H. Al-Assam, T. Kuseler, S. Jassim and S. Zeadally, "Privacy in Biometric Systems", in S. Zeadally & M. Badra (eds), Privacy in a Digital, Networked World: Technologies, Implications and Solutions, Springer, ISBN 978-3-31908469-5, pp. 235-263, October 2015

Privacy in Biometric Systems

Hisham Al-Assam, Torben Kuseler, Sabah Jassim

Applied Computing Department, University of Buckingham, Buckingham, MK18 1EG, UK

Sherali Zeadally

College of Communication and Information, University of Kentucky, Lexington, KY, 40506, USA

H. Al-Assam, T. Kuseler, S. Jassim and S. Zeadally, "Privacy in Biometric Systems", in S. Zeadally & M. Badra (eds), Privacy in a Digital, Networked World: Technologies, Implications and Solutions, Springer, ISBN 978-3-31908469-5, pp. 235-263, October 2015

1. Introduction

Biometrics are physiological and/or behavioral characteristics of a person that have been used to provide an automatic proof of identity in a growing list of applications including crime/terrorism fighting, forensics, access and border control, securing e-/m-commerce transactions and service entitlements. In recent years, a great deal of research into a variety of new and traditional biometrics has widened the scope of investigations beyond improving accuracy into mechanisms that deal with serious concerns raised about the potential misuse of collected biometric data. Despite the long list of biometrics' benefits, privacy concerns have become widely shared due to the fact that every time the biometric of a person is checked, a trace is left that could reveal personal and confidential information. In fact, biometric-based recognition has an inherent privacy problem as it relies on capturing, analyzing, and storing personal data about us as individuals. For example, biometric systems deal with data related to the way we look (face, iris), the way we walk (gait), the way we talk (speaker recognition), the way we write (handwriting), the way we type on a keyboard (keystroke), the way we read (eye movement), and many more. Privacy has become a serious concern for the public as biometric systems are increasingly deployed in many applications ranging from accessing our account on a Smartphone or computer to border control and national biometric cards on a very large scale. For example, the Unique Identification Authority of India (UIDAI) has issued 56 million biometric cards as of January 2014 [1], where each biometric card holds templates of the 10 fingers, the two irises and the face. An essential factor behind the growing popularity of biometrics in recent years is the fact that biometric sensors have become a lot cheaper as well as easier to install and handle. CCTV cameras are installed nearly everywhere and almost all Smartphones are equipped with a camera, microphone, fingerprint scanner, and probably very soon, an iris scanner.

Biometrics can be a very effective tool to keep us safe and secure, prevent individuals from applying for multiple passports or driving licences, and keep the bad guys out or under control. However, the fact that we are surrounded by so many biometric sensors does limit our privacy in one way or another. The price we might have to pay for using many biometrics-reliant applications such as access control to a building, authorizing payments in supermarkets and public transports is the loss of privacy as a result of being tracked in almost all of our daily life activities. Furthermore, recent research into biometrics shows that more and more personal information can be revealed from biometric data such as gender, age, ethnicity, and even some critical health problems such as diabetes, vision problems, Alzheimer's disease, etc. Such confidential information might be used, for example, to discriminate between individuals when it comes to insurance, jobs, border entry enforcement etc.

This chapter is mainly concerned with privacy issues and solutions surrounding the use of biometrics as a means of recognizing individuals. As biometric security and biometric privacy are strongly related, it is useful to highlight the difference between these two topics first. **Biometric security** is concerned with protecting biometric data against theft for impersonation of the owner of the biometric data. **Biometric privacy** is concerned with preventing misuse of the biometric system for purposes of tracing and gaining information that may result in the person's loss of civil rights, discrimination against the person, victimization and/or even denial of access to services.

The rest of this chapter is organized as follows; section 2 provides essential background information on biometrics while section 3 discusses several privacy concerns about biometrics. Privacy solutions proposed to address these concerns are then explained in section 4. Outstanding challenges and opportunities for future research directions are discussed in section 5.

2. Background on Biometrics

A reliable identity management system is a key component to prevent identity theft and satisfies the increased security requirements in a wide range of applications ranging from controlling international border crossings to accessing remotely stored personal information and assets. Establishing the identity of a person is a key task in any such identity management system. Typically, there are three ways to establish the identity of an individual, each of which has its own advantages and limitations[2]:

- ***Knowledge-based authentication***, or "something you know", that typically relies on a memorized password or PIN. A random and long password offers a strong security mechanism for user authentication. However, in practice, humans have difficulties in memorizing complex passwords, and passwords that they can easily remember are often short and therefore simple to guess or determined by a brute-force / dictionary attack.
- ***Object-based authentication***, or "something you have", which relies on the physical possession of an object, such as a token. The main drawback of a physical token is that, when lost or stolen, an impostor can gain unauthorized access.
- ***Identity-based authentication***, or "something you are", i.e. ***biometrics***. Biometric-based authentication offers an advantage over other authentication factors in that a legitimate user does not need to remember or carry anything. Furthermore, biometric-based authentication is known to be more reliable than traditional authentication due to the fact that it is directly linked with the identity of individuals. However, there exist several challenges, as we explain later in this chapter, which make biometric systems far from perfect. For example, unlike other credentials such as PINs, passwords, or smart cards, once biometric related information is compromised, it is impossible to make this information private again.

Biometric systems aim to identify or verify individuals' identity based on physical characteristics (e.g., face, iris, fingerprint, DNA, or hand geometry), and/or behavioral characteristics (e.g. speech, gait, or signature). A typical biometric system has two stages, enrolment and recognition. Figure 1 illustrates the process of the biometric enrolment stage, in which a user starts by presenting their biometric data to a biometric sensor (usually in a controlled environment). If the quality of the captured biometric sample is found to be adequate, the enrolment process proceeds to a pre-processing procedure to prepare the sample for the next step. A feature extraction technique is then used to extract a digital discriminating feature vector of the individual, called Biometric Template (BT), which will then be stored (often also called "enrolled") alongside the individual's identifier (ID) in a database.

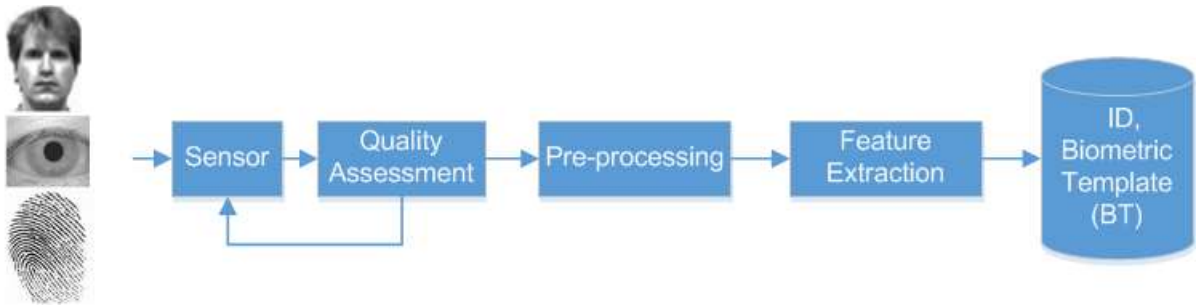

Figure 1: A typical enrolment stage of a biometric system (the face image was used from the Extended Yale Face Database B [3])

At the recognition stage, biometric systems can function in two modes depending on the application context, namely authentication or identification mode.

2.1 Biometric-Based Authentication

Biometric-based authentication (also known as verification) is a one-to-one comparison of a freshly captured biometric sample(s), known as query, against an enrolled BT as illustrated in Figure 2. In this mode, a user claims an identity and the biometric system aims to verify the authenticity of the claimed identity (e.g., the system answers the question: "Are you who you say you are?"). For example, authentication might be used when a user wants to access his/her bank account or computer. The matching process uses a distance or similarity function to calculate a score indicating the similarity between the stored BT and the fresh feature vector extracted from the query sample. If the matching score is high enough, i.e. close enough to the enrolled template, the biometric system grants access to the user. Otherwise the requested access is rejected. The term "high enough" is determined by the administrator depending on the level of tolerance necessary for the specific application. This allows the system administrator to adjust the rates of false acceptance (i.e. wrongly accepted imposters as genuine users) and false rejection (i.e., wrongly rejected genuine users) to the desired levels. Typically, there is a trade-off between the False Acceptance Rate (FAR) and the False Rejection Rate (FRR), in which the reduction of one rate causes an increase in the other. Most biometric systems are configured to be highly secure by maintaining a very low (e.g. 1 in 10,000) FAR and an acceptable FRR. In an access control system, for example, it will generally be less problematic to have a false rejection by asking the genuine user to re-scan their biometric, rather than a false acceptance in which an unauthorized individual will be granted access.

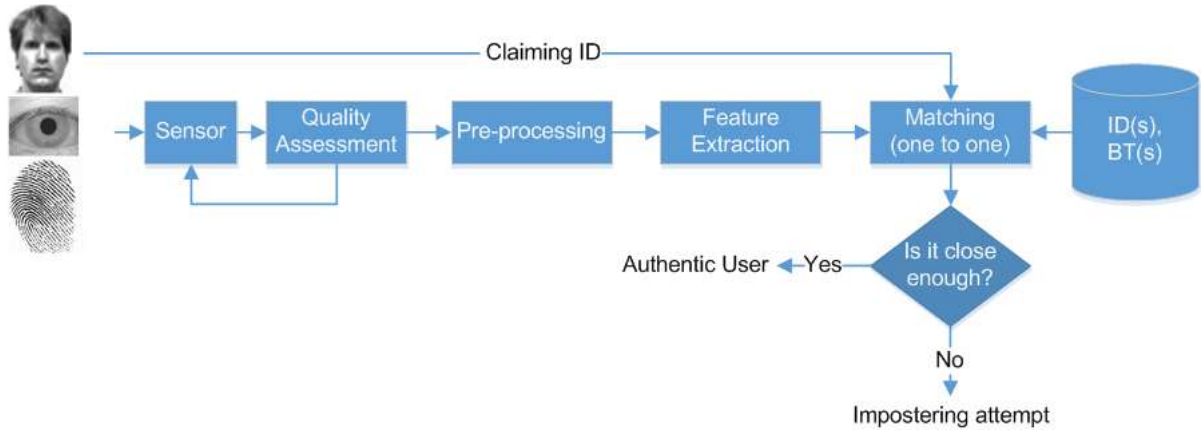

Figure 2. Typical biometric system in authentication mode

2.2 Biometric-Based Identification

Biometric-based identification is a one-to-many comparison of the query against all templates in the database as illustrated in Figure 3. In this mode, a biometric system aims to identify an individual by searching the set of available identities or the system returns 'Not enrolled' if the matching module of the biometric system cannot find the identity. Identification functionality can be further classified into positive and negative identification. In positive identification, an individual attempts to positively identify themselves to the system without explicitly claiming an identity (i.e., the system answers the question: "Are you someone who is known to the system?"). Positive identification might be deployed for example to grant access to resources such as buildings or computers where the system knows the set of enrolled users. In contrast, in negative identification (also known as screening), an individual

attempts to conceal their true identity and the system aims to answer the question: "Are you who you say you are not?". Screening might be used by national border agencies to check if a passenger's identity is on a watch-list or by authorities to prevent issuing multiple national ID cards, passports, or driving licences to a single individual.

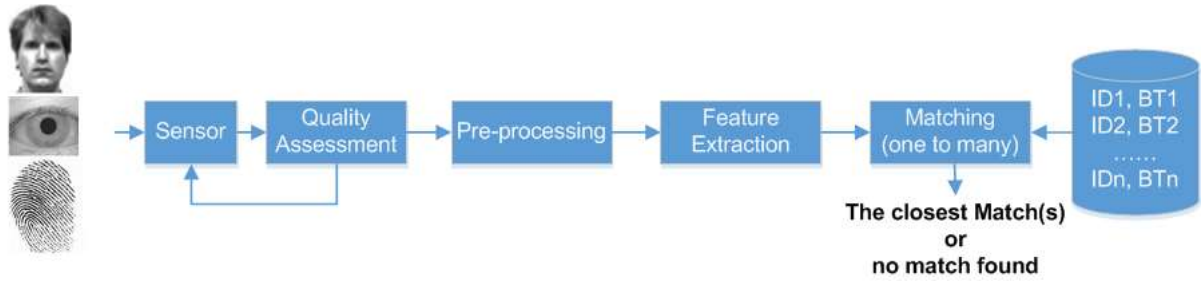

Figure 3. Typical biometric system in identification mode

Biometric systems such as face recognition can be deployed in identification and authentication modes, depending on the application. For example, face-based authentication can be used to provide access control (i.e. letting the genuine person in), while face-based identification can also be applied as a 'watch list' system to find some particular individuals in a crowd, i.e. keeping the targeted people out.

2.3 Challenges in Biometric Systems

Over the years, a large number of biometric modalities (also called biometric traits) together with a variety of feature extraction and matching schemes have been investigated. The suitability of any biometric modality for an application depends on several factors such as universality, uniqueness, invariance over time, measurability, usability, and cost [4]. The challenges in biometric research activities have expanded recently to include the maintenance of privacy and security of biometric systems beside the traditional work to improve accuracy, scalability, and usability. In other words, the challenge in biometrics is to design a system that is highly accurate, easily scalable to large datasets, convenient to use, and secure at the same time. In what follows, several challenges of biometric systems are briefly explained, leaving further detailed discussions on biometric privacy concerns to section 3.

2.3.1 Biometric Accuracy

An ideal biometric system should have perfect accuracy, i.e. it always recognizes genuine users and rejects imposters correctly. However, in practice, a biometric system can make four types of errors:

i) *False Non-Match Rate* (FNMR), also known as False Rejection Rate (FRR): it occurs when two samples, for example collected at different times, of the same biometric modality of an individual are not recognized as a match.

ii) *False Match Rate* (FMR), also known as False Acceptance Rate (FAR): it occurs when two samples from different individuals are incorrectly recognized as a match.

iii) *Failure to Enrol Rate* (FTER): it occurs when an individual is unable to present the required biometric modalities (for example because of a finger or hand cut), is unable to interact correctly with the sensor, or the captured biometric samples quality is very poor.

iv) *Failure to Capture Rate* (FTCR): it occurs when a biometric sample provided by an individual during the recognition stage cannot be acquired or processed reliably.

In practice, these biometric errors can occur due to the following factors [5]:

- **Noisy sensor data**: defective or improperly maintained sensors can lead to the capture of low quality and noisy biometric samples, which results in a significant reduction in the recognition accuracy by increasing the FRR of the biometric system.
- **Non-universality**: a biometric modality can be considered universal when every individual in a target population is able to present the biometric modality for recognition. Although universality is an essential requirement, not all biometric modalities are perfectly universal. The National Institute of Standards and Technology (NIST) has reported that it is not possible to obtain good quality fingerprint images from two percent of the population, for example people with hand-related disabilities, manual workers with many cuts and bruises on their fingertips, and people with very oily or dry fingers [6]. Non-universality leads to higher FTER and FTCR in a biometric system.
- **Inter-class similarity**: this term is used to refer to similarity of biometric samples from different individuals. It is strongly linked with the uniqueness of biometric features and is indicative of discriminative ability of the biometric modality (i.e., the greater the inter-class similarity the higher the FMRs).
- **Intra-Class variation**: typically, two biometric samples of the same individual are always different, which results in FNM errors explained earlier. These intra-class variations may be due to improper interaction of the user with the sensor (e.g., changes in rotations or poses), changes in environmental conditions such as lighting conditions and inherent changes in the biometric modality such appearance changes due to ageing or facial hair.
- **Biometric scalability**: Ideally, the number of enrolled individuals should have no significant effect on the performance of the biometric systems in terms of both accuracy and speed. When a biometric system is set up to function in the authentication mode, scalability is not a problem because each authentication attempt involves one-to-one matching i.e. matching the query with the stored template of an individual. However, the number of enrolled individuals has crucial impact on the performance of biometric systems in the identification mode, where one-to-many matching is required to have a biometric sample identified. For example, if the size of a database is a million, and each matching requires 1 millisecond, then the time required to identify one individual would be more than 16 minutes. Therefore, biometric identification systems that operate on large scale databases involve some kind of filtering or indexing based on extrinsic (e.g., gender, ethnicity, age, etc.) or intrinsic (e.g., fingerprint pattern class) factors to prune the search procedure [7].

2.3.2 Security and Privacy of Biometric Systems

Public acceptance of biometric systems has a crucial impact on their success due to potential/perception of misuse of the collected biometric data. The growing deployment of biometric systems as a proof of identity tool for access control to physical facilities, entitlement to services, and in the fight against crime and terrorism has become a necessity in modern days, but it is also becoming a source of privacy and security concerns. Traditionally, the focus of biometrics research has been on accuracy, speed, cost, and robustness challenges but gradually the scope widened to security and privacy issues of biometric systems. Questions like: "What if my biometric data has been stolen or misused?" have recently attracted attention not only to reassure users about privacy intrusion but also to prevent misuse of stolen data.

Although a biometric-based authentication system is known to be more reliable than traditional authentication schemes, the system is subject to failure due to intrinsic factors mentioned earlier or due to adversary attacks. The security of biometric systems can be undermined in various ways. For

example, a biometric template can be replaced by an impostor's template in a system database or be stolen and replayed [8]. As a result, the impostor can gain unauthorized access to whatever the owner has authorized access to. Moreover, it has been shown that it is possible to create a physical spoof starting from biometric templates [5]. For example, a "hill climbing attack" on a biometric system can be used to generate a good approximation of the target template in a finite number of iterations [9]. It is also possible to reconstruct fingerprint images from standard templates, which might then fool the fingerprint recognition system [10]. Furthermore, certain biometric data is not secret and can be easily acquired without the knowledge of the user. Individuals usually unintentionally leave (poor-quality) fingerprints everywhere such as on a glass or a hidden camera can capture an image of a face or iris [11]. In fact, the level of secrecy and privacy varies greatly among different biometric modalities (e.g., the covert acquisition of face images or voice samples is much easier compared to collecting retina or palm vein samples). The effect of all these attacks on the security and acceptability of biometrics are not difficult to imagine and their consequences are far from limited to individuals. However, the related privacy concerns of such attacks and misuses of a system by insiders and/or secondary users are far from obvious. Section 3 discusses these biometric privacy concerns in more detail.

2.4 Multi-Modal and Multi-Factor Biometric Recognition

Multi-modal and/or multi-factor biometric solutions have been proposed to overcome most of the aforementioned challenges that could degrade the performance of a biometric system. **Multi-modal systems** rely on combining two or more biometric modalities to establish the identity of an individual. For example, face, voice, and signature were combined together in the EU-funded SecurePhone FP6 Project [12] to provide a strong mean of authentication for mobile devices. Multi-modal biometrics have been deployed in a wide range of applications such as border entry/exit, access control, law enforcement, and network security. It has been demonstrated that using a combination of biometric modalities can significantly improve recognition accuracy by reducing FNMR and FMR. In addition, such an approach provides a secondary means of recognition if biometric samples of sufficient quality cannot be acquired from a particular individual. On the other hand, **multi-factor biometric systems** typically combine biometric data with knowledge-based and/or object-based authentication factors to produce a single representation of individuals. Multi-factor recognition can be very effective to improve recognition accuracy and is at the same time very easy to implement. For example, face biometric recognition can be combined with a 4-digit PIN to significantly lower false acceptance rates. More details on exploiting multi-factor recognition as a means for generating cancellable/revocable templates to improve the privacy of biometric systems will be presented in section 4.

3. Privacy Concerns With Biometrics

The growing number of applications that use biometrics coupled with the increased capabilities of biometric sensors in terms of resolution, accuracy, and capturing biometric data unobtrusively, introduces new challenging problems for maintaining privacy. In the past, fingerprints were only used to identify potential suspects at crime scenes, i.e. the number of collected, analyzed, and stored fingerprints was relatively small. Nowadays, thousands of applications and devices use fingerprints to identify legitimate users. For example, Apple's latest iPhone generation, the iPhone 5s, features "Touch ID", a fingerprint identity sensor that allows iPhone users to use their fingerprint instead of a PIN code to unlock their iPhones. Another Smartphone example is the "Vital Signs Camera - Philips" app[13], already downloaded by hundreds of thousands of users. This app allows you to "Measure your heart rate and breathing rate from a distance, simply by using the camera of your iPad or iPhone!". Although the accuracy of the taken measurements might be not as good as measurements from dedicated heart rate monitors, these apps enable nearly everybody to easily and extensively collect sensitive biomedical data of any person in their proximity.

Improved sensor technology has also an impact on maintaining/undermining privacy, in particular for biometric sensors that can work and collect data remotely (i.e., from a distance) without the individual's consent. Today, many of us (i.e., everybody living in an urban area) are monitored regularly. In 2011, it was estimated that on average a citizen of London, UK, is caught around 100 times per day on a CCTV camera. This number is expected to increase due to continued reduction in the cost of CCTV camera production, installation, maintenance and automatic data analyses.

The ease with which biometric data can be collected, processed, and stored has led to a large and fast growing number of huge biometric datasets on local (e.g., individual companies), national (e.g., United States Visitor and Immigrant Status Indicator Technology (US-VISIT)) and international (e.g., European fingerprint database (EURODAC)) levels. This ever-increasing amount of information available about a human person was firstly named by Irma van der Ploeg as the "informatization of the body" [2]. This growing digitization of the human body away from its natural, very diverse form of physical existence into standardized digital code and information "may eventually affect embodiment and [human] identity as such" and finally offend human dignity [3]. Undoubtedly, recent advances in surveillance and sensors technologies will rapidly accelerate the speed by which this fully digitized and "informatized" body will become reality. It is questionable if fair information principles, and here in particular, the **principle of proportionality** stating "*that identification systems should only be implemented if the benefits are worth the social costs, including the invasion of privacy, loss of autonomy, social discrimination, or imposition of conformity*", are always respected [4]. It is more likely that technology advances will increase the risk of misuse of the available information as a result of unethical and/or illegal practices, if the users' sensitive data and privacy is not adequately protected.

However, it is important to note that it is the utilization of the biometric system that determines the impact on privacy, not the biometric modality itself [5]. For example, a company could legitimately use a face image recognition system to restrict access to sensitive and private company data. Also, face images from a CCTV camera could be used to identify potential suspects at a crime scene. It is worth noting that the same biometric modality (face) is used in different applications; once to protect privacy, and once to infringe it.

The privacy concerns about biometrics emerge from four main biometric data misuses that are described below. It is important to highlight that the threat to privacy can either arise from the inside or from the outside of the involved systems and organizations. A threat coming from the inside can be for example a person (e.g., a system administrator), who works for one of the involved organizations.

These people are often called secondary users. A threat from the outside can be for example an attacker, who has no further relation to the involved organizations or individuals and tries to attack the systems just for his benefit (e.g., to sell the stolen or collected private information).

Unnecessary and unauthorized collection

To preserve the individual's privacy as much as possible, the amount of data collected should be always minimized. Biometric systems should only be used in scenarios where the system or organization security will benefit from the installation. For example, if access to a specific area in a company does not need to be protected, no fingerprint or face recognition system should be installed at the entry points to that area. However, additional systems of that kind are often installed by companies, just to monitor and record employees' behavior. This is a typical example of a privacy threat coming from the inside.

Unauthorized and concealed collection of biometric data (e.g., via hidden cameras) is another privacy risk and often performed from the outside. As mentioned before, cameras are now widely used to monitor our everyday life. Very often, people benefit from this monitoring, for example traffic jams or over-crowded underground stations can be easily and quickly detected and such information can be passed on to the other passengers to avoid these situations. However, this extensive data collection and analysis can also lead to privacy concerns. In 2012, politicians in Argentina announced that they will create a new centralized biometric database containing face images of Argentina's citizens. This announcement immediately raised resistance and critics pointed out that this new system could discourage political engagement and protests, because the database could also be used to help identify undesired demonstrators and suppress political activities. Another example of a biometric related privacy concern occurs in night clubs and bars in cities like Chicago and San Francisco. These bars use their security cameras now together with face detection software to broadcast real-time information on the number of male and female visitors in the club, together with their average ages groups. This information can then be used by others to decide which bar to visit.

Unauthorized use and application of cross-matching

A further privacy concern arises from the fact that an individual's biometric data collected for different purposes and unrelated applications can be cross-referenced by comparing stored biometric templates. This allows, for example, the linking of bank datasets and financial records to medical related datasets, if both involved organizations (i.e. banks and medical agencies) hold the same biometric record/template of that individual. The actual sharing could either happen if an insider of one organization illegitimately shares the sensitive data with the other organization for his own financial benefits [14], or if both organizations agree to share the data within a strategic relationship benefitting both of them [15]. An example of a negative consequence of this type of information/application cross-matching and data sharing could be that a mortgage application of an individual is declined. The mortgage issuing bank has automatic access to the person's financial status via its own user records. If this bank has now also access to the applicant's medical records, a combined assessment could indicate that the mortgage risk is too high and the application is declined. Instead, an assessment of the financial status only could lead to an acceptance of the mortgage application.

Function or purpose creep

Function or purpose creep occurs when the biometric information collected by an application for one specific purpose (e.g., to give access to certain material or places) is also used in a completely different application scenario without the user's consent. One famous example of a large scale

biometric function creep is the European Dactyloscopy (EURODAC) fingerprint database for identifying asylum seekers [16]. The original purpose of this database was to "help the effective application of the Dublin convention on handling claims for asylum." However, soon after the database was established, access to the data was also granted to other police and law enforcement agencies. This function creep then finally led to an official statement of the European Data Protection Supervisor (EDPS) saying that [17]:
"Just because the data has already been collected, it should not be used for another purpose which may have a far-reaching negative impact on the lives of individuals. To intrude upon the privacy of individuals and risk stigmatizing them requires strong justification and the Commission has simply not provided sufficient reason why asylum seekers should be singled out for such treatment."

Similar concerns were also raised in the United States where innocent U.S citizens were imprisoned by mistake because of a large scale fingerprint sharing program called Secure Communities. This program administered by the FBI and the Department of Homeland Security wrongly identified James Makowski as an illegal immigrant and he was placed in a maximum security prison for two months before the authorities realized their error and released him.

Disclosure of medical related information

Biometric sensors may intentionally or unintentionally collect additional information (i.e., information beyond the data required to perform the intended task of biometric-based user identification / authentication, which may then reveal highly sensitive and personal information about the observed individuals). This contradicts the right of "informational privacy" that is, beside the physical and decisional privacy, one of the three elements of privacy every human should have [18]. "Informational privacy" refers here to the freedom of a person to decide who has access and is allowed to collected, process, and store personal information about him/her. One example where this right can be easily broken is biometrics-based on motor skills. Data collected via a distant video camera for gait recognition, may also reveal physical handicaps of that individual. This surplus of collected data could then be used to discriminate or intimidate that individual. This situation becomes even more of a problem when these actions are happening silently from a distance without the individual being aware of the ongoing process, or openly applied to vulnerable groups such as immigrants as well as the general public in the form of a biometric border [19].

The possible consequence that an individual will be discriminated against because of sensitive information revealed about him/her immediately raised the question within the research community, if "privacy" really is at the center of the problem or if the "discrimination" following an information disclosure is the real problem [20]. People are not put at risk just because their ethical background, age, gender, or sexual orientation was revealed from the collected biometric data. The discrimination and the social actions against them based on the data expose them to real risks. However, addressing this general problem of mankind on the social and psychological level is extremely difficult. Researchers working in the field of biometrics continue to focus mainly on how to enhance the individual's biometric data privacy in the first place.

To protect the individual's privacy as much as possible, the following principles should be followed to address and minimize the above mentioned three privacy problems [21]:

- **Identity privacy**: Binding of the stored biometric data and the individual's additional identity information such as age, gender, etc., should be minimized and protected. A close, unprotected link between the biometric data and the other stored identity information allows cross-referencing

this information with data from other sources to generate, for example, more detailed user profiles.

- **Irreversibility and unlinkability**: Collected biometric data should be converted into a different, application specific and non-reversible form before it is stored in the database. This prevents application cross-matching and the use of biometric data outside its intended original application.

The following sections highlight examples of biometric modalities used today and what kind of - potentially discriminating and privacy effecting - additional information can be extracted from the collected biometric sensor data. It is important to mention that the biometrics modalities and their corresponding biometrics sensors vary in terms of their actual usage in today's available applications, complexity of the involved biometric sensors, amount of additional information that can be revealed from the collected data, and the risk to which they expose the individual's privacy.

Fingerprints

One of the most widely used biometric modalities is the fingerprint. Fingerprint sensors are for example integrated in laptops to allow or deny access to the computer and used to identify individuals at border control or within company premises. Beside their original aim to reliably identify an individual in the aforementioned scenarios, research has showed that fingerprints or images of an entire finger can be used to reveal further information about the person (e.g., medical disorders like Down- or Turner syndrome).

Research further identified a correlation between fingerprints and the sexual orientation, i.e. homosexuality[22]. These research results are highly controversial within the academic research community because it was identified as being far away from being conclusive [23] and also human fingers are formed during prenatal development which can be seen as well before sexual orientations are developed. However, its publication in a well-known neuroscience journal clearly attracted attention within the general public [24] and may have persuaded the public to prejudge people.

Handwriting and voice/speech

The handwriting style and voice/speech are further biometric modalities that can be used to identify individuals as, for example, used in the "SecurePhone" project to sign contracts on Smartphones. However, research showed that degradations in handwriting skills and changes in the writing style can also be a sign of the Alzheimer's disease [25]. It was shown in particular that writing of cursive letters are challenging for people suffering from Alzheimer's disease and that changes and anomalies in how they write cursive letters can be identified by a biometric system. This is in particular applicable to human signatures which normally contain several cursive letters and paths. Similar findings were published on the detection of Parkinson's disease [26]. The study showed that two simple writing tasks can differentiate healthy individuals from individuals suffering from Parkinson's disease. Signs of Parkinson's disease can also be detected by visible speech impairments [27] identified for example through regular voice/speech-based recognition which has become increasingly popular. Technologies such as Apple's Siri are used now by millions of people on their iPhones and iPads [28]and could easily analyze and detect speech changes during normal operation.

But not only medical disorders such as Alzheimer's and Parkinson's disease can be identified by analyses of an individual's handwriting[29]. Research results have also suggested that more common and wide-spread social and health problems such as misuse of alcohol [30] or marijuana [31] can be detected via handwriting analyses too. This information about an individual can then, for example, be

very interesting to an employer during a job interview or to monitor existing employees and their performance.

Retinal vascular and vein pattern

Currently biometric modalities such as retinal or vein images are not widely used because these modalities are seen as more intrusive compared to fingerprints or handwriting. A retinal scanner illuminates the blood vessels in the eye using infrared light and then captures the reflected light for processing. This is seen as a potentially dangerous procedure to the eye and the eyesight by many people[32]. However, because of their high accuracy and advances in the scanner technology[33], it can be assumed that they will become more acceptable and popular in the near future. Nonetheless, today, available retinal scanners are already able to reveal medical conditions a person might have if the retinal image is examined by an automatic detection algorithm such as Automated Detection of Diabetic Retinopathy (ADDR) [34] or a human expert. Beside the given example of ADDR as one possible health condition revealed via retina scans, more than 100 genes have already been identified as contributing to human hereditary retinal degenerations[35]. This knowledge imposes a great privacy risk, as individuals might be rejected for certain jobs or have to pay higher health insurance premiums if the genes which are responsible for the retinal degeneration are also known to be contributing to other medical conditions. One such example is the USH2A gene, which is known to cause retinitis pigmentosa (a degenerative eye disease that causes severe vision impairment and often blindness), but also contributes to the Usher-Syndrome (genetic disorder resulting in hearing loss). This cross-reference could easily be made and negative implications could arise for the individual, regardless if this individual really develops a medical condition such as the Usher-Syndrome in his/her life or not.

Similar to the technology used to capture retinal pattern are vein pattern sensors. A Near-Infrared (NIR) sensor illuminates the region of interest (e.g., palm) and the reflected signals are then used to capture an image of the vein pattern structure. An example of a commercial solution is the BASEmetric™ Finger vein authentication (VeinID) device, used in several hospitals in Ohio, United States, to help with returning patient identification. However, researchers showed that the captured vein structure can also reveal sensitive information about possible health conditions (e.g., palm veins can reveal the Hypothenar Hammer Syndrome (HHS) [36]). HHS is caused by repetitive use of the hand "as a hammer", as for example in contact sports such as boxing or fighting. This knowledge could persuade people to prejudge individuals as aggressive or violent if the privacy of this information is not adequately protected and becomes public.

The examples discussed above clearly show the importance of privacy within the biometric area and that sensitive and personal biometric data needs to be protected so that it cannot be used outside its original collected and designed purpose. The following section 4 introduces several privacy-aware biometric solutions to address the aforementioned concerns.

4. Privacy-Aware Biometric Solutions

Over the last few years, several privacy-aware biometric solutions have been investigated to overcome some of the privacy concerns presented in section 3. As stated earlier, a biometric template is a sensitive representation of its owner that can be exploited in different ways to compromise user privacy. This section reviews several privacy-aware template processing schemes and highlights their pros and cons. It also presents other effective solutions such as match-on-card and privacy-preserving multi-factor biometric for local and remote authentication.

Privacy-aware template processing schemes mostly transform biometric template feature vectors into other private (i.e., personalized) vectors and secure domains. Such transformations preserve the anonymity of their owners while maintaining the capability of distinguishing them from other individuals. Such processes protect privacy at the design stage rather than being an aftermath action adopted as an add-on service at later stages. Although privacy-aware template processing schemes have continued to mature in academia over the last decade, they have not yet been widely adopted by commercial and governmental organizations either due to the extra cost needed to incorporate these schemes or simply because user privacy is not a priority yet for such organizations. However, with increased public awareness of biometric privacy and security issues, biometric experts are expecting a growing deployment of such schemes in the near future.

An ideal privacy-aware biometric template processing scheme must satisfy four properties [8]:

i) **Diversity**: templates cannot be used for cross-matching across different databases in which users can be tracked without their permissions.
ii) **Revocability**: templates can be revoked and new ones can be issued whenever needed.
iii) **Security**: it is computationally infeasible to reconstruct the original template from the transformed one.
iv) **Performance**: recognition accuracy must not degrade significantly when the protection scheme is applied.

The concepts of **revocability or cancellability** of biometric templates and **private biometric cryptosystems** have been developed as measures to improve user's privacy in biometric systems [37]. **Revocability** means that biometric templates are no longer fixed over time and could be revoked in the same way as lost or stolen credit cards are. The main approaches for privacy-aware revocable biometric templates are based on the use of a non-invertible (or infeasible to invert) secret personalized transformation of the biometric feature vectors. **Private biometric cryptosystems** work by generating anonymous biometric keys and hashes that can be used as a proof of identity. The main approaches are based on user-linked helper data (e.g., a secure sketch) extracted from the biometric feature vector. Existing helper schemes and secure sketches use a combination of quantization and error correcting codes. The created/extracted helper data should not reveal much information about the biometric template itself or from a fresh biometric sample.

It can be argued that each of the above privacy-aware template schemes has its own advantages and limitations in terms of the level of privacy provided, computational cost, storage requirements, applicability to different kinds of biometric representations and ability to handle inter-class variations in biometric data (i.e., maintaining the accuracy [5]). Therefore, the requirement of each system should be analyzed before recommending the right solution.

4.1 Parameterized Feature Transformations

The basic idea behind parameterized feature transformation is to use a function F to transform the original biometric template to a private and secure domain. The function F typically depends on a parameter or a key called a Transformation Key (TK). This TK is applied at the enrolment stage to transform the original template and generate a cancellable version of it. At the matching stage and for each recognition attempt, the same TK is applied on the freshly captured biometric samples to guarantee that the matching process takes place in a private and secure domain. Following this approach, revocation of a template simply requires a change of the TK.

Depending on the characteristics of F, feature transformations can be further categorized into salting and non-invertible transforms. In salting, F is invertible i.e., if the TK and the cancellable template are known, the original template or a good approximation of it should be recovered. However, it is assumed to be computationally infeasible to reconstruct the original template using the transformed template even if the TK is known in the non-invertible transform.

The TK can be user- or system-based depending on the usage scenarios and/or application, which enables privacy-aware feature transformations to be deployed in both authentication and identification mode. The following sections describe two examples of feature transformations, namely random projections and secret-based shuffling, followed by an illustration to demonstrate how feature transformation can be used in authentication and identification modes.

4.1.1 Feature Transformation using Random Orthonormal Projections

Several proposed schemes to produce cancellable biometrics involve the use of Random Orthonormal Projections (ROPs) to map biometric features onto private and personalized domains. ROP is a technique that uses random orthonormal matrices to project data points into other spaces where the distances among the data points before and after the transformation are preserved. The distance preserving feature has made ROPs ideal for biometric systems to improve privacy and security whilst maintaining an acceptable level of accuracy. ROP has been proposed as a secure transform for biometric templates and it was used to meet the revocability property [38] and as a standalone template protection scheme in a salting approach to generate a cancellable template for fingerprint [39] and face image data [40],[41]. However, a quantization step might be added to make the transform more difficult to invert [42]. ROP has also been used as a building block for generating a private biometric-based key from biometric data [43], [44] to be used as a cancellable template in the recognition process as explained in section 4.2. ROP-based transformations used to generate privacy-aware templates are typically created as follows:

i) Generate m pseudo random vectors or real values based on a secret key.

ii) Apply Gram-Schmidt orthogonalization on the generated random vectors to produce an orthonormal matrix. A matrix A is called an orthonormal matrix if it is orthogonal and each column/row vector has a unit norm, equivalently $AA_t = I$, where A_t is the transpose of A and I is the identity matrix of the same size as A.

iii) Transform the original template feature x to a secure domain using matrix product: $y=Ax$.

An efficient method of generating orthonormal matrices [45] exploits the fact that small size orthonormal matrices can be generated without a need for the Gram-Schmidt procedure, which is ill-conditioned for high dimensional spaces. Let x be the feature vector of size n, A be an $n \times n$

orthonormal random matrix, b a random vector of size n, and P a permutation matrix of size n. Then the transformation

$$y=P(Ax+ b) \qquad (1)$$

defines a distance preserving mapping of the space of n-dimensional vector space R_n that enhances privacy while preserving the intra-class variation (i.e., while maintaining the same level of recognition accuracy) [45].

4.1.2 Feature Transformation using Secret-Based Shuffling

Another example of a privacy-aware feature transformation is secret-based shuffling to create revocable versions of iris templates [46]. A shuffling key of size *k* generated from a secret (e.g. password, PIN, or a random key) is used to shuffle an iris code that is divided into *k* blocks. As illustrated in Figure 4, if a bit in the key is 1, the corresponding iris code block is moved to the beginning; otherwise it is moved to the end.

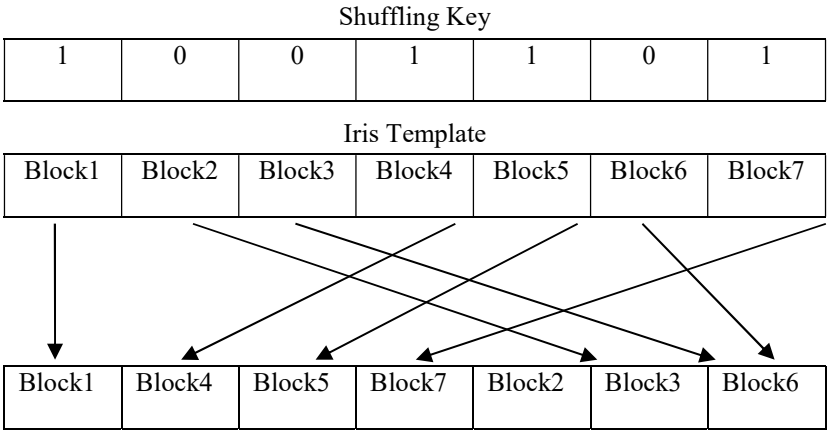

Figure 4: Simple Secret-based shuffling for iris codes [46]

4.1.3 User-Based Feature Transformations for Privacy-Aware Authentication

User-Based Feature Transformations (UBFTs) are typically multi-factor biometric recognition schemes that rely on applying user-based transformation keys on biometric features. These multi-factor biometric authentication schemes have been proposed to enhance privacy and/or accuracy of biometric systems. Figure 5 illustrates the general operations of a multi-factor UBFT approach during enrolment and authentication stages. Typically, UBFTs employ transformation keys generated from passwords/PINs or the keys are retrieved from a token. If a user is subscribed to x different systems, there will be x different cancellable versions of their biometric template by changing the user- and/or system-based secret. Arguably, this privacy-preserving approach improves authentication anonymity and makes it infeasible to track users across different systems or databases.

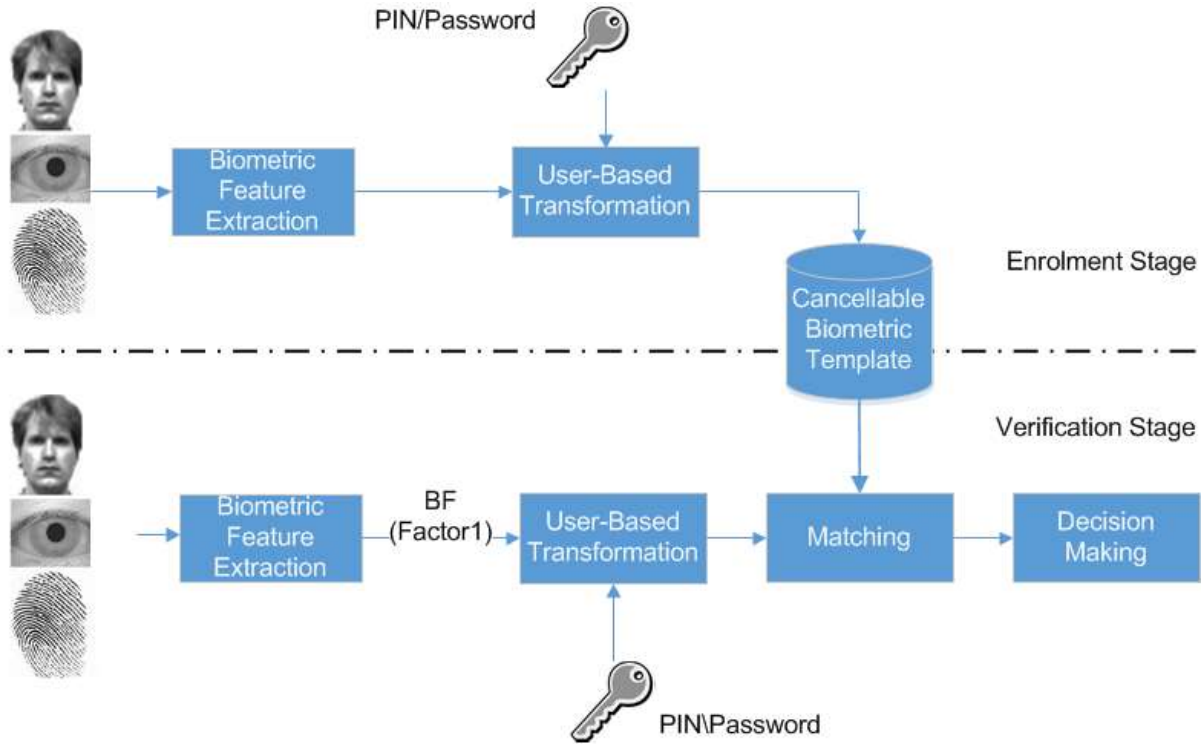

Figure 5: General operations of a Multi-factor biometric authentication system based on UBFTs approach during enrolment and authentication stages

4.1.4 Parameterized Feature Transformations for Privacy-Aware Identification

Clearly the above UBFTs cannot be applied in a biometric identification mode where the system, for example, is supposed to identify individuals on the watch list without expecting them to declare their identity or presenting any additional information. Therefore, the transformation key in this scenario should be solely a system-based transformation. Figure 6 shows how a parameterized feature transformation can be used in privacy-preserving identification mode. It can be argued that such transformations can provide a good level of anonymity if the transformation is selected sensibly.

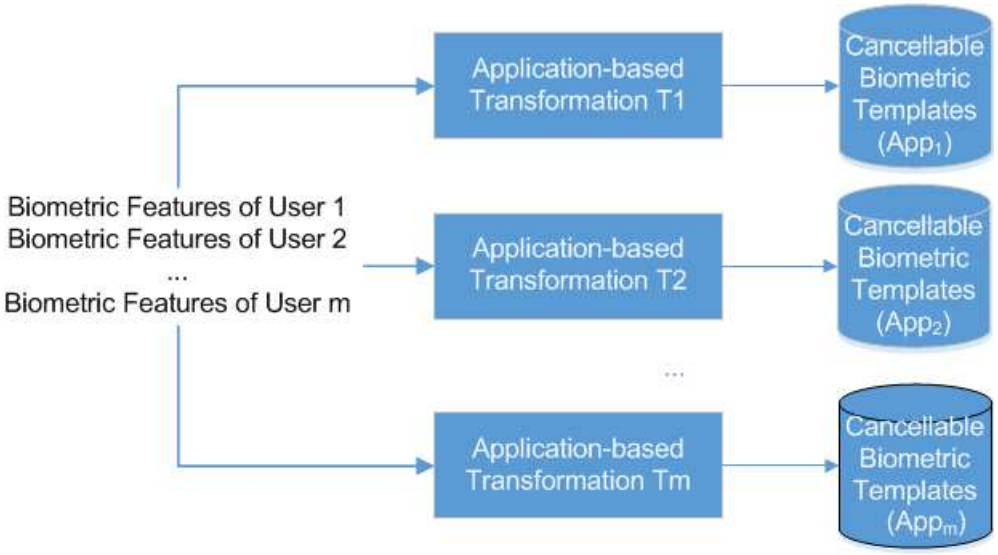

Figure 6. Parameterized feature transformations for privacy-aware identification

4.2 Private Biometric Cryptosystems

Private Biometric cryptosystems have been developed to provide stronger security mechanisms and to create revocable representations of individuals by combining biometrics with cryptography. Biometric cryptosystems, also known as private biometrics or biometric encryption, use **Privacy by Design** to directly address the privacy and security concerns associated with biometric systems. Typical biometric cryptosystems employ additional authentication factor(s) such as a password, PIN or token to improve the privacy of a standalone biometric system by generating revocable biometric keys that are not permanently linked with the user's identity. In general, there are three approaches to implement biometrics cryptosystems: (i) key release (ii) key generation and (iii) key binding.

In **key release schemes**, both the cryptographic key and the biometric data are stored as two separate entities and the key is released only when the user is biometrically authenticated. This method is straightforward and easy to implement, but has two major drawbacks [47]:

i) Biometric templates are not secure;
ii) The biometric matcher can be overridden.

In **key generation schemes**, a cryptographic key is directly derived from the biometric data without storing it anywhere. Such methods suffer from unacceptably high FRR [11].

In **key binding schemes**, the biometric template and the key are coupled to form a *biometric lock* [48] in a way that makes it computationally infeasible to retrieve the key without previous knowledge of the user's biometric data. While biometric data are fuzzy due to intra-class variations, cryptographic keys have to be repeatable every time. To bridge this gap, key binding schemes typically rely on error correction techniques such as Error Correcting Codes (ECC). The ECC algorithm is typically selected after analyzing error patterns of inter-class and intra-class variations of biometric samples. In other words, the selected ECC should tolerate (correct) up to a fixed number of bits (the so called threshold of the system). In key binding schemes, a cryptographic key is randomly generated during the enrolment stage but independent of the biometric template(s) and can be changed whenever needed. The Fuzzy Commitment scheme [48] is one of the earliest methods of binding biometrics and user keys. To commit (bind) a binary key K, a codeword C is generated based on K using a predefined error correcting code. The ultimate commitment will be $(h(K), BL)$, where $BL = B \oplus C$ is the biometric lock, B is a binary biometric template and h is a cryptographic hash function. To remove a commitment, an individual has to provide a fresh biometric sample B' to be XORed with BL, which results in a codeword C'. If B' is close enough to B, decoding C' should yield the same key K where $h(K)$ can be used to verify that the right key is released.

Figure 7 depicts a generalized version of such a system [11]. At the enrolment stage, biometric samples are captured and input to a feature extraction procedure that outputs biometric template(s). Thereafter, a user-based transformation (e.g., personalized and private random orthonormal projection) is applied to transform the extracted biometric template into a private domain. Finally, a binary representation of the biometric sample is produced to be bound to the cryptographic key. To allow for the intra-class variations, error correcting techniques should be used whereby intra-class variations between biometrics samples at the enrolment and key retrieval stages can be considered as noise. The adopted error correction techniques should be capable of correcting up to a specific number of bits which depends on the intended key size, biometric template size, and the amount of tolerated distortion in the biometric data to accommodate adequate variation in user samples.

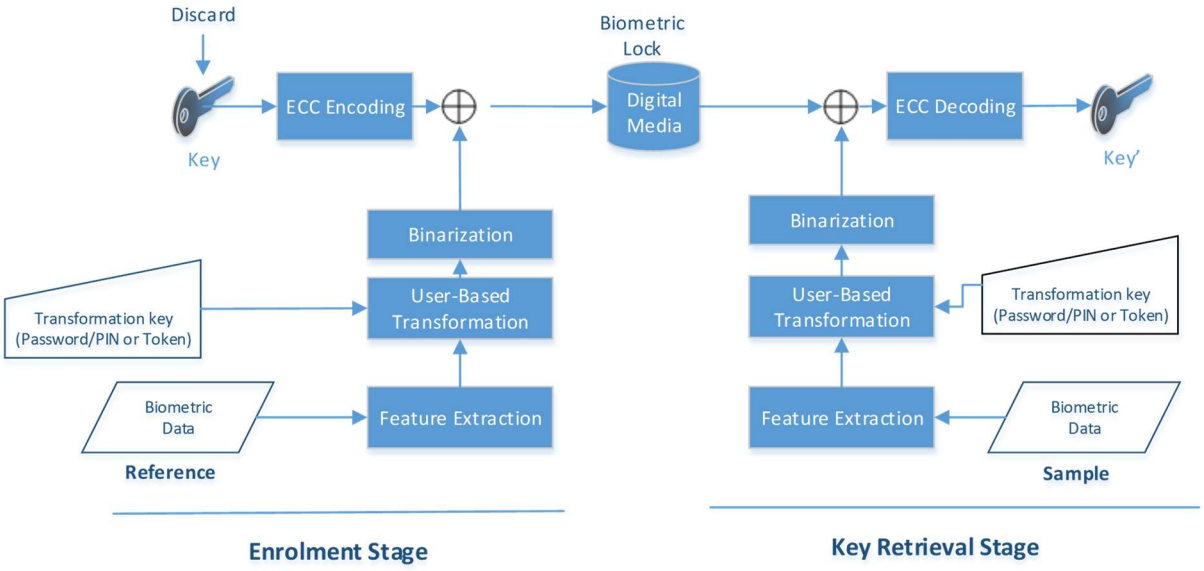

Figure 7. General private biometric cryptosystem (key binding scheme)

The encoded cryptographic key is XORed with the binary representation of biometric data to yield the biometric lock or helper data. The key is then discarded and the biometric lock and the hash of the key are stored. At the authentication stage (key retrieval stage), the binary representation is calculated using a fresh biometric sample in the same way as described above and then XORed with the biometric lock. Next, the adopted error correcting technique in the decoding mode is used. The correction succeeds and the original cryptographic key is reproduced if the difference between the reference biometric sample(s) and the fresh biometric sample is within the predefined threshold (i.e., the fresh biometric sample belongs to the same individual). The predefined threshold is determined in the same way as before when defining a biometric authentication threshold through a training protocol that is application dependent, where appropriate tolerance of error rates is chosen in terms of FAR and FRR.

Private biometric cryptosystems can theoretically be extended to function under the identification mode in the same way illustrated in Figure 6. However, incorporating error correcting techniques makes any identification process very slow. To improve the efficiency, a hybrid privacy-aware watch-list face recognition system [49] can be used, which was successfully deployed for Ontario Lottery and Gaming Corporation Self-Exclusion Program. The system is hybrid in nature because it combines a commercial face recognition module with a private biometric cryptosystem component. To improve the privacy, the system uses two databases; one contains biometric templates of the commercial face recognition along with biometric locks, while the other contains personal and private information about individuals. A biometric cryptosystem is used to conceal the relationship between a self-excluded person's face template and his/her other personal information. The commercial face recognition is used first to check whether a freshly captured biometric sample matches any biometric template on the watch-list. If it does, the biometric cryptosystem uses the corresponding biometric lock to release a key that will identify the record of personal information in the second database. The templates and biometric lock use different biometric feature vectors to prevent interoperability between the two modules.

5. Challenges and Solutions – Current trends

Security measures and technologies involve the collection of information about various people including their biometric data. This raises serious questions as to whether, and to what extent, the privacy of the biometric data owner (i.e., the individual) has been breached. A moderate level of invasion into an individual's privacy is sometimes considered as an acceptable cost of enhanced personal safety and society security. However, the acceptable level of privacy invasion is not yet clearly defined in the trade-off between security and privacy. International efforts have been made to come up with a common understanding of the security-privacy trade-off at both state and citizen level to suggest best practices and guidelines to policymakers. For example, the SurPRISE (Surveillance, Privacy and Security) project [50] is a three year project (2012-2015) funded by the European Union (EU) under the Seventh Framework Programme (FP7) for Research and Technology Development. It aims to examine the trade-off between security and individual privacy and addresses questions such as: "Does more security justify less privacy?" and "What is the balance between these two?". It consults with citizens from several EU member and associated states on the question of the security-privacy trade-off as they evaluate different security technologies and measures.

The IRISS (Increasing Resilience in Surveillance Societies) project [51] (EU, FP7, 2012-2015) aims to investigate the development and deployment of surveillance technologies and their impact on citizens' privacy and democratic rights. Another example is the TURBINE (TrUsted Revocable Biometric IdeNtitiEs) project [52] (EU, FP7, 2007-2013), which investigates effective solutions on how to enable an individual to revoke an identity for a given application and create different "pseudo-identities" for different applications. The project suggested best practices for privacy preserving biometric data processing. Another example is the 3DFace project [53] (EU, FP6, 2006-2009), in which the objective was to develop a prototype of an automated border control biometric system incorporating privacy enhancing technology based on 2D and 3D face images.

Match-on-card technologies and other user-side matching devices are examples of solutions that have been proposed as effective privacy-preserving biometric solutions due to fact that storage and matching of biometric samples are all done under user's full control. However, more research needs to be carried out to come up with practical solutions on how to extend such technologies to be suitable for both identification and authentication modes. Other future research directions could investigate the feasibility of implementing privacy-preserving solutions at the hardware level. For example, is it possible to design a biometric sensor (e.g., camera, iris scanner, fingerprint scanner) to capture biometric data that serves the purpose of biometric recognition without revealing any extra bit of information to the outside?

5.1 Privacy-aware Remote Biometric Recognition for Cloud Services

The increasing trend of many business organizations, government agencies and customers to shift their services and data onto the cloud necessitates the need for secure and privacy-aware remote authentication schemes that are capable of preserving anonymity and are immune against fraud and identity theft at the same time [54]. However, the open nature of unattended remote authentication makes the privacy and security of biometric systems important issues. Hybrid challenge/response schemes that combine feature transformation and a private biometric cryptosystem can be used for example as a privacy-aware remote biometric authentication for cloud services [55]. Face modality was chosen for the implementation due to camera availability on almost all mobile devices and laptops. At the enrolment stage and to address some privacy concerns highlighted earlier, only a

cancellable version of the user's biometric features X_{AC} and a hash of a PIN used to generate ROP are stored in the cloud authenticator's database as illustrated in Figure 8.

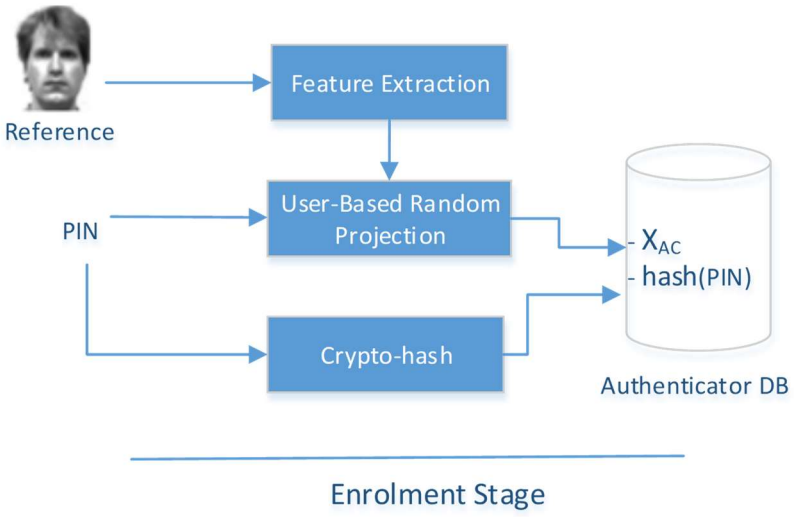

Figure 8. Enrolment stage of the privacy-aware authentication scheme for cloud service

As a case study, a user can use a Smartphone or tablet PC that has a camera to capture face images along with a 4-digit PIN to generate a user-based transformation key to be used for ROP. It is worth highlighting the fact that combining biometrics with the other authentication factors in this scheme enhances privacy while intra-class variations of biometric samples are preserved (i.e., it does not compromise accuracy) [55].

At the authentication stage and after extracting the biometric feature vector and applying ROP, the resulting cancellable feature vector X_C is combined with a one-time authenticator random challenge vector V by simple addition to produce a one-time privacy-aware cancellable feature vector X_O, which will be permutated based on a permutation key generated from the PIN as illustrated in Figure 9. As mentioned earlier, due to the differences between the user's captured biometric sample and the enrolled biometric sample(s) stored by the authenticator, ECCs can be used to eliminate the effect of this noise. In this case study, a Reed-Solomon (RS) ECC is chosen to correct up to 30% of the biometric feature vectors. This 30% threshold is determined in a similar manner to define biometric authentication thresholds (i.e., a training protocol is used to determine appropriate tolerance error rates in terms of FAR and FRR). At the cloud authenticator side, if the correction succeeds, the process generates a key K' that matches the key bound to the user. This can only happen if the difference between the reference biometric sample(s) and the fresh biometric sample is within the predefined threshold (i.e., the fresh biometric sample belongs to the same individual).

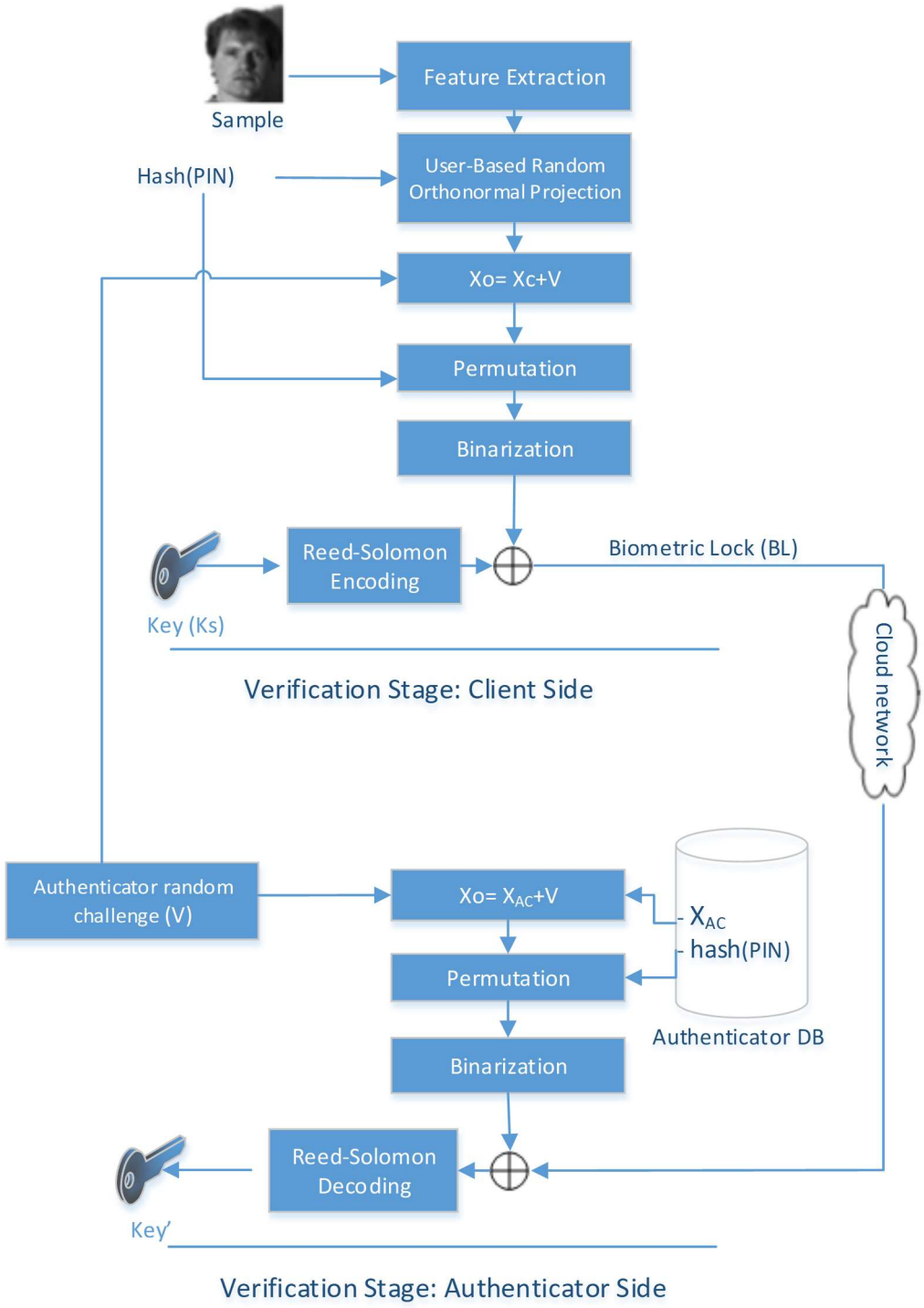

Figure 9. Authentication stage of the privacy-aware authentication scheme for cloud service

5.2 Conclusion

The fact that biometric systems by their very nature collect more information than just the individual's fingerprints, retinal patterns or other biometric data has precipitated an urgent need for new legislation to enforce privacy-preserving measures on biometric data collection, processing, and template storage. At a basic level, most biometric systems will record when and where a person is at the time of a scan, not to mention all the additional privacy concerns we have discussed earlier. Although data

privacy and data protection acts exist in almost all countries, those related to biometric privacy and security are not mature enough yet, as they are still at very early stages.

The problem of privacy of biometric systems cannot be attributed solely to technology. No matter how secure the technology is, biometric systems insiders, and secondary users as well as third parties such as insurance companies, employers, and financial organizations can become a source of attack or privacy concern. In other words, the problem is the combination of people and technology. Hence, technological solutions need to be complemented by a legal framework while educational- and ethical-based tools are required to improve privacy for all of us.

Bibliography

[1] The Unique Identification Authority of India, http://uidai.gov.in/ (Accessed 08 Sep 2014).

[2] Ross, A., Nandakumar, K., Jain, A., *Introduction to biometrics*. Springer, 2011.

[3] Georghiades, AS., P. N. Belhumeur, and D. J. Kriegman, "From Few to Many: Generative Models for Recognition under Variable Pose and Illumination," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 6, pp. 643–660, 2001.

[4] Li, SZ., Jain, AK., *Encyclopedia of Biometrics*. Springer, 2009.

[5] Nandakumar, K., "Multibiometric Systems: Fusion Strategies and Template Security", 2008.

[6] NIST_Report, "NIST Report to the United States Congress. Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability," Nov 2002.

[7] Bhanu, B., and Tan, X., "Fingerprint Indexing Based on Novel Features of Minutiae Triplets," vol. 25, no. 5, pp. 616–622, 2003.

[8] Jain, AK. , Nandakumar, K. and Nagar A., "Biometric Template Security," in *EURASIP Journal on Advances in Signal Processing*, pp. 1-17, 2008.

[9] Adler, A., "Vulnerabilities in biometric encryption systems," in *Proc. of the 5th Int Conference on Audio and Video-Based Biometric Person Authentication*, vol. 3546, pp. 1611-3349, 2005.

[10] Cappelli, R. , Lumini, A., Maio, D., and Maltoni, D., "Fingerprint Image Reconstruction from Standard Templates," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29(7), pp. 1489-1503, 2007.

[11] Hao, F., Anderson, R., Daugman, J., "Combining cryptography with biometrics effectively," *IEEE Transactions on Computers*, pp. 1081--1088, 2006.

[12] The Secure Phone Project, http://www.secure-phone.info/ (Accessed 08 Sep 2014).

[13] Philips Electronics Nederland B.V. (2013, July) Vital Signs Camera - Philips on the App Store on iTunes, https://itunes.apple.com/gb/app/vital-signs-camera-philips/id474433446?mt=8,

Accessed 08 Sep 2014

[14] Hoeksma, J. (2009, Oct) E-Health Insider: Private medical records offered for sale, http://www.ehi.co.uk/news/ehi/5311 (Accessed 08 Sep 2014).

[15] Hasson, P. "The Five Country Conference: Joint Enrollment and FCC Information Sharing Project," US Department of Homeland Security , 2009.

[16] VÉDRINE, H. "COUNCIL REGULATION (EC) No 2725/2000," *Official Journal of the European Communities*, Dec 2000.

[17] European Data Protection Supervisor (EDPS) Peter Hustinx, EURODAC: erosion of fundamental rights creeps along, Sep 2012.

[18] Woodward, J.D., "The Law and the Use of Biometrics," in *Handbook of Biometrics*, Anil K. Jain, Patrick Flynn, and Arun A. Ross, Eds.: Springer, ch. 18, pp. 357-380, 2008.

[19] Amoore, L., "Biometric borders: governing mobilities in the war on terror," *Political geography*, vol. 25, no. 3, pp. 336-351, 2006.

[20] Bennett, C.J., "In defense of privacy: the concept and the regime," *Surveillance \& Society*, vol. 8, no. 4, pp. 485-496, 2011.

[21] Nanavati, R., "Biometric Data Safeguarding Technologies Analysis and Best Practices," Defence R&D Canada – Centre for Security Science, Tech. rep. Dec 2011.

[22] Hal, J., Kimura, D., "Dermatoglyphic asymmetry and sexual orientation in men," *Behavioral neuroscience*, vol. 108, no. 6, p. 1203, 1994.

[23] J. Woodward, "Biometrics: Identifying Law and Policy Concerns," in *Biometrics: personal identification in networked society*, Anil K Jain, Ruud Bolle, and Sharath Pankanti, Eds.: Springer, 1999, ch. 19, pp. 385-406.

[24] LeVay, S., *Queer science: The use and abuse of research into homosexuality.*: The MIT Press, 1996.

[25] Forbes, K.E., Shanks, M.F., Venneri, A., "The evolution of dysgraphia in Alzheimer's disease," *Brain research bulletin*, vol. 63, no. 1, pp. 19-24, 2004.

[26] Rosenblum, S., Samuel, M., Zlotnik, S., Erikh, I., Schlesinger, i., "Handwriting as an objective tool for Parkinson's disease diagnosis," *Journal of neurology*, vol. 260, no. 9, pp. 2357-2361, 2013.

[27] Tsanas, A., Little, M.A., McSharry, P. , Spielman, J., Ramig, L., "Novel speech signal processing algorithms for high-accuracy classification of Parkinson's disease," *Biomedical Engineering, IEEE Transactions on*, vol. 59, no. 5, pp. 1264-1271, 2012.

[28] Darell, R.: Siri Update: How, When & What We Use Her For. In: Bit Rebels. (Accessed 08 Sep 2014)

[29] Faundez-Zanuy M., "Biometric applications related to human beings: There is life beyond security," *Cognitive Computation*, vol. 5, no. 1, pp. 136-151, 2013.

[30] Shin, J., Okuyama, T., "Detection of alcohol intoxication via online handwritten signature verification," *Pattern Recognition Letters*, vol. 35, pp. 101-104, 2014.

[31] Foley, R.G., Miller, A.L., "The effects of marijuana and alcohol usage on handwriting," *Forensic science international*, vol. 14, no. 3, pp. 159-164, 1979.

[32] Moody, J., "Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use.," *Issues in Informing Science \& Information Technology*, vol. 1, 2004.

[33] Farzin, H., Abrishami-Moghaddam, H., Moin M.S., "A novel retinal identification system," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, no. 280635, pp. 1-10, 2008.

[34] Patton, N., "Retinal image analysis: concepts, applications and potential," *Progress in retinal and eye research*, vol. 25, no. 1, pp. 99-127, 2006.

[35] Berson, E.L, "Retinal degenerations: planning for the future," in *Recent Advances in Retinal Degeneration*.: Springer, 2008, pp. 21-35.

[36] Hartung, D., Busch, C., "Why vein recognition needs privacy protection," in *Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on*, *Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on*, 2009, pp. 1090-1095.

[37] Ratha, N.K. , Connell, J. H. and Bolle RM., "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40(1), pp. 614–634, 2004.

[38] Goal, N., Bebis, G., and Nefian, A., "Face recognition experiments with random projection," , *Proc. SPIE*, vol. 5779, , 2005, pp. 426–437.

[39] Teoh, A.B.J., Ngo, D.C.L, Goh, A., "BioHashing: two factor authentication featuring fingerprint data and tokenised random number," , *Pattern Recognition*, vol. 37(11), 2004, pp. 2245-2255.

[40] Feng, YC., Yuen, PC. and ,Jain AK., "A Hybrid Approach for Face Template Protection," vol. 6944, p. 694408, 2008.

[41] Yongjin, W., and Plataniotis, KN., "Face Based Biometric Authentication with Changeable and Privacy Preservable Templates," pp. 1-6, 2007.

[42] Al-Assam, H., Jassim, S.A., "Security evaluation of biometric keys," *Journal of Computers & Security*, vol. 31, no. 2, pp. 151-163, 2012.

[43] Andrew, B., Teoha, D, Ngoa, CL., and Alwyn G., "Personalised cryptographic key generation based on FaceHashing," *Computers & Security*, vol. 23, no. 7, pp. 606-614, 2004.

[44] Goh, A., and Ngo DC., "Computation of Cryptographic Keys from Face Biometrics," pp. 1-13, 2003.

[45] Al-Assam, H., Sellahewa, H., and Jassim, S.A., "lightweight approach for biometric template protection," *Proceedings of SPIE*, 2009.

[46] Kanade, S., Camara, D., and Dorizzi, B., "Three factor scheme for biometric-based cryptographic key regeneration using iris," *Biometrics Symposium*, pp. 59-64, 2008.

[47] Nandakumar, K. Jain, A.K. Pankanti, S, "Fingerprint-Based Fuzzy Vault: Implementation and Performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744-757, 2007.

[48] Juels, A., and Wattenberg, M., "A fuzzy commitment scheme," , *in Proceedings of ACM Conference on Computer and Communications Security (CCS)*, Singapore, 1999, pp. 28–36.

[49] Marinelli, T., Stoianov, A., Martin, K., Plataniotis, K.N., Chibba, M., DeSouza, L., Cavoukian, S.A., "Biometric Encryption: Creating a Privacy-Preserving Watch-List Facial Recognition System," *Security and Privacy in Biometrics*, pp. 215-238, 2013.

[50] Surveillance, Privacy and Security (SurPRISE), http://www.surprise-project.eu/ (Accessed 08 Sep 2014)

[51] Increasing Resilience in Surveillance Societies (IRISS) project, http://www.irissproject.eu/ (Accessed 08 Sep 2014)

[52] Turbine project, http://www.turbine-project.eu/ (Accessed 08 Sep 2014)

[53] 3Dface Project, http://www.3dface.org/ (Accessed 08 Sep 2014)

[54] Kuseler, T., Al-Assam, H., Jassim, S.A. and Lami, I.A., "Privacy preserving, real-time and location secured biometrics for mCommerce authentication," in *Mobile Multimedia/Image Processing, Security, and Applications 2011*, *Mobile Multimedia/Image Processing, Security, and Applications 2011*, vol. 8063, SPIE, Bellingham, WA, Apr 2011.

[55] Al-Assam, H., Jassim, S.A. "Robust Biometric Based Key Agreement and Remote Mutual Authentication," , *The 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Liverpool, UK, 2012, pp. 59-65.