics of a genuine user, e.g. lifting fingerprint impressions from objects touched by persons.

(ii) Replay attack: It is possible for an adversary to intercept or acquire a digital copy of the stored biometric sample and replay this signal bypassing the biometric sensor [85].

(iii) Trojan Horse[1] attack: The feature extractor can be replaced by a program which generates the desired feature set.

(iv) Spoofing the features: The feature vectors generated from the biometric samples are replaced by the set of synthetically generated (fake) features.

---

[1] Virus program(s) that hide within a set of seemingly useful software programs to facilitate unauthorized access to a hacker

(v) Attack on matcher: The matcher can also be subjected to a Trojan Horse attack that always produces high (or low) match scores irrespective of which user presents the biometric at the sensor.

(vi) Attack on template: The template generated during the user enrolment/registration can be either locally stored or at some central location. This type of attack can either modify the stored template or replaces it with a new template.

(vii) Attack on communication channel: The data being transferred through a communication channel can be intercepted for malicious reasons and then modified and inserted back into the system.

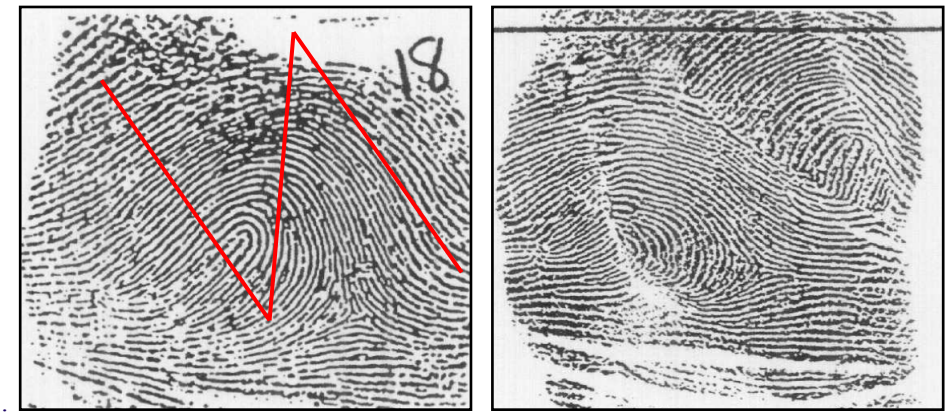
(viii) Attack on decision module: The final decision generated by the biometric system can be overridden by a Trojan Horse program.

A biometric matcher is typically only a part of a larger information and security management system. Therefore, the non-biometric modules in the overall system can also introduce some security flaws. An example is the iris-based access control system in a New Jersey School [71]. Sometimes, a user will prop the door open, so anyone can enter the school, bypassing the security offered by the biometric module. Another scenario could involve disabling the power supply or damaging the sensor that can make the whole biometric security system ineffective [44]. Jain et al. [48] provide extended discussion on typical biometrics system vulnerabilities, which are also summarized in figure 6.

1.4.1.3.1 Biometrics Alteration and Spoof Detection

The border control officials are seeing an increased use of altered fingerprints (see figure 5), used by individuals who do not want to be identified because they have prior criminal records [114]. Several biometrics technologies deployed today are susceptible to attacks in which static facial images [85], fake fingerprints, and static iris images can be used successfully as biometric samples. These fraudulent samples are processed by the biometric sensors as original biometric sample from the registered users and then attempted to be verified as the enrolled users. The use of spoof detection technologies is increasingly becoming an essential component of biometrics systems. The liveness detection and exploitation of biological properties of the biometrics sample is the heart of these approaches; for example, Daugman [72] has identified several approaches for the detection of spoof iris samples, including changes in the wavelengths offered by live tissues to the incident infrared illumination; the fingerprint spoof attacks has been successfully detected from a range of approaches [50], [120], including the measurement

of percentage of oxygen in the blood and skin distortion analysis. The second generation biometrics technologies face increasing challenges to develop significantly enhanced capabilities in identifying and rejecting altered and/or spoof biometrics samples using increasingly sophisticated techniques, *i.e.* surgery, fabrication, and simulation.



(a) (b)

Figure 5: Fingerprint alteration. (a) Original fingerprint and (b) an instance of an altered fingerprint. The criminal made a "Z" shaped incision (illustrated in the left figure) into each of his fingers, switched two triangles, and stitched them back into the finger.

1.4.1.3.2 Template Protection

A template is essentially a compact representation (a set of invariant features) of the biometric sample that is stored in system database. If the security of stored templates is compromised, the attacker can fabricate physical spoof samples to gain unauthorized access. Such efforts have been detailed in [42], [43] and [9]. The stolen templates can also be abused for other unintended purposes, *e.g.* performing unauthorized credit-card transactions or accessing health related records. Figure 7 (c) shows an example of a reconstructed fingerprint image from its minutiae representation (b), which is typically employed for fingerprint templates.

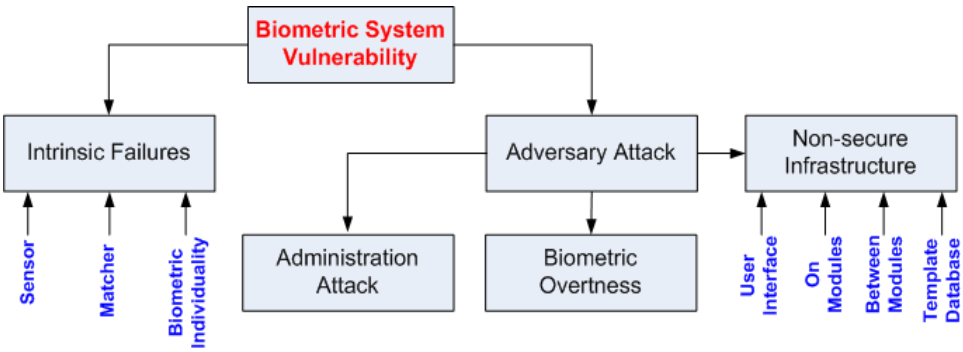
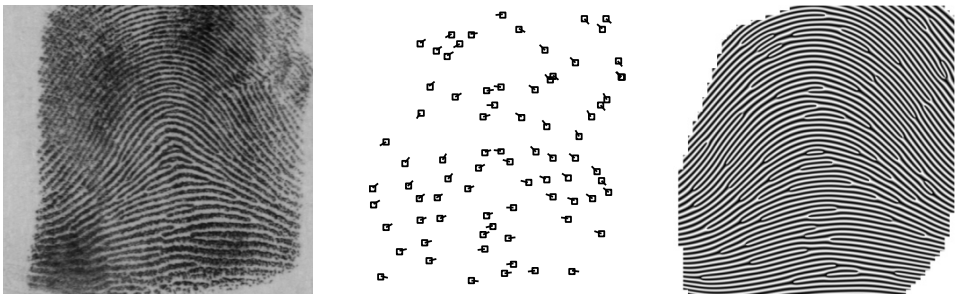


Figure 6: Biometric system vulnerabilities.



(a) (b) (c)

Figure 7: Reconstructing a fingerprint image from minutiae template [9]. (a) Original image, (b) minutiae template, (c) reconstructed fingerprint. Images in Figs. 7(a) and 7(c) can be matched with high accuracy.

An ideal template protection scheme for a biometric system should have the following four properties [48]: (a) Diversity: The cross-matching of secured templates should be ensured in such a manner that the privacy of the true owner of the template is ensured; (b) Revocability: When the biometric template is compromised, it should be possible to revoke the compromised template and reissue a new template based on the same biometric trait; (c) Security: It should be extremely difficult to generate the original biometric feature set from the protected biometric templates, (d) Performance: The template protection scheme should not degrade the matching performance.

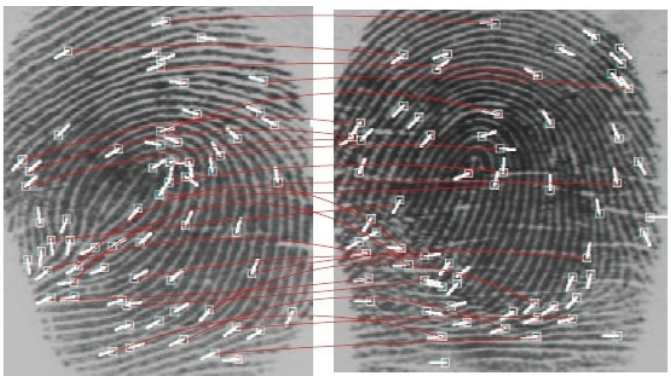


Figure 8: Two fingerprint images from the same finger showing the variability in minutiae localization [5].

One of the key challenges for second generation biometric systems relates to the development of a template protection scheme that can simultaneously meet all the four requirements. The *intra-class variability* (figure 8) in the feature vectors from successive biometric samples of the same user limits the usage of standard encryption techniques (RSA, AES, *etc*.). The available template protection techniques [25] can be broadly classified into two categories (see Jain *et al*. [48]): *feature transformation approach* and *biometric cryptosystem*. The characteristics of the transformation

function can be used to further categorize the techniques into *salting* or *non-invertible transforms*. The salting schemes are capable of recovering original templates but only when a secret key is made available. The *non-invertible transforms* are one-way functions which make it extremely difficult to recover the original template from the transformed template even if the secret key is made available. In biometric cryptosystems, some public information about the templates, also referred to as *helper data*, is made available. While the helper data does not reveal any significant information about the original template, it is useful during the matching process to generate the cryptographic keys. The biometric cryptosystems can be further classified into *key binding* or *key generation* depending on derivation/extraction of helper data. In the *key binding* cryptosystem, the helper data is obtained by binding the biometric template with the key. The template protection schemes like fuzzy vault [52], shielding functions [53], and distributed source coding [54] are typical examples of a *key binding* cryptosystem. The fuzzy vault schemes for template protection has been implemented for a number of biometric modalities; fingerprint [55], face [56], iris [57], palmprint [58], and signature [59]. In a *key generating* cryptosystem, the helper data is only derived from the original biometric template while cryptographic keys are generated from the helper data and query biometric template. While direct key generation from the biometric feature is an attractive scheme, it suffers from low discriminability, *i.e.* it is difficult to simultaneously achieve high key entropy and high key stability [48].

The available template protection schemes cannot yet simultaneously meet all the four requirements of revocability, diversity, security, and high performance. They are also not yet mature enough for large-scale deployment and require extensive analysis of their *cryptographic strength* [121]. It is unlikely that any single template protection scheme can meet all the application requirements. Therefore, hybrid scheme, which can avail the advantages of different template protection schemes, should be pursued.

1.4.1.4 Large-scale Applications

Biometric systems that can effectively and efficiently operate in ultra large-scale applications, *i.e.* those capable of supporting hundreds of millions of registered users, have a number of potential opportunities. Such systems will be able to support National ID programs or improve homeland security, e-commerce, and more effective implementation of social welfare programs in countries with large population (e.g., India, China and United States). The expectations from biometrics systems for such large-scale applications can be summarized as follows: (i) high accuracy and throughput under varying operating conditions and user composition, (ii) sensor interoperability, (iii) rapid collection of biometric data in harsh operating environments with virtually no failure to enrol rate, (iv) high levels of privacy and template protection, and (v) secure supporting information/operating systems.

The selection of biometric modality for large-scale applications is a judicious compromise between performance, convenience/ease in acquisition, cost, compatibility with legacy databases, and application constraints. In order to consider the requirements of large-scale identification, consider the following example involving fingerprint-based identification. Fingerprint identification system performance is measured in terms of its *false positive identification* rate (FPIR) and *false negative identification* rate (FNIR). A false positive identification occurs when the system finds a hit for a query fingerprint that is not enrolled in the system. A false negative identification occurs when it finds no hit or a wrong hit for a query fingerprint enrolled in the system. The FPIR is related to the FMR of the fingerprint matcher as $FPIR = 1 - (1 - FMR)^N$, where N is the number of users enrolled in the system. Hence, as the number of enrolled users grows, the FMR of the fingerprint matcher needs to be extremely low for the identification system to be effective. For example, if a FPIR of 1% is required in a fingerprint identification system with 100 million enrolled users, the FMR of the corresponding fingerprint matcher must be of the order of 1 in 10 billion. To meet such a stringent FMR requirement, it is necessary to use a multimodal biometric system (e.g., all the ten fingerprints of a person or a combination of fingerprint and palmprint) or to use demographic data to filter the database. This illustrates the need to continuously decrease the error rates of fingerprint matchers for successful deployment of large-scale identification systems.

The four most popular biometric modalities deployed today are face, fingerprint, iris and hand geometry. The first generation biometric systems typically employed a single modality, primarily fingerprint (ten prints), for large-scale applications. While the automated border crossing in several countries (*e.g*. USA and Japan) requires authentication using fingerprints, the system in the United Kingdom is based on iris [16] and the one in Australia is based on face [17]. The FBI has [100] embarked on its New Generation Identification (NGI) project for law enforcement applications that will fuse fingerprints, face, and palmprints along with some *soft biometrics* such as scars, marks, and tattoos (SMT) [78].

The government of India has recently announced a new project, called Unique ID [32] to deliver multipurpose unique identification number to its over one billion citizens. This ongoing project is expected to create the largest biometric database on the planet and, on its successful completion, it can become a model of very large-scale usage of biometrics in *e*-governance. It is generally believed that the retrieval of biometrics templates from the database of India's billion plus population will require highly efficient indexing techniques [118] for biometric data. Therefore, the design and development of efficient and effective large-scale indexing techniques for the (multi-) biometric data is

another challenge in the efficient usage/deployment of large-scale biometric systems. The *individuality* or the achievable recognition performance from the chosen biometric modality is another important criterion when millions of identities need to be discriminated. The presence of identical twins is also a problem that needs consideration in large-scale applications [18]. In this context, *multimodal biometric systems* that can simultaneously employ multiple biometric modalities (*e.g.*, multiple fingers, two irises, finger and iris, *etc*.) are expected to offer higher accuracy and can also address the problem of non-universality. There is range of biometric fusion methodologies [35] proposed, but, it appears that the simple *sum rule*, with proper normalization of matching scores, does an adequate job in most cases. Biometrics systems that can simultaneously acquire multiple modalities are expected to become popular in large-scale deployments with data collection in the field. A prototype (figure 9(b), (c)) of an acquisition device that can *simultaneously* acquire five fingerprints, palmprint, and shape of a hand is described in [106] while [23] details a device to acquire fingerprints, palmprints, face images, iris images, signature details and soft biometrics data such as scars and tattoos (figure 10);.

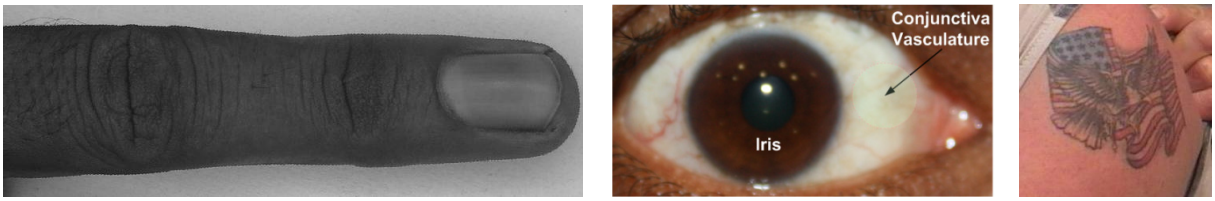
(a) (b) (c)

Figure 9: Multibiometric data acquisition. (a) A multibiometrics acquisition system from Printrak [23] to acquire fingerprints, palmprints, face images, iris images, signature details and soft biometrics data such as scars and tattoos; (b) full hand multispectral scanner from Lumidigm [106] and (c) a sensed hand image from (b).

1.4.1.5 Soft Biometrics

S*oft biometrics* are those human characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals [73]-[74]. Examples of soft biometrics used in law enforcement include scars, marks, tattoos, color of eye, and

hair color. In several biometric system deployments, such *ancillary information* is acquired and stored along with the primary biometric during the enrollment phase. These characteristics can be potentially exploited in three ways: (i) to supplement as the features in an existing biometrics system, (ii) to enable fast retrieval from a large database, and (iii) to enable matching or retrieval from a partial or profile face image with soft biometric attributes, *i.e.*, facial marks.



(a) (b) (c)

Figure 10: Emerging soft biometrics. (a) Image sample for knuckle biometrics, (b) conjunctival vasculature, and (c) tattoo image.

There are several studies in the literature which have demonstrated the effective usage of soft biometric characteristics for performance improvement. Wayman [77] proposed the use of soft biometric traits like gender and age for filtering a large biometric database. Jain et al. [74] demonstrated that the performance of a fingerprint matching system can be effectively improved (~5%) by incorporating additional user information like gender, ethnicity, and height. Jain and Park [75] have utilized micro-level facial marks, *e.g.* freckles, moles, scars, *etc.*, to achieve face recognition performance improvement on an operational database. Scars, marks and tattoos (SMT) are the imprints that are typically employed by law enforcement agencies for identification of suspects. The SMT provide more discriminative information, as compared to other personal indicators such as age, height, gender, and race, and can be effectively used in assisting suspect identification. Lee *et al*. [78] have conducted a study to employ these imprints for content-based tattoo image retrieval.

There have been some efforts to extract novel anatomical, physiological, and behavioural characteristics (gait [76], [93], ear [69], [117], footprints [13]-[14], periocular [80], finger knuckle [66]-[68], keystroke dynamics [91], and nose shape [6], [10]) and investigate their potential to support human identification (see figure 10). Several other physiological characteristics that have been extracted for the purpose of biometric identification include arterial pulse [19]-[20], fingernails [28], odour [29], bioelectric potential [8], knee x-rays [7], frontal sinus [11]-[12], and otoacoustic emissions [31]. These efforts explore and identify additional sources of *soft biometrics* to either improve the performance of traditional (hard) biometric modalities or to help provide identification in the absence of primary biometric attributes. Some of these characteristics can be simultaneously acquired along

with the more popular biometric modalities; for example conjunctival scans [4] can be acquired along with iris while periocular biometrics [80] is more suitable for simultaneous acquisition with face images. However, the *persistence* and *permanence* of these body attributes and behavioural characteristics is not yet known.

1.4.2 Application Perspective

Biometric systems are often felt invasive, since the sensors directly interact with the human body to capture person-specific data that is considered *privileged*. The stigma of forensic and criminal investigations has been known to influence the user acceptance of the first generation biometric systems. Biometric traits are part of human body and behaviour and therefore, releasing this information to a biometric system during enrolment or verification can threaten the personal privacy of some users. Biometric traits can be used to track a person over time; this will be technologically possible when biometric recognition at-a-distance becomes mature and when we learn to *mine* and *link* vast amounts of sensor and demographic data. In addition, by linking the biometric database with other databases (*e.g.* user's credit card transactions), we know where the person has been and at what time. In addition to the personal privacy, there are also concerns that biometric data can be exploited to reveal a user's medical conditions. Such information is privileged that could be potentially used to discriminate some users for employment or benefits purposes (*e.g.*, health insurance). Table 1 lists some of the known medical indicators that are believed to have some association with the corresponding biometric modalities.

Table 1: Privacy concerns with biometric modalities

Biometric Modality	Possible Indicators of user's health
Retina	Eye related disease (e.g. diabetic retinopathy)
DNA	Genetic diseases or susceptibility to specific disease, gender
Palmprint	Prediction of congenital heart disease and laryngoscopy in diabetics
Face	Facial thermograms for fever and related medical conditions/diseases
Gait	Physical disability

The deployment of biometric systems by several countries to safeguard border security has necessitated the adoption of new policies and security measures. These measures, including the use of biometric technology often interfere with the existing national data and privacy protection policies [126]. The development of technical standards is generally perceived as a sign of maturity in the protection and exchange of electronic data. In this context, the biometrics standards support interchange ability and interoperability, ensure high degree of privacy and security, while reducing the development and maintenance costs for biometrics technologies. The current efforts in developing such biometric standards [81]-[84] are focussed on specifications for collection, storage, exchange and transmission of biometric data, file formats, technical interface, performance evaluation and reporting standards for biometrics related solutions. The International Civil Aviation Organization (ICAO) mandates that the biometric data (fingerprint/face/iris) in *e*-passports should conform to SC37 [27] biometric data interchange format. The BioAPI [84] consortium, on the other hand, is the collective efforts of more than 120 companies to develop specifications for a standardized application programming interface (API) which is compatible with wide variety of biometrics products. It is hoped that the *second generation biometrics technologies* will further promote such efforts in the formulation of new international standards for uniform practices pertaining to biometric data collection (in less than ideal conditions), usage, storage, exchange for cross-border and inter-organization applications.

There are also some concerns that biometrics systems may exclude some potential user groups in the society. The definition and the context of personal privacy vary in different societies and are somewhat related to the cultural practices. Some social practices, especially in rural population (which should be the target group for providing social and economic privileges by providing them legal identity [32]), may not relate biometrics with personal privacy concerns. Some cultural groups or religious exercises/convictions/practices may not permit blood samples for DNA extraction [86] while some religious practices may forbid 'complete' (multiple) biometrics enrolment. Wickins [34] has explored the vulnerabilities of a typical user population falling in to six groups: people with (i) physical and/or learning disability and (ii) mental illness, people of certain (iv) race and (v) religion, and those that are (iii) elderly and (vi) homeless. The second generation biometric technologies need to ensure that such user groups do not suffer disproportionately as a result of deployment of biometric systems.

Policy formulations in the selection and deployment of biometrics technologies can also have different impact on the privacy concerns. Some technologies are more likely to be associated with privacy-invasive requirements, *e.g.* covert biometric identification, and therefore more prone to personal privacy risks than others. Privacy groups such as [30] provide privacy risk assessment for various biometrics technologies in four key areas. The privacy risks from the selection and deployment

of biometrics technologies can however be extended into five areas and is summarized in table 2. This table outlines the widely perceived concerns related to template security and on the use of large centralized databases, which often includes function creep.

Table 2: Rating Technology Risks for Personal Privacy

Privacy Impact	*Key Areas of Biometrics System Deployment*				
High	Identification	Covert	Physiological	Biometric Images	Centralized/Large Database
Low	Verification	Overt	Behavioural	Encrypted Templates	Localized/small Database

In view of potential legal and ethical challenges, several privacy commissioners and data protection offices have now formulated new guidelines for the deployment and usage of biometrics technologies in government organizations and private sectors, *e.g.* [45]. Table 3 lists some usage of identification technologies, including biometrics, that have raised privacy concerns. Table 3 highlights concerns about the use of advanced technologies, including biometrics and resulting controversy on the standard policies to protect fundamental ethical values. These values are primarily concerned with privacy, trust, liberty, autonomy, equality, informed consent that is widely perceived to be available to all the citizens in a democracy. While the primary obligation of a state is to ensure the safety and security of its citizens, it is also necessary to protect and respect fundamental rights and values. Some of these rights

Table 3: Incidents of Privacy and Social Challenges

Technology Deployment	Reference	Benefits	Concerns
Street View from Google	[62]	Remote View, Security/Traffic	Personal Privacy
Privacy Controls in Facebook	[63]	Sharing Images, Contacts	Child Safety, Personal Privacy
DNA Tests for Asylum Seekers	[64]	Immigration Security	Profiling, Discrimination
Mandatory DNA Tests for Orphans	[65]	Finding Natural Parents	Privacy Rights, Discrimination
Fingerprint for Attendance	[79]	Efficient/Accurate Monitoring	Personal Privacy, Social Concerns
Age Verification in Facial Images	[85]	Supervision, Tobacco Control	Personal Privacy, Spoofing

are also legally enforceable and include right to respect for personal/private life and the right for equal treatment. The ongoing ethical and legal debate in the deployment of biometrics technologies has suggested [122] that any interference with these rights must be proportionate.

It is expected that over time, the concerns and demands for protecting security and privacy will actually increase. Biometric technology has the potential to offer and ensure individual freedom and therefore, one of the key challenges for the second generation biometric technologies is to provide an appropriate balance between privacy and security (figure 11).

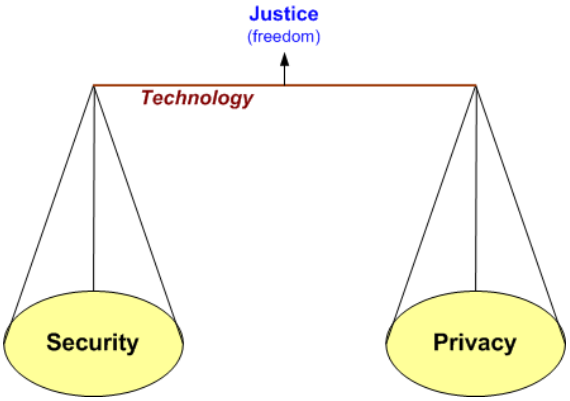


Figure 11: Second generation biometric technologies need to ensure a balance between privacy and security.

1.4.2.1 The Hong Kong Smart ID Card Experience

The Hong Kong international airport is one of the busiest airports in the world and annually handles about 31 million landing or departing passengers [127]. The Hong Kong immigration department's automated fingerprint based passenger clearance system, *i.e. e*-Channel, provides one of the successful examples of high-speed immigration control at border crossings. The biometric border crossing between Hong Kong and Shenzhen has an enrolment of more than 1,600,000 users and handles about 400,000 border crossings every day. This is one of the busiest border crossings in the world and has resulted in detention or arrest of more than 50,000 persons since 2005. The deployment of 361 passenger *e*-Channels at all border crossings in Hong Kong ensures a maximum of 15 minutes of waiting time for 95% of Hong Kong residents and for 92% of visitors [3]. The usage of biometrics based high-speed border clearance at borders is not limited only for the passenger traffic. The automated vehicle clearance system employed at all border control points in Hong Kong has provided effective solution to mounting traffic needs using fingerprint based smart identity cards for 80 *e*-Channels used only for vehicular traffic (figure 2-h). The fingerprint based mandatory Hong Kong identity cards issued to all Hong Kong residents are not limited for their usage in border controls but

find wide range of applications in e-governance from authentication and access to government online services, hospitals, banks, social welfare schemes to property transactions. In addition, these smart cards also promote secured *e*-transactions [61], *i.e*. threats from hackers and online theft, as the residents can store their own encrypted public keys to ensure secured online digital identity.

A small fraction of population can sometime find difficulties to successfully clear the e-Channels due to dry, wet or poor quality fingers. There are, however, alternative manual or regular channels in the vicinity to avoid delay in passenger clearance. It is worth noting that, to the best of our knowledge, privacy concerns and misuse of Hong Kong identity cards have not been reported. The benefits offered by the Hong Kong identity cards apparently outweigh the potential privacy concerns and the Hong Kong residents do not seem overly concerned with the privacy issues [47] which are more effectively regulated by the office of privacy commissioner [70]. In summary, the successful usage of *smart* Hong Kong identity cards since 2005 provides a model for the effective deployment of biometrics technologies for the benefits of citizens in e-governance, e-commerce and in high-speed border crossings.

1.5 Concluding Remarks

There are four technological developments that will lead to evolution of second generation biometrics systems; (i) emergence of potentially new biometric traits, (ii) added value offered by soft biometrics, (iii) effective use of multiple biometric traits for large-scale human identification, and (iv) technologies to ensure a high degree of privacy, security and flexibility in the usage of biometrics systems. The expectations and the challenges for the second generation biometrics technologies are huge. The development of second generation biometrics technologies is going to be cumulative and continuous effort, rather than resulting from a single novel invention. The low cost of biometrics sensors and acceptable matching performance have been the dominating factors in the popularity of fingerprint modality for commercial usage. Continued improvements in the matching performance and gradual reduction in cost of biometrics sensors can be cumulative enough to alter the selection of biometrics modalities in future. The development of smart sensing technologies will allow the researchers to effectively exploit extended biometric features and develop high performance matchers using efficient noise elimination techniques. Such multifaceted efforts can achieve the much needed gains from the second generation biometrics technologies at faster pace.

We believe that social and privacy concerns associated with biometrics technologies can be effectively handled with a two-fold approach. Firstly, the personal privacy should be regarded as an

essential component of biometrics technologies. Policy makers, system developers and system integrators must ensure that these technologies are used properly. Secondly, the policy issues (ethical and legal framework) relating to the deployment of biometrics technologies should be clearly formulated to demarcate the conflict of interests among the stakeholders. The development of widely acceptable biometrics standards, practices and policies should address not only the problems relating to *identity thefts* but also ensure that the advantages of biometrics technologies reaches, particularly to the underprivileged segments of society [32] who have been largely suffering from *identity hacking*. In our opinion, based on the current biometric deployments, the security, and benefits they offer far outweigh the apparent social concerns relating to personal privacy. Hong Kong identity cards should be a promising model to judge the benefits and concerns in future deployments of biometrics technologies.

It is widely expected that sensing, storage, and computational capabilities of biometric systems will continue to improve. While this will significantly improve the throughput and usability, there are still fundamental issues related to (i) biometric representation, (ii) robust matching, and (iii) adaptive multimodal systems. These efforts along with the capability to automatically extract behavioural traits may be necessary for deployment for surveillance and many large scale identification applications.

Acknowledgement

The authors thankfully acknowledge Dr. Jianjiang Feng, Tsinghua University, Dr. Salil Prabhakar, DigitalPersona, Dr. Karthik Nandakumar, Institute for Infocomm Research (I2R), and Abhishek Nagar, Michigan State University for their constructive comments and suggestions.

1.6 References

1. Jain AK, Ross A, Pankanti S (2006) Biometrics: A tool for information security. *IEEE Trans Inf Forensics Security*, vol. 1, no. 2: 125-143
2. Jain AK, Flynn PJ and Ross A (eds.) (2007) Handbook of Biometrics, Springer
3. E-Channel. Immigration Department, Hong Kong. http://www.immd.gov.hk/ehtml/20041216.htm. Accessed 30 January 2010
4. Crihalmeanu S, Ross A, and Derakhshani R (2009) Enhancement and Registration Schemes for Matching Conjunctival Vasculature. Proc. 3rd IAPR/IEEE International Conference on Biometrics, Alghero, Italy
5. Pankanti S, Prabhakar S, and Jain AK (2002) On the Individuality of Fingerprints. IEEE Trans Pattern Anal Mach Intell, vol. 24, No. 8: 1010-1025

6. Drira H, Amor BB, Daoudi M, and Srivastava A (2009) Nasal region contribution in 3D face biometrics using shape analysis framework. Proc. 3rd IAPR/IEEE International Conference on Biometrics: 357-366
7. Shamir L, Ling S, Rahimi S, Ferrucci L, and Goldberg IG (2009) Biometric identification using knee X-rays. Int J Biometrics, vol. 1, no. 3: 365-370
8. Hirobayashi S, Tamura Y, Yamabuchi T, and Yoshizawa T (2007) Verification of individual identification method using bioelectric potential of plant during human walking. Japanese J Appl Phys, vol. 46, no. 4A: 1768-1773
9. Feng J and Jain AK (2009) FM Model Based Fingerprint Reconstruction from Minutiae Template. Proc. ICB 2009, Alghero, Italy: 544-553
10. Song S, Ohnuma K, Liu Z, Mei L, Kawada A, Monma T (2009) Novel biometrics based on nose pore recognition. Optical Eng, vol. 48, no. 5
11. Falguera JR, Falguera FPS, and Marana AN (2008) Frontal sinus recognition for human identification. Proc SPIE, vol. 6944, Orlando, Florida: 69440S
12. Tabor Z, Karpisz D, Wojnar L, Kowalski P (2009) An automatic recognition of the frontal sinus in x-ray images of skull. IEEE Trans Biomed Eng, vol. 56, no. 2: 361-368
13. Nakajima K, Mizukami Y, Tanka K, and Tamura T (2000) Footprint-based personal recognition. IEEE Trans Biomed Eng, vol. 47, no. 11: 1534-1537
14. Uhl A and Wild P (2008) Footprint-based biometric verification. J Electronic Imaging, vol. 17, 11016
15. A History of Fingerprinting. South Wales Police. http://www.south-wales.police.uk/fe/master.asp?n1=8&n2=253&n3=1028. Accessed 30 January 2010
16. Iris Recognition Immigration System (IRIS). UK Border Agency. http://www.ukba.homeoffice.gov.uk/managingborders/technology/iris. Accessed 30 January 2010
17. Introducing SmartGate. Australian Government. http://www.customs.gov.au/webdata/resources/files/BR_introSmrtGt0409.pdf. Accessed 30 January 2010
18. Sun Z, Paulino A, Feng J, Chai Z, Tan T, and Jain AK (2010) A Study of Multibiometric Traits of Identical Twins. Proc SPIE Biometrics, Florida
19. Joshi AJ, Chandran S, Jayaraman VK, and Kulkarni BD (2008) Arterial Pulse Rate Variability Analysis for Diagnoses. Proc ICPR, Tampa, Florida: 1-4

20. Irvine JM, Israel SA, Scruggs WT, and Worek WJ (2008) Eigenpulse: robust human identification from cardiovascular function. Pattern Recognit, vol. 41, no. 11: 3427-3435
21. Biometrics Market Intelligence. http://www.biometricsmi.com. Accessed 30 January 2010
22. Second Generation Biometric Passport Introduced in Hungary as well. National Development Agency Hungary. http://www.nfu.hu/content/3419. Accessed 30 January 2010
23. Printrak LiveScan 4000 Ruggedized. Printrak Division. http://www.morpho.com/MorphoTrak/PrinTrak/prnt_prod/pp_Ls-4000.html. Accessed 30 January 2010
24. Serkan T (2009) Women uses tape to trick biometric airport fingerprint scan. CrunchGear. http://www.crunchgear.com/2009/01/02/woman-uses-tape-to-trick-biometric-airport-fingerprint-scan. Accessed 30 January 2010
25. LaCous MK (2008) Match template protection within biometric security systems. US Patent No. 7454624
26. Henry T. F. Rhodes (1956) Alphonse Bertillon, Father of Scientific Detection. Abelard-Schuman, New York
27. Standing Committee 37 ISO Standards Development. http://isotc.iso.org/livelink/livelink?func=ll&objId=2262372&objAction=browse&sort=name. Accessed 30 January 2010
28. Topping A, Kuperschmidt V, and Gormley A (1998) Method and apparatus for the automated identification of individuals by their beds of their fingernails. U.S. Patent No. 5751835
29. Ramus SJ and Eichenbaum H (2000) Neural correlates of olfactory recognition memory in rat orbitofrontal cortex. J Neuroscience, vol. 20: 8199-8208
30. Best Practices for Privacy-Sympathetic Biometric Deployment. BioPrivacy Initiative. http://www.bioprivacy.org. Accessed 30 January 2010
31. Using M. A. Swabey, S. P. Beeby, A. D. Brown, and J. E. Chad (2004) Otoacoustic emission as biometric. Proc ICBA, LNCS vol. 3072: 1-34
32. Creating a unique identity number for every resident in India (Working paper - version 1.1). UIDAI. http://uidai.gov.in. Accessed 30 January 2010
33. Face Recognition cigarette vending machines. PROnetworks. http://www.pronetworks.org/forums/face-recognition-cigarette-vending-machines-t102463.html. Accessed 30 January 2010
34. Wickins J (2007) The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. Sci Eng Ethics, vol. 13: 45-54

35. Ross A, Nandakumar K and Jain AK (2006) Handbook of Multibiometrics. Springer.
36. Wood G (2009) US man 'stole 130m card numbers'. BBC. http://news.bbc.co.uk/2/hi/business/8206305.stm. Accessed 30 January 2010
37. Unger R (2007) Lifeprints: Deciphering your life purpose from your fingerprints. Crossing Press. http://www.handresearch.com/news/lifeprints-richard-unger.htm. Accessed 30 January 2010
38. Biometrics History. NSTC. http://www.biometrics.gov/Documents/BioHistory.pdf. Accessed 30 January 2010
39. History of Fingerprinting. FINGERPRINTING. http://www.fingerprinting.com/history-of-fingerprinting.php. Accessed 30 January 2010
40. Abate AF, Nappi M, Riccio D, and Sabatino G (2007) 2D and 3D face recognition: A survey. Pattern Recognit Letters, vol. 28, issue 14: 1885-1906
41. Bowyer KW, Hollingsworth K and Flynn PJ (2008) Image Understanding for Iris Biometrics: a Survey. Computer Vision and Image Underst, 110(2): 281-307
42. Adler A (2004) Images can be reconstructed from quantized biometric match score data. Proc. Canadian Conf Electrical Computer Eng, Niagara Falls: 469-472
43. Ross A, Shah J, and Jain AK (2007) From templates to Images: Reconstructing fingerprints from minutiae points. IEEE Trans Pattern Anal Mach Intell, vol. 29, no. 4: 544-560
44. Abdullayeva F, Imamverdiyev Y, Musayev V, and Wayman J (-) Analysis of security vulnerabilities in biometric systems. IIT of ANAS and San Jose State University. http://danishbiometrics.files.wordpress.com/2009/08/1-13.pdf. Accessed 30 January 2010
45. Privacy Commissioner Responds to Public Enquiries about the Issue of "Employer Collecting Employees' Fingerprint Data for Attendance Purpose". Privacy Commissioner of Hong Kong. http://www.pcpd.org.hk/english/infocentre/press_20090716.html. Accessed 30 January 2010
46. Higaki T (2007) Quotes of the Day. TIME. http://www.time.com/time/quotes/0,26174,1685967,00.html. Accessed 30 January 2010
47. MacManus R (2009) Hong Kong's Octopus Card: Utility Outweighs Privacy Concerns. ReadWriteWeb. http://www.readwriteweb.com/archives/hong_kongs_octopus_card.php. Accessed 30 January 2010
48. Jain AK, Nandakumar K, and Nagar A (2008) Biometric template security. EURASIP J Advances in Signal Processing, Special issue on Biometrics
49. Dewan SK (2003) Elementary, Watson: Scan a Palm, Find a Clue. The New York Times. http://www.nytimes.com. Accessed 30 January 2010

50. Reddy PV, Kumar A, Rahman SMK, and Mundra TS (2008) A new antispoofing approach for biometric devices. IEEE Trans Biomel Circuits & Sys, vol. 2, no. 4: 284-293
51. Ratha N, Connell JH, and Bolle RM (2001) An analysis of minutiae matching strengths. Proc Intl Conf Audio and Video-based Biometric Authentication, Halmstad, Sweden: 223-228
52. Jules A and Sudan M (2002) A fuzzy vault scheme. Proc IEEE Intl Symp Inf. Theory, Lausanne, Switzerland: 408
53. Tuyls P, Akkermans AHM, Kevenaar TAM et al (2005) Practical biometric authentication with template protection. Proc 5th Intl Conf Audio- and Video-based Biometric Person Authentication, Rye Town, NY: 436-446
54. Draper SC, Khisti A, Martinian E et al (2007) Using distributed source coding to secure fingerprint biometrics. Proc ICASSP, Hawaii: 129-132
55. Uludag U and Jain AK (2006) Securing fingerprint template: Fuzzy vault with helper data. Proc. CVPR Workshop on Privacy Research in Vision, New York: 163
56. Feng YC and Yuen PC (2006) Protecting face biometric data on smartcard and Reed-Soloman Code. Proc CVPR Workshop on Biometrics, New York: 29
57. Lee YJ, Bae K, Lee SJ et al (2007) Biometric key binding: Fuzzy vault based on iris images. Proc Intl Conf Biometrics, Seoul: 800-808
58. Kumar A and Kumar A (2009) Development of a new cryptographic construct using palmprint based fuzzy vault. EURASIP Journal on Advances in Signal Processing, ASP/967046
59. Freire-Santos M, Fierrez-Aguilar J, and Ortega-Gracia J (2006) Cryptographic key generation using handwritten signature. Proc SPIE Conf Biometric Technologies for Human Identification, Vol. 6202, Orlando: 225-231
60. NIST Report to the United States Congress (2002) Summary of NIST Standards for Biometric Accuracy, Tamper Resistance and Interoperability
61. Hong Kong Post e-Cert. http://www.hongkongpost.gov.hk/index.html. Accessed 30 January 2010
62. Bangeman E (2009) Swiss privacy commissioner says "nein" to Google Street View. Ars technical. http://arstechnica.com/tech-policy/news/2009/08/swiss-privacy-commissioner-says-nein-to-google-street-view-swiss-privacy-commissioner-says-nein-to-google-street-view.ars. Accessed 30 January 2010
63. Denham E (2009) Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA). Office of the Privacy Commissioner of Canada. http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm. Accessed 30 January 2010

64. Doward J (2009) DNA tests for asylum seekers 'deeply flawed'. guardian.co.uk. http://www.guardian.co.uk/world/2009/sep/20/asylum-seeker-dna-tests. Accessed 30 January 2010
65. Argentina Forces Dirty War Orphans To Provide DNA. CBS News. http://www.cbsnews.com/stories/2009/11/21/ap/world/main5727307.shtml. Accessed 30 January 2010
66. Woodard DL and Flynn PJ (2005) Finger surface as a biometric identifier. Computer Vision and Image Underst, vol. 100, no. 3: 357-384
67. Kumar A and Ravikanth Ch (2009) Personal authentication using finger knuckle surface. IEEE Trans Inf Forensics & Security, vol. 4, no. 1: 98-110
68. Kumar A and Zhou Y (2009) Human identification using knucklecodes. *Proc BTAS 2009*, Washington DC
69. Yan P and Bowyer KW (2007) Biometric recognition using 3D ear shape. IEEE Trans Pattern Anal Mach Intell, vol. 29, no. 8: 1297-1308
70. Investigation Report: Employer Collecting Employees' Fingerprint Data for Attendance Purpose. Privacy Commissioner Hong Kong. http://www.pcpd.org.hk/textonly/english/infocentre/press_20090713a.html. Accessed 30 January 2010
71. Cohn JP (2006) Keeping an Eye on School Security: The Iris Recognition Project in New Jersey Schools. National Institute of Justice J, No. 254. http://www.ojp.usdoj.gov/nij/journals/254/iris_recognition.html. Accessed 30 January 2010
72. John Daugman's Webpage. University of Camb. http://www.cl.cam.ac.uk/~jgd1000. Accessed 30 January 2010
73. Jain AK, Dass SC and Nandakumar K (2004) Can soft biometric traits assist user recognition?. Proc SPIE Vol. 5404, Biometric Technology for Human Identification, Orlando: 561-572
74. Jain AK, Dass SC and Nandakumar K (2004) Soft Biometric Traits for Personal Recognition Systems. Proc of International Conference on Biometric Authentication, Hong Kong: 731-738
75. Jain AK and Park U (2009) Facial Marks: Soft Biometric for Face Recognition. Proc Int Conf Image Process, Cairo, Egypt
76. Kellokumpu V, Zhao G, Li SZ et al (2009) Dynamic texture based gait recognition. Proc ICB 2009, Alghero, Italy: 1000-1009

77. Wayman JL (1997) Large-scale Civilian Biometric Systems - Issues and Feasibility. Proc Card Tech / Secur Tech ID

78. Lee J-E, Jain AK, and Jin R (2008) Scars, Marks and Tattoos (SMT): Soft Biometric for Suspect and Victim Identification. Proc Biometric Symposium, Biometric Consort Conference, Tampa, Florida

79. HK Privacy Commissioner: Fingerprint collection excessive. MIS ASIA. http://www.mis-asia.com/news/articles/hk-privacy-commissioner-fingerprint-collection-excessive. Accessed 30 January 2010

80. Park U, Ross A, and Jain AK (2009) Periocular Biometrics in the Visible Spectrum: A Feasibility Study. Proc BTAS, Washington DC

81. Registry of USG recommended Biometric Standards. Biometrics.gov. http://www.biometrics.gov/Standards/StandardsRegistry.pdf. Accessed 30 January 2010

82. National and International Biometric Standards. NIST. http://www.itl.nist.gov/div893/biometrics/standards.html. Accessed 30 January 2010

83. Electronic Biometric Transmission Specifications. Department of Defense. http://www.biometrics.gov/Standards/DoD_ABIS_EBTS_v1.2.pdf. Accessed 30 January 2010

84. BioAPI Consort. http://www.bioapi.org. Accessed 30 January 2010

85. Magazine photos fool age-verification cameras. Pink Tentacle. http://pinktentacle.com/2008/06/magazine-photos-fool-age-verification-cameras. Accessed 30 January 2010

86. Volokh E (2007) Religious Freedom and DNA Gathering. Volokh Conspiracy or CNET news http://volokh.com/2007/02/26/religious-freedom-and-dna-gathering Feb. 2007 or http://news.cnet.com/Feds-out-for-hackers-blood/2100-7348_3-6151385.html Accessed 30 January 2010

87. Médioni G, Choi J, Kuo C-H, and Fidaleo D (2009) Identifying noncooperative subjects at a distance using face images and infrared three-dimensional face models. IEEE Trans Systems, Man, Cybernetics – Part A: Systems and Humans, vol. 39, no. 1

88. Daugman J and Malhas I (2004) Iris recognition border-crossing system in the UAE. BIOMETRICS. http://www.cl.cam.ac.uk/~jgd1000/UAEdeployment.pdf. Accessed 30 January 2010

89. Matey JR, Ackerman D, Bergen J et al (2008) Iris recognition in less constrained environments. In: Ratha NK, Govindaraju V (eds.) Advances in Biometrics Sensors, Algorithms and Systems. Springer, London

90. Proença H, Filipe S, Santos R, Oliveira J, and Alexandre LA (2009) The UBIRIS.v2: A database of visible wavelength iris images captured on-the-move and at-a-distance. to appear in IEEE Trans Pattern Anal Mach Intell, available online, 2009.
91. Bender S and Postley H (2007) Key sequence rhythm recognition system and method. US Patent No. 7206938
92. Jain AK and Feng J (2009) Latent Palmprint Matching. IEEE Trans Pattern Anal Mach Intell, vol. 31, no. 6: 1032-1047
93. Tao D, Li X, Wu X et al (2007) Analysis and Gabor Features for Gait Recognition. IEEE Trans Pattern Anal Mach Intell, vol. 29, no. 10: 1700-1715
94. New Biometric Technology Improves Security and Facilitates U.S. Entry Process for International Travelers. US Department of Homeland Security. https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-fingerprint_consumer_friendly_content_1400_words.pdf. Accessed 30 January 2010
95. Fast border passage with iris scan. Schiphol. http://www.schiphol.nl/AtSchiphol/PriviumIrisscan/FastBorderPassageWithIrisScan.htm. Accessed 27 September 2009
96. Ranger S (2006) Photos: Iris scanning at the airport. Silicon.com. http://www.silicon.com/management/public-sector/2006/04/13/photos-iris-scanning-at-the-airport-39158086/. Accessed 10 October 2009
97. Walt Disney World Resort. http://disneyworld.disney.go.com/. Accessed 30 January 2010
98. Integrated Automated Fingerprint Identification System or IAFIS. CJIS. http://www.fbi.gov/hq/cjisd/iafis.htm. Accessed 30 January 2010
99. Veeramachaneni K, Osadciw LA, Varshney PK (2005) An Adaptive Multimodal Biometric Management Algorithm. IEEE Trans Sys Man & Cybern., Part-C, vol. 35, no. 3: 344-356
100. Nakashima E (2007) FBI Prepares Vast Database of Biometrics. The Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html. Accessed 30 January 2010
101. Kumar A, Kanhangad V, and Zhang D (2010) A new framework for adaptive multimodal biometrics management. to appear in IEEE Trans Inf Security Forensics, available online
102. Tronci R, Giacinto G, Roli F (2007) Dynamic score selection for fusion of multiple biometric matchers. Proc. 14th IEEE International Conference on Image Analysis and Processing, ICIAP, Modena, Italy: 15-20

103. Poh N, Wong R, Kittler J et al (2009) Challenges and research directions for adaptive biometric recognition systems. Proc ICB, Alghero, Italy
104. Nandakumar K, Jain AK, and Ross A (2009) Fusion in multibiometric identification systems: what about the missing data?. Proc ICB, Alghero, Italy: 743-752
105. Iris at a distance not yet mature enough, says UAE. Biometric Technology Today, issue 2, vol. 2009, pp. 1, Feb. 2009.
106. Rowe RK, Uludag U, Demirkus M et al (2007) A Multispectral Whole-hand Biometric Authentication System. Proc Biometric Symposium, Biometric Consort Conference, Baltimore
107. Matey JR, Naroditsky O, Hanna K et al (2006) Iris on the move: acquisition of images for iris recognition in less constrained environments. Proc IEEE, vol. 94: 1936-1947
108. Sun Z, Tan T, Yang Y et al (2005) Ordinal palmprint representation for personal identification. Proc CVPR 2005: 279-284
109. Singh R, Vatsa M, Ross A et al (2009) Online learning in biometrics: A case study in face classifier update. Proc BTAS'2009, Washington, DC
110. Lee HC and Gaensslen RE (2001) Advances in Fingerprint Technology. CRC Press.
111. Jain AK, Feng J, Nagar A and Nandakumar K (2008) On matching latent fingerprints. Proc. CVPR Workshop on Biometrics: 1-8
112. Evaluation of Latent Fingerprint Technologies 2007. NIST. http://fingerprint.nist.gov/latent/elft07/. Accessed 30 January 2010
113. Indovina M et al ELFT Phase II (2009) An Evaluation of Automated Latent Fingerprint Identification Technologies. NISTIR 7577
114. Singh K (2008) Altered fingerprints, Interpol report. INTERPOL. http://www.interpol.int/Public/Forensic/fingerprints/research/alteredfingerprints.pdf. Accessed 30 January 2010
115. Zhang D, Kong WK, You J et al (2003) Online palmprint identification. IEEE Trans Pattern Anal Mach Intell, vol. 25, no. 9: 1041–1050
116. Kumar A (2008) Incorporating cohort information for reliable palmprint authentication. Proc ICVGIP 2008: 583-590
117. Bhanu B and Chen H (2008) Human Ear Recognition by Computer, Springer
118. Mhatre A , Palla S, Chikkerur S et al (2005) Efficient Search and Retrieval in Biometric Databases. Proc SPIE Defense and Security Symposium, vol. 5779: 265-273

119. Grother P, Salamon W, Watson C et al (2009) MINEX II – Performance of match on card algorithms Phase II/III report. NIST Interagency Report 7477. http://fingerprint.nist.gov/minexII/minex_report.pdf. Accessed 30 January 2010

120. Antonelli A, Cappelli R, Maio D et al (2006) Fake finger detection by skin distortion analysis. IEEE Trans Inf Forensics & Security, vol. 1: 360-373

121. Nagar A and Jain AK (2009) On the security of non-invertible fingerprint template transforms. Proc First IEEE Intl Workshop Inf Forensics & Security (WIFS 2009), London

122. The Forensics Use of Bioinformatics: Ethical Issues, Nuffield Council on Bioethics, Cambridge Publishes, Cambridge, London, 2007.

123. Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability. NIST. http://www.itl.nist.gov/iad/894.03/NISTAPP_Nov02.pdf. Accessed 30 January 2010

124. Hong L (1998) Automatic Personal Identification Using Fingerprints. Ph.D. Thesis. Michigan State University

125. Barack Obama Pictures. FANPIX.net. http://www.fanpix.net/gallery/barack-obama-pictures.htm. Accessed 30 January 2010

126. Clarke R (2000) Beyond the OECD Guidelines: Privacy Protection for the 21st Century. Roger Clarke's Web-Site. http://www.rogerclarke.com/DV/PP21C.html. Accessed 30 January 2010

127. Hong Kong Immigration Department Annual Report 2007-2008, 2009. Hong Kong Immigration Department. http://www.immd.gov.hk/a_report_07-08/eng/chapter02/index.htm. Accessed 30 January 2010

128. PalmSecure. http://www.fujitsu.com/us/services/biometrics/palm-vein. Accessed 20 February 2010

129. Kumar A and Prathyusha KV (2009) Personal authentication using hand vein triangulation and knuckle shape. IEEE Trans Image Processing, vol. 38, no. 9: 2127-2136

130. DNA Fingerprint Identification. http://www.fingerprinting.com/dna-fingerprint-identification.php, Accessed 20 February 2010