Integrating biometric authentication into multiple applications

By

Morné Breedt

23376873

Submitted in fulfilment of the requirements for the degree

Magister Scientiae in Computer Science

in the

Faculty of Engineering, Built Environment and Information Technology,

University of Pretoria

October 2005

Abstract

Integrating biometric authentication into multiple applications

Candidate: Morné Breedt
Study Leader: Prof MS Olivier
Department: Computer Science
Degree: MSc (Computer Science)

The Internet has grown from its modest academic beginnings into an important, global communication medium. It has become a significant, intrinsic part of our lives, how we distribute information and how we transact. It is used for a variety of purposes, including: banking; home shopping; commercial trade — using EDI (Electronic Data Interchange); and to gather information for market research and other activities.

Owing to its academic origins, the early developers of the Internet did not focus on security. However, now that it has rapidly evolved into an extensively used, global commercial transaction and distribution channel, security has become a big concern. Fortunately, the field of information security has started to evolve in response and is fast becoming an important discipline with a sound theoretical basis.

The discipline views the twin processes of identification and authentication as crucial aspects of information security. An individual access attempt must be identifiable prior to access being authorised otherwise system confidentiality cannot be enforced nor integrity safeguarded. Similarly, non-denial becomes impossible to instigate since the system is unable to log an identity against specific transactions. Consequently, identification and authentication should always be viewed as the first step to successfully enforcing information security.

The process of identification and authorisation is, in essence, the ability to prove or verify an identity. This is usually accomplished using either one or a combination of the following three traditional identification techniques: something you possess; something you know; or something you are. A critical consideration when designing an application is which identification method, or combination of methods, from the three described above to use. Each method offers its own pros and cons and there are many ways to compare and contrast them.

The comparison made in this study identifies biometrics as the best solution in a distributed application environment. There are, however, two over-arching hindrances to its widespread adoption. The first is the environment's complexity — with multiple applications being accessed by both the public and the private sectors — and the second is that not all biometrics are popular and no single method has universe appeal.

The more significant hindrance of the two is the latter, that of acceptance and trust, because it matters little how good or efficient a system is if nobody is willing to use it. This observation suggests that the identification system needs to be made as flexible as possible. In a democratic society, it could be argued that the best way of ensuring the successful adoption of a biometric system would be to allow maximum freedom of choice and let users decide which biometric method they would like to use. Although this approach is likely to go a long way towards solving the acceptance issue, it increases the complexity of the environment significantly.

This study attempts to solve this problem by reducing the environment's complexity while simultaneously ensuring the user retains maximum biometric freedom of choice. This can be achieved by creating a number of central biometric repositories. Each repository would be responsible for maintaining a biometric template data store for a type of biometric. These repositories or "Biometric Authorities" would act as authentication facilitators for a wide variety of applications and free them from that responsibility.

Keywords

Security, Biometric, Authentication, Biometric Authority, Iris recognition, hand recognition, fingerprint, privacy, passport, visa, BIOAPI

Contents

List of Figures

List of Tables

List of Code Fragments

Chapter 1 Introduction

Introduction

The Internet was born in America in the 1960s. Initially, it was used as an academic and research tool for government, educational and non-profit organisations [62]. Keen to ensure it remained so, the National Science Foundation implemented a restriction policy during this early period to keep it out of reach of the business community [62]. However, as telecommunication networks grew, the National Science Foundation decided to alter its usage policy and allow companies to take advantage of this new medium. The relaxation allowed commercial enterprises to:

1. Conduct transactions over public networks for home shopping and banking purposes [62];
2. Use EDI (Electronic Data Interchange) to facilitate transactions between trading partners [62, 69, 70];
3. Gather information for market research and other activities [62, 68];
4. Perform information distribution transactions [62].

The academic birth of the Internet is significant because it was not an environment that prompted its early developers to focus on security [59]. Its rapid growth since then into an extensively used, global commercial transaction and distribution channel [refer to 62 for more information] has naturally brought security concerns to the fore [67]. Fortunately, the field of information security has started to evolve in response to this rapid growth and is fast becoming an important discipline with a sound theoretical basis [58]. The discipline is divided into five supporting pillars [58]:

- Identification and authentication –identifying yourself and proving your authenticity;
- Authorisation – authorising access to resources;
- Confidentiality – ensuring only authorised individuals can view the content of data or software;
- Integrity – ensuring that only authorised individuals can change the content of data or software;
- Non-denial - ensuring an individual cannot deny the authorisation of a transaction, like changing the content of data.

The identification and authentication pillar is listed first because it is crucial to the entire process and facilitates the other four pillars. If an individual's identity is unknown access cannot be authorised since system confidentiality cannot be enforced nor integrity safeguarded. Similarly, non-denial is impossible to instigate since the system is unable to log an identity against specific transactions. Consequently, identification and authentication should always be viewed as the first step to successfully enforcing information security [58].

Identification and the mechanisms

The process of identification and authorisation is, in essence, the ability to prove or verify an identity. This is usually accomplished using either one or a combination of the following three traditional identification techniques: something you possess; something you know; and something you are [58].

Something you possess

A possession is often referred to as a "token" and can be created from a multitude of different physical objects. One of the earliest examples of the use of a token is the amulets used by Bronze Age priests to signify their office.

There are two basic types of tokens in use today: manual and automated. If a token is described as manual it means that the identification process requires some form of human intervention. In other words, that a person will make the final decision of whether an identity is correct or not. Paper ID documents and passports are good examples of manual tokens.

Automated tokens, conversely, do not require human intervention during the identification process. In other words, the identity is verified by a system/computer. Examples of automated tokens or "machine-readable" tokens include: magnetic-stripe cards; memory cards; hand-held password generators; smart cards [58]; optical stripe cards (an optical stripe is a device much like a compact disk and can hold up to 4 megabytes of data) [54], and printed barcodes [54]. It is worth noting that most of the tokens mentioned above are in widespread use today granting access to physical assets (for example, doors into buildings) and logical assets (for example corporate networks or bank accounts).

Something you know

In this instance, the knowledge referred to should not be commonly held, but secret. Passwords, pass-phrases, and personal identification numbers (PINs) [58] are all examples of commonly used secrets. Typical, secret-driven applications include: computer and building access (using a number pad) and withdrawing cash from an ATM machine (in conjunction with a magnetic-stripe card).

Something you are

Identifying an individual through what "they are" requires measuring one or more of their biological features. Biological features can be either physiological characteristics like fingerprints or behavioural traits like an individual's signature [1]. The process of extracting and measuring these features is known as biometric authentication and covered in more detail in Chapter 2.

Identification mechanisms in a distributed world

Passwords vs. Tokens vs. Biometrics

A critical consideration when designing an application is which identification method, or combination of methods, from the three described above to use. Each method offers its own pros and cons and there are many ways to compare and contrast them. For the purposes of this introductory discussion, however, the comparison has been focussed on the two main ways an identification system can "fail": if an unauthorised person is granted access or a legitimate, authorised user is rejected.

Tokens

1. Can be forged and used without the knowledge of the original bearer. For example, a forger can "steal an identity" and create a fake ID document using another person's information. Armed with the forgery, fraudulent transactions can be authorised without the original bearer's knowledge.
2. Can be lost, stolen or given to someone else. In any of these instances, an illegitimate person will be able to fraudulently transact with the system by impersonating the original bearer.

Passwords

1. Can be obtained or "cracked" using a variety of techniques, including:
    a. Common password usage – a lot of people use common passwords like "guest", "password", "pword", "help", "coffee", "coke", "aaa" etc [53]. Similarly, people often create passwords from pertinent information about themselves, like the name of a child or pet, which might be easily obtained [53];
    b. Exhaustive or "brute force" attack [53] – this is an attack where all possible passwords are used;
    c. Dictionary attack – a variant of the brute force attack that uses words from a specific list (for example, the English dictionary) [59];
    d. Using programs/tools to crack the password – a lot of programs and tools are available to crack passwords (refer to [59] for some details on Windows NT password cracking and the tools available).
2. Can be disclosed. If the password is disclosed to an individual they will be able to gain access to areas, information etc. that they are not authorised for.
3. Can be forgotten. Although this is not a security threat directly, it does place an additional burden upon an organisation's administration (if an individual has forgotten his/her password and needs to be issued with a new one).

Biometrics

1. Can be forged – for example, a forged signature could be accepted by a signature recognition system if performed skilfully enough [3].
2. Can be destroyed – a biometric characteristic's ability to be read by a system can be reduced. An individual's fingerprints, for example, can be affected by cuts and bruises [14] and can even be destroyed by excessive rubbing on an abrasive surface or through exposure to certain chemicals like acids etc.

Analysis of the reasons cited above suggests there are three main ways an identification system can be compromised: through forgery (unauthorised copying); through transportability (moving the identification method or device between individuals – the disclosing of a password, for example), and through loss or damage. These have been summarised and contrasted in Table 1-1 below:

	Something you have	**Something you know**	**Something you are**
Forgery	Yes	Yes	Yes
Transportability	Yes	Yes	No
Lost/damage	Yes	Yes	Yes

Table 1-1 Comparison of identification techniques

When deciding which identification method to use in a particular application, the application's environment is a key consideration and, if this basic comparison is applied to a remote, distributed environment like the Internet, the fact that it is impossible to transport an individual's biometric characteristics emerges as critical. Transportability and forgery are major concerns in an environment where the user can be located anywhere and enjoys anonymity. In such circumstances, presenting fraudulent passwords or tokens is both easy to do and hard to detect.

Some biometrics can be forged, but the fact that a measurement must be made to authorise a transaction ensures the individual must also be present (to be measured) and offers a superior level of security, in itself, to tokens or passwords.

For this reason, and the relative complexity required to forge most biometrics, solutions based on biometric identification methods appear to offer the best security when transacting in remote, dispersed environments like the World Wide Web.

Why this study?

Although biometric identification systems appear to be the best solution for distributed application environments, there are two over-arching hindrances to their widespread adoption. The first is the environment's complexity — with multiple applications being accessed by both the public and the private sectors — and the second is that not all biometrics are popular (due to privacy issues and other sociological factors, see chapter 5) and no one method has universe appeal (certain individuals prefer fingerprint and others iris recognition).

Perhaps the more significant hindrance is that of acceptance and trust because it matters little how good or efficient a system is if nobody is willing to use it. This observation suggests the identification system needs to be made as flexible as possible. It could be argued that the best way of ensuring its successful adoption would be to allow maximum freedom of choice and let users decide which biometric method they would like to use. Although this approach is likely to go a long way towards solving the acceptance issue, it increases the complexity of the environment significantly. The system must now be capable of both integrating a single biometric identification method into a wide variety of applications and a wide variety of biometric identification methods into a single application.

This study attempts to solve this problem by reducing the environment's complexity while ensuring the user retains maximum biometric freedom of choice. This can be achieved by creating a number of central[1] biometric repositories. Each repository responsible for maintaining a biometric template data store for a type of biometric (each type can have a number of different sub-types to allow for different manufacturers and equipment). These repositories or "Biometric Authorities" would act as authentication facilitators for a wide variety of applications and free them from that responsibility.

Problem statement

"***How should we implement a biometric solution to allow a user to select their biometric of choice and use this biometric to facilitate authentication across a multitude of applications?***"

To place this question within context, this study begins with an overview of the field of biometrics and the different types of biometrics in use today. The investigation of possible solutions to the problem follows and starts with an examination of how an appropriate biometric for an application can be determined.

Once how to determine an appropriate biometric solution has been established, a possible model for implementing a biometric authority will be discussed. This will include supporting factors including a trust relationship model similar to that of certificate authorities (CA) and a biometric rating mechanism to ensure that the biometric being used is appropriate for the application.

This study will conclude with an assessment of possible usages of a biometric authority in both an "electronic" or digital world setting (for example, the Internet) and a "non-electronic" world setting (for example, passports).

[1] The word central is used since this will be the central point where all biometric templates will be stored.

Organisation and outline

This document has been divided into three main sections: theoretical background (chapters 2 - 5); discussion of the model (chapters 6 and 7), and finally the possible implementations (chapter 8) and conclusion.

Background

Chapter 2 introduces the field of biometrics. This chapter will also introduce the generic model underlying most biometric systems and outline various accepted ways of measuring the performance of a biometric system.

Chapter 3 will focus on physiological biometrics including:

- Fingerprint;
- Hand Geometry;
- Iris recognition;
- Facial Recognition.

Chapter 4 will focus on the following behavioural biometrics:

- Signature recognition;
- Keystroke dynamics;
- Speaker recognition.

Chapter 5 discusses the issues that require consideration when selecting a biometric for a specific application.

Model

Chapter 6 provides an overview of a possible model which could be used to facilitate both the use of a biometric across multiple applications and the use of multiple biometrics across an application.

Chapter 7 examines the supporting infrastructure needed by the model. This will include a trust relationship model and a rating system for biometrics.

Applications

Chapter 8 will assess the viability of the model in the Internet world and how it could be used to help identify an individual for eCommerce purposes etc.

Chapter 9 will assess the viability of using such a model to biometrically-enable passports.

Conclusion

Chapter 10 concludes the study with a review of the development of both the field of biometrics and the Internet, and an assessment of their future roles within society.

Chapter 2 Introduction to Biometrics

Introduction

Biometric authentication is considered the automatic identification, or identity verification, of an individual using either a biological feature they possess (physiological characteristic like a fingerprint) or something they do (behaviour characteristic, like a signature) [1]. Consequently, there are a wide variety of biometric features that can be used to identify individuals. Table 2-1 (below) lists the main commercial systems currently available according to the type of biometric feature being measured.

Behavioural	**Physiological**
Signature	Fingerprinting
Voice/speech	Retina scanning
Keystroke dynamics	Iris
Gait (walking pattern)	Hand geometry
	Facial recognition
	Palm printing
	Facial thermographs
	Finger geometry

Table 2-1 Commercially available biometric systems grouped by type

As an introduction to the field of biometrics, this chapter will focus on the three initial considerations that need to be taken into account when assessing biometric systems:

1. Characteristics – a standard means of assessing the usability or usefulness of a given biometric trait as an authentication mechanism;
2. Commonality – the generic components common to every biometric system;
3. Effectiveness – ways of testing the performance of an individual biometric.

Chapters three and four discuss several of the behavioural and physiological biometrics mentioned above in greater detail.

Biometric characteristics

There are five main characteristics used to determine whether or not a physiological or behavioural biological trait can be used as a biometric authentication mechanism. These characteristics are:

1. **Robustness** – this characteristic measures the stability of the biometric trait in question. In other words, the ability of the biometric to stay constant or unchangeable over time [4, 66]. Robustness becomes important in situations where the biometric trait can be physically changed - be it intended or accidental. Fingerprints, for example, can get worn away or be damaged [4, 14] (see Figure 2-1 for examples of a normal and worn fingerprint.)

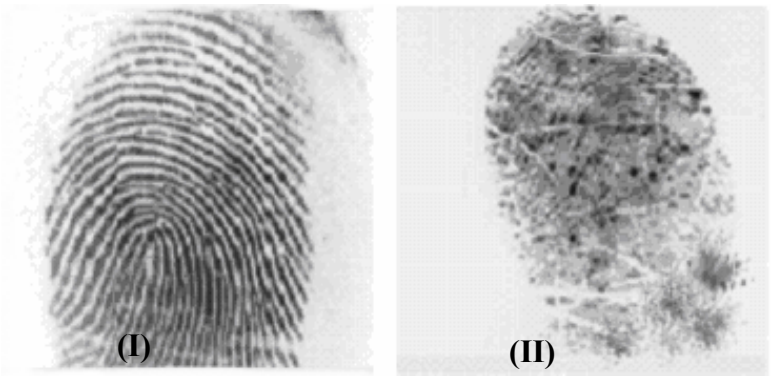

Figure 2-1 An example of (I) a normal fingerprint will be ideal for use in fingerprint recognition, and (II) a damage fingerprint as one can see most of the groves are missing and you do not really get any pattern except for the scar lines.

2. **Distinctiveness** – this characteristic measures the complexity or potential differences in a particular biometric trait's patterns and helps determine how large a population sample can be used [4, 66].
3. **Accessibility** – this quality measures how easy the particular biometric trait is to get to and measure [4]. Foot geometry, for example, would not be very accessible since individuals would have to remove their shoes first.
4. **Acceptability** – this characteristic questions how readily individuals will adopt a biometric system based on the trait in question [4]. For most people acceptance is linked to how intrusive they feel the system is. This feature is a critical factor in the embracing of biometric technologies and is discussed in more detail in later chapters.
5. **Availability** – this characteristic ascertains how many different, independent samples the system could potentially acquire from an individual [4]. For instance, studies have shown that a person is capable of supplying six nearly independent fingerprints [4]. In other words, out of a possible 10 fingers only 6 will, on average, produce unique samples.

Generic biometric system components

The three main components or elements of biometric authentication systems are: enrolment, templates and matching [66].

The enrolment phase is the period during which individuals introduce themselves to the system. The system captures the biometric sample presented by individual through an appropriate scanning device and then saves it in a format that can be used for future identification. In many respects, this process mimics the process of recognition used by human beings on first meeting when each memorises characteristics the other has, for example, the position of a mole, the sound of their voice or the colour of their eyes. Perhaps the biggest difference between them is the amount of information retrieved, the biometric system will usually gather a much larger and more detailed amount of information.

The biometric system then looks for unique patterns and information within the sample it has taken. In the case of a fingerprint, for example, the amount of circles, ridge flow, ridge frequency, location and position of singular points are all unique features (see Figure 2-2). For more information on fingerprints, refer to [8].

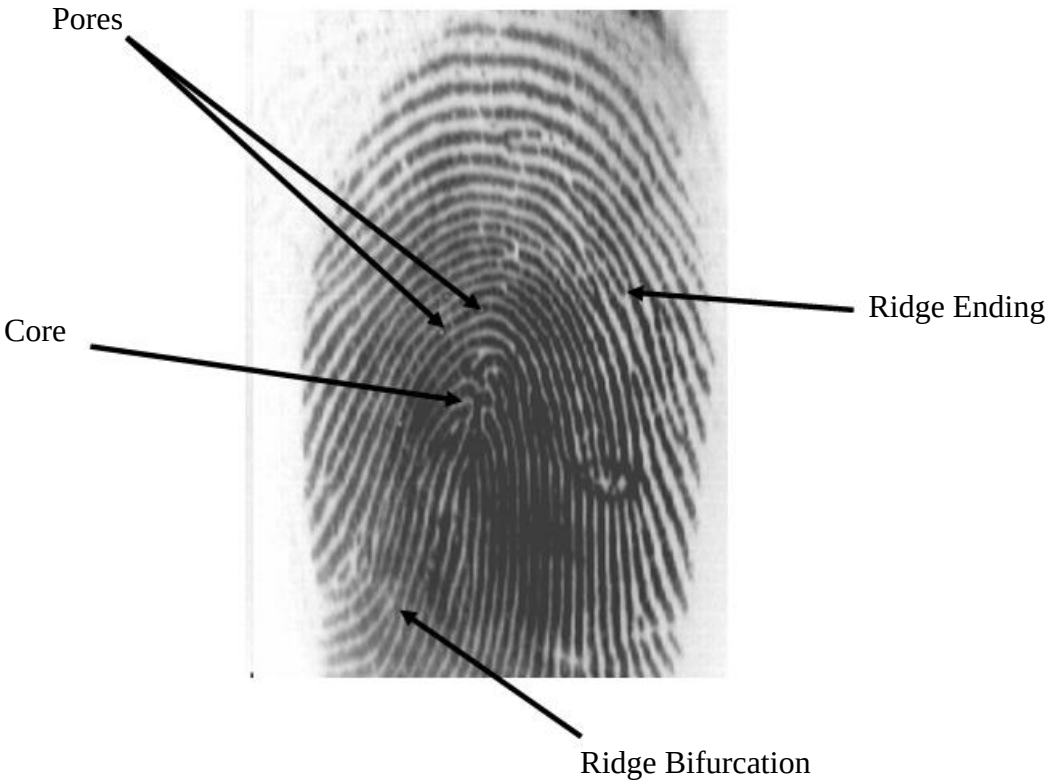

Figure 2-2 A fingerprint sample; the ridge structure, singular points and pores can be seen

The number of unique (statistically independent) features present in a particular biometric trait determines the overall uniqueness of the biometric and is recorded as a number of "degrees of freedom". Each biometric has a different number of degrees of freedom [60]. For example, iris recognition offers over 250 [11].

When the biometric system's sensor captures a sample (for example, a fingerprint) it can save the data as an image (i.e. jpeg, bitmap, tiff). This is referred to as the 'raw' biometric sample [5]. Once the biometric system has the raw biometric sample it can perform recognition by simply matching one raw sample to another.

A more elegant and effective way to perform a match is to encode the captured image into a binary representation through one of numerous different methods and making use of this encoding for matching [4, 5]. These binary encodings are known as biometric templates [4, 63, 66] if deliberately stored in order to perform subsequent matches (thus the enrolled binary representation) and a biometric sample [4, 63] if the binary representation will be used for matching against already stored templates (i.e. authentication). One of the objectives of this encoding process is to reduce the size of the template to the smallest binary array possible. For example, the iris code [49] produced during enrolment is 512 bytes [11].

Once the template has been generated, the next step during the enrolment cycle is to store the template for future recognitions. The medium used for storage depends upon the application's requirements or the preference of the developer. Common storage mediums include:

- Central databases
- Distributed databases

- Smartcards
- Magnetic cards

The remaining component, matching, is the process of comparing one biometric sample to another [66]. The matching element of biometric authentication has two main functions [4, 66]:

1. To prove your identity [4, 66]
2. To disprove your identity [4, 66]

The first function describes an attempt to positively link a presented sample to a previously enrolled template within the system. There are two ways this can be done [61]:

- A one-to-many search of the database
- A one-to-one search

A one-to-many search of the database compares one biometric sample to the many templates in the database. An individual presents his or her biometric sample without giving their identity, relying on the system to search many templates and try and find a match for the presented sample. This one-to-many search is better known as identification [63], recognition or one-to-many verification.

In a one-to-one search, an individual presents a 'live' biometric sample and a stored template to the system. The system will then compare the two in order to find a match. A one-to-one search is known as verification [63], authentication or one-to-one verification.

The second function of biometrics is to disprove a person's identity, also known as negative identification, and can be accomplished in the same way as positive identification (through either a one-to-one or one-to-many search). The main difference is that for negative identification the results need to be a non-match.

Generic Model

Although biometric systems differ from each other technically, all biometric systems follow the same generic model, described by Wayman [4, 61], (as seen in Figure 2-3) when attempting to positively or negatively identify or verify and individual. The model is divided into five sub-sections or stages: data collection; transmission; signal processing; storage, and decision-making [4, 61].

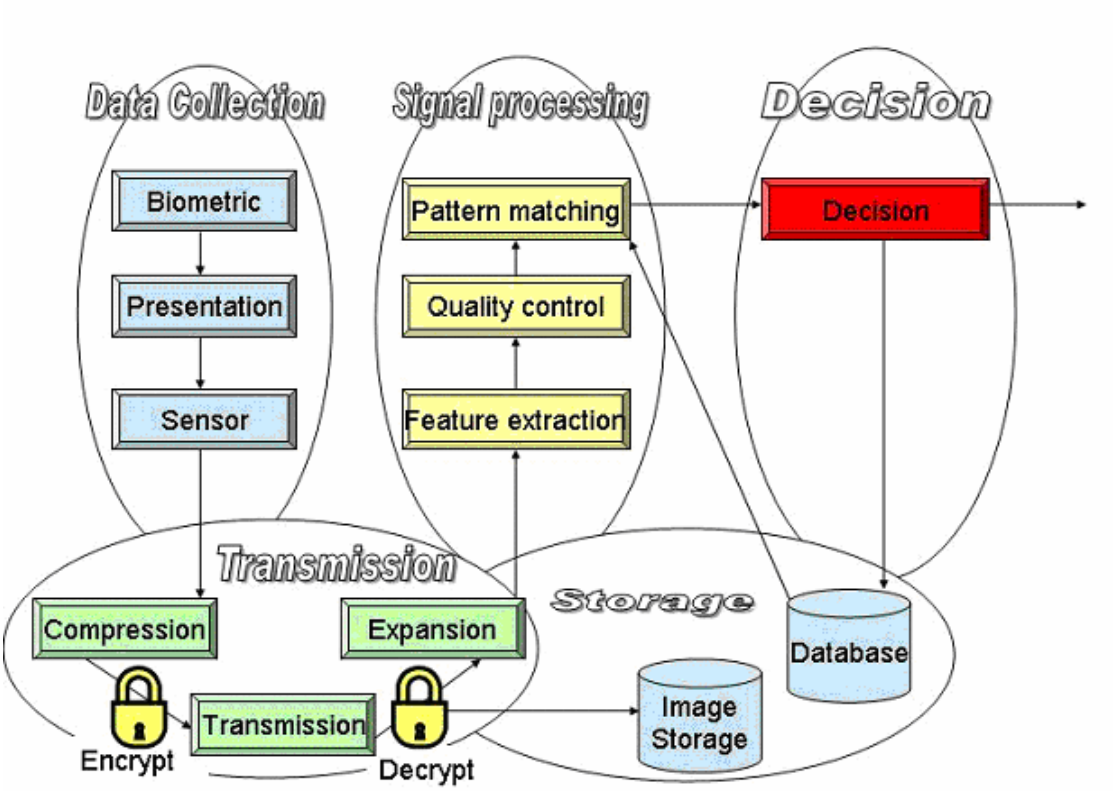

Figure 2-3 Generic model for biometric systems [Adapted from 10] (Refer to the Appendix 1 for a colour version of the figure)

Data Collection

All biometric systems, whether behavioural or physiological, start with the collection of a unique biometric sample (this occurs in the data collection sub-system). As illustrated in Figure 2-3 above, the biometric is presented to a sensor that gathers or captures the biometric data and converts it into an electric signal or "image". It is important to note that these "images" are rarely identical (even if a physiological trait) because the process of presenting the biometric for capturing introduces a behavioural component that is highly variable [4].

Biometric recognition will always be affected by human behaviour during the sample gathering stage (even if the system is only compensating for very small deviations). If a biometric is habitual, the amount of deviation will be small, but if it is not the developers of the system will have to develop extra checks to ensure the biometric is presented correctly. For example, when presenting an iris to a sensor it assumes that there will be a pupil (from which to construct concentric circles in order to transform the image to an template), but if the sensor is unable to find the pupil, the individual must be prompted to present his or her eye again.

Although it is human to vary one's actions (preventing the possibility of presenting identical samples), it is, however, unacceptable for the scanner to do so. The scanner must be stable and perform similarly each time it is used. If the sensor varies in its measurement it will increase the probability for false matches and false rejections and increase the chance of the biometric system being rendered useless.

In summary, the data collection sub-system will be responsible for acquiring the biometric sample and transforming it into an electronic output. The output of the sub-system depends on:

1. the biometric being measured;
2. the way in which the biometric is presented;
3. the technical characteristics of the sensor used.

If any of the above characteristics changes, it will affect the repeatability and the uniqueness of the biometric.

Transmission

There are a number of biometric systems available that acquire the biometric in one location and process it in another in order to centralise administration of the system and reduce costs. In such a centralised biometric system (where the processing/storage server is physically located in a different location) a transmission system is required. Moreover, if a great amount of data is to be transmitted, a compression system will also be needed [4].

As illustrated in Figure 2-3, the sensor's output from the data collection sub-system will be compressed and encrypted for security before transmission and decrypted and expanded again after transmission. All of this occurs before processing and storing the sensor output. It is important to note that the process of compression and expansion generally causes quality loss in signal (signal loss increases as the compression ratio increases). The compression techniques employed by each biometric system vary as each system tries to minimize signal loss.

If a public network, such as the Internet, is going to be used to transport the biometric "image" it would seem prudent to include encryption prior to transmission and it could be argued that Wayman's generic model would benefit from this inclusion.

Signal processing

Once the biometric has been extracted by the sensor and, if needed, transmitted to the processing unit, it will be matched against the database. The gathered "image" (the data collection system output) needs to be prepared for this process and in the model, processing is divided into three sections: quality control, feature extraction, and pattern matching [4].

The feature extraction process requires an accurate or true biometric pattern to work with from the "image" gathered by the sensor. This means that a "cleaning" process must be used to access the quality of the image and filter out the noise generated by the sensor and transmission of the "image".

Once "cleaned", the system starts to search the pattern for unique, repeatable features; the features that are redundant or unimportant are ignored. After the features have been identified, they are digitised into a binary representation; this binary representation is usually considerably smaller than the original "image" gathered by the sensor and cannot be reversed back into the original sample, this digital representation is known as the template.

After the feature extractor has processed the sample, it is ready to be used in one of the two main functions of a biometric system: enrolment or authentication. For both functions pattern matching is essential because the purpose of pattern matching is to compare the given or presented sample to a number of templates stored in the database (the number of templates used will depend on whether it

is performing identification or verification). During the comparison process, the pattern matching algorithm determines how many features match and how many do not and this measurement is then given to the decision-making sub-system. Pattern matching is used during enrolment to ensure that no duplicate templates are added into the database as well as identifying (one-to-many) or verifying (one-to-one) an individual during recognition.

Decision-making

The decision-making sub-system receives data from the signal-processing unit regarding the amount of non-matches or dissimilarities. The amount of dissimilarities between a biometric sample and template is known as the Hamming Distance [11]. These dissimilarities are then used in a statistical matching process (the test for statistical independence incorporated by Daugman [11], for example). The reason for using a statistical matching process is to allow for the variances created during the presenting of the live sample mentioned earlier. For example, an individual will rarely place their finger in the exact same place and way on a fingerprint scanner [13].

To perform the statistical match, the Hamming Distance is used in conjunction with a system policy. The system policy specifies a cut-off Hamming Distance for a biometric. In other words, if your Hamming Distance is higher than this threshold, the system will reject the sample and a non-match will occur, but if the Hamming Distance is lower than the prescribed threshold it will be deemed a match.

Many biometrics allow the operators of the system to specify the cut-off threshold and this, in turn, could affect the accuracy of the biometric (refer to [5] for more details on the effect of adjusting this threshold).

Storage Sub-system

Within biometric systems there are two different types of data that can be stored in the biometric database. The first is the hashed biometric code or template [4] (produced after feature extraction and used in the future for recognition) and it can be stored on a number of different mediums: a central database, smartcards, magnetic strips etc. [4].

The second type that can be stored is the raw biometric [4] (gathered from the sensor in the data collection sub-system). There are two good motivations for storing the raw biometric data and not just the template. Firstly, the ability to "re-issue" the biometric code quickly and easily [4] (by running the raw biometric through the feature extraction phase again) and, secondly, the ease with which the feature extraction and decision-making phases can be modified [4] (by simply running the raw biometric through the new algorithms). Obviously, these advantages allow the biometric system to be upgraded to a new version (or new vendor) easily and without the hassle of re-enrolling all the users.

An important point to consider when developing such a system is that each individual sub-system can generate errors that then propagate throughout the rest of the system. Although the error might not harm the sub-system it originated from, it could produce a fatal error further on in the system. This is why the integration of each sub-system is critical and developers should test carefully both prior to and post-integration.

Effectiveness of a biometric system

Biometric performance

In order to determine the performance of a biometric system a number of different factors need to be assessed. One of the key performance measurements is the "failure to enrol rate". In other words, the number of times the system experienced a problem when enrolling the individual. Other aspects include:

- **Failure to acquire rate** [5] **–** the percentage of attempts that resulted in a failure to acquire;
- **False match and non-match rate** [5] **–** the percentage of false accepts (wrong identification) and the percentage of false rejects (not identifying an enrolled person) produced by the system;
- **Penetration rate or penetration coefficient** [5, 61] **–** if a database is used for recognition, the penetration rate will be the average portion of the database that needs to be searched in order to perform the identification;
- **Bin error rate** [5, 61] - the percentage of samples not capable of being matched against the database due to using the incorrect bin (refer to [61] for more info on the bins);
- **User throughput** [5] **–** the number of users passing through the system during a specific time span (generating an elapsed time average per single transaction);
- **Matching algorithm performance** [5, 61] **–** the throughput of the matching algorithm. In other words, the number of matches performed per second or minute by the algorithm. This measurement can be divided into two separate parts: the speed of both a one-to-one search and a one-to-many search [61];
- **Sensitivity to population and environment** [5] **–** the performance difference exhibited if the user population or the environment within which the system operates is changed.

For a more detailed discussion on the performance factors of biometrics interested readers can refer to [61].

Accuracy of decisions

There are four possible outcomes from any biometric system: acceptance of an authentic identity; rejection of an authentic identity; acceptance of an impostor and rejection of an impostor. The two obviously most desirable results are the acceptance of an authentic identity and rejection of an impostor, while the other two can be considered as errors. Thus, during the development of a biometric system the aim is always to try and maximise the acceptance of authentic identities and rejection of impostors.

Figure 2-4 (below) illustrates the two bell curves created by using the Neyman-Pearson [11, 60] formalism for decision problems in which the prior probabilities are not know and the error costs are not fixed, but the posterior distribution is known[11].

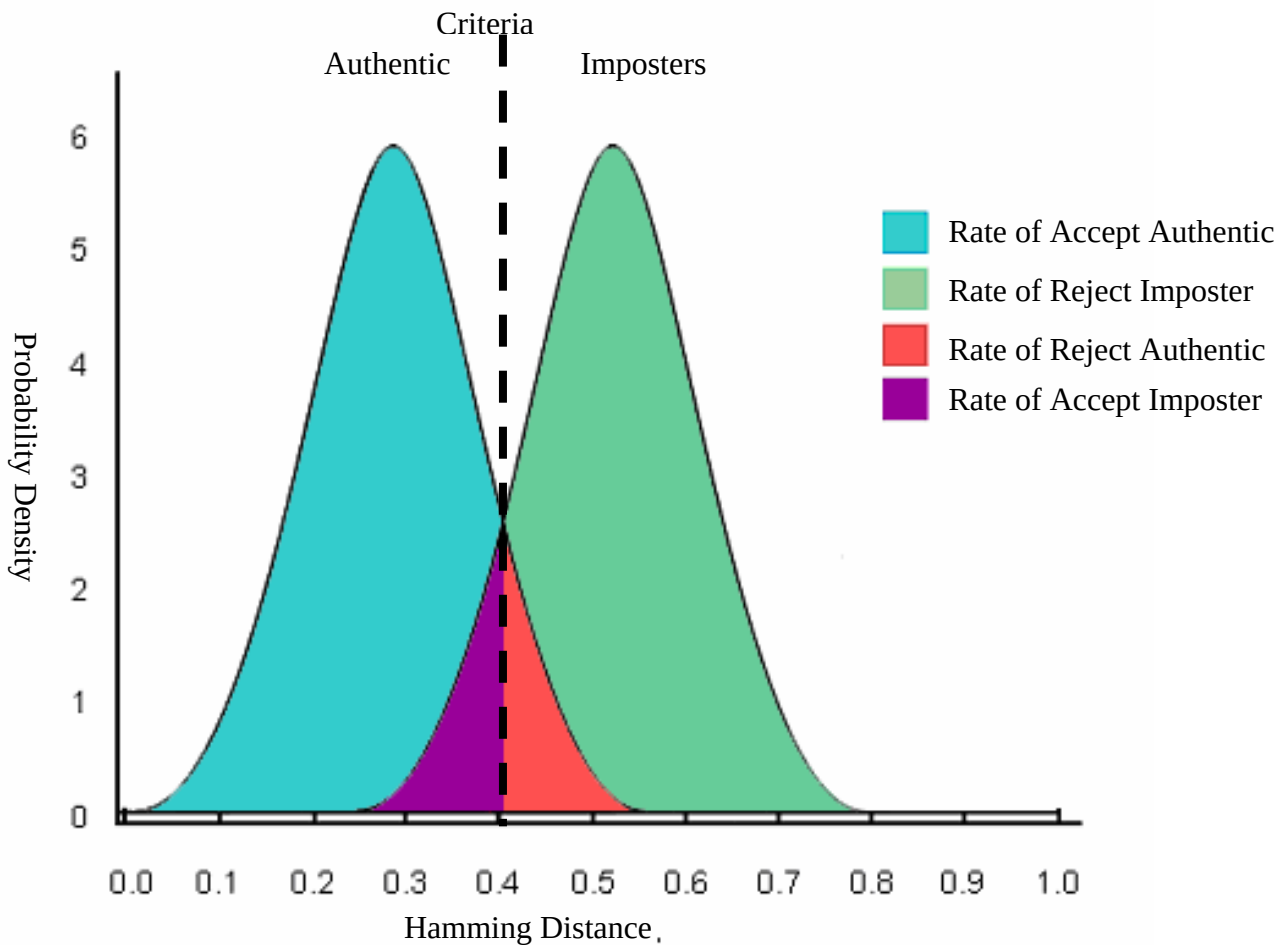

Figure 2-4 Neyman-Pearson formalism for decision under uncertainty. Adapted from [11, 60] (Refer to the Appendix 1 for a colour version of the figure)

The bell curve on the left plots the distribution of authentic users against the Hamming Distance and the bell curve on the right conversely plots the distribution of impostors against the Hamming Distance. The Hamming Distance or threshold (criteria) selected in this instance is 0.4. This means that a sample with a Hamming Distance smaller than 0.4 will be accepted, whereas a higher value than 0.4 will be rejected. The problem illustrated by this diagram is the inevitable cross-over between the two bell curves. The diagram demonstrates how, wherever the criteria or threshold is set, the system will incorrectly reject a certain number of authentic identities and accept a certain proportion of the impostors. While it is possible to reduce the incidence of one of these errors, it is only at the expense of the other.

Figure 2-5 (below) indicates the common trade off made between false accepts and false rejects in most biometric systems [5].

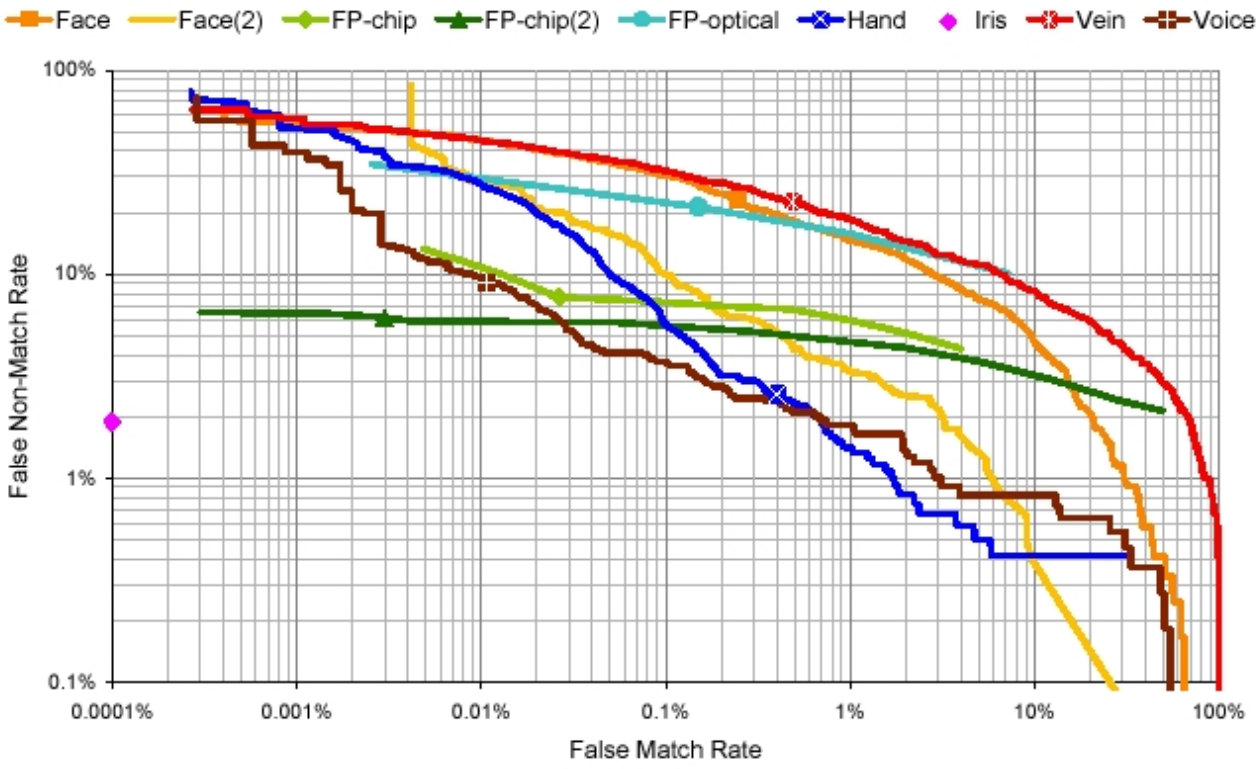

Figure 2-5 False accept and false reject trade off. FP-chip = Fingerprint chip, FP-chip(2) = Fingerprint chip 2, FP-optical Fingerprint optical, Vein= Vein pattern. (The lower and further left on the graph, the better the performance) [5] © Crown Copyright 200x. Reproduced by permission of the Controller of HMSO. (Refer to the Appendix 1 for a colour version of the figure)

Conclusion

Biometric authentication is one of the most exciting technological developments of recent history and looks set to change the way most people live. Its compelling advantages suggest that soon travel and most payment systems will require biometric authentication to positively prove beyond doubt the identities of the individuals involved in the transactions.

This chapter has served to expand the concepts behind biometric authentication, explain how such systems work and how to calculate their effectiveness. The next step is to start relating the theory to real-world applications and the next chapter starts this process by examining the use of specific physiological and behavioural biometrics in context.

Chapter 3 Physiological biometrics

Introduction

As stated previously, biometric identification techniques are based on measuring characteristics a person either has or actions they perform in a specific way. These personal traits can be classified as either physiological or behavioural. This chapter is devoted to a review of the main physiological biometrics while the following chapter will assess the main behavioural biometrics in more detail.

Physiological biometrics are, as the name suggests, based on the physical characteristics a person possesses. The physiological biometrics under review in this chapter will be:

- Fingerprint;
- Hand Geometry;
- Iris recognition;
- Facial Recognition.

Fingerprint

Biometric identification techniques based on reading fingerprints are among the most established and widely used. Dating back to the beginning of forensics, fingerprint identification has become a major crime fighting tool [8, 64]. Close observation of an individual's fingerprint reveals an organised, textured pattern that is almost unique [8]; a uniqueness which makes it an ideal way of identifying a person.

One of the major downsides to fingerprinting, however, is that the human hand is almost always "working" and interacting with its environment. This leaves a person's fingerprints exposed and, by increasing the possibility of them being altered, reduces their robustness or stability. It is possible for the same finger to give completely different readings because it has been affected by bruises or injuries [14], peeling of the skin [14], dryness of the finger [14] etc. (see Figure 3-1).

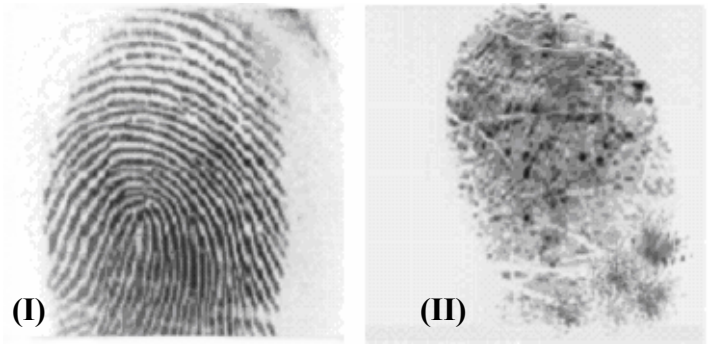

Figure 3-1 An example of
(I) a normal fingerprint — ideal for use in fingerprint recognition, and
(II) a damaged fingerprint — note the absence of recognisable grooves or a discernible pattern aside of the faint scar lines.

Although the fingerprint can easily be damaged, it remains a viable biometric and offers enough advantages to ensure it will continued to enjoy widespread use.

How does fingerprinting work?

The three stages in the biometric identification process model (see biometric chapter) will be used to explain how fingerprinting works: data collection; signal processing, and decision making.

Data collection

Due to the popularity and long lifespan of fingerprinting, there are a multitude of scanners on the market manufactured by dozens of companies. Almost all of the scanners available can, nonetheless, be divided into two main types: optical or solid-state sensors [13, 14].

Optical sensors operate on the principle of a Frustrated Total Internal Reflection (FTIR) [14]. These scanners consist of a glass plate illuminated by a LED light. A user places his or her finger on the glass plate and the LED light is activated. The pattern of ridges on the illuminated fingerprint can be established because the ridges reflect the light back at the sensor and the furrows between them do not (although, technically, the furrows also reflect the light, but at an angle the system ignores). The sensor captures an image of the fingerprint by recording the reflected light using a CCD (Charge-Coupled Device) array.

The second type of fingerprint scanners, solid-state sensors, can be divided into three groups [14] of scanners: capacitive; pressure sensitive, and temperature sensitive.

A capacitive sensor captures a fingerprint image by making use of an array of capacitors. The sensor measures the voltage between the array to establish the pattern of fingerprint ridges and furrows [14].

Pressure sensitive sensors consist of a top layer of elastic, piezoelectric material which can determine the pressure difference between the ridges and furrows of the fingerprint. This "impression" is then converted into an electrical signal representing the fingerprint [14].

Temperature sensitive scanners measure a fingerprint by determining the temperature difference between the ridges of the fingerprint — touching the sensor's surface — and the furrows or valleys of the fingerprint — just above the sensor's surface. As with pressure sensitive scanners, this difference is then converted into an electrical signal representing the fingerprint [14].

Even though we have a multitude of sensors available the sensors are however not the only factor that would affect the quality of a scan, different conditions also have an effect on the quality of the image captured by a sensor. If the finger is dry, for example, the image generated will not be as clear as when the finger is slightly moist. See Table 3-1 below for more factors.

Condition	Impact
Manual work	Medium
Dirty finger	Medium
Weather	Medium
Cuts and bruises	High
Placement on scanner	High

Table 3-1 Different factors affecting a fingerprint read [14]

Signal processing

Once an image has been captured by one of the sensor mentioned above the conversion of this image into a usable digital form can commence. Converting the captured image of a fingerprint into a binary representation of its features is a complex process and, while there are many opinions on the subject of feature extraction, there are two main extraction techniques: minutiae representation and Gabor-filter (texture-based) representation [8, 13, 14]. It is worth noting that the more advanced systems often make use of a hybrid between the two [28].

A minutiae representation of a fingerprint is calculated by analysing the position of tiny points called minutiae [13] (the end points and junctions of print ridges). A typical example of minutiaes detected in a fingerprint can be seen in Figure 3-2.

Figure 3-2 A fingerprint gathered using a solid-state sensor with the minutiaes marked in red [13]. Reprinted under permission [13]. (Refer to the Appendix 1 for a colour version of the figure)

A Gabor-filter representation of a fingerprint generates a template by making use of mathematical functions called Gabor filters. Gabor filters are specialised equations used to extract local image features [48]. A number of Gabor filters have been developed specifically to extract the features of various biometric characteristics during signal processing. These equations are applied to the image using a constant frequency with varying orientation (see [13] for more details) — each orientation producing a different texture image of the same image. An example of a Gabor filter with varying orientation can be seen in Figure 3-3 which illustrates both (a) the original image and (b) the results of applying a Gabor filter to the image (using multiple orientations) [adapted from 13]. The texture information generated is then digitised and either stored or used for recognition.

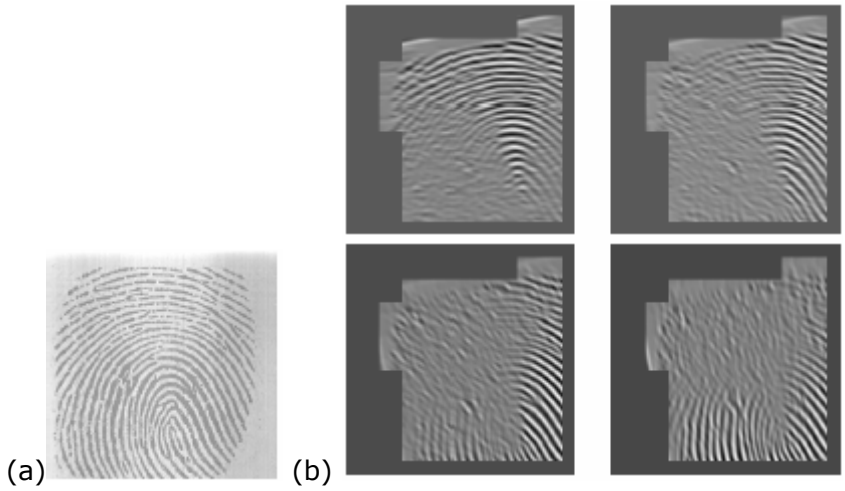

Figure 3-3 An example of
(a) template gathered using solid-state sensor, and
(b) Result of applying Gabor filter equation to the template using different orientations 0o, 22.5o, 45o, and 67.5o (adapted from [13]). Reprinted under permission [13].

Decision making

The decision making process for fingerprinting can differ from vendor to vendor, but basically works on the principle of statistical difference. The system will determine the number of differences between the features extracted (minutiae or Gabor-filter) from two templates (usually a previously captured (enrolled) and stored template against a newly captured sample). If the number of differences is below a specified percentage, the fingerprint is said to be a match (a detailed description about the matching of fingerprints can be gathered from [8] and [13]).

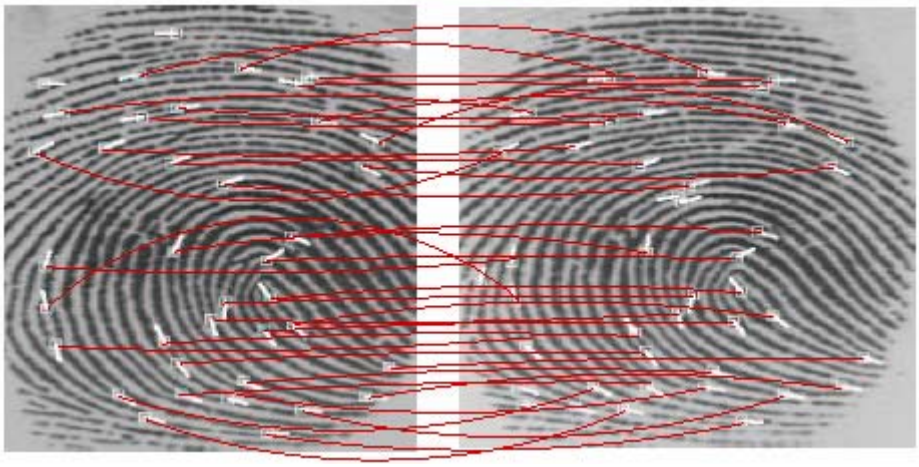

Figure 3-4 Minutiae matching between two different fingerprint templates [8]. Reprinted under permission [8]. (Refer to the Appendix 1 for a colour version of the figure)

Hand geometry

Hand geometry is one of the oldest biometrics, dating back more than 20 years [7]. It is also the closest related biometrics to fingerprint, and works on the geometry or shape of the human hand [16, 17].

Inner workings of hand geometry

Data Collection

There are numerous scanners available capable of biometrically capturing the geometry of an individual's hand, but almost all of them work on the same principle and use cameras.

Figure 3-5 Hand geometry sample

A typical example of a captured hand can be seen in Figure 3-5 above. The scanner used an ordinary camera to capture a black and white image (the colour of the skin is not used in hand geometry) of the hand. This figure illustrates a top view of the hand, but many of the scanners on the market also capture a side image of the hand. A side image can be captured in several ways, most notably either using a side-mounted mirror to reflect the image (Jain, Ross and Pankanti [17]) or by installing an extra camera — although this option increases the production cost of the scanner.

Generating the template

The template generated during the feature extraction phase is usually only a 9 byte feature vector [12]. This is quite small due to the limited amount of information being recorded. The feature information contained within the template will include information about the width of the fingers at different intersections, the width and thickness of the palm, the length of the fingers etc [17]. Hand geometry does not compare detailed information like a hand's wrinkles or skin colour [17].

In order to obtain these feature vectors [16] (the width of the fingers at different intersections, the width and thickness of the palm, the length of the fingers etc) hand geometry utilizes a variety of different techniques (see [16] and [17] for two examples), but commonly relies upon the placement of axes (feature vectors) on the hand. The placement of the axes is often assisted by using fixation pegs. These both guide the placement of the user's hand and act as control points in the placement of the axes [17].

If the system does not make use of fixation pegs it has to incorporate a more sophisticated method of placing the aforementioned axes on the hand. In [16] the authors made use of a LoG edge detector to obtain a single-pixel-width boundary of the hand. They then used signature analysis to place the feature vectors on the hand similar to those in Figure 3-6 below.

Once the system has identified all the feature vectors required they are recorded within a hand geometry template.

Figure 3-6 The geometric features extracted. Adapted from [17].

Why use hand geometry

Hand geometry is not a very unique biometric mechanism - about 1 in every 100 [4] individuals exhibit the same hand geometry. This is primarily because hand geometry only uses very simple measurements and does not make use of the detailed information available (the wrinkles on the hand, skin texture, skin colour, etc). The method's lack of uniqueness makes it unsuitable for identifying individuals (one-to-many comparisons) in large populations. Hand geometry can, however, be incorporated effectively for verification (one-to-one comparisons). Moreover, this can be viewed as a plus in terms of acceptance because many argue that verification does not invade an individual's privacy to the extent that identification does [17, 65]. In other words, verifying that an individual is who he or she claims to be rather than identifying them from scratch.

Other positives of hand geometry include its relatively inexpensive cost, ease-of-use, the fact that sensors are not affected by the condition of the skin [17] like dryness, dirt etc., and the small size of the template (usually 9 bytes [12]) allows a number of different storage mediums like smart cards, barcodes, magnetic stripe cards, etc. to be used.

The iris

The iris is the pigmented tissue lying behind the Cornea that gives an eye its colour and controls the amount of light entering the eye by varying the size of the papillary opening. In other words, the coloured ring surrounding the pupil of the eye.

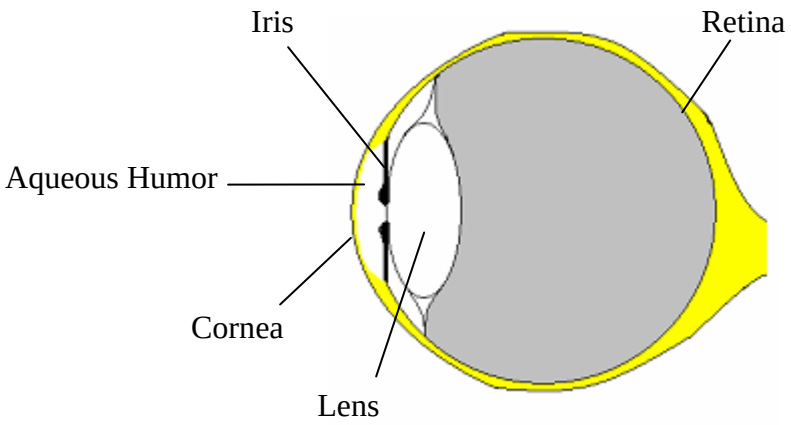

Figure 3-7 The human eye (Refer to the Appendix 1 for a colour version of the figure)

The iris begins to form during the third month of gestation (the period in the womb between conception and birth). The shape or pattern of the iris (the crypts and other shapes) starts to develop by the eighth month; the shapes formed during this period will remain the same until a few minutes after death (the colour of the eye can however change during the first year after birth).

In Figure 3-7 you can see the iris's physical location in the front of the eye behind the Cornea (the clear membrane in front of the eye). Its location, sheltered by the Cornea and Aqueous Humor, also highlights how well protected it is for an externally visible organ.

How does Iris recognition work?

Data collection

An image of the iris is collected using a specialized monochrome camera. This camera is capable of capturing an image when the iris radius is between 100 and 140 pixels [45, 50].

The complex inner mechanics of the sensor used in iris recognition is beyond the scope of this study, but two important parts of the process require examination. The first is how the system locates the area used for recognition (the iris itself) and ignores the rest of the image — the sclera (the white of the eye) and the pupil. The second is how the system ensures that the sample taken by the camera is of a suitable quality for performing recognition and a living sample from a real eye.

Locating the Iris

One of the most important aspects of iris recognition is the ability to locate the iris within the eye. With the correct "location algorithm" it is possible to locate the iris, determine the quality of the image and determine if the eye is a living eye. The basis of the location algorithm can be viewed in (1) [11, 50]. This location algorithm was developed by Dr John Daugman[2] (the main researcher in the field

[2] http://www.cl.cam.ac.uk/users/jgd1000/

of iris recognition) a mathematician at Cambridge University. The location process begins by assessing the quality of the image taken. Once the quality has been assessed and approved, the inner and outer bounds of the iris need to be located. This is achieved by applying the complex mathematical equation below (1).

$$\max(r, x_0, y_0) \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r, x_0, y_o} \frac{I(x, y)}{2\pi r} ds \right| \quad (1)$$

Using the equation above (1) divides the search for the iris into three phases [11, 50]. The first phase is a very rough search that is only interested in locating the transition from iris to sclera, the outer boundary of the iris. Once this first search has identified the outer boundary of the iris, the second phase will determine the transition from iris to pupil, the inner boundary of the iris. The search for the pupillary boundary commences in the centre of the confined area identified by the first search. Initially, this second search turned out to be a problem for Daugman because the pupil is not always darker than the iris. To overcome this problem, he added an absolute value to the equation to prevent it producing negative results. (interested readers can refer to Daugman's research [11,50] for more information). Once the operator (1) has detected both the outer (limbus) and pupillary boundaries, it can be altered to detect the upper and lower eyelids in the third search phase [50]. Figure 3-8 gives an indication of the boundaries located during the three search phases.

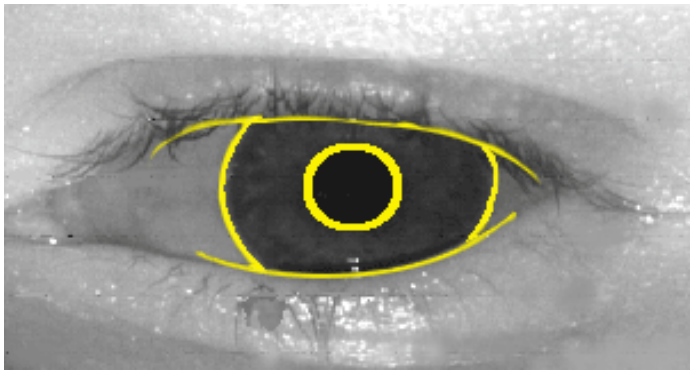

Figure 3-8 The boundaries located during the iris search phases (Refer to the Appendix 1 for a colour version of the figure)

Is that an eye or not?

It is important to note that the image capture process used in iris recognition is not a sudden recording or "snapshot". The camera does not capture an instant, single image at the flick of a switch, but uses real time video feedback instead. The software then assesses the quality of the frames [11] being submitted and only once it is happy with the quality of the image (an eye is present, the eye is in focus and not too obscured by the eyelids) will it collect the image for processing.

The software establishes the quality of the image using two enhanced versions of the original equation (1). The complexity of this transformation and how the two new equations — (2) and (3) — are created are beyond the scope of this study, but the complexity of the mathematics is clearly illustrated below (interested readers can refer to Daugman's work [11] for more information on the equation changes).

$$\max(n\Delta, r, x_0, y_0)\left|\frac{1}{\Delta r}\sum_k\left\{\left(G_\sigma((n-k)\Delta r)-G_\sigma((n-k-1)\Delta r)\right)\sum_m I\left[\left(k\Delta r\cos(m\Delta\theta)+x_0\right),\left(k\Delta r\sin(m\Delta\theta)+y_0\right)\right]\right\}\right| \quad (2)$$

$$\max(n\Delta, r, x_0, y_0)\left|\frac{1}{\Delta r}\sum_k\left\{\frac{\left(G_\sigma((n-k)\Delta r)-G_\sigma((n-k-1)\Delta r)\right)\sum_m I\left[\left(k\Delta r\cos(m\Delta\theta)+x_0\right),\left(k\Delta r\sin(m\Delta\theta)+y_0\right)\right]}{\Delta r\sum_m I\left[\left((k-2)\Delta\cos(m\Delta\theta)+x_0\right),\left((k-2)\Delta\sin(m\Delta\theta)+y_0\right)\right]}\right\}\right| \quad (3)$$

With the new equations, (2) and (3), Daugman not only assesses the quality of the feedback but also determines whether the feedback given is that of a live eye. The first means is testing the movement of the eyelids [11]. The second, and more accurate test, depends on detecting the presence of pupillary unrest or hippos [11]. Pupillary unrest, with respect to the iris, is involuntary oscillations in the diameter of the pupil caused by fluctuation in both the sympathetic and parasympathetic innervations of the iris sphincter muscle. The pupil will also dilate according to the amount of light available [11] and, to assist in the process of checking for a live eye, different cameras will try and vary the light conditions. For example, some use multiple lights flickering on and off.

Signal processing

The size of the iris image captured varies according to the amount of light available in the environment and reflexive oscillations of the pupil, the zoom capabilities of the camera used, and distance between it and the eye. To overcome this, Daugman [11] suggests identifying zones of analysis within the iris. These zones allow a standardized set of areas to be created within the iris image, regardless of iris or pupil size.

Once all the zones of analysis have been identified, feature extraction can begin. One of the most effective ways of extracting textural information from an image is the computation of 2-D Gabor[3] phasor coefficients. These 2-D Gabor filters are specialized filter banks that extract information from a signal at a variety of locations and scales. Consequently, they are capable of providing information about the orientation and spatial frequencies present within the image; in other words, the "what" as well as the 2-D position or "where" [11]. The 2-D Gabor filter proposed by Daugman [11] for use in iris recognition is listed below (4).

$$G(r,\theta)=e^{-i\omega(\theta-\theta_0)}e^{-(r-r_0)^2/\alpha^2}e^{-(\theta-\theta_0)^2/\beta^2} \quad (4)$$

Although the iris code is 512 bytes [49] (4096 bits), the converted image is actually a 2048 phase bits template [11]. The additional 2048 bits that make up the 4096 bits are known as mask bits. These mask bits are used to indicate whether or not any region of the iris image was obscured by eyelids, contained any eyelash, occlusion, specular reflection (reflection of light by the cornea), the edges of contact lenses, or poor signal quality. Once all the phase information has

[3] As noted earlier Gabor filters are members of a family of functions, originally developed by Dennis Gabor in 1946, that optimizes the resolution in both the spatial and the frequency domains [49].

been extracted and converted into a bit representation or "final" iris code, the decision making part of the recognition process can begin.

Decision making

The iris recognition decision making process relies on the failure of the test of statistical independence. This test involves so many degrees of freedom that the test is guaranteed to be passed when two different irises are being matched, but will fail when two identical irises are compared.

The way the first iris system utilised the test for statistical independence was by making use of a simple Boolean Exclusive-OR (XOR) operator and applying it to the 2048 phase bits [11] (this was before the addition of the mask bits [50]). A Boolean Exclusive-OR is an operator which will detect the difference between two bit arrays. The two arrays are compared by XORing pairs of bits and the results of each comparison form a new bit array. In the XORing process, if two similar bits are XOR'd, the result will be a "0", but if two different bits are XOR'd, the result will be a "1". For instance, if we have two bit arrays A and B (A = 0010011001 and B = 0110110000) and the XOR operator is applied, a new bit array, C, (C = 0100101001) will be generated (see Figure 3-9 below).

0	XOR	0	=	0
0	XOR	1	=	1
1	XOR	1	=	0
0	XOR	0	=	0
0	XOR	1	=	1
1	XOR	1	=	0
1	XOR	0	=	1
0	XOR	0	=	0
0	XOR	0	=	0
1	XOR	0	=	1

Figure 3-9 Example of an XOR between two binary arrays

The XOR $\otimes$ operator was incorporated initially to determine the Hamming distance (HD) between two iris codes (the HD is a fraction of disagreeing bits between two iris codes). The HD distance for two 2048 phase bits iris codes was computed using (5) [11], where Ai and Bi are the current bits being XOR'ed.

$$\mathrm{HD} = \frac{1}{2048} \sum_{i=1}^{2048} A_i \otimes B_i \tag{5}$$

The inclusion of masked bits in the iris code required the way in which the Hamming distance is calculated to be changed. Daugman still applied the XOR operator to the two 2048 bit phase iris codes, but masked (AND'd) both of their corresponding masked bit vectors in order to prevent non-iris factors from influencing the iris comparison [50]. The added AND operator $\cap$ providing extra error checking and ensuring that the compared bits are uncorrupted by eyelashes, eyelids, specula reflection and other noise. The new formula for determining the HD is given in (6) [50].

$$\mathrm{HD} = \frac{\left\|(codeA \otimes codeB) \cap maskA \cap maskB\right\|}{\left\|maskA \cap maskB\right\|} \quad (6)$$

In (6) the phase code for the two iris codes are represented as codeA and codeB and the masked bit codes are represented as maskA and maskB. It is important to note that the two operators $\otimes$ and $\cap$ are applied in vector form to binary strings in a single machine instruction. These binary strings can be as long as the word length of the CPU. Thus, for a normal 32-bit CPU, any two integers between 0 and 4 billion can be XOR'd in a single machine instruction to generate a third integer (whose bits — in a binary expansion — are the XOR of the bits in the original two integers [50]). Consequently, if (6) is implemented in parallel, 32-bit, blocks the system is capable of rapid iris code comparisons. To put it in perspective, an old 300 MHz CPU is capable of performing 100 000 iris code matches per second [50].

These comparisons are then related back to the test of statistical independence using the Hamming distance derived using (6). In other words, if the two iris codes that are being compared produce a HD below a certain value, the comparison fails the test of statistical independence and the two iris codes are deemed to match.

A possible base threshold that would ensure a high level of confidence was calculated by Daugman to be an HD of 0.33 [50]. In other words, two iris codes would fail the test of statistical independence if the HD produced in (6) was smaller than 0.33. One of the main reasons this number was picked as the threshold for iris recognition is that it ensures the odds of a false match being generated by the system are 1 in 4 million [50]. This ensures that when performing an exhaustive search through a large database of irises, the level of confidence is quite high when a match (HD ≤ 0.32) is found in the database. This high level of confidence is required since a one-to-many operation is much more demanding than a one-to-one operation and the chances for a false match much higher. To determine the probability of making a false match in a large database, the size of the database and the probability of making a false match in a one-to-one situation need to be known. Armed with those two values, the formula shown in (7) can be used to calculate the probability. In (7) P1 is the probability for a false match in a one-to-one operation, and Pn is the probability of making a false match in a database of size n.

$$P_n = 1 - \left(1 - P_1\right)^n \quad (7)$$

If, for example, a biometric system is accurate 99.9% of the time when performing one-to-one comparisons (verification), only 0.1% of its matches will be false. Thus P1 = 0.001. If the database size is now increased from 1 to 100, Pn will equal 0.095 and so the chances of a false match will rise to 9.5%. If the database size is further increased to 4000, Pn = 0.982 and the chances of a false match become quite high (98.2%).

Even though the HD ≤ 0.32 criteria produces a false match rate in an iris one-to-one comparison of 1 in 4 million and allows for high levels of accuracy even in large database searches, Daugman wanted to be sure. Consequently, he decided to exploit the rapid attenuation of the HD distribution created by binomial combinatorics (see Table 3-2 for some of the values of this distribution) and adjust the HD so that the Pn < 10-6, regardless of the database size. Table 3-2

below illustrates how, to maintain this criteria in a database of 1 million irises, the HD has only to be raised slightly from 0.33 to 0.27.

HD Criterion	Probability of a false match
0.26	1 in 10^{13}
0.27	1 in 10^{12}
0.28	1 in 10^{11}
0.29	1 in 13 billion
0.30	1 in 1.5 billion
0.31	1 in 185 million
0.32	1 in 26 million
0.33	1 in 4 million
0.34	1 in 690 000
0.35	1 in 133 000

Table 3-2 Illustrates the probability of a single false match rate for various HD in a one-to-one operation [50]

Facial Recognition

Facial recognition is one of the fastest growing biometrics in terms of research and development. Many experts view it as the field's "holy grail" because of the alluring advantages it offers and, consequently, it is fast becoming a global standard for airports, casinos, etc. Also referred to as the "Big Daddy" of biometrics because of its potential to overshadow all the other biometric techniques, facial recognition offers the following compelling advantages:

(i) Facial recognition stands the greatest chance of enabling long distance recognition via the infrastructure already in place at casinos, banks, supermarkets and in other public places.
(ii) Given the correct infrastructure and appropriately developed Artifical Intelligence (AI) software, facial recognition systems could potentially pick out a person within a large crowd without human intervention.
(iii) A biometric sample, in this case the face, could be captured without an individual's knowledge.
(iv) Facial recognition systems could be put in place relatively inexpensively in organisations already using closed circuit camera surveillance systems.
(v) Governments and other organisations already have a large database of photos at their disposal, allowing for the development of large recognition systems like a biometric passport system or employee biometric ID card.

Although an obviously attractive option for many organisations, including governments, there are several significant obstacles facing its development:

(i) Human faces consist of very similar shapes since all faces are, basically, made out of the same facial structures in almost the same geometric positions [32].
(ii) Face shapes differ between races, adding extra complexity to the system.
(iii) There are a wide variety of user and environmental factors that have to be negotiated. For example, ambient lighting conditions can vary immensely during image capture and the subject might be standing in a different pose or exhibiting a different facial expression [32].
(iv) It is relatively easy to alter facial characteristics using prosthetics, makeup, facial hair etc, and some systems can even be confused by a person wearing glasses.

All of the above points are relatively good deterrents in themselves, but perhaps the single biggest deterrent is the threat to personal privacy. The fact that an individual's face can be captured and recognised without their knowledge alarms most people because it represents a massive threat to their civil liberties.

Inner workings of facial recognition

Due to the large amount of interest in facial recognition, there are numerous systems available and a variety of different methods of extracting and parsing an image of a face into a biometric template. For the purposes of this study, the two predominant means of feature extraction will be assessed, along with the data capture and decision making processes.

Data capture

The sensor used in the facial recognition process is a normal camera, capable of capturing an image of a face in enough detail to perform recognition. Environmental factors such as lighting have a huge affect on the image taken (see chapter 5 for more info on environmental factors). Other factors such as distance between the device and the person, pose of the person, and facial expression of the person all also have an impact in the data (photo) being collected. Most of these factors, nonetheless, can be removed during the data collection phase using a variety of normalisation techniques. The lighting, for example, can be optimised by filtering the image using a bandpass filter like the Laplacian [32]. The distance issue can be resolved by scaling the image and/or using image plane rotation and other techniques. A lot of other normalisation techniques exist, but are beyond the scope of this document and interested readers should refer to [32, 33, 34, and 35].

Feature Extraction

Although there are a number of different ways and mechanisms through which the features of a face can be extracted and digitised, two main ones [32] have emerged: geometric and pictorial. The geometric approach uses the spatial configuration of facial features (location of lips, nose, ear etc.). The pictorial approach uses filters on an image-base representation of the face. There is also a hybrid approach which combines these two main approaches and represents the face as an elastic graph of local texture features [35].

Geometric approach

The geometric approach makes use of the location of facial features or "landmarks" like the eyes, ears, mouth etc. Numerous different mechanisms have been developed for this, but, in essence, the system will locate the eyes, mouth, ears and ovoid shape of the subject's head by looking for edges, curves, colour blobs (like the iris located in the white sclera) and known shapes (like the rectangle of the nose or oval shape of the head) [36]. See Figure 3-10 for an example of the points located within the face.

Figure 3-10 Points indicating possible references the system will identify during geometric feature extraction (Refer to the Appendix 1 for a colour version of the figure)

Once all the different points and shapes have been identified, they will be converted into feature vectors consisting of distance measurements, angle size and curve measurements etc.

Pictorial approach

The pictorial approach makes use of different filters to represent the face. The main filters used are Gabor wavelets (interested readers can refer to "Face Recognition by Elastic Bunch Graph Matching" [35] for a more detailed discussion of Gabor wavelets).

Dealing with different poses and the Decision making process

Before entering the decision making phase, the facial recognition system must try to compensate for the wide variety of poses that might have been captured during feature extraction. This is one of the main problems encountered during the process because a subject can look left, right, up, down or even in a combination of directions. Their eyes can be open or closed, and they may be smiling or frowning, etc.. Over the years, multiple solutions have been proffered for dealing with this problem, but two have emerged as particularly favoured. The first is template-based faces [32] and the other is face bunch graphs [35]. Both these methods are discussed in further detail below, predominantly to illustrate the complexity of the task of dealing with different poses.

Template based

Beymer [32] introduced the first template-based system and required subjects to make multiple poses during the enrolment process. During enrolment, each individual image is allocated a template group according to the pose of the user. For example, a left-up pose where the subject is looking left and up. The method Beymer used to group the images into templates was by identifying the location of the eyes and nose lobs of the person in the picture. These locations would be recorded and then evaluated against predetermined templates; once the closest match was found the image would be saved under that template group.

Correspondingly, when a recognition is performed, the image is first matched to a template group and then compared only to images in the database conforming to the same template group.

Face bunch graph

The face bunch graph method of facial recognition constructs face graphs from the captured images and compare them to previously enrolled face graphs. In order to generate a face graph, the system identifies a number of points located on the face like the eyes, corner of the mouth and tip of the nose [35]. These points or nodes are then numbered and known as fiducial points. At each fiducial point a Gabor filter is applied. These filters generate feature information around the node called a jet [35]. Then, to complete the face graph, the nodes are connected to the edges [35] (see Figure 3-11 for an example).

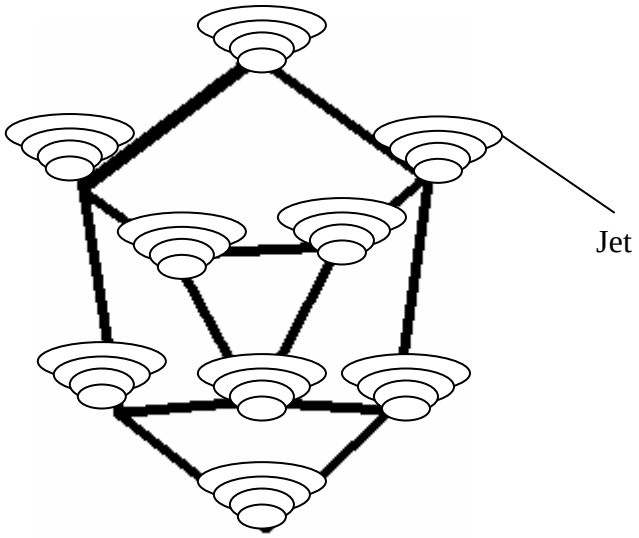

Figure 3-11 A Face graph adapted from [35].

During enrolment, the system will construct a graph, like Figure 3-11 above, with different jets and distances between nodes (i.e. different edges) for different poses and place them in a stack like structure (one on top of the other). This stack of possible poses is called a face bunch graph [35] because of the way the jets bunch together at each jet (an example can be seen in Figure 3-12 below).

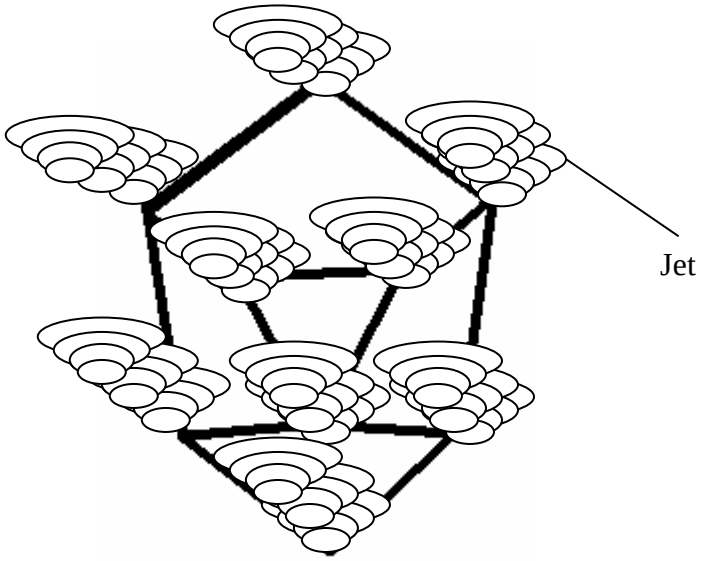

Figure 3-12 A Face bunch graph adapted from [35].

In order to handle the possibility of multiple poses during recognition, a face node graph is generated from the captured sample and compared to an appropriate face graph and jets selected from the previously captured or enrolled face bunch graph. The system can then compare the two and determine a match (see [35] for more information).

Decision making

Once the most appropriate (corresponds best to the current pose) images or face bunch graph have been selected from the database, the system can make a YES/NO decision. The decision making process for facial recognition differs from system to system, but predominantly compares the differences between the feature vectors generated during either the geometric and pictorial feature extraction phase and, consequently, makes use of statistical difference.

The brief discussion above illustrates how complex and difficult it is for the system to make an accurate YES/NO decision regardless of the pose of the individual. Not only do a large number of templates need to be stored within the database, but a lot of pre-processing needs to happen before an accurate YES/NO can be given (see [32 - 36] for more detailed discussions of the decision making process).

Conclusion

The purpose of this chapter has not been to arm the reader with an in-depth knowledge of the main physiological biometrics — fingerprint, hand geometry, iris recognition, and facial recognition, but rather to illustrate how these biometrics are surprisingly similar in design. They all function according to the generic model and predominantly use of the same techniques, like Gabor filters. The following chapter will assess the major behavioural biometrics — signature recognition, keystroke dynamics, and speaker recognition — in a similar fashion.

Chapter 4 Behavioural Biometrics

Introduction

As mentioned previously, a behavioural biometric is a biometric based on something that a person does in a unique way. In this chapter, the following behavioural biometrics will be reviewed:

- Signature recognition;
- Keystroke dynamics;
- Speaker recognition.

Signature Recognition

Signature recognition as identification/verification means has been around for some time now and is probably one of the most extensively studied biometrics [18 – 27, 29]. Traditionally, signature recognition has been used mostly in the business arena — primarily signing cheques, contracts and other important documents. The person receiving the signed document (contract, cheque etc) performs a manual verification, through pattern recognition, to ensure that an authorised person signed the document.

Although signature recognition has been around for some time now, automating the recognition process remains challenging because the human signature is not always identical and can change drastically over time [18, 20]. Changes in a person's signature can be the result of a wide variety of factors including advancing age, their mental or physical state etc. [20]. Due to the changing or dynamic nature of the human signature, extensive research has been conducted and two main areas types of signature recognition [24] developed: *on-line* recognition [24, 26] which dynamically gathers data for verification using, for example, a stylus and electronic tablet [26], and *off-line* recognition [19, 21, 22, 23] — making use of a static sample, a scanned image of a signature for instance, to perform a match against a database.

Off-line signature recognition

As mentioned previously, off-line signature recognition does not make use of specialised electronic tablets or writing pads to capture a signature, but rather relies on a simple image. This approach is very limiting because none of the other dynamic features present, like the pressure of the pen or its speed, angle etc., can be recorded. This restriction of information makes it quite a complex task to develop an off-line recognition system and, consequently, has become the research mission for many academics [19 - 23]. Due to the large interest in this field, a large number of methods have been developed. For example, 2D wavelets are capable of extracting both static information and dynamic curvature information [21]. Neural networks, which can be taught to recognise an individual signature, is another fascinating method [20]. Other systems include: Granulometric size distributions [22], and HMM (Hidden Markov models) [23, 29] to name but a few (interested readers can refer to [19 – 23, 29] for more information).

The question remains: if off-line recognition is such a complex task why are so many researchers seeking a solution to it? The first reason is that gathering a sample for off-line recognition is so much more natural and convenient. An individual can simply write on a piece of paper instead of having to use an unwieldy contraption like an electronic pad and stylus. Secondly, and

perhaps most importantly, signatures remain the traditional means of authenticating common documents like cheques and contracts. So, if we can institute systems capable of automatically matching signatures on these existing, paper-based, documents we will be able to drastically reduce fraud without the massive expense and upheaval of altering existing commercial infrastructures like banks.

On-line signature recognition

Although more work has been done on off-line authentication, it is more appropriate to examine on-line authentication systems as part of this study since these offer a more directly compatible set of advantages and characteristics with physiological systems like fingerprinting or iris recognition. In particular, on-line systems are also designed to operate in real-time and generate instant yes/no decisions. For the purposes of this study, two different types of on-line signature recognition systems will be examined. The first type makes use of an electronic tablet pad and stylus [24, 25] to simulate pen and paper, while the second uses cameras to track movement during the signing process [26, 27].

Sensors

There are two main types of sensors used for signature recognition: scanner–based or camera-based systems. The scanner-based systems are available in a variety of shapes and forms, for example, the tablet pad and stylus combination. Moreover, the tablet and stylus sensors often differ dramatically between manufacturers. For example, the tablet might be used to just capture the static information of the completed signature (its shape and curves) or the speed with which the signature was drawn as well. Similarly, the stylus may have sensors which detect the pressure exerted on the tablet or its angle relative to the tablet [24] while other systems might mount these sensors on the tablet [24]. The other scanner or "pad" type sensor is a pressure pad which works on the same principle as the tablet pad, but the writable area consists of pressure-sensitive sensors which detect the movement of the pen or stylus.

The other type of sensor, the camera-based type, is a novel idea and its inner workings are extremely fascinating [26, 27]. A camera is mounted in a specific position — focussed on the area where the user will sign his/her name. The camera is then responsible for capturing the movements of the pen during the signing process. Once the system has received a video stream of the signing process from the camera, it will start to analyse each frame in order to [26] (i) detect the point of the pen (this can be a complicated process in itself, for instance, if different pens are used the system might not be capable of recognising the pen, see [26] for more information); (ii) track and predict the movement of the pen; (iii) track the speed of writing; (iv) determine the angle of the pen; (v) determine static information (like the shape of the signature etc.).

Feature Extraction

The sensors used normally capture two types of information sets [24, 25]. Firstly, a set of spatial (static) information like the shape of the signature and, secondly, a set of dynamic information like the speed of writing, the angle of the pen etc. Once all of the information has been gathered, it will be passed and represented by a number of different vectors. It is important to note that the signals received from the sensors must first be normalised and smoothed before all the vectors can be extracted. This is again due to the wide variance possible between signatures. A good example of this is the fact that an individual can sign his or her name using any baseline they like (see Figure 4-1 for an example of different

baselines) and , consequently, the signature needs to be rotated first (see [25] for more information).

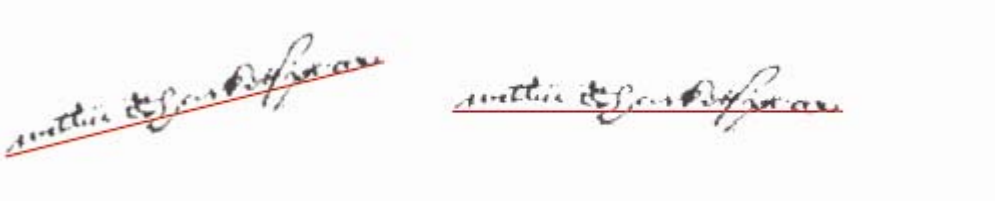

Figure 4-1 Example of a signature using different baselines

Decision making

Once all the features (dynamic and static) have been extracted and converted into vectors, the matching process can begin. Many matching algorithms and techniques have been developed, including Dynamic Time Warping [27] and Hidden Markov Models (an in depth discussion of the available decision making algorithms is beyond the scope of this study, but interested readers can refer to [23, 25, 26, 27, 29]).

Application of Signature recognition

Signature recognition is not a very effective biometric, especially when the system is going to be used infrequently by a person since it is unlikely to be able to adapt its templates to the person's ever changing signature. While this limitation makes it unlikely to break into the market of biometric access control (physical or logical) in the near future, it does stand a great chance of becoming a major tool in fraud prevention. On-line signature recognition could, for example, be used to prevent credit card fraud [18] if the cardholder's signature is stored within the card's magnetic strip and the system can verify the signature of the cardholder, using an electronic signature scanner, before authorising the transaction. Moreover, off-line systems could be used to prevent cheque fraud. In this instance, an off-line system could compare scanned-in cheques against signature templates stored in a database. This type of system could then be easily expanded to cover a wide range of documents.

Moving towards a more modern way of writing, the next section examines keystroke dynamics — identifying a person by the way they type.

Keystroke Biometric

What makes a person's signature unique is that it is affected by their physical and psychological makeup. This uniqueness factor has been almost universally accepted (although never proven) and prompted a large percentage of the biometric community to start hypothesising that the way a person types could similarly be affected by their physical and psychological makeup [31]. A lot of research started to appear on keystroke dynamics and the majority of researchers came to the conclusion that it is a behavioural biometric relatively unique to an individual [30, 31].

Keystroke dynamics overview

Keystroke dynamics can be viewed as one of the cheapest biometrics methods available today [31] since it does not always require specialised hardware. In most cases, a normal keyboard will suffice [31, 66] (although, specialised plug

and play keyboards with hardware and firmware built-in do exist and offer the advantage of being able to perform authentication directly on the keyboard itself).

Regardless of the hardware being used, the sensors will detect the following two main features [30, 31]: the time between pressing the key down and releasing the key, also know as "dwell time", and the time between successive keystrokes, known as the "flight time". Once this information has been gathered the two patterns can be converted into vectors. Once converted, the vectors can be compared to a stored template using the test of statistical independence (see [30, 31 and 11] for more information). Another method developed for keystroke authentication requires training neural networks to recognise a specific typing rhythm; the only problem is that it can be quite time consuming to retrain the neural network to recognise a new user when they are added to the system [31].

Keystroke dynamics applications

The different applications keystroke dynamics could be used for can be divided into two classes: static or continuous authentication [31]. The difference between the two classes is that static authentication only occurs at a specific point in an application, for example, the login screen [31], whereas continuous authentication is a continual process throughout the use of the application [31, 66]. The advantage of the continuous over the static approach is that the application can ensure that the person interacting with it has not change since they logged in [31].

Possible keystroke applications include:

- Login into a computer-based system where the user's username and password could be combined with some other information like his or her name repeated a few times — in order to give the system enough information to perform recognition [15, 31, 66].
- When working on secure documents — the document could be protected by performing verification every x seconds and closing the document if a match is not achieved [31, 66].
- Another interesting application could be if the person operating a computer system needs to be alert all the time [31], should the typing pattern of the person start to resemble a pattern due to drowsiness, the system could issue an alert and attempt to rouse the person.

Speaker recognition

Speaker recognition is a behavioural biometric based on an individual's speech pattern (speech is the result of a complex sequence of transformations occurring at several different levels including: semantic, linguistic, articulatory, and acoustic [41]).

Speaker recognition is quite a large field of study because it is ideal for telephonic transactions [39]. Speaker recognition can be divided into two main areas according to the speech material used: *text-dependent (fixed-text)* and *text-independent (free-text)* systems [38, 39, 40, and 42].

Text-dependent

Text-dependent systems are ones in which the text or words uttered by the user are already known to the system. There are two main ways text-dependent systems work: either by having users remember a specific word or phrase which

has been enrolled into the system [43] or by using a text-prompt system [43]. As the latter's name implies, the system generates an on-screen prompt of the words the user is required to say. In order to increase security, such a system can randomly generate the words and thereby reduce the possibility of an impostor fooling it using an audio recording [43].

Text-independent

Text-independent or free-text systems allow the speaker to say any word, phrase or sentence they want. Although this type of system is, arguably, the most convenient and user-friendly, it is also considerably more complex, [43]. Consequently, text-independent systems require much larger samples for enrolment and recognition (text-dependent systems usually require 2-3 second samples for training and verification while text-independent systems require 10-30 seconds for training and 5-10 seconds for verification [40]).

Basic workings of speaker recognition

A person's voice is affected by features classified as either inherited and learned [39]. Inherited features (also known as static features) are those features that are influenced by the anatomy of a person [39]. These inherited features remain fairly stable (except when a person, for example, has a cold influencing their nasal tract) across the lifespan of a person once they have reached puberty [39]. These features are also very difficult to mimic because they are directly related to the physical build of a person [39].

Learned features or dynamic features are things that are not determined by a person's physical makeup and include things like: speech style, tempo, and other behavioural speech patterns [39].

Normalisation of the voice

Before the features can be extracted, the captured voice sample needs to be cleaned and have all noise, background sounds, and disturbance caused by telephonic transfer etc. removed. This process of normalisation [39] is a feature of facial recognition and other biometrics as well, but what makes voice normalisation so interesting is how the system tries to normalise the time of the sample.

When one is performing text-dependent recognition it is crucial that the time span of the word spoken is the same as the stored template. Repeating the same word at exactly the same length each time can be quite difficult. For example, the word "user" can be pronounced either long or short depending on how the speaker stretches the "u" sound [39]. The system has to allow for this and alter the word entered by the user by enlarging or compressing the sound. This can be accomplished in a number of ways, including: O'Shaughnessy's [39] method of dividing the sample into frames and altering the appropriate frame, the SOLA method for time scaling [9], and Dynamic time warping [39, 40].

Feature extraction

In the previous section, the two features that affect the makeup of the human voice were described, but what exactly is a speaker recognition system looking for in a voice and how does it extract the features?

Some of the features looked for in a voice recording include (refer to [41] for more details):

(i) Intensity of the signal.
(ii) The pitch of the signal (influenced by the vocal cord vibrations).

(iii) The Short-term Spectrum — a three dimensional representation of speech with the coordinates being time, frequency and energy [41].
(iv) Predictor Coefficient — a linear prediction analysis method where the speech waveform is predicted as a linear weighted sum of past samples. The predictor coefficient will be the weight which minimise the mean-squared prediction [41].
(v) Format frequency and bandwidths, the resonance frequency caused by the vocal tract is known as the format frequency.
(vi) Nasal Coarticulation — when a person speaks the sounds produced are influenced by the shape of the vocal tract, but due to the slow movement of the articulators this shape is not only dependent on the current sound being produced but also the previous sounds, this occurrence is known as coarticulation. Nasal Coarticulation is coarticulation that occurs when a person produces nasal sounds (see [41] for more).
(vii) Spectral correlation — a high correlation exists between short tem spectrums at different frequencies.
(viii) Timing and speak rate.

An in depth discussion on exactly how the above mentioned features or parameters are extracted is beyond the scope of the document, but the process makes use of techniques like: linear predictive coefficients (LPC), amplitudes of filter bank outputs, and fundamental frequency-F0s (interested readers can refer to [37 - 42]).

Decision making and learning

As with most biometrics, a large number of different decision making algorithms are available for speaker recognition, but most rely on statistical difference using either Euclidean and Mahalanobis distance (see [37 – 42] for more in-depth discussions). The learning aspect of the decision making process is nonetheless very interesting.

Although a physical characteristic like the nasal tract can influence the voice [39], speaker recognition is classified a behavioural biometric. This is because the characteristic being measured has the tendency to change. The voice, in fact, is one of the most easily influenced characteristics being subject to the influence of a person's emotional state [40], any biological factor that affects the vocal cords and age. As a result of this, a speaker recognition system constantly has to teach itself (re-enrol almost) in order to accommodate the changing person.

Figure 4-2 gives a representation of the learning cycle during recognition [40]. When a voice sample is given it is first normalised and then passed through to the feature extraction phase. Once the input is ready for recognition, it is passed to the decision making module which will generate a yes/no decision. If a yes is received the template that was matched will be updated with the new information gathered from the input. If a no decision is reached, the system can (i) retrieve the next template and try the decision process again (if performing identification) or (ii) simply return a negative match (if attempting verification).

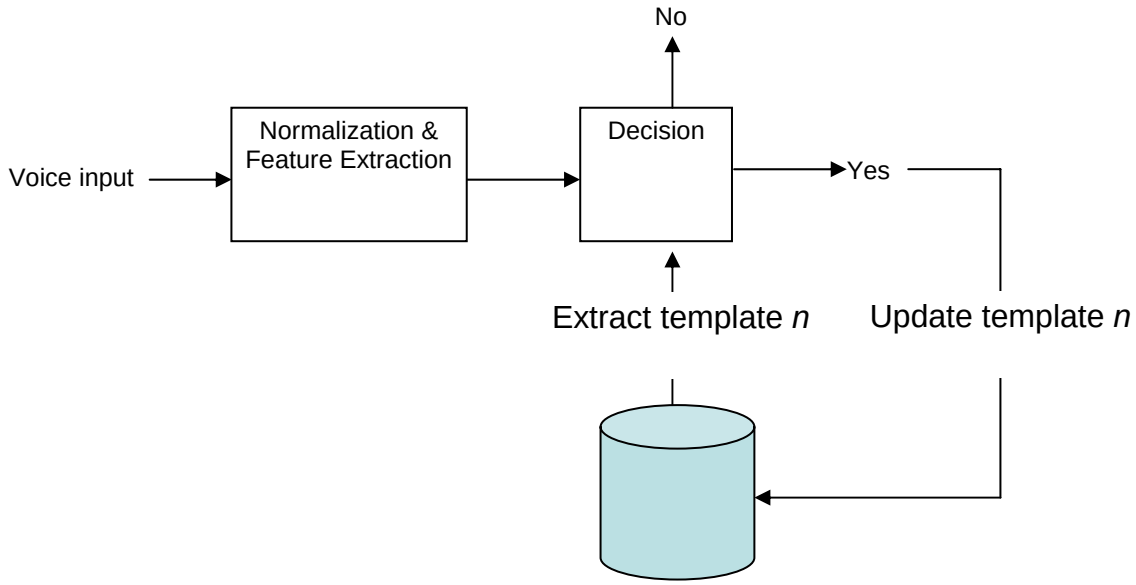

Figure 4-2 Recognition and learning process. Adapted from [40]

Conclusion

In this and the preceding chapter, the main physiological and behavioural biometrics have been reviewed and it has become apparent that the inner workings of behavioural biometric systems are usually a lot more complex than physiological systems. A necessity attributed to the fact that a person's behaviour can be dramatically influenced by their emotional state and, consequently, such systems have to try to compensate for such changes. Most behavioural systems try to resolve this issue by dynamically re-enrolling a person on each use — as in Figure 4-2 – a process that often results in a completely different template to the original being stored. Physiological systems are therefore generally much easier to develop than behavioural systems because it remains easier to train an individual to use a reader (for example, a camera or fingerprint reader) than to develop software that models a human being's behaviour.

Chapter 5 Biometric Applications: Picking the right biometric.

Introduction

Although biometrics can be used in many creative ways, the main function of a biometric is identification or to perform a match between two biometric samples. Despite performing such a seemingly simple task (identification) that it is mostly deemed a supporting task, it would be unwise to merely pick any biometric and use it. Before one can implement a biometric, a business case needs to be created to determine whether the use of a biometric is justified [1]. According to Wayman [1], biometric systems are often not adopted, not because of technical inabilities, but because the business case was not sufficient to justify the use of a costly biometric above alternatives that might be faster, cheaper and easier to integrated into existing systems.

This chapter will examine some of the external factors — in addition to justifiable business case — that affect the working and acceptability of biometrics in the implementation environment.

Three areas of concern

Wayman [1] and others [66] suggest a number of different things one has to look at to determine whether or not a biometric will work in a specific environment. For the purposes of this discussion, these concerns have been assembled into three groups:

- Application specifics;
- Environmental;
- People.

As well as assessing these three factors, this chapter will conclude with an implementation example — designed to illustrate how these factors should be considered during deployment of a biometric — for positive identification in grant payments.

Environment

The environment needs to be assessed from two perspectives:

1. The environment within which the system will reside and operate;
2. The working/living environment of the people using the system.

The environment within which the system will reside and operate

One of the key factors to be considered when installing any equipment is the environment it will be used in. Typical questions to ask would include: whether it be exposed to extreme heat or cold; whether it will be exposed to large amounts of dust etc. This observation holds true for biometrics, but there will be some specific factors that require consideration when installing biometric systems. The first question one has to ask when installing a biometric system is whether the system will be placed outside or inside [1]. If the system is going to be placed inside many of the problems experienced in external environments are removed. The main environmental factors (some experienced inside and others outside) to consider are: lighting and dust/dirt.

Lighting

Different biometrics are affected differently by environmental factors. Some factors can cause a biometric system to fail completely and others will have no discernable effect. Lighting is one factor that often breeds uncertainty: will there be enough light for the biometric to function or will there be too much? Biometrics that can be heavily affected by light include: facial recognition [32] and iris recognition [4].

A live testing of iris recognition undertaken by the author proved this point. In order to investigate the validity of using iris recognition in rural areas (where operating and maintaining fixed biometric sites would be prohibitively expensive), the system was tested in the veldt. The remoteness of the locations and ruggedness of the terrain precipitated the use of 4X4 vehicles to gain access. The smallest assembly was opted for — in this case the Panasonic Authenticam and a Laptop — to reduce storage space and improve ease of transport. Since it was assumed direct sunlight could be an issue, a marquee tent was erected to provide shading. Despite the tent, the initial attempt at enrolling and recognising users was a complete failure. The system did not capture a single sample for us to perform recognition on. Using the system's feedback window, the images being returned by the camera were closely examined.

At first glance, the images being returned seemed sufficient, but it soon became apparent that the subjects' eyes were too well lit. The human iris is protected by the cornea, a transparent protective membrane, but this membrane also reflects a certain amount of light (see [44] for more details on spot reflection and the countermeasures taken to overcome the problem). During the first testing phase in the marquee, the reflection generated by the cornea was so much that a large percentage of the iris was simply a bright glare. A closer inspection of the tent revealed that, while it provided some shade, a lot of light was still coming in through the windows (which had been closed using net curtains) and through the material of the tent itself. The marquee was constructed from a very strong plastic like material with a high shine factor. This shiny surface, combined with its reflective white colouring, caused the light within the tent to bounce off the walls; a condition responsible for the unusually bright glare affecting the camera.

Once the cause of the glare had been isolated, it was possible to create more suitable ambient lighting conditions by placing additional curtaining around the inside of the entire tent. The enrolling of users proceeded successfully once the environment had been managed correctly.

Dust/Dirt

If a biometric sensor is being used in a very dusty environment, not only are any moving parts at risk of being damaged, but dust build-ups can affect the accuracy of the biometric. Fingerprinting is a good example of a biometric technique that can be affected by dust. The build-up of dust and grime on the sensor could affect the quality of the print provided. In [14] Jain, Prabhakar and Ross estimate that dirt and oil will have a medium effect on the quality of fingerprint captures.

The work/living environment of the people using the system

It is also important to understand the environment users of the system will be working in to determine the best biometric. Failure to anticipate the operational environment for the application could lead to high failure rates because either the type of work users are doing and/or the environment they are doing it in

damages the required biometric feature or hinders its capture. Things to look at include: dust, humidity and temperature, equipment and tools used to perform work, chemicals and other fluids.

Dust

The effect of high levels of dust has already been stated, but it is important to note that, even if a system is not going to be placed in an area where dust and dirt will be an issue, if the biometric in question (for example, finger) is covered with dirt the sensor might experience problems providing a good quality biometric sample.

Humidity and temperature

Humidity can affect certain biometrics, usually those which involve touch, like fingerprinting. In fingerprinting, for instance, the humidity of the environment can affect the dryness of the user's hands and fingers. In [14] examples can be seen where fingers give different readings when they are moist and when they are dry, thus affecting authentication.

Equipment and tools used to perform work

The human hands are perhaps the oldest and most frequently used tools of all. Consequently, the hand has to withstand the trials and tribulations of a normal day's work. As mentioned previously, with a biometric like fingerprint recognition, cuts and bruises will have a high effect on the quality of the sample given [14].

Chemicals and other fluids

Chemicals and other fluids fall into the same category as tools and equipment used, but because these substances can also cause damage to the human hand — for example, acid dissolving a fingerprint pattern — they are important enough to raise in their own right.

Another important point to remember is that chemicals or fluids can damage a sensor as well. Someone who has been handling chemicals, especially acidic ones, will go to some effort to remove the material from their hands, but might not anticipate the damage that could be done to the sensor. Diesel, for example, might not damage a person's skin, but could a biometric sensor.

Having looked at the environmental factors around them, attention must now be paid to the people using the systems themselves and, in particular, why the acceptance of biometrics systems may be hindered.

People

There are usually two different types of biometric systems users: those actually using them and the operators maintaining them. Since the operators will very rarely be required to present biometric samples, this section will focus on the people required to use them. In [66], people-related concerns were identified as a major hindrance to the acceptance of a biometric system. The issues raised can be divided into three main areas:

- Informational privacy;
- Physical privacy;
- Religious objections.

The three issues above are what might be called "emotional" issues since they are driven by fear — a fear of lost privacy or a fear of physical harm. While important, there are "non-emotional" people-related issues that need to be

included and so a fourth point entitled that has been added to this list (see below).

Information Privacy

Woodward, Webb, Newton, Bradley and Rubenson [66] identify three main concerns relating to information privacy. The first is "function creep" — the process of using information for something other than what it was initially intended for [66, 84, and 85]. The second is "tracking" since a lot of people feel that, given access to a large amount of information relating to a person, governments could start to develop into "Big Brother" institutions capable of tracking a citizen's every move [66, 85]. The final concern raised under information privacy is the misuse of data [66]; the capture and replay of a biometric in an online environment or even reproducing the biometric, for example.

Physical Privacy

Issues relating to physical privacy include: stigmatization; actual harm, and hygiene [66].

Stigmatization

A lot of biometrics have a certain stigma attached to them and can deter people from using the system [85]. Fingerprinting, for example, has an undeserved stigma from association with criminal activities [66, 84]. For years fingerprinting has been used by the criminal justice departments to identify criminals who could have been at the scene of a crime [84] and, because of this, people feel that they are being criminalised when asked to give a fingerprint — especially when this fingerprint submission is a mandatory event [66].

Actual harm

Concerns relating to actual harms can be divided into two areas. The first is damage to an individual from the scanner, for example, the laser used in retinal scanning [66, 85]. The second concern is when individuals fear that an impostor might want to sever a limb, like their finger, in order to fool the system [66, 85].

Hygiene

A concern often raised about working with touch-based biometric scanners is the transfer of illnesses [66, 84]. If, for example, hand geometry is being rolled-out to a large population group it might be rejected because of the fear of diseases, like AIDS, being transferred by an infected person with a cut hand using the scanner. However, not only touch-based systems generate this fear. Members of the iris recognition industry are often asked whether eye diseases like "pink-eye" can be transferred by the camera.

Religious objections

Different countries have different cultures and religious beliefs, and people will reject anything considered contrary to their cultural or religious dictates. A lot of Christians, for example, believe biometrics represent the "Mark of the beast" as described in Revelation, 13:16–18 [66, 84, 85] and this could end up prohibiting their use.

Non-emotional Factors

Physical build of the people

The prevalence of some disabilities and diseases amongst a system's users is another important consideration. Taking iris recognition as an example, users obviously require an eye with an iris so individuals who suffer from aniridia will be unable to use the system. Aniridia is an eye disease characterised by the lack of proper iris development [81]. People who are blind may also find it difficult to use iris recognition since most systems require the user to place their eye in the correct location using visual aids (lights or mirrors). Similarly, people suffering from pronounced nystagmus — involuntary tremors or shaking of the eyes [80] — may experience difficulty presenting a stable iris image since their eye is constantly moving. If the system is to be used in a location showing high prevalence of the aforementioned illnesses or disabilities, it might be better to use a different biometric, for instance, fingerprinting.

Another important consideration when installing a biometric is whether people will be physically able to access/reach the system. Using the example of iris cameras again, while these cameras are normally mounted at eye-level for normal users, can the system also accommodate midgets or people confined to wheelchairs whose eye-level could be considerably lower than that of an average user?

Education

When selecting an appropriate biometric, the level of training the population group will require to use the system needs to be ascertained. If, for example, the population group has not been exposed to high levels of education or similar systems, the implementers might have to undertake extensive training programmes. In such instances, it may prove more viable to utilise a simpler system which requires minimal, if any, training.

This can be an important consideration even in the case of systems traditionally deemed easy to use. For example, a fingerprint sensor is generally accepted as very straightforward to use, but, if taken to a rural African village which contains people who have never seen a radio or television let alone anything as "high tech" as a fingerprint scanner, teaching the people how the system works and to use it might require a substantial investment. Another good example of this is signature recognition where a foundational requirement is the ability to write.

Application specific factors

Once the environment and individuals the system will be applied to have been assessed and understood, the biometric method itself has to be related back to the ascertained environment to ensure it is appropriate. For example, if the application has to identify individuals (one-to-many search) in a population size in excess of 1 000 000, the biometric feature must be highly unique. Hand geometry, for instance, would not work since about 1 in every 100 people [4] have the same hand geometry. Wayman describes some of the factors that need to be considered in [1] and the most important of these have been summarised below.

Errors

It is important to "step back" from the application and critically assess the possible errors the system can produce, as well as the rate of errors produced.

The main errors to investigate would be likely enrolment errors and false accept/reject errors.

Enrolment errors

Being the first point of contact between the system and the user, enrolment errors are a critical part of assessing any biometric system. Studies conducted by the Centre for Mathematics and Scientific Computing National Physical Laboratory [5] observed that, during enrolment, certain systems like voice and fingerprinting sometimes required multiple attempts before a good enrolment template was achieved. Enrolment errors like the one mentioned above can precipitate an average enrolment time of between 2 to 5 minutes just capturing the biometric template — not to mention all the personal information of the individual. If enrolment takes 3 minutes per individual, and there are 100 000 users to enrol, it will take ± 209 days working 24 hours a day (3 min x 100 000 users = 300 000 minutes / 60 = 5000 hours / 24 = 208.33 days). A lengthy enrolment process like this could be unacceptable for certain applications [1], especially if the application requires all individuals to be enrolled before becoming operational.

False accepts and false rejects rate

The fundamental function of a biometric is to compare a newly captured biometric sample with an enrolled template and find a match. In other words, the function of a biometric system placed, for example, at a gate is to control access by ensuring that unauthorised personnel are kept out and authorised personnel are allowed through.

The *accuracy* of this process is measured by its false accept and false reject rates. False accepts, as the name implies, occur when the biometric system accepts a person who has not been enrolled in the database. And false rejects occur when a person who is enrolled is not identified. The false accept and false reject rates thus measure the decision errors for the system [5].

Most security officers will focus mainly on the false accept rate, to ensure that no unauthorised individual is given access. But a biometric which constantly rejects authorised individuals, a PC-based logon, for example, will not be used for long. When picking a biometric for a system, developers have to look at the possible false accept and false reject rates of the biometric system. Usually, nonetheless, the false accept and false reject rates can be altered by adjusting the system's decision criteria (moving the threshold which has authentic users on one side and impostors on the other). The only problem with adjusting the decision criteria is that limiting the number of false accepts often increases the false reject rate (see [5]). Consequently, the system developer has to determine what level of false accepts is acceptable and what level of false rejects is acceptable. Again, it is important to examine the environmental context when looking at false accept/reject rates for possible impact. For example, dry conditions experienced in winter can affect the quality of a scan and, consequently, the false accept/reject rates.

Ease of use

An important question to ask is: how easy is it to use the biometric system? When looking at the usability of the system the first factor to determine is whether the system will be mandatory or optional; either options raising its own issues.

Mandatory

If a system will be mandatory, for example salary payments or physical access control to an office block, the organisation has to look at the amount of training which will be required for their personnel. If the system is difficult to use and a lot of training is required, the cost of implementing and maintaining the system increases. This increase in cost could justify the purchasing of a more expensive, but easy to use and reliable system, for example, iris recognition.

Optional

When a system is optional people often have to be "bribed" into using it (by giving them some sort of benefit). For example, replacing username and passwords with a biometric will increase the level of security for online banking, but if the system is difficult to use it is likely to be rejected and the only way people will move from the convenience of usernames and passwords will be if, for example, the charges are lower.

Frequency of use

The frequency of use by the users almost falls within the ease of use discussion above. However, the frequency of use by a system will determine if the system is a habitual or non-habitual system [1]. This is important because if a system is non-habitual, the time spent using the system could increase because users forget how to and need to be retrained. It is therefore important when installing a system that is considered non-habitual to ensure it is as easy to use as possible.

Also, as mentioned previously, a behavioural biometric does change slightly and the system usually adapts itself for this change by re-enrolling an individual each time they are recognised. If the system in question is non-habitual and used only once every three months it (the system) would not be capable of adapting enrolled templates (re-enrolling) to a sufficient degree to prevent a false reject.

Template size

Template size becomes a serious consideration when there could be storage limitations [1]. Of particular importance is the fact that not all biometric templates can fit on a magnetic stripe card or smartcard [1]. It must also be remembered that some biometric techniques — like template-based facial recognition systems [32] — use more than one template.

User throughput required

If a biometric system is installed at, for example, an airport's passport control it is quite important that the biometric system be capable of processing a large number of individuals quickly. It is therefore important, once the need for a biometric system has been identified, to determine the number of users the system has to handle in a specific time frame [1]. The amount of people a system can process, for example, per hour, will also affect the decision on how many sensors need to be installed in one area. In the end, the system selected might not be the quickest, but the most cost-effective (budget plays quite an important role as mentioned by Wayman [1]). For instance, 20 fingerprint sensors might deliver the same throughput as 5 iris cameras and be considerably cheaper.

Security level required

The security level required by the system is perhaps quite an obvious aspect to assess when dealing with biometrics, but specific factors to consider include:

- Security requirements when transmitting over the net (encryption levels and replay prevention);
- The ability to "trick" the biometric (ensuring that live samples are used);
- The uniqueness of the biometric (number of degrees of freedom).

The following case study has been included to illustrate how the considerations discussed above can be applied in the field.

Case Study

The Payment Problem

Over the years, Africa has been struck by numerous disasters including droughts, insect pests, exhaustive farming of the lands, ruthless dictators, civil wars etc. Due to these incidents, large parts of Africa have been left famine stricken, disease ridden and in poverty (refer to [52] for rural poverty and income distribution in South-Africa). A lot of countries and organisations are, fortunately, helping Africa with food and monetary aid, but it is a huge and ongoing problem.

Moreover, the donations of money and food often don't reach the people who need them most because of corruption at a political level or because rife fraudulent 'double aid' claims deplete resources. Consequently, aid suppliers are starting to demand that mechanisms are put in place to ensure that aid payments are made to the correct people and only once per payment cycle.

The Proposed Solution

To assist aid suppliers, a system must be implemented to positively identify the people to whom the aid is to be given. This will also aid them in tracking payments made during a specific payment cycle. It is suggested the proposed solution will need to be mobile due to transportation and infrastructural problems. There are two main business requirements for such a pan-African payment solution:

1. Positive identification and tracking (accomplished in this instance by making use of a biometric), and
2. The solution must be mobile and capable of going into different areas of Africa.

The system can be defined as follows:

"A biometrically-enabled, mobile aid payment system designed to bring aid to the underprivileged people of Africa. This system will help prevent fraudulent payment and ensure that aid reaches the right people."

The system will be a publicly accessed system, available across the continent and must, therefore, be capable of:

- Containing a central biometric database for all the enrolled people;
- Being mobile and not permanently linked to the server (thus a biometric database is required at each payment station);

- Handling a "representative" (a person(s) who can accept payments on behalf of someone not capable of reaching the payment centre);
- Ensuring that payment occurs only once per payment cycle (be it weekly or monthly);
- Ensuring a high throughput of people during payment, and
- Reconciling nightly any payments made.

Developing the system

As mentioned at the beginning of this chapter, the first step when developing a biometric system is to select an appropriate biometric by analysing key factors.

Analysing the Factors

Environmental issues

One of the main requirements for the system is that it needs to be portable and operate in a wide variety of areas, from city to bush. These factors are, at best, difficult to control therefore it is important to demonstrate a best and worst case scenario and analyse the associated problems therein.

Best case scenario:

- a fixed structure/building e.g. town hall;
- constant stable energy supply;
- controlled temperature and humidity according to specification;
- correct lighting;
- dust-free.

Worst case scenario:

- rural areas, no fixed building e.g. erect a tent;
- no steady power supply;
- payments will be made all year round, thus variances in temperature and humidity will be great;
- possible dusty areas;
- variances in light.

As demonstrated, the environment for the payments system will be a "living" environment (constantly changing) and require the system to be able to handle varying climate conditions (temperature and humidity) as well as dust and light.

Environmental factors

Since the payment solution will be implemented at various locations it is impossible to stipulate that it will only be used by a certain subset of people (performing one specific job or living in one specific area) and so varied work and living environments must be factored in.

Work

Some of the jobs held by rural area dwellers can be seen in Figure 5-1. From the figure it is apparent that the largest percentage of jobs held by rural dwellers are jobs which require manual labour e.g. farming. There is also a high number of artisans and construction workers.

Living environment

Living conditions in the areas will differ substantially, from modern brick houses to corrugated iron shacks or even traditional mud huts [51]. Areas surrounding the houses are usually small with some vegetables grown to provide food for the family [51]. A lot of the areas suffer from water shortages due to bad infrastructures, low rainfalls and environmental erosion [51]. The areas are predominantly dry and dusty. It is also important to note that water will often be collected in 25 litre drums by the women and children from water points which can be miles away from their homes [51]. Household sanitation levels are extremely low, with people often making use of unhygienic pit toilets [51].

Turn Page

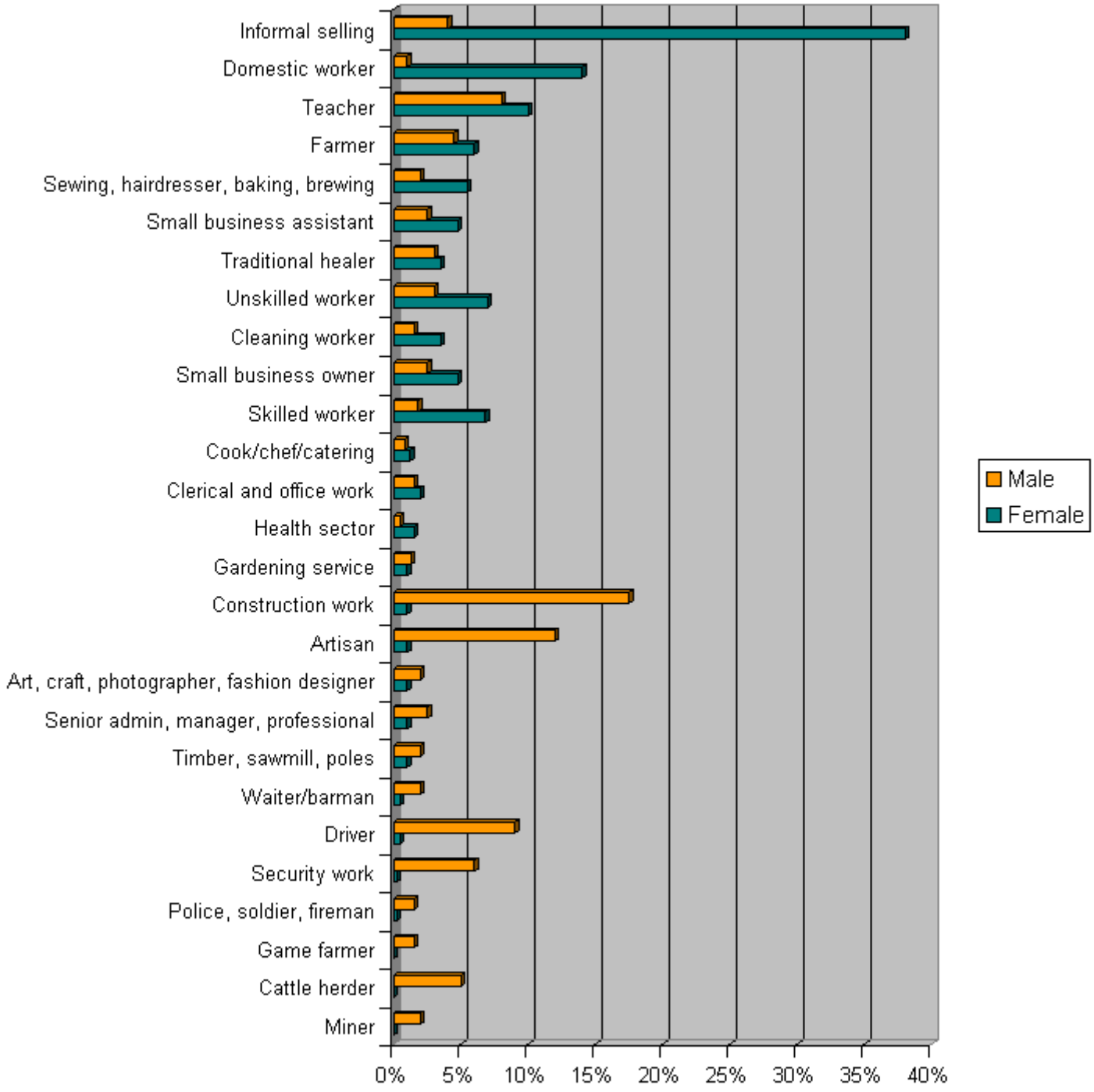

Figure 5-1 Different type of work perform by rural residents in South Africa (adapted from [51]) (Refer to the Appendix 1 for a colour version of the figure)

The above analysis of the working and living environment suggests that the subject population are likely to perform a lot of manual labour, fetching water, farming and such. Consequently, the hands and fingers of individuals could potentially be damaged due to these large amounts of manual labour.

People

Culture and religion

In Africa there are a large number of tribes with varying cultures and religions, for example, Shangaan, Pedi, Swazi and Zulu. Making provision for the education of those using the payment system will be crucial because the system will have to cope with numerous religious and cultural belief systems.

Health

Due to the high poverty and illiteracy rates in Africa, health problems and the spread of diseases is phenomenally high. Life threatening diseases such as HIV/AIDS prevail across all age group and sexes, with a multitude of other communicable diseases following [51].

Education level

The education level of the people will vary, but the main aid recipients will have an extremely low level of education. In South Africa, Collinson and Wittenberg [51] gather the following data on the education level in rural areas:

- 40% of adults aged 25-59 have received no formal education;
- 6% of people have completed secondary school and only 3% went on to some form of post-secondary education;
- Almost all the people in the age group of 15-24 have attended primary school, but only 46% enrolled into secondary school;
- Adult female literacy is about 56% and adult male literacy round about 62%.

Psychological stigma

There are many stigmas attached to biometrics anyway, but it is likely that many aid recipients will have never seen a computer and, consequently, may be scared of the technologies involved in the system and reluctant to use it.

From the above discussion it would appear important to select a biometric that will not be offensive to the religious and cultural beliefs that are likely to be encountered. The system also needs to be relatively easy to use since education levels are likely to be low for a large size of the population. The biometric also needs to require limited touching because of the high prevalence of communicable diseases and the fear (which may be ungrounded in most cases) of contracting a disease from the biometric sensor.

Application specific factors

The application specific factors can be divided into the main stages of the system. These stages will be: enrolment, recognition & payment, and reconciliation.

Enrolment

The requirements for the enrolment stage are:

1. The system will be a public system and used by a large amount of people so multiple enrolment stations will be required.
2. The enrolment station needs to be mobile in order to reach all people especially in rural areas.
3. "Representatives" will be used by individuals unable to make it to the payment station so the person and his/her "representative" will need to be present during the enrolment.
4. To prevent a "representative" from claiming the aid and not handing it over to the intended recipient a "representative" account will only be valid for a certain amount of time.

5. Each enrolment station needs to upload its entire enrolment database of biometric templates to the central server on a nightly basis.
6. Each enrolment station needs to update its biometric database from the central server to ensure that it has all the enrolled templates and not allowed any double enrolments.

Recognition & payment

Requirement for the recognition and payment stages are:

1. Ensure a high user throughput to avoid lengthy queues.
2. Ensure that payments are only made once per payment cycle per person or "representative".
3. Ensure payments are made to the intended recipient by using a biometric-based recognition system.
4. Backup identification mechanism in case biometric recognition cannot be performed.
5. Payment logs will need to be kept.

Reconciliation

Reconciliation requirements are:

1. Reconciliation nightly to the central server (informing the system who received payment at which payment station).
2. All payment stations will need to download the reconciliation log if payments span multiple days. This is necessary to ensure that a person who has received payment at one station does not travel to another and receive another payment.

Most of the application specific considerations for selecting a biometric have been highlighted in the requirements of the main sectors (enrolment, recognition & payment, and reconciliation), but because it will be a public system used by a large number of people, the system will also have to be easy to use and have a very small "footprint" i.e. a small template size. This is because the enrolment stations and the central server need to synchronise every night and the biometric sample for each payment in the log needs to be uploaded as part of the nightly reconciliation process.

All the concerns discussed above have been summarised in Table 5-1 to provide an overview of what is required from the biometric system.

Application specific factors	Environmental	People
Must handle large population size	Sensors and supporting equipment must be small	Non-invasive (limited touch)
Must be easy to use	Will be subject to varying weather conditions	Easy to educate people to use
High user throughput	Will be exposed to lots of light	The least "offensive" biometric
Small template size	Lots of manual work done by users	
High security level	System will exposed to dusty environments	

Table 5-1 Summary of biometric requirements for payment system

Once the requirements have been established, the most appropriate biometric for the system can be identified. This task can be achieved by short

listing a few biometrics and then rating them against a checklist (decision Table 5-3) to see which one gives the highest score.

Setting Up a Decision table

Short listing Fingerprint and Iris

Looking at the requirements for the system, one of its main features is that it will be a public system which will be used fairly regularly, perhaps once a month or week. From this, it can be deduced that the user population size will be a relatively big and that the users will be non-habitual.

These two factors eliminate behavioural biometrics like signature and voice recognition because these systems need to re-enrol a user on a regular basis (see chapter 4) in order to reach peak performance; hence it is more suited to applications that are habitual and used on a regular basis.

Secondly, biometrics which cannot handle large numbers would be equally unsuitable and this eliminates facial recognition because all faces are, basically, made out of the same facial structures in almost the same geometric positions [32]. Similarly, hand geometry would be excluded because about 1 in every 100 people has the same hand geometry [4] in a large population of say 1 million this would mean that 10 000 individuals have the same hand geometry which could give you an unacceptable false accept/reject ratio.

For the remainder of this discussion, fingerprint and iris will be short listed because they are both physiological biometrics (re-enrolling is unnecessary) and both can handle large numbers (see chapter 3).

Application factors

High user throughput

Table 5-2 compares the amount of users matched per minute by fingerprinting and iris recognition. In the table there is one iris solution and three fingerprint solutions. Two of the fingerprinting solutions use a chip or solid state sensors; the other makes use of an optical scanner. This table establishes that the fingerprint-chip (2) and iris recognition solutions can perform a high enough amount of matches per second.

Biometric	Matches per minute
Fingerprint-chip	60
Fingerprint-chip (2)	2,500
Fingerprint-optical	50
Iris	1,500,000

Table 5-2 Comparison of times taken for comparison [3]

Small template size

The template size for fingerprints varies according to manufacturer. Opticon technologies[4], for example, produce a template size of 451 bytes per finger; the Verid+™ system from TSSI[5] uses a template size of 52 bytes. The iris system has

[4] http://www.opticom-tech.com
[5] http://www.tssi.co.uk

a template size of 512 bytes [49] thus both systems require relatively small template sizes and will be ideal for the application.

High security level

It is relatively easy to falsify the human fingerprint in order to fool a fingerprint sensor. By making use of gelatine, similar to the type found in sweets, a plastic mould can be made to create a fake finger. This plastic mould is also relatively easy to make; for example, you could take your fingerprint and have it printed on a copper circuit board to create a stencil or mould. Consequently, the fingerprint system we select (if the fingerprint route is opted for) needs to check for a living finger by checking the sample's temperature, for a heart beat etc.

Fooling an iris system is relatively difficult; not only is the eye very rich in detail, but the apparatus required to fool the iris system is extremely bulky and impossible to conceal from the system's operators. For this reason, iris is a much more secure system than fingerprinting.

Sensors and supporting equipment must be small

Both fingerprint and iris recognition use small sensors (although exact size depends upon the hardware manufacturer used). The supporting equipment for both systems is likely to be a PC (which stores the templates and recognition software). So both systems are small enough to provide the mobile solution required.

Environmental

Will be in varying weather environment

Fingerprinting may struggle to deal with varying temperature conditions. During the rainy season, for example, a person's fingers may be relatively moist and produce good fingerprint readings, but during the dry season, the same person's fingers may produce bad readings [14]. The human iris, on the other hand, is not affected by changing weather conditions.

Lighting

The effect of light on the fingerprint system will vary depending on the type of sensor used. If the sensor is an optical sensor it could be affected by light, but most solid state sensors are not affected. Iris is affected by lighting conditions and requires a controlled lighting environment.

Manual work

Fingers can be damaged relatively easy, especially in a manual working environment. The ridges on the finger can be rubbed off if friction is applied to the finger — effectively leaving the person 'without an identity.' And, as pointed out in [14], damage to the finger affects the quality of the fingerprint read quite dramatically. The iris is a more robust biometric — if for no other reason than how seriously people will try to protect their eyes.

Dust Implications

As mentioned previously, fingerprints are affected by dust [14], particularly if it is on the sensor. The same holds true for iris recognition, if the camera lens is

covered in dust there will be a high error rate, but the dust build-up needs to be much more severe to affect iris recognition.

People

Non-invasive (limited touch)

Fingerprinting requires a person to touch the sensor to get a reading. For hygiene reasons, this may not be best suited to the current African health climate. Fortunately, iris recognition, in itself, requires almost no touch (the only time you would have to touch it is if you want to adjust the height of the sensor). Although the Iris sensor requires no touch some individuals may still be afraid to place their eye in front of the sensor, but this number would be a lot less that with fingerprints.

Training

Both systems are relatively easy to use, especially after a few uses (which will be required for enrolment).

The least "offensive" biometric

Fingerprinting has criminal connotations and can, therefore, be labelled as being offensive. With iris, there are very few psychological stigmas attached since it is a simple photograph being taken.

	Fingerprint	Iris
Large population size	✓	✓
Ease to use	✓	✓
High user throughput	✓	✓
Small template size	✓	✓
High security level		✓
Sensors and supporting equipment must be small	✓	✓
Resistant to varying weather conditions		✓
Resistant to light	✓	
Manual work		✓
Dust implications		✓
Non-invasive (limited touch)		✓
Training	✓	✓
The least "offensive" biometric		✓

Table 5-3 Summary of the results (Decision table)

Looking at the above table, it is clear that iris recognition outperforms fingerprinting when it comes to a mobile payment system and would be the best choice for the proposed rural payment system (see Table 5-3).

Conclusion

There are a lot of new and exciting applications that make use of biometrics for positive identification and the need for biometric applications is being boosted by increases in identity theft. As a result, not only are there many different biometrics available, but many have already been successfully integrated into

mission critical systems. In each instance, nevertheless, the same fundamental question must always be answered: which biometric is best? The answer must be the one that suits the solution's needs and budget the best. Cost vs. accuracy charts and many other aspects need to be considered. Picking the right biometric can be a lengthy process because developers need to ensure the system can perform the required function to a predetermined performance level, is fool-proofed and environmentally appropriate.

Chapter 6 Biometric Authority - The Model

Introduction

At the beginning of this study, the following problem statement was given:
"***How should we implement a biometric solution to allow a user to select their biometric of choice and use this biometric to facilitate authentication across a multitude of applications?***"

Having looked at the field of biometrics in general, it is now possible to address the above question by developing a model. In order to do this, the problem statement, and what it implies, needs to be thoroughly assessed. Upon closer examination, the problem statement can be divided into two distinct problems. Although separate, the one will, nevertheless, dictate how the other should be accomplished. The first problem that needs to be addressed is: how can we integrate a single biometric into a number of different applications? Once that issue has been resolved, the second problem is: how to shape this integration so that it gives users the freedom to choose their preferred biometric?

Expanding the problem statement

The problem statement requires that the architecture of any proposed model allows a single biometric to be integrated into a multitude of applications, and in such a way that a user can select their biometric of choice. This 'freedom of choice' allows for the creation of a number of uncertainties and so the problem statement needs to be restated. In order to allow for the sporadic randomness found in human nature, the problem statement should be reformatted as follows:
"*How should we implement a biometric model which will allow us to integrate a single biometric into a number of applications as well as allowing us to integrate multiple biometrics into a single application?*"

This new problem statement allows a user to pick any biometric (so long as it follows the prescribed model) and use it in a single application or multiple applications. The last criteria that needs to be added to the problem statement is the storage medium required. Will it be a central database containing all the templates or will it be a single storage device per user like a smartcard or magnetic stripe card?

Central database vs. single storage device (smartcards)

Without going into a detailed technical study of databases and smartcards (the main focus in this study is the biometric model), this section will briefly motivate using a database over a single storage device like a smartcard (it is referred to as a single storage device because only one user's templates will be stored on it).

Both storage mechanisms, databases and smartcards, have undergone years of research and development and thus both mediums are very secure and effective so for this comparison we will not be looking at the security and protection mechanisms (encryption techniques, firewalls, etc.) of the data within a database or smartcards. Firstly we will look at some negatives of a smartcards and a database approach, after this discussion we will look at some positives associated to each approach.

Smartcard negatives

The first negative we will look at for smartcards or single storage devices is a false database. A false database is one which has been reproduced or fabricated by an impostor, but will be viewed as legitimate by the system. For example, a system which makes use of fingerprinting and stores templates on smartcards carried by the users could be compromised by an individual who has knowledge of the biometric enrolment and card generation processes being used. Such an individual would be capable of producing fake cards i.e. a fake or false database. This could allow unauthorised individuals to pass as legitimate users since they would be carrying 'valid' cards (their own biometric templates being stored on the card).

The second negative is that the smartcard can be lost or stolen and would thus require the reissue of a new card to the individual not only will a cost be incurred by the individual but he/she will have to go through the trouble of re-enrolment. The next negative is the possible damage or corruption of data on the smartcard which will once again result in re-enrolment and reissue of a smartcard. The Fourth negative is the memory limitation of a smartcard and other single storage devices; a smartcard can only contain a limited amount of data ranging from 8k to 1 Megabyte or more [82]; this could be a limiting factor for biometric template storage.

The next negative is limited upgradeability, say for example in the unlikely event that a individual or group is capable of falsifying smartcard as described previously the issuing authority might want to change their encryption technique etc. In this event all the smartcards already issued will have to be recalled and either reprogrammed or reissued.

The last negative we will look at for this discussion is the prevention of dual enrolment; this is when for example an individual tries to enrol multiple times with different identities. By only making use of smartcards there is no way the authorities can biometrically check to ensure the person has not enrolled twice but would have to rely on traditional identification mechanisms such as driver licenses, passports etc. all of which could be falsified.

Database negatives

The first negative we have with a database approach is the possible loss of privacy since an individual's data will be kept in a central location; please refer to the following chapter for a more detailed discussion of privacy. The second negative is cost, a database would be expensive to setup and maintain due to license issues and required maintenance to ensure the database is available 24 hours a day. Since a database is only useful when individuals can connect to it and make use of the data in it the third negative we are faced with is the reliance on network availability, if the network to the database is down the client systems will come to a stop. The last negative we will look at for a database approach is the possibility of data corruption which could result in the re-enrolment of a number of individuals unless proper backups were in place.

Having looked at the negatives associated to the two storage media we can now move on to the positives.

Smartcard positives

The first positive we will have with a smartcard system is a greater feeling of privacy since the individual will be in control of his/her own biometric data stored on the card. The second positive is that the smartcard card system will be

relatively cheap to setup and maintain. The final positive is that the smartcard system can act independently i.e. we do not need network connectivity to facilitate authentication to a server; it will all be done at the client.

Database positives

The first positive we have with a database is auditability since all the templates are stored at a central location. It will thus be easy to run regular audits on the templates to ensure that the data has not been changed or corrupted. The next positive is that it is easy to facilitate change. If for example we wanted to change the encryption mechanism used for the storage of the templates it can easily be done, we need not recall and reissue cards as with the smart card approach. The third positive is the ability to biometrically prevent dual enrolments by performing identification against the stored templates on the individual before enrolment. The next positive is the availability of storage memory; with the availability of data clusters etc. we will be able to store a large amount of data relating to an individual (although this is a big plus it does however cause big alarm for privacy since we will be able to store and retrieve a lot of information relating to an individual). The last positive is the ability to backup user data to prevent data loss when for example a data corruption occurs.

Smartcard	**Database**
False Database (forgery)	Possible loss of privacy
Costly to upgrade	Costly maintenance
Lost or stolen	Reliant on network availability
Possible damage/corruption of data	Possible corruption of data
Memory limitations	
Cannot prevent dual enrolments	

Table 6-1 Negatives of the two storage media

Smartcard	**Database**
Feeling of greater privacy	Audibility
Cheaper setup and maintenance cost	Easy to facilitate change
Self operation (no network connectivity needed)	Possible to check for duel enrolment
	Large amount of memory available
	Backups are possible

Table 6-2 Positives of the two storage media

Having looked at the positives and negatives of the two storage media, summarised in Table 6-1 and Table 6-2, I am sure that other individuals will be able to list a lot more negatives and positives and the debate on which medium is the best and most suited could become a very long and lively one. I am sure this debate is one that will continue for some time which I believe a lot will be related to privacy issues rather than technical inabilities of the storage media. And although privacy is a very important issue (privacy is discussed in more detail in the following chapter), with the correct policies and procedures in place to protect privacy I would prefer to use a central database since with a database we will be able to:

1. Biometrically prevent dual enrolment under different identities,
2. prevent false databases as discussed above,
3. and lastly the data on the server can be audited regularly to ensure no alteration to the decision making sub section (if located on the server) and storage subsection.

The decision to make use of a central database now needs to be incorporated back into the expanded problem statement as follows:
"*How should we implement a biometric model with a central template database which will allow us to integrate a single biometric into a number of applications as well as allow us to integrate multiple biometrics into a single application?*"

Armed with a detailed problem statement, an appropriate model can be established. The first step is to examine past initiatives which have attempted to facilitate the use of a single biometric across multiple applications. This information then needs to be assessed in conjunction with the specific problems that need to be addressed by the model, and then, finally, the model itself can be developed.

Past Initiative

This development (integrating a single biometric across multiple applications) has been attempted by making use of Application Programming Interfaces or APIs. An API is a collection of defined software interactions [87] which an application can use to access services provided by a module. For example, an API could be used to access the functions of a hardware device like a graphics accelerator card. Over the years, a number of biometric APIs have been developed, for example, the Speaker Verification API (SVAPI) [87], the Human Authentication API (HA-API) [87, 88], the Biometric API (BAPI) [87], and the BioAPI [63, 87]. The one biometric API from the list above that seems to be making the most advances is the BioAPI, especially after March 1999 when the BioAPI, HA-API and BAPI consortiums decided to merge and form the new BioAPI consortium [87]. The merger resulted in the following as inputs for the new BioAPI specification [63]:

- HA-API 2.0, dated 22 Apr 98, plus proposed extensions from draft Version 2.02, dated 17 Feb 99;
- Draft BioAPI Level H Reference Manual, dated 25 Feb 99;
- BAPI SDK Version 1.1, High Level API - Level 3, dated 1 Jun 98;
- Draft BioAPI/UAS Specification Release 1.0 Version 1.2, dated April 99.

From the above mentioned inputs, an API was developed to facilitate the easy integration of biometric systems into applications. Having looked at the history of biometric APIs, the following sections will now examine the workings of the BioAPI.

Workings of BIOAPI

The BioAPI API model aims to abstract the three main, high-level, functions of a biometric system. The three functions are: enrol; verify, and identify. These three functions are described by the BioAPI specification [63] as follows:

- Enrol — the process of capturing a sample, processing it into a template and giving it back to the application [63].
- Verify — the process of capturing a sample, processing it into a usable form and matching it against a provided template. A yes/no result is passed back to the application [63].
- Identify — the process of capturing a sample, processing it into a usable form and matching it against a collection of templates. A list is then returned to the application indicating how the sample matched up to the top candidate(s) in the collection [63].

To abstract these main functions, the BioAPI specification documents a number of data structures and API functions a developer can use to integrate a biometric solution into their application (if the biometric solution follows the BioAPI standard). Below is an outline of the high level working of BioAPI (readers

interested in the finer detail of the BioAPI, please refer to the BioAPI Specification Version 1.1 [63]). Figure 6-1 illustrates how the BIOAPI will allow a client/server biometric system to function.

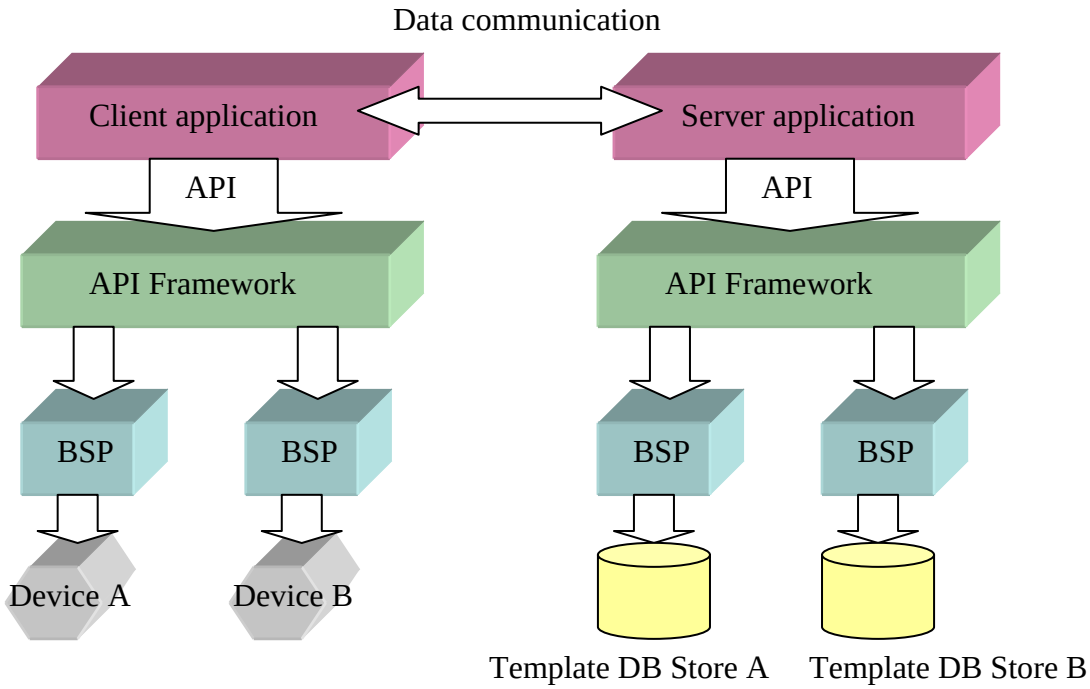

Figure 6-1 Client/Server biometric System implementing BioAPI adapted from [64 and 88] (Refer to the Appendix 1 for a colour version of the figure)

The figure illustrates how the client application communicates with the API framework — according to the BioAPI standard interfaces documented in the specification (see BioAPI Specification Version 1.1 [63]). The API framework will then communicate with a Biometric Service Provider or BSP (developed by the biometric vendor) which, in turn, will control the biometric device.

By making use of this model the client application need not concern itself with which biometric device is being used and one BSP and biometric device can simply be replaced by another BSP and device. For example, a fingerprint BSP and its corresponding fingerprint scanner could be removed and replaced with an iris BSP and iris camera without major impact on our client application.

On the sever side, the server application communicates with the API framework in a similar fashion to the client. The framework then communicates with a server BSP which will perform server side biometric functions, for example, matching the biometric sample (captured by the client application and transmitted to the server) to the templates in the data store. As with the client application, the BSP and template data store can be swapped out with another without the server application being affected.

Armed with an understanding of how biometric APIs work, a detailed analysis of their appropriateness as a solution to our problem statement can be undertaken.

Why not biometric APIs?

It is quite clear that the API approach allows nearly any biometric to be integrated into an application which requires user authentication. There are, however, a few glitches in this approach. The main problem is that the integration of the API is at code level i.e. if the desire is to use a biometric system via the API, the API interface needs to be coded either directly into the application's main source or a plug-in mechanism (where the API is bundled into a separate add-on for the applications).

This raises several issues. Foremost amongst them, the fact that it means the application programmers would have to develop the application to a specific API and, consequently, the application would only be able to make use of biometric systems which adhere to that specific API. This could be solved by insisting that either the application should support all biometric APIs or that each biometric system should implement all biometric APIs, or through the use of multiple add-on plug-ins. Obviously, the problem with the first two solutions is the development load created. It seems unrealistic to expect all applications to integrate every biometric API since the developers of the application would then be likely to spend more time integrating biometric APIs than developing the core functions of the application and vice versa. The multiple add-on plug-ins option is also a problem because the applications would have to manage these plug-ins and this would add extra complexity to the application and, likewise, distract the developers from developing its core functions. Now fortunately the APIs available are moving towards one standard and the above problem would disappear, but currently there are a number of different "standards" (BAPI, SVAPI, BIOAPI, etc.) and not one; thus the above problems still exist.

Technological evolution would also present problems if "code level integration" is used. For example, what happens when a new biometric comes onto the market and revolutionizes biometric authentication, but needs to perform new, unsupported (by the current APIs) operations to work? To resolve this, the biometric consortiums would have to alter their API specifications to include these functions and the application vendors would have to produce software patches. But what if the application vendor no longer exists or they view the application as a legacy system and require an, often costly, upgrade? And even if the patches are actually made available, what about having to patch a large system with at least three different applications and over 5 000 users? This could be an organization's IT administrator's worst nightmare.

From the above discussion, the following issues with APIs can be identified:

- Vendor lock-in. Although making use of an API should prevent vendor lock-in, the system still uses a set of APIs which may not be used by all biometric systems and, therefore, could restrict the system to only the biometrics which incorporated that specific API.
- Difficult to facilitate change. As mentioned previously, APIs may need to change which means that some applications may not be capable of making use of a biometric system through the new biometric API.
- If an API changes for any reason, migrating an organisation's application across to the new API could incur large administration costs.
- If the applications make use of different plug-ins each application needs to manage its own set a functions, but this would be better, architecturally, if moved to a central point. This would provide us ease of administration, also we do not to patch the application if change is required.

The above section briefly discusses the concerns with using biometric APIs. Although they do present concerns, these are outweighed by their inherent advantages and the best solution would appear to be one which uses them, but does not integrate them at the code level.

What do we want to accomplish with the model

A brief overview of what the system should accomplish can be established by looking at the following scenario. John is a regular office worker who has access to an application containing his entire clientele's data. He also has access to another application linked to his corporate data. In order to protect this data John is using a username/password protection mechanism. John feels that this security mechanism is not sufficient and decides to go the biometric route. John does his research and concludes that fingerprint recognition will be the biometric best suited to his needs.

The problem John now faces is: how does he get his applications to work with his chosen biometric (since during his research he concentrated more on whether he would be comfortable using the biometric, it would work in his office environment and give him an appropriate level of security rather than its technical implications)? Although it could be argued that John should have checked to see if both applications support the chosen biometric and that he can use the biometric without going to the extent of upgrading his applications, it suits the purposes of this model that he didn't. The aim of this model is that the user should not have to worry about the technical details and can concentrate purely on which biometric they feel most comfortable with. In other words, John selects a biometric, purchases and installs the hardware and software and, seamlessly, starts to use biometric authentication. This ideal is illustrated in Figure 6-2 below.

In the figure, the Biometric Authorities maintain a central database of users' biometric templates. The applications will request user authentication from the Biometric authorities. One application can connect to multiple Biometric Authorities (see Application B) and multiple applications can also connect to one Biometric Authority (see BA 1). To achieve the above environment, a number of things need to be in place. The following section highlights the problems that could be faced creating such an environment and outlines a model capable of surmounting these hurdles.

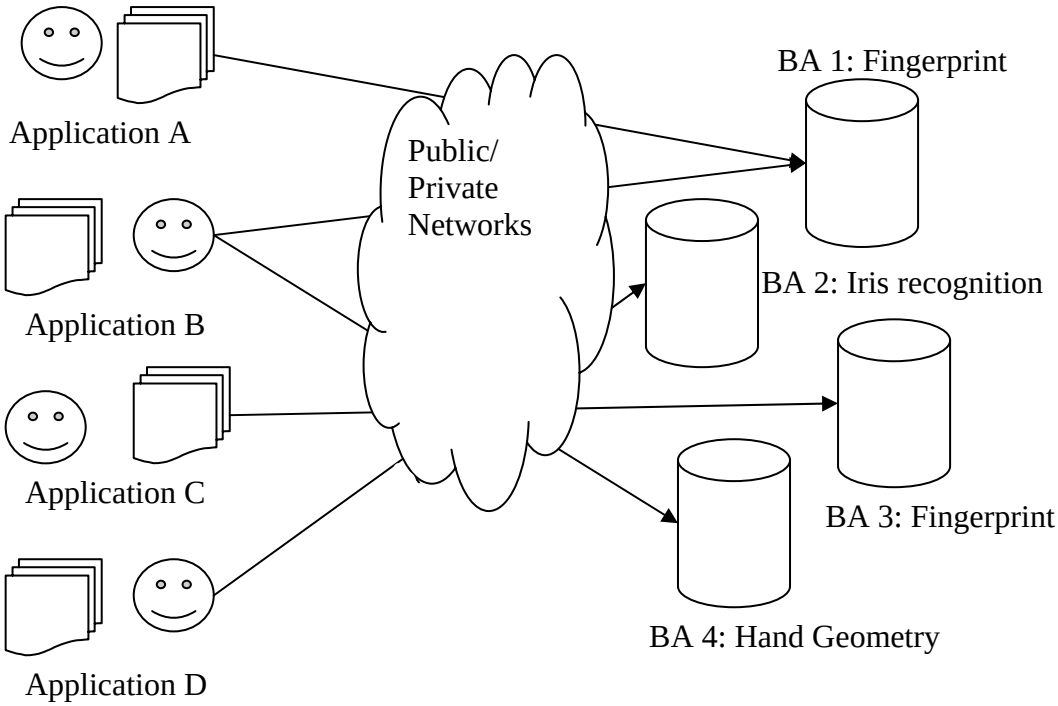

Figure 6-2 Biometric Authorities providing authentication service to a multitude of clients.

The Roadblocks

The above discussion of APIs looked at some of the reasons why APIs are not sufficient in an online environment with multiple applications; the problems mentioned above are, however, not the only ones. In this section, the other roadblocks needed to be overcome in order to successfully role out multiple biometrics to a number of different applications will be identified and examined. The discussion will look at both implementation and security concerns.

Implementation Concerns

As mentioned previously, a possible implementation scenario can be seen in Figure 6-2 with a number of different Biometric Authorities (BA) maintaining a central database of templates for their specific biometric solution and a number of different applications interacting with the BAs for authentication.

Within this specific scenario (Figure 6-2) there are certain aspects that need to be addressed:

- Firstly, since there is a multitude of Biometric Authorities (BA), how will the application know which Biometric Authority to connect to? A mechanism to identify the appropriate Biometric Authority will, therefore, be needed.
- The second problem is the response time of the BAs (since a long wait will hinder user productivity).
- As depicted in chapter 5, when picking a biometric for an application there are a number of aspects that need to be taken into consideration to ensure the biometric will work in the application. A mechanism to ensure that the biometric the users have chosen will be functional in the environment is, therefore, also needed.

- This scenario also requires that the client is communicating with a valid BA (to ensure it is not talking to a fake Biometric Authority issuing fraudulent responses i.e. false database).
- The BA also needs to be sure it is communicating with a valid client. The reasons for this are: firstly, the need to ensure a client is not trying to perform a denial of service attack on the server by flooding it with a lot of useless authentication requests and, secondly, not providing a fake client with a lot of response data which could be analysed in order to find loopholes in the system.

Security Concerns

Putting a system in place with the potential to be distributed to hundreds, even thousands, of users through public networks (as in Figure 6-2) could make the application open to a number of security issues which would not normally (in a closed controlled environment) be that significant.

Biometric systems have eight main areas which can be at risk [71, 72] (see Figure 6-3).

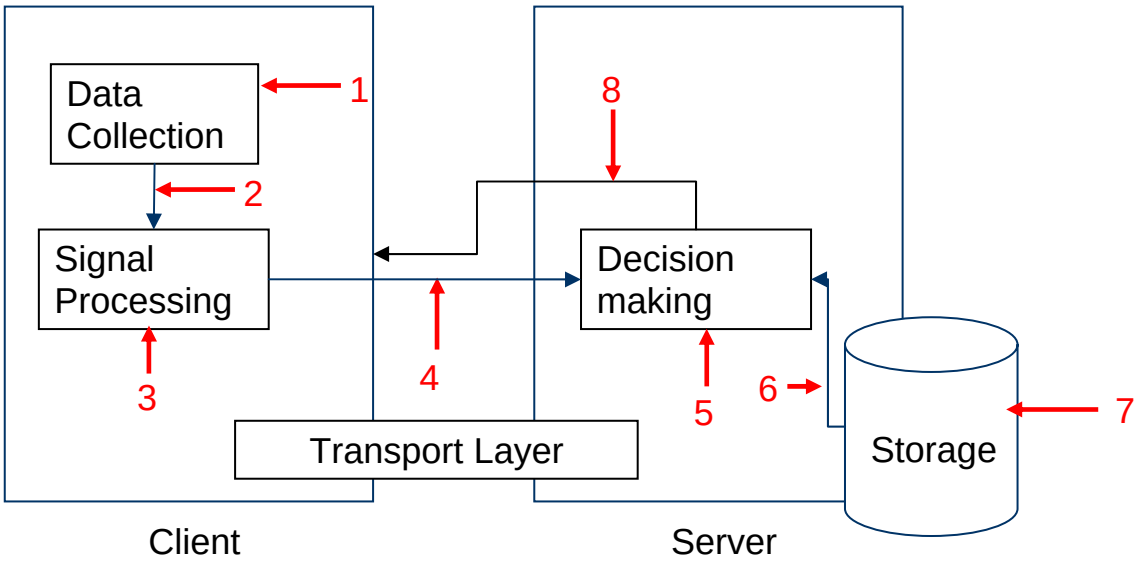

Figure 6-3 Security concerns (Adapted from [71, 72])

The first area is the data collection sub-system. The main concerns faced here are: (i) that a user presents a fake biometric to the sensor or perhaps an altered one to the sensor which would force it to produce a fraudulent image; (ii) the replay of a previously captured sample or the alteration of the raw sample when it is being transmitted from the decision making sub-system to the signal processing sub-system; (iii) the signal processing sub-system is tricked into producing a feature template generated by the attacker and not the true values; (iv) the feature template could be altered while being transmitted to the decision making sub-system; (v) an attacker overrides the matching module to produce fake scores for the matching of two samples; (vi) the attacker could try and alter the templates while they are being transmitted from the data store to the decision making module (since the decision making module needs to perform a match against stored templates); (vii) the attacker could try and alter the templates directly on the server; (iix) the final attack is the alteration of the response produced by the decision making module before it reaches the client

(the interested reader can refer to [71, 72] for a more in-depth discussion on the security concerns).

Having looked at the possible roadblocks that could be faced, the following section with briefly summarised the problems in a set of requirements for the model.

Model requirements

1. The first main requirement for the model will be to provide trusted biometric authentication.
2. The second requirement is to secure the authentication by:
   2.1. Supplying a mechanism to identify and authenticate the Biometric authority.
   2.2. Supplying a mechanism to identify the client and ensure it is a valid subscriber to the biometric authority.
   2.3. Safeguarding all communication in order to prevent:
      2.3.1. alteration of the captured sample before being transmitted to the server;
      2.3.2. alterations to the captured sample while being transmitted;
      2.3.3. alteration of the response given by the server;
      2.3.4. individuals from gaining large biometric samples of individuals.
3. The next main requirement is to provide a mechanism to ensure the biometrics' performance is acceptable for the application i.e. quick response time.
4. The model should be capable of supporting multiple biometric systems.
5. Within the model we want to move the biometric integration (making use of APIs) away from the physical application to ensure the application need not worry about installing and managing plug-ins. Consequently, moving the responsibility for installing and managing the different biometric plug-ins to a dedicated module/programme (the application should interact with this module/programme directly and not the biometric system).
6. The model needs to provide flexibility in the sense that it:
   6.1. enables the application to easily use new biometric devices which could make use of new API standards;
   6.2. allows for the use of legacy biometric systems;
   6.3. is easily upgradeable.

Having looked at all the requirements and pitfalls, the next section looks at the model itself and, specifically, how it can overcome the inherent problems in order to satisfy all of the above requirements.

The Model

Process Flow

Before we move on to a detailed discussion of the model we will briefly look at the basic process flow we wish to accomplish with the aforementioned model.

Firstly a user (after much research and deliberation) will select his/her biometric authority of choice, which could provide any biometric (fingerprint, iris, etc.) provided by any supplier. Once the user has made a decision they can either visit a branch of the BA or a representative can be sent to the user's residence. The representative will now confirm the identity of the individual making use of ID documents, birth certificates etc. After the identity has been verified the representative will enrol the user's biometric into the system. The system will check for duplicate users and biometric templates to prevent a user from enrolling multiple times with different identities. Once the enrolment is done the

representative can give the user all the equipment he/she needs (biometric sensor) as well as the appropriate software (certificate pool application – see below, client module pool application – see below). He will then generate a Biometric Authority Certificate which the user will install on his/her system. The user will also receive a private key relating to the public key on the certificate (see certificate section for more detail).

Once the user has received his/her certificate from the biometric authority they now need to install this certificate into a certificate pool in order to use it. This certificate pool will be an application containing a list of all the BA certificates the user has installed (if they have multiple certificates). The certificate pool will be discussed in more detail later. When an application now requires authentication it will query the certificate pool, in order to select the certificate for the application.

Once the application has the certificate it will extract from the certificate the information pertaining to the location of the biometric authority as well as information about the client module to use. The application will now query the client module pool on the client computer to see if it contains the module it requires. The client module pool will maintain all the client modules installed on the client computer. We will look at the client module pool in more detail later. If the client module is not present in the client module pool the client module pool will retrieve and install the appropriate module from the biometric authority. Once the module has been installed the application can access the module through the client module pool. The application will now request biometric authentication of the person the certificate belongs to through the client module pool. The client module pool will activate the appropriate client module which will produce a feature template from a raw biometric sample taken by the scanner. Once the client module pool has the feature template it will be transmitted to the server for authentication. Once the response of the authentication has been received from the server the client module will give it to the application which can continue with its operations.

Basic Overview

Having looked at the process flow we will now look at the finer detail which needs to be in place in order to securely accomplish the above process. As mentioned previously, the two main phases or functions of any biometric system are enrolment and identification. In this study, the main focus is on the identification process and how it can be distributed across multiple applications.

A basic model for the identification procedure in a central database system can be viewed in Figure 6-4. This figure gives an indication of how the 5 sub sections from the generic model (see chapter 2) could be distributed.

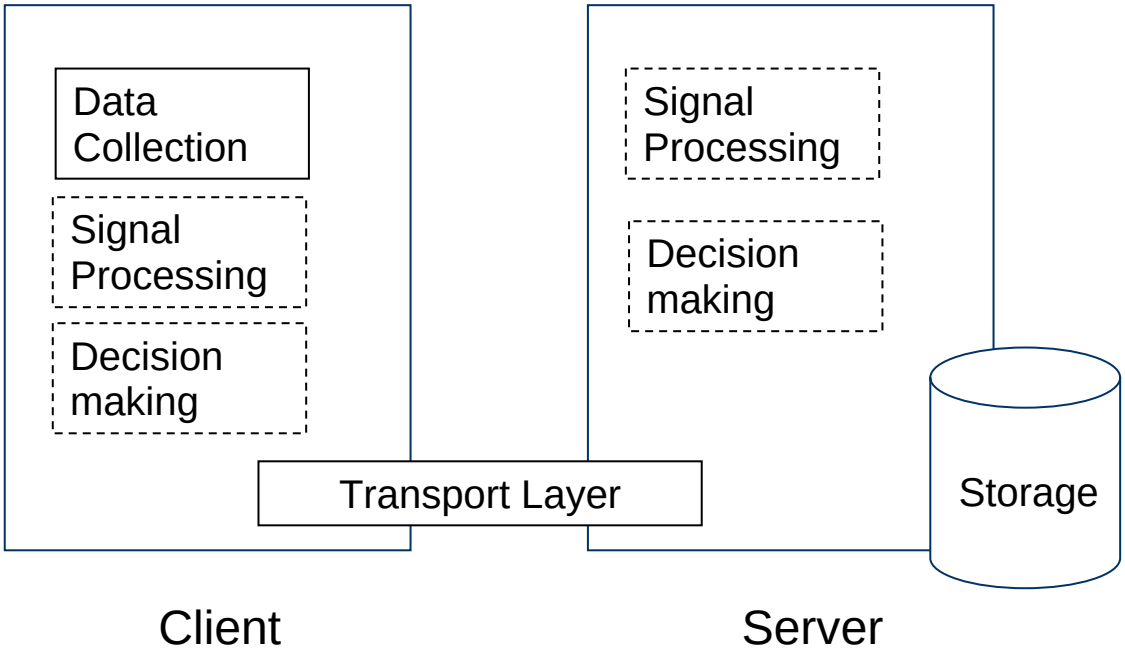

Figure 6-4 Possible distributions of 5 subsections for a distributed application

As with any distributed system, there are two main modules: a client and a server module. In the figure, these two modules are combined by the transport layer sub-section. There is also the data collection phase on the client and the storage system on the server. The remaining two modules (signal processing and decision making) have the option to be on either the client or server. The possible combinations are:

- Option 1: Signal processing module on the client and decision making module on the client. In this scenario, the data collection module will collect a raw biometric sample and give it to the signal processing module to extract all the features. Once the features have been extracted the decision making module will request templates from the storage system (making use of the transport sub-section) to compare the newly captured sample to. The decision will then be given back to the client. In this scenario all the processing occurs on the client.
- Option 2: Signal processing module on the client and decision making module on the server. In this scenario, the data collection module will collect a raw biometric sample and give it to the signal processing module to extract all the features. Once the features have been extracted this feature template will be communicated to the server through the transport sub-section. Once the server receives the feature template the decision making module will compare the template to the ones in the storage sub-section. In this scenario, the processing is split between the client and server, and there will be less network traffic since only one feature template is transmitted from the client to the server unlike the above option which, in the event of a recognition, would require multiple templates to be sent from the server to the client.
- Option 3: Signal processing module on the server and decision making module on the server. In this scenario, the client will collect the raw biometric sample (using the data collection module) and transmit the sample to the server making use of the transport sub-section. Once the server has received the raw sample, the features will be extracted (signal processing module) and a match (decision making module) will be performed against the templates held in the storage sub-section. In this scenario, most of the processing is done on the server. There will also be

minimal network traffic (as option 2), but, usually, the raw sample is bigger than a feature template.

If we weigh up the three options above, option 2 and option 3 will be the preferred options — especially in a distributed application on the Internet where keeping network traffic to a minimum is a priority. If upgradeability (in the event that the biometric feature extraction and decision modules need upgrading) is factored in, Option 3 will have the least amount of impact since only one area would be affected and the users will be unaffected. A comparison of the three options can be seen in Table 6-3.

	Client impact (processing)	**Server impact (processing)**	**Network usage**	**Impact of upgrade on user**
Option 1	High	Low	High	High
Option 2	Medium	Medium	Low	Medium
Option 3	Low	High	Medium	Low

Table 6-3 Comparison of three distribution options

For a distributed application across the Internet, Option 2 seems the most effective solution, for the following reasons:

1. To keep network traffic to a minimum during every day usage. It seems preferable to transmit one small feature template for recognition (which could be an every day task) and a bigger upgrade packet (which may only occur once a month) than a small upgrade packet, but larger raw biometric sample transmitted for recognition.
2. To prevent possible access to raw biometric sample. The signal processing module produces a feature template which, as mentioned previously, can be viewed as a one way hash which can not be worked back to the original raw sample. By transmitting this feature template instead of the raw biometric sample, the system is preventing someone from monitoring the network and gathering raw samples which they can use to steal an individual's identity.

The basic foundations of the model are as follows: A client and server connected through the transmission sub-section. The client will include the data collection and signal processing modules, and the server will contain the decision making module and storage sub-section.

Now that the fundamental building blocks are in place, a more detailed discussion of the elements within the model can take place.

Elements of the model

Now that we know which subsections will reside on the client and on the server we can look at the client and server in more detail looking at how we will exactly accomplish the aforementioned process flow. Firstly in the following sections we will look at the structure of the client followed by the operation of the certificate and certificate pool. We will then look at the client modules and client module pool, the client section will then be completed with a look at the biometric scanners.

After the client has been discussed we will look at how the server will be structured. After the structure we will look at the template store and how we will perform verification.

The Client

The established security and implementation concerns, as well as the principal requirements, have prompted the following additions (see Figure 6-5 below) to the client environment.

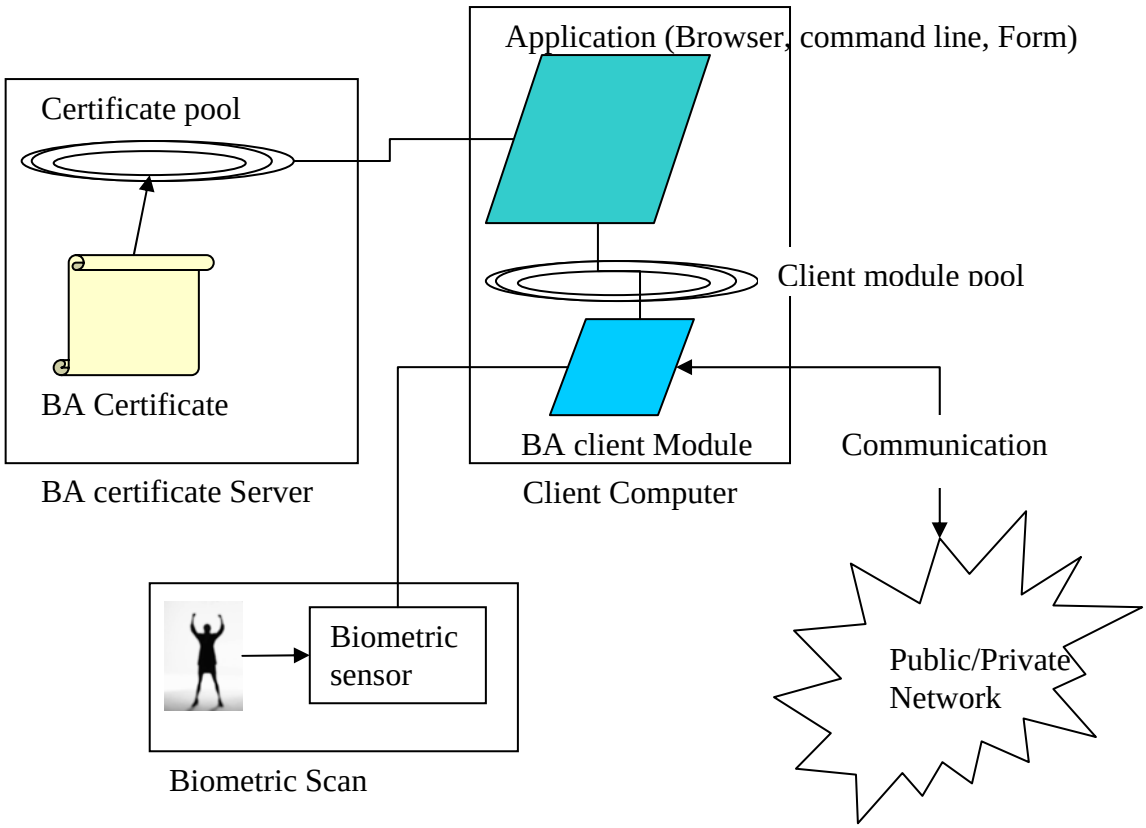

Figure 6-5 Client Side of the Model

Looking at the above figure, the first thing to note is that there are now two distinct computers. The first is the client computer which will have the biometric sensor connected to it using a communication port for example USB, serial, parallel port, etc. It will also contain the client application which will require authentication. In order for the client application to communicate with the appropriate module (remember that multiple biometrics can be connected to one computer and application) a Client Module Pool (CMPOOL) has been created. The CMPOOL will load and control the appropriate client module which, in turn, will be responsible for producing a feature template from the biometric sensor (more on this later).

The second computer in the model is the certificate server which will contain a certificate pool of users' Biometric Authority certificates. These BA certificates will be used by the client application to gather information about the user and his/her Biometric Authority in order to perform the authentication. One thing to note about the certificate pool is that it does not need to reside on a separate computer it could reside on the client machine (in a single computer environment).

The following sections will look at the three modules of the client (certificate scan, client module and biometric scan) in more detail.

Certificate scan

In the following section, the certificates and the application which will be used to maintain these certificates will be examined. It may seem a bit out of place to use these sections to kick off the discussion of the model, but since BA certificates are used extensively throughout the model they need to be understood first. So this section will start with a brief overview of traditional digital certificates. Once the inner workings of the *biometric authority certificate* and the *certificate pool* have been established, the exact roles of the client and server during authentication will be inspected.

Certificate background

PKI

An example of two individuals, John and Pieter, working in company X, who wish to communicate with each other in a secure fashion will be used to explain how digital certificates work. The most popular mechanism for secure communication is to use a secure "key" to encrypt a message. For example, a message can be encrypted by John before transmission and then Pieter, when he receives the message, can decrypt it using the same key. Pieter and John can be sure that their communication is secure because only the two of them have the secret key. They can also now be sure that only the other could have sent the message (since he is the only other person with knowledge of the secret). This type of encryption (which uses one key for both encryption and decryption) is known as symmetric encryption.

The problem with symmetric encryption is that John and Pieter needed to meet up in order to exchange the secure key. But what if John and Pieter lived in different countries? This would make meeting each other very difficult. There are ways the one can get a secret key to the other, but how can one be sure it is received by the other? To solve this uncertainty, John and Pieter can decide to communicate with each other making use of Asymmetric encryption which makes use of two keys; a private key and a public key.

Before establishing how asymmetric encryption will work in the above example, some definitions need to be established:

1. Asymmetric encryption — during asymmetric encryption, the system will use different keys to encrypt and decrypt a message or a document. This implies that communicating parties do not need to share a single key. Instead, with asymmetric encryption they use a key "pair": a public and a private key (as discussed above) [53, 58]. To encrypt a message or data packet, the sender will use the recipient's public key (which is publicly available). Once encrypted, this message can only be decrypted with the private key of the public key; assuming that the private key of the user is kept secret [53, 58]. One important thing to note about a private and public key is that they operate as inverses [53]. This means that a message that is encrypted with a public key can be decrypted with the private key and a message encrypted with a private key can be decrypted with its corresponding public key [53]. An example of a commonly used asymmetric encryption mechanism is the Rivest-Shamir-Adelman (RSA) encryption algorithms developed by Rivest, Shamir and Adelman [53, 76].
2. Public Key — a Public key is the publicly available key of a Public Key Cryptography system (used to encrypt messages intended for the owner and also to decrypt (verify) signatures made by its owner [53, 58]).
3. Private Key — the private key is the secret key in a Public Key Cryptography system (used to decrypt incoming messages encrypted with the user's public key). The private key will also be used to sign outgoing

messages [53, 58]. An important thing to note is that the method used to generate a public/private key pairing is such that each public key has only one private key and vice versa.

The way the Asymmetric encryption will work in our example is, say John wants to send message A to Pieter, he will first have to get Pieter's public key. There are a number of different ways John can get Pieter's public key — Pieter can simply mail it to him or could have published it on an electronic directory on a server somewhere [as described in 53 and 57].

Regardless of how he gets Pieter's public key, John will now use it to encrypt message A into E(A). The encrypted message, E(A), can now be sent to Pieter. On reception, Pieter can now decrypt E(A) with his private key to reproduce A. Although the message is secure, how can Pieter be sure that John sent it? In our symmetric encryption example above, Pieter was assured of this since only he and John shared the single secure key, but in our Asymmetric example anyone in the world can have his public key (especially if it was published on a electronic directory). To enable Pieter to be sure that John was the sender of the message — and not someone impersonating him — another element can be added: a digital signature.

A digital signature is an electronic signature produced by encrypting a message with a private key so that the identity of the sender can be verified [53, 76]. It can also be used to ensure the integrity of the content of the message by confirming that it has not been changed during transmission [53, 76]. The above is true since it is only possible to decrypt a signature with the user's public key if they have encrypted it with their private key (which is kept secret). If the signature is successfully decrypted with the public key, then the user must have sent it. This second function of the signature is accomplished by comparing the decrypted message to the original. If the decrypted message matches the original message it is certain that the original has not been changed.

So all John has to do before sending the message is to encrypt the message with his private key (which only he has) to produce a digital signature. This signature and message can now be encrypted with Pieter's public key and transmitted to him. Pieter can then decrypt the encrypted message with his private key to produce message A. He will then decrypt the digital signature using John's public key and, if the two decrypted messages match, Pieter can be sure that: 1) John sent it and 2) the message was not altered during transmission.

The communication between John and Pieter has been made secure, but how can John be sure he has Pieter's public key and not that of someone who is masquerading as Pieter? To solve this issue we need to add a further element: the digital certificate.

A digital certificate is a digital data structure that binds the public key to the identifying information of a subject (this could be a user, server program etc.) in the certificate. This digital data structure is digitally signed by its issuing authority by making use of its private key. Combined with this digital signature, the certificate can now be used to assure any third party (wishing to use the public key) that the associated private key is held by the subject identified in the certificate and not someone else [53, 58, and 78].

Therefore, in order for John and Pieter to be sure they have each other's legitimate public keys, they need to obtain a digital certificate as well. This certificate, which can be published in exactly the same fashion as the public keys,

will be signed by a third party they both know and trust. For the sake of this example, let's call this person Kathryn. To create the certificates, both John and Pieter will give their public keys to Kathryn. She will place each one in a certificate and sign it with her private key. John and Pieter can then send their certificates to each other.

Since both John and Pieter know Kathryn and have her public key they can validate the authenticity of each other's certificate (i.e. validate the authenticity of the public key) by looking at the signature with Kathryn's public key. Usually the known, trusted person or entity that signs digital certificates and vouches for a certificate's authenticity is known as a certificate authority [53, 79].

The inclusion of the certificate authority (CA) would appear to complete the secure communication mechanism, but how can we ensure that an individual wishing to authenticate a signature has the signer's (CA's) public key? In the example of John and Pieter, since both work for Company X, the company could institute a policy giving each employee Kathryn's certificate (i.e. her public key) when they begin their term of employment. Thus, everyone in the organisation will have the organisation's authorised CA's public key with which they can verify the certificate of any other employee in the company. This works well in the limited environment of a single organisation, but in a distributed environment getting a CA's certificate and ensuring it is authentic can be a difficult task unless an appropriate trust model (as the one with Kathryn) is in place. Trust models will be discussed in more detail in the following section.

This assessment of traditional digital certificates illustrates how a certificate can authenticate our client and server (with an appropriate trust model in place) and safeguard communication. In the following section, how Biometric Authorities could issue certificates and their use in the model will be examined.

Biometric Authority Certificate

Having looked at traditional digital certificates we can now look at the biometric authority certificate, but before we do that we need to look at what the certificate will be used for. In the above process flow we mentioned that from the certificate we will extract the identity of the Biometric authority in order to contact the authority. In the process flow the certificate will also be used to identify which client module (see client module section for more detail) to use for authentication. Other uses of the certificate not mentioned in the process flow are to identify the individual, indicate the rating of the biometric being used to the application (see below), and finally secure the communications between the client and biometric authority.

To accomplish the above the BA certificate would be very similar to the digital certificates (as discussed above) currently used by Certificate Authorities like Thawte[6], but with a few alterations. The BA certificate will need to contain the following information:

- Issuing authority information;
- Identity and supporting information about the individual;
- A digital tag identifying which client module to use;
- Address of the Biometric authority to use;
- Rating of the Biometric Authority;
- Public Key of a PKI public/private key pair;
- Digital signature.

[6] http://www.thawte.com

The BA certificate must include the information or data listed above for the following reasons:

- Issuing authority information — the issuing authority's details are required to ensure that the certificate can be trusted. This is vital because a certificate is only useful if the issuer of the certificate can be trusted (similar to college degrees in that they are not worth the paper they are written on unless issued by an accredited institute.)
- Individual's information — the individual's information will be used as part of the authentication step (the client application will send the user's details to the server along with a biometric sample for a one-to-one authentication).
- A digital tag identifying which client module to use — in the event of a user subscribing to multiple Biometric Authorities, the client application needs to be able to select the appropriate module for authentication process (each of these client modules will receive a unique digital tag during production).
- Rating of the Biometric Authority — certain biometrics will fail if used in an unsuitable application or environment (see chapter 5) and, since the users will be able to choose their preferred Biometric Authority, the client application needs to be sure this biometric will function to the standards it requires.
- Public Key of a PKI public/private key pair — this public key will be used by the server to create a secure 'tunnel' between the server and client (making use of encryption to ensure the safe communication of data).
- Digital signature — the issuing Biometric Authority will sign the BA certificate to ensure the validity of the certificate, as well as the integrity of the data contained within it.

Having looked at what the digital certificate will contain, and the purpose of this information, the next question is: how do we manage the user's certificates? The answer is to create a Certificate Pool and this is examined in the following section.

Certificate Pool

In the above model, the Certificate Pool Application (CPA) can be described as: "*a network application which installs and manages certificates in a certificate repository, in order to provide applications access to these certificates when biometric authentication is required*".

As the above definition states, the Certificate Pool will be a network application, residing on a computer as a service (in a Windows environment) or a daemon (in a UNIX environment), listening for commands from the client computer (see Figure 6-6). The main function of the certificate pool will be to store the Biometric authority certificates of individuals and make them available to applications in order to perform authentication of the individual.

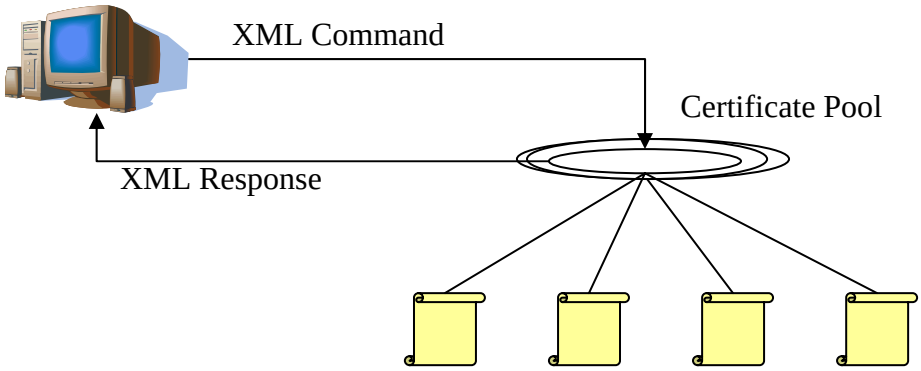

Figure 6-6 The certificate pool managing certificates through XML commands from clients

To accomplish this, the client computer will issue commands either through a Certificate Pool Admin Console or the application (requiring authentication) itself. For the purpose of this study, the command/response packets will be depicted in XML format. XML (eXtensible Markup Language) is a standard developed for data representation and exchange on the World Wide Web [73] and is ideal for cross-platform communication (its format/syntax is also much easier for people to decipher, hence the reason why it is advocated in this study, but the reader needs to be aware that XML is not the only option available — a binary data bundle, for example, could be used as an alternative — provided it is available in a known structure in order for the server and client to read it). The functions of the certificate pool will include:

- Installing certificates – this will place the certificates in the certificate pool for usage later. Refer to the Install certificate section on page 74 and Code fragment 6-1 to Code fragment 6-4;
- Listing certificates – if a user has more than one certificate the listing can be used so that he/she can pick the one they prefer to use. This would be an uncommon occurrence since it would be uncommon for an individual to want to use more than one biometric but for the sake of completeness this command has been added. Refer to the List certificates section on page 76 and Code fragment 6-5 and Code fragment 6-6;
- Retrieving certificates – once the user has selected his/her certificate to use the application needs to have a copy of the certificate the retrieve command will get one for it**.** Refer to the Retrieve certificates section on page 77 and Code fragment 6-7 and Code fragment 6-8;
- Removing certificates – in the event that a user wishes to withdraw its certificate from the pool the remove command will be used. Refer to the Remove certificate section on page 77 and Code fragment 6-9 and Code fragment 6-10.

Having listed the command of the certificate pool the next sections will now look at the inner workings of these commands and just how each will be accomplished.

Install certificate

A software management tool will be required to help users install certificates in the pool. For the purposes of this study, the tool will be known as the Certificate Pool Admin Console (CertPAC). To install a certificate, the CertPAC will first require the user to enter the address of their certificate pool (this could be their local computer or a server). Once the address has been entered the CertPAC will

connect to the certificate pool and send a hello packet (Code fragment 6-1).

```
<certpoolcommand>
        <certpoolcommand action=”HELLO”>
</certpoolcommand>
```

Code fragment 6-1 CertPAC hello message

Once the certificate pool receives the hello message it will respond to the client computer with a hello response. The response will contain a welcome message from the certificate pool (see Code fragment 6-2).

```
<certpoolresponse>
        <certpoolresponse action=”HELLO”>
        <welcome_note>
                Welcome to Company  XYZ’s certificate Pool server
                version 1.1
        </welcome_note>
</ certpoolresponse >
```

Code fragment 6-2 Certificate pool hello response

Now that the connection has been established, the CertPAC will ask the user to browse to their BA certificate. Once the CertPAC application has the certificate, it will create a copy of the certificate and encrypt the copy using the public key on the certificate. The CertPAC will then extract the name of the issuing authority from the certificate. It will also query the system for the username of the user logged in. All of this information, including the encrypted certificate, will be placed inside an install packet and transmitted to the server (Code fragment 6-3).

```
<certpoolcommand>
        <certpoolcommand action=”INSTALL”>
        <issuer>
                BA name
        </issuer>
        <user>
                johndoe
        </user>
        <certificate>
                4YAxuFDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </ certificate>
</certpoolcommand >
```

Code fragment 6-3 CertPAC install command

Code fragment 6-3 reveals how the entire XML document is in text format even though the certificate is now encrypted binary data. This text representation for the binary certificate is derived by making use of base64 encoding. Base64 is an encoding mechanism which represents 6 bits of binary data as a printable character [74, 75]. Please note, as mentioned previously, XML and base64 are only used for example purposes and the above code fragments could be structured digital packets.

Once the certificate pool receives the certificate it will add the certificate to its repository under the user's name. An important thing to note is that the user is allowed to have more than one certificate, thus the certificate repository will contain a list of all the certificates for a user. Once added, the certificate pool will respond with a certificate installed packet (Code fragment 6-4) which will contain a success field — a Boolean value stating whether or not the certificate has been installed.

```
<certpoolresponse>
        <certpoolresponse action="INSTALL">
        <success>
                true
        </success>
        <response_note>
                Certificate added for johndoe
        </response_note>
</ certpoolresponse >
```

Code fragment 6-4 Certificate installed response

List certificates

The 'list certificates' command will be used by the CertPAC or the client application requesting authentication in order to produce a list from which the user can select a certificate for either retrieval or deletion — the 'list certificates' command and corresponding response can be seen in Code fragment 6-5 and Code fragment 6-6 respectively.

```
<certpoolcommand>
        < certpoolcommand action="LIST">
        <user>
                johndoe
        </user>
</certpoolcommand >
```

Code fragment 6-5 List certificates command

```
<certpoolresponse>
        <certpoolresponse action="LIST">
        <certificate>
                <issuer>
                        BA name 1
                </issuer>
        </certificate>
        <certificate>
                <issuer>
                        BA name 2
                </issuer>
        </certificate>
</certpoolresponse>
```

Code fragment 6-6 List certificates response

Retrieve certificates

Using the above command presents the user with a list of their certificates. Once the user selects the required certificate, the application will issue the 'retrieve' command. The response to the application will contain the encrypted version of the certificate (see Code fragment 6-7 and Code fragment 6-8 for the command and response). To decrypt the certificate, the application will then ask the user for the certificate's corresponding private key. This key will then be used to decrypt the certificate and, once decrypted, the application will either use the certificate to perform a biometric authentication or store it on the client computer (in the event that the user lost their original certificate). An important thing to note is that, since the certificate is being encrypted with the public key on the certificate, only the user's private key can decrypt it. This ensures that only the rightful owner can read the certificate despite the certificate pool being a public service within the organisation.

One last note on the retrieval process: before the application uses the certificate it will make sure it is a valid certificate and that it was issued by a valid Biometric Authority by examining its digital signature. Once the application has confirmed it is dealing with a valid certificate, it will then check the rating of the Biometric Authority. If the rating is higher or equal to the rating required by the application, the application will continue with its operations

```
<certpoolcommand>
        < certpoolcommand action="RETRIEVE">
        <user>
                johndoe
        </user>
        <issuer>
                BA name 2
        </issuer>
</certpoolcommand >
```

Code fragment 6-7 Retrieve command

```
<certpoolresponse>
        <certpoolresponse action="RETRIEVE">
        <certificate>
                <issuer>
                        BA name 1
                </issuer>
                <data>
                        4YAxuFDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
                </data>
        </certificate>
</certpoolresponse>
```

Code fragment 6-8 Retrieve response

Remove certificates

This command will be used to remove certificates from the certificate pool. The command and corresponding response can be seen in Code fragment 6-9and Code fragment 6-10.

```
<certpoolcommand>
        < certpoolcommand action=”DELETE”>
        <user>
                johndoe
        </user>
        <issuer>
                BA name 2
        </issuer>
</certpoolcommand >
```

Code fragment 6-9 Delete command

```
<certpoolresponse>
        <certpoolresponse action=”DELETE”>
        <success>
                true
        </success>
        <certificate>
                <issuer>
                        BA name 1
                </issuer>
                <data>
                        4YAxuFDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
                </data>
        </certificate>
</certpoolresponse>
```

Code fragment 6-10 Delete command

Client module

In the beginning of the discussion of the model during the process flow we mentioned a client module which would be an application plug-in written by the Biometric vendor to accomplish two main functions: data capture and signal processing. Thus the main function of the model will be accomplished through the module – authentication. As a result, this module will control the biometric sensor in order to capture raw samples and process these samples to produce a feature template. The problem with the client module is that, on its own, it is unable to perform the entire authentication and so the system will need an additional application, able to control the module and request sample captures and feature template extractions.

This application would then be responsible for sending the template for authentication and processing the response. The problem with this approach, as discussed previously, is that the integration with the biometric is now at application level and this creates additional difficulties.

To overcome this problem, a Client Module Pool (see below), which will be responsible for the integration of the client module, will need to be created. All of the activities of the client module will thus be controlled through a Client Module Pool (CMPOOL). The application requiring authentication will communicate with the client module, making use of command/response packets, through the Client Module Pool to allow for easy integration between the application and client module. The communication of the CMPOOL and application will occur as if it is a normal network communication.

Although the CMPOOL makes the interaction between the application and client module extremely easy, the interaction between the client module and CMPOOL is a little more complicated. The reason for this is that the client module (in this model) is not an application like the CMPOOL, but rather a plug-in for the Client Module Pool. This allows for multiple modules that can be loaded by the CMPOOL and used for authentication, but how can the interaction between the client module and the CMPOOL be made easier? The answer is by making use of the aforementioned biometric APIs, like the BioAPI.

The process will begin with the CMPOOL calling methods to receive the feature template from the module (these methods will have to comply with the selected biometric API standards to help simplify the integration). The CMPOOL will then transmit the template to the server for authentication, receive the response, and pass it back to the client application. Additional elements required will include an identifier — used to identify the module — and a digital signature — to ensure the authenticity of the module and that it has not been altered in any way. This signature will be generated by the issuing authority of the module (for example, the BA) making use of its digital certificate. The focus of this study will not be on the client module, but the CMPOOL since it will be responsible for loading the client module and controlling/managing interaction with the application.

Client Module Pool (CMPOOL)

The CMPOOL is an application residing on a computer as a service (in a Windows environment) or a daemon (in a UNIX environment), listening for commands from client applications. The CMPOOL will be responsible for managing biometric client modules (as mentioned previously, these will capture biometric samples and extract the feature templates). The CMPOOL will, thus, be the main interaction point making use of APIs. Due to this, it is important to note that it will be this application, the CMPOOL, which needs to be upgraded if new APIs and/or client modules are released. Thus, through the CMPOOL the complexity of integration and upgrade is moved away from the application to an external application, namely, the CMPOOL.

An important aspect of this CMPOOL application is that it does, nonetheless, need to reside on the client computer (since the CMPOOL will need to load the client module, which controls the biometric sensor and produces a feature template for authentication, and, in order for the client module to control the biometric sensor, it needs to be active on the same machine as the sensor). Thus, the CMPOOL (which loads and controls the client module) needs to be on the same machine as the sensor. The Client Module Pool will be responsible for the following tasks:

- Client module lookup – the CMPOOL will maintain a number of different client module plug-ins (that's if the user make use of multiple biometrics) the lookup command will be issued by the application asking the CMPOOL if it has the appropriate module available. Refer to the Client module

lookup section on page 80 and Code fragment 6-11 and Code fragment 6-12;

- Client module install – if the CMPOOL does not have the correct module this command will be issued to the CMPOOL indicating that it will have to retrieve and install the client module from the BA. Refer to the Client module install section on page 81 and Code fragment 6-13 to Code fragment 6-18;
- Client module load – if the CMPOOL has the client module (determined during the lookup command) the application will instruct the CMPOOL to activate the module through the load command. Refer to the Client module load section on page 83 and Code fragment 6-19 and Code fragment 6-20 ;
- Authentication of the user – once the CMPOOL has loaded the client module the application can request an authentication result from the CMPOOL through the authentication command. Refer to the Authenticate section on page 84 and Code fragment 6-21 to Code fragment 6-24.

The following sections will now look at these commands in more detail. During this discussion the reader will notice that the certificates discussed earlier will be used to a great extend. It usages will include: determine which client module to use; help facilitate the install of the client module; and also safeguard the communication between the CMPOOL and the Biometric Authority during authentication.

Client module lookup

The client module lookup will be used by the client application to check if the client module described in the certificate is present on the computer. The client application will therefore issue the LOOKUP command as detailed in Code fragment 6-11.

```
<clientpoolcommand>
        < clientpoolcommand action=”LOOKUP”>
        <issuer>
                BA name 2
        </issuer>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
        <BA_address>
                www.ba2.co.za
        </BA_address>
</clientpoolcommand >
```

Code fragment 6-11 Lookup command

When the CMPOOL receives the lookup command, it will check in its module directory (which contains all the installed modules) whether any of the modules has the specific module id (as specified in the certificate) and that it was issued by the issuer specified. It will also check with the BA to see if the installed client module is the latest version of the client module (ensuring that we are using the latest software). If the module is present and valid, it will inform the client in a lookup response with the present flag set to ‘true’, if not present or a newer version is available the present flag will be set to ‘false’.

```
<clientpoolresponse>
        <clientpoolresponse action=”LOOKUP”>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
        <present>
                true
        </present>
</clientpoolresponse>
```

Code fragment 6-12 Lookup response

Client module install

If the client module was not found by the lookup command (or the module is out dated) the application will issue the CMPOOL with an install command as formatted in Code fragment 6-13. The install command will contain the module id of the client module, as well as the address of the biometric authority (all of this information will be extracted from the certificate by the application).

```
<clientpoolcommand>
        < clientpoolcommand action=”INSTALL”>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
        <BA_address>
                www.ba2.co.za
        </BA_address>
</clientpoolcommand>
```

Code fragment 6-13 Install Command

Once the install command has been received by the CMPOOL, it will contact the Biometric Authority and request the module. The Biometric Authority will respond by transmitting the client module to the CMPOOL (if the Biometric Authority does not recognise the module an unknown module response will be given). The communication between the CMPOOL and the Biometric Authority will be performed in the same manner as above, by making use of XML (see Code fragment 6-14 to Code fragment 6-16).

```
<bacommand>
        <bacommand action=”MODULE_REQUEST”>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
</bacommand>
```

Code fragment 6-14 Module request from client module pool

```
<baresponse>
        <baresponse action="MODULE_REQUEST">
        <unknown_module>
                true
        </unknown_module>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
</baresponse>
```

Code fragment 6-15 Unknown module response from BA

```
<baresponse>
        <baresponse action="MODULE_REQUEST">
        <unknown_module>
                false
        </unknown_module>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
        <module>
                5SSeFDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </module>
</baresponse>
```

Code fragment 6-16 Known module response from BA

When the CMPOOL receives the response from the BA it will first check to see if the unknown module field is set to true or false. If true, the CMPOOL will inform the application through the response illustrated in Code fragment 6-17.

```
<clientpoolresponse>
        <clientpoolresponse action="INSTALL">
        <unknown_module>
                true
        </unknown_module>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
</clientpoolresponse>
```

Code fragment 6-17 Unknown module response from client module pool

On reception of the unknown module response, the client application will inform the user of the error.

If the CMPOOL receives the module (base64 encoded) from the BA (see Code fragment 6-16), it will first decode the base64 encoding of the module and then place the module in its installed client module directory. It will then inform the client application of the install in a known module response (see Code fragment 6-18).

```
<clientpoolresponse>
        <clientpoolresponse action=”INSTALL”>
        <unknown_module>
                false
        </unknown_module>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
</clientpoolresponse>
```

Code fragment 6-18 Known module response from client module pool

Client module load

Once the client application knows the CMPOOL has the appropriate module, it will issue the load command to the CMPOOL. This command will prompt the client module to load the module and make it active (in order to perform authentication). Before the CMPOOL loads the module, it will, however, perform an authentication of the module by looking at its digital signature and making sure it was issued by the issuer supplied in the command and that the module was not altered (by making use of the issuing authority’s digital certificate). This is done to ensure that the signal processing sub-section is legitimate and not altered to produce a fake template. The load command and response can be seen in Code fragment 6-19 and Code fragment 6-20.

```
<clientpoolcommand>
        < clientpoolcommand action=”LOAD”>
        <issuer>
                BA name 2
        </issuer>
        <BA_address>
                www.ba2.co.za
        </BA_address>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
</clientpoolcommand >
```

Code fragment 6-19 Load command

```
<clientpoolresponse>
        <clientpoolresponse action=”LOAD”>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
        <success>
                true
        </success>
</clientpoolresponse>
```

Code fragment 6-20 Load response

On a successful load response, the client will now issue the ‘authenticate’ command.

Authenticate

The authentication command received from the application can be viewed in Code fragment 6-21.

```
<clientpoolcommand>
        <clientpoolcommand action=”AUTHENTICATE”>
        <BA_address>
                www.ba2.co.za
        </BA_address>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
        <certificate>
                S43FDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </certificate>
</clientpoolcommand>
```

Code fragment 6-21 Authenticate command

Once the client pool receives the authenticate command, it will request a feature template from the client module with the id specified in the module id field (if this module needs to be loaded see above). The client module will then activate the biometric sensor and receive a raw sample. The feature will then be extracted from the raw sample and a feature template produced. This template will then be passed to the CMPOOL. Once the CMPOOL has the template, it will initiate communications with the server. In order to secure the communication, the CMPOOL will make use of a digital certificate and create a secure session. A possible protocol to use for this secure stream could be the secure sockets layer (SSL) protocol, which creates digital certificates to authenticate the server and client if needed [58]. SSL also encrypts the communication using asymmetric and symmetric encryption [58]. As soon as the secure connection has been established, the CMPOOL will request a random unique key from the server which it will use to sign the raw sample with (more on this in the server section). Once the CMPOOL has a signed feature template, it will send it to the server along with the user’s identification information (extracted from the certificate) in an authenticate request packet (see Code fragment 6-22).

```
<bacommand>
        <bacommand action="AUTHENTICATE">
        <user>
                John Doe
        </user>
        <user_id>
                988223452
        </user_id>
        <btemplate>
                S43FDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </btemplate>
</bacommand>
```

Code fragment 6-22 Authenticate command from CMPOOL

On reception of the authenticate command, the server will perform a verification on the user specified. Verification (one-to-one) has been opted for instead of identification (one-to-many) to speed up the authentication process. The server will then transmit a response back to the CMPOOL (more on this later).

Before transmitting the response, the server will sign it with the random key generated at the beginning of the transaction. The server will then transmit it back to the client in an authentication response packet (see Code fragment 6-23). Upon reception of the packet, the CMPOOL will check to ensure that the response (received in base64 encoding) was signed with the session key, which will expire after a set time, and also that it was not altered during transmission (using the digital signature).

```
<baresponse>
        <baresponse action="AUTHENTICATE">
        <user>
                John Doe
        </user>
        <user_id>
                988223452
        </user_id>
        <results>
                43S43FDe/josJV4hAHAAA==
        </results>
</bacommand>
```

Code fragment 6-23 Authenticate response from BA

The CMPOOL will now hand the response to the client (Code fragment 6-24).

```
<clientpoolresponse>
        <clientpoolresponse action=”AUTHENTICATE”>
        <certificate>
                S43FDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </certificate>
        <success>
                true
        </success>
</clientpoolresponse>
```

Code fragment 6-24 Result packet passed to client application

The response packet to the client application will contain the following information: the certificate used (this identifies the user, the BA and is also used for encrypting the communication), and whether or not the verification was a success (a Boolean value in the success field).

Why all the commands?

Could all of the commands specified above not be incorporate into one? The answer is yes: the client application could pass a single command, via the certificate, to the CMPOOL and request authentication. The CMPOOL could then, using its own logic, lookup the module (download it if necessary), load it, request authentication and pass the results back to the application (see Code fragment 6-24). The reason for adding all the extra commands is to allow the application more control over the process if required. The simplest and an easiest integration option, the single command from the client application, can be viewed in Code fragment 6-24.

```
<clientpoolcommand>
        <clientpoolcommand action=”AUTHENTICATE_HIDDEN”>
        <certificate>
                S43FDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </certificate>
</clientpoolcommand>
```

Code fragment 6-25 Single authenticate command

Having established the roles of certificates and the client module, the biometric scanning process needs to be examined.

Biometric Scan

As mentioned previously, the data collection process makes use of biometric scanners to capture a biometric sample and transform it into a raw sample (for processing by the client module). For the purposes of this study, the scanner can be anything from an optical fingerprint scanner to a normal web camera (used during facial recognition). Although the model is flexible with regards to the scanner used, the system still needs to make sure that the scanner is an authorised scanner and not a replacement generating fake readings or false raw samples. This is particularly important in a distributed environment, such as the World Wide Web, since the Biometric Authority cannot monitor the scanner used.

Consequently, some form of identification mechanism for the scanners is required.

A possible solution would be to issue each scanner with its own digital certificate and embed this certificate within the scanner. This would allow the client module to verify the authenticity of the scanner before accepting a biometric sample from it. Moreover, the certificate can not only be used to positively identify the sensor, but to ensure the integrity of the biometric sample as well. By signing the raw biometric sample using the certificate, the client module can verify that the sample is from a legitimate source and establish trust that the sample has not been altered since it left the scanner (data integrity). Although this is a possible solution a possible threat still exists. How could we prevent an attacker from removing the certificate from a valid scanner and placing it in another false camera? One possible solution is to try and "bind" the certificate to the camera by making use of a unique identifier embedded into the hardware. The certificate could thus only be used in conjunction with the unique identifier embedded in the hardware.

The Server

Now the client-side of the system has been examined, we can move on the server side (see Figure 6-7) and its inner workings to facilitate the authentication discussed in the previous sections.

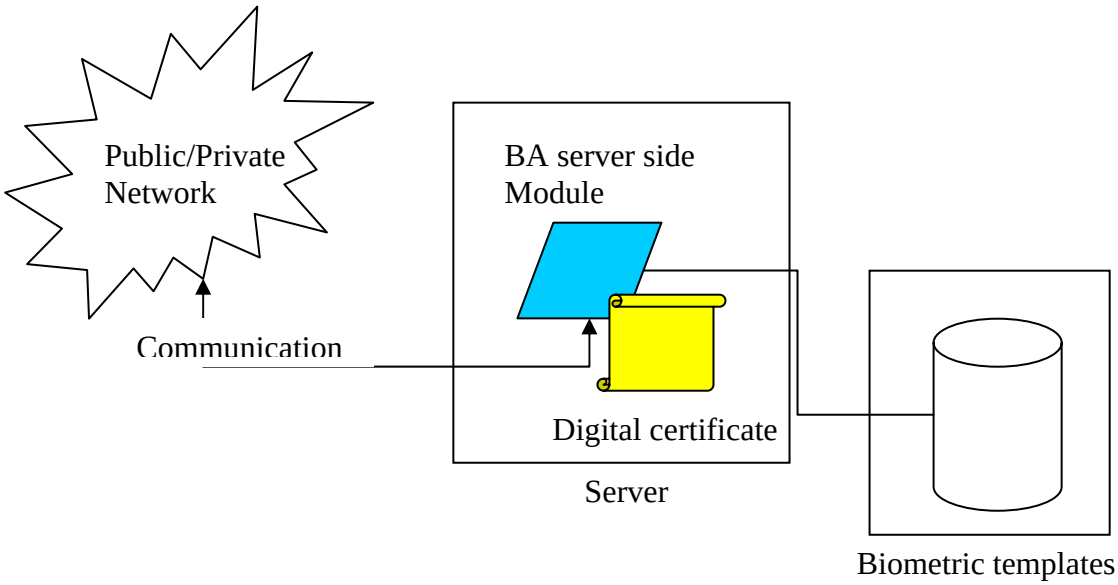

Figure 6-7 Server Side of the Model

The first observation to make is that the server has been divided in to two parts: the BA server side module and the templates database. The server also contains a digital certificate which will be used by the server module (these two components are discussed in more detail in the following two sections).

Template Data Store

In the beginning of this document, a number of the possible attacks a biometric system can face were listed. Within the list, there are two possible attacks

relating to the template database. Firstly, the alteration of the templates on the data store and, secondly, altering the template while being communicated from the data store to the matching module. The implication of any one of the above attacks is that the matching process could be fooled into generating a positive result. For this reason it is crucial that the biometric template be stored and transmitted in encrypted format, be it asymmetric or symmetric encryption.

Server module

The module known as the "server module" will be responsible for most of the server side action which includes:

- Distributing client modules;
- Performing verification.

Since the distribution of the client module has been discussed in great detail in the section above, this section will concentrate on the verification action of the server including the security techniques used to facilitate more trust in the authentication and response.

Performing verification

As mentioned previously, once the CMPOOL has received the feature template from the client module it will initiate communications with the server. Again, this communication will be made secure by using digital certificates. In particular, the certificate of the server will be used in order to: firstly, authenticate the server (making sure it is not a fake server), and, secondly, to set up the secure connection using a secure protocol (for example, SSL). This security can also be taken one step further and the actual client can be authenticated by making use of the individual certificate in order to prevent unauthorised users connecting to the server.

In the previous sections, the use of a random unique session key has been mentioned (to sign the feature template and the response). The model incorporates the secure key for two reasons: firstly, because the digital signature allows the system to check the integrity of the template (making sure it has not been altered in any way whatsoever during transmission), and, secondly, because it helps the system to prevent the replay of captured samples.

Once the server has generated the random key, it will be stored on the server with a timestamp attached. Then, when the server receives the signed template, it will first check to see if it was signed by one of the stored generated keys. If it was signed by one of the keys, the following will occur: first, the key will be checked to make sure it has not expired (i.e. that the timestamp is not older than a specific time). This will ensure that a sample cannot be reused more than a few minutes, hours or days later. Secondly, the server will then check to see whether the key has been used already. A key is considered 'used' once the server has received a template signed by that key. If the key has not been used, it will be flagged as used and the server will perform the verification (also know as one–to-one authentication — a one-to-one authentication mechanism is used due to speed issues), just to reemphasise we are making use of verification instead of identification in order to speed up the entire process since an identification could take up a lot of time depending on the database size. Coming back to the key if the key has, however, 'expired' or been flagged as used, the server will simply view the template as a replay attack and ignore it.

The results of the verification are then signed (using the same key) and encrypted with the public key of the user (found in their Biometric Authority certificate). This will ensure that only the legitimate user can decrypt the

response and will try to prevent a replay attack, in a similar manner as for the template, by signing the response with the random unique key.

The last area of concern with regards the server is its security. Aside of the usual preventative measures (firewalls, anti-virus software etc), the BA will be expected to periodically audit the system's sub-sections (the decision making module and storage sub-section) for anomalies. As mentioned previously, possible attacks on biometric systems include the alteration of the decision making sub-section and the template database. If an anomaly is detected during these periodical audits, the sub-section can simply be overwritten with an original copy.

Having described how the model's operational procedures and security mechanisms in some detail, it seems appropriate to review the arrangement in reference to the requirements established at the start of this chapter.

How have we addressed the implementation and security concerns?

In the beginning of this chapter a list of minimum requirements that needed to be addressed by the model for a successful, secure implementation was established. These requirements are listed below, together with the steps taken to meet them.

- The first main requirement (number 1) of the model was that it should be able to provide trusted biometric authentication. To accomplish this, three techniques have been incorporated: a rating system was added to the certificate (to aid an application in determining whether the biometric chosen is suitable, for example, whether its false accept and false reject rates are adequate); a digital signature is included in the client module (to ensure it is from a specific, legitimate source and that the data collection and feature extraction processes have not been compromised), and, thirdly, a periodic audit of the server's decision making and storage sub-sections was added.
- The second requirement was to secure the authentication process itself — this was accomplished by making use of digital certificates to:
    1. identify and authenticate the Biometric Authority as per requirement 2.1;
    2. identify the client and ensure it is a valid subscriber to the Biometric Authority (requirement 2.2);
    3. prevent alteration of the captured sample while being transmitted to the client module (achieved by embedding a certificate within the sensors) which relates to requirement 2.3.1;
    4. prevent a person from intercepting biometric samples through 'eavesdropping' by setting up a secure tunnel for communication (requirement 2.3.4).

  We also made use of a random digital key to prevent:
    1. alterations to the captured sample while being transmitted ;
    2. alterations to the response given by the server, which satisfies requirement 2.3.2 & 2.3.3.
- Requirement 3 was to provide a mechanism to ensure the biometrics' performance is suitable for the application. To satisfy this requirement, a rating mechanism was included in the BA certificate and the model employs verification to ensure fast authentication.
- The next requirement (number 4) was to be capable of supporting multiple biometric systems and this was accomplished by making use of different client modules.

- Within the model, the level of biometric integration (making use of APIs) was moved away from the physical application to circumvent upgrade issues and the complexities of installing and managing multiple plug-ins. To achieve this, the model makes use of a CMPOOL (acting as a buffer between the client module and the application) this satisfies requirement 5.
- Requirement number 6 was for the model to be flexibility, in the sense that it:
    1. would enable the application to easily use new biometric devices (requirement 6.1) (providing the devices could make use of new API standards). For this requirement the CMPOOL was developed to be a network type application (integration between the CMPOOL and application would therefore not be at code level). Since the CMPOOL is the only application to interact with the client modules it would be the only part needing upgrading and since integration is not at code level this process is extremely easy to administer);
    2. allows for the use of legacy biometric systems (requirement 6.2) (once again, the CMPOOL's usage in the model allows for this since its sole function is biometric authentication it needs to cater for as many APIs as possible, including legacy systems);
    3. is easily upgraded (requirement 6.3) (the placement of the 5 generic models and use of the CMPOOL will aid this, for example, if the decision making process needs to be updated the server's module is the only thing that needs updating. Similarly, if the feature extraction process, residing on the client, needs to be upgraded, the CMPOOL will simply install the new module as previously discussed).

Conclusion

This chapter has introduced a model which could allow for both the use of a single biometric across multiple applications as well as allowing multiple biometrics to use a single application. The proposed model has also been tailored to address the implementation and security concerns raised. The main features of the model are:

- Client module pool which is responsible for maintaining and loading of the client modules.
- Client module or plug-in which is the integration point into the biometric sensors.
- Biometric certificates and supporting certificates which was used to determine which client module to use; help facilitate the install of the client module; safeguard the communication between sensor and the client module as well as the client module pool and biometric authority.
- Certificate pool which is responsible for maintaining the user's biometric certificates
- Finally server which is responsible for storing user templates and performing authentication.

The next chapter builds upon this foundation and examines the three broad areas that are critical to any biometric application: security; value, and acceptability. The first area, security, will be addressed by placing the model within its broader context and introducing a trust model for the digital certificates. The second area, value, will be addressed through a detailed analysis of the biometric rating mechanism, and the third area, acceptability, will open up the important discussion of user privacy and the application's role within society.

Chapter 7 Implementation concerns for the model

Introduction

In the previous chapter, a model which would allow us to distribute a biometric to a number of different applications by making use of a central biometric data store was discussed. The core elements of the model — the client, client modules, client module pool, biometric authority certificate, certificate pool, and the Biometric Authority's server — were also assessed. These are described as 'core' elements because they are critical to the operation of the model. For example, if the certificate pool or client module pool are not operational, the entire model will not work.

Having looked at these core components, it is important to expand the discussion to look at factors which, will not technically affect the smooth operation of the entire model, if they are not implemented or addressed adequately the model's implementation could still fail. The following factors could affect the success of the model because they influence the security of the model, the value of the authentication process and the overall acceptability of the model. The three factors are: the rating system (designed to indicate to the application whether or not the biometric in question will meet its requirements); the trust model required for the digital certificates (in particular, how a trusted and efficient PKI implementation is necessary to ensure adequate security), and privacy (since the proposed creation of a central database of information always raises such concerns).

Rating the biometric

In chapter 5 of this study, the factors that need to be addressed when picking a biometric for a specific application were introduced. That initial discussion was important because it laid the foundations for determining a biometric rating system. The first question, nonetheless, might well be: why is such a rating system required? The answer refers back to the freedom of choice the system must allow users. If a user can select their biometric of choice from the wide range available, the system needs to be able to determine if the BA and its hardware are adequately suited for its need. In other words, if a high level of trust is required by the application the system needs to be able to assess whether the selected biometric can deliver enough confidence. To achieve this, the Biometric Authority certificate was expanded to include a rating field.

A number of questions need to be asked when deciding this rating. Firstly, can the biometric function in the environment the application will be used in? Secondly, will it perform according to the applications requirements (for example, will it be capable of handling a certain throughput)? Although sociological factors like hygiene, privacy and stigmatisation could potentially be assessed as well, the purpose of this rating system is to assess the biometric in relation to the environmental and application-specific problems raised previously in Chapter 5 from a technical perspective.

In the following section possible ways of grouping biometrics into 'areas of function' are explored. Please note that these groups have been made purely for demonstration purposes at this stage and some of the factors could be removed, extended or added to.

Environment

In chapter 5, the environment was divided up into two distinct types: the environment the sensor will be in, and the environment the people using the system will be working in. For the purposes of this discussion, these two types can be amalgamated into one by taking the more extreme as the benchmark. In other words, if the biometric sensor is placed in a dust free environment, but the user works in a dusty environment, the sensor will need to be categorised as one capable of being used in a dusty environment.

For demonstration purposes, the following sections list a possible distribution and corresponding rating based on environmental factors. This would allow the application to compare the biometrics' rated environment against the application-required environment to see if they match. The proposed distributions are: office environment; covered external environment; exposed external, and, finally, industrial environment. If a biometric sensor or its users will be placed in one of these distribution areas, the sensors/biometric chosen should be capable of an acceptable operation in this type of environment.

- **Office environment** — an office environment refers to an area where the people and sensors are placed in an almost dust free environment. The lighting within the environment is controlled, and the climate (humidity, temperature etc) is kept at a constant level. The users here do not perform manual labour so their biometric samples (for example, hands or fingers) are unlikely to be damaged.
- **Covered external environment** — a covered external environment refers to an area where, although outside, the dust and lighting is at the same level it would be in an office environment. The main difference is the climate, which can be dynamic within this environment. The humidity can be either high (wet) or low (dry) and the temperature can be warm or cold. The users in this environment will perform very light manual labour so the chances of damaging their biometric samples will still be slim.
- **Exposed external** — in this environment, the users or sensors might be exposed to some dust and/or strong light. As with a covered external environment, the climate will also be undetermined and potentially dynamic. The users here will perform medium manual labour, meaning that their hands and fingers might suffer some damage, for example, slight cuts and bruises. The users' biometric could be slightly dirty in this environment and, therefore, it is likely to be covered by a small amounts of grime.
- **Industrial environment** — an industrial environment will be the extreme environment. Here the users and sensors will be exposed to large amounts of dust, dirt, chemicals and strong light. The users' biometric samples may be covered with large amounts of grime. The users themselves will perform high amounts of manual labour and, therefore, potentially a great amount of damage could be done to their biometric samples — to such an extent that they may no longer be usable.

Before moving on to the application specific factors in the rating system, it is important to note that not all biometric methods are similar and, consequently, will not react to environmental aspects in the same way. For example, in an intensive manual labour environment, the hand or finger of a person might be damaged, but not their eye. So all the factors (dust, light, manual labour etc.) need assessment before the viability of specific biometrics can be determined.

Application-specific factors

This section focuses on the application-specific factors that can affect the efficiency of a biometric. The application factors include: the error rate (false accepts and false rejects rate); user throughput, and sensor security. Once again, when an application looks at the rating of a biometric it can compare its required aspects for, say, error rate and see if the biometric is adequate.

- **Error rate** — the fundamental function of a biometric is to compare a newly captured biometric sample to an enrolled template and find a match. To determine a biometric sensor's error rate, the odds of an impostor being accepted and an enrolled user rejected need to be calculated.
- **User throughput** — to determine this, the number of users a sensor can scan within a specific time span needs to be calculated.
- **Security** — when talking about security in terms of the rating system, it is how difficult it is for a person to fool the system using a fake biometric (for example, a false finger) that is determined; in other words, how much effort/money will be expended to do so.

Having looked at the environmental and application-specific factors, it is important to reiterate that the above discussion is designed purely to provide a feel for the kind of ratings required and that the list given above is not a definitive list, but rather meant to serve as a start to the discussion.

Who will rate the biometrics?

One last question that needs to be answered is who will rate the biometric for the Biometric Authority? One solution would be to simply let the BAs themselves rate the biometric. The problem with this approach is the potential temptation for BAs to start rating biometrics incorrectly in order to win more clients. To overcome this problem it might be best to institute a trusted rating authority with the sole mandate for rating the various biometrics. For example institutes like the SABS in South Africa or the international institute ISO could rate the biometrics for the authorities and give them a seal of authenticity.

Having proposed a possible rating distribution mechanism, the various trust models available can be discussed.

Trust Models

In the discussion of the biometric model, how digital certificates can be used to authenticate the players in a secure communication (as per the example of John and Pieter) was examined. During this discussion, how the authenticity of a certificate can be verified by making use of a Certificate Authority (CA) was briefly looked at, but how can the CA itself be trusted?

To solve this quandary, the system will need to have a trust model in place which will allow the signatures on a digital certificate to be traced to a 'known and trusted' entity. This section will briefly introduce two methods of achieving this: the single CA approach [79] and the configured plus delegated CA approach [79].

Single CA

The single CA model is actually the model used in our John, Pieter and Kathryn example. In the single CA model, there is only one Certificate Authority and it issues and signs certificates for the entire world [79]. Every piece of hardware and software must be configured with this CA's public key [79]. Provided that has

been done, anything (a user, piece of hardware or software) wishing to authenticate a certificate simply checks to see if it was signed by the single CA.

Configured plus delegated CA

The configured plus delegated CA approach is a very well know and widely used model which is currently being implemented within a number of web browsers [79]. This model works around a number of main Certificate Authorities. These main certificate authorities are known as configured CAs because their public keys are configured into every piece of hardware or software (as was the case with the single CA) [79]. Each of these configured CAs can authorise other CAs to grant certificates; in essence, vouching for the other CA by signing their digital certificate and stating that they are a trusted entity which can issue and sign certificates. These CAs are known as delegated CAs [79] and can also delegate and create further CAs themselves. If the system wishes to authenticate a certificate it will check to see if the certificate was signed by a configured CA. If it was not signed by one of the configured CAs it will be assumed that the CA is a delegated CA. The system will then check to see who signed the delegated CA's certificate. If the delegated CA's certificate was signed by a configured CA, the system knows it can trust the delegated CA and, thus, the certificates signed by that CA. If the delegated CA's certificate was not signed by a configured CA, the system will assume the signing authority was also a delegated CA and go through the procedure again. The system will continue this way until it reaches either a dead end and, therefore, an invalid certificate or a configured CA.

Other trust models

It should be noted that these two trust models are not the only trust models around. Other models that exist include: the single CA plus RA-model; the Oligarchy model; the Top-Down model etc. and the interested reader should refer to work carried out by Perlman — An overview of PKI trust models[79].

A trust model for the biometric authority model

The trust model used is an important part of the overall biometric model because digital certificates are used extensively throughout the authentication process in order to identify the user and biometric authority as well as secure communications. So how to select the most appropriate one? Although this decision requires extensive researching that is outside the scope of this present study, for the purposes of this discussion the configured plus delegated CA model is favoured, if nothing else because it is a proven method that has already been successfully model implemented in a number of web browsers across the world. Moreover, this existing, large pool of CAs could be used by the Biometric Authorities straight away.

Having discussed the rating system and trust models required, it is time to examine one of the most important aspects of any biometric implementation: privacy.

Privacy

What is privacy

There are a number of different definitions for privacy; the Oxford dictionary, for example, states that privacy is being private and describes private as: belonging to a person or group not public; confident; secluded.

Prabhakar, Pankanti and Jain [84] describe privacy as: the ability to lead your life free of intrusions, to remain autonomous, and to control access to your personal information [84].

When applying the above definitions of privacy to biometrics, the concerns raised can be divided into two types: physical privacy and information privacy [66]. In chapter 5, the physical privacy issues of stigmatisation [66, 84, and 85], personal harm [66, 85] and hygiene [66, 84] were discussed. The information privacy issues were also briefly looked at. Using the model discussed in chapter 6 would seem to solve most of the physical privacy issues (stigmatisation, personal harm and hygiene) because individuals are given the freedom to choose their own biometric. Information privacy, on the other hand, is much more significant when using a central database because the biometric templates will be administrated or controlled by a single organisation. If it was a distributed system, smartcard-based, for example, it would be less of an issue because the user would be in charge of their template database (i.e. the card). Consequently, this chapter will focus on information privacy issues.

What information privacy concerns does biometrics introduce?

This chapter will re-introduce the concerns raised in Chapter 5 in more detail. The information privacy issues examined will include: the loss of anonymity; scope creep; the 'big brother effect', and, finally, the risk of a stolen biometric.

The loss of anonymity

One of the critical aspects of Prabhakar, Pankanti and Jain's [84] definition of privacy is personal anonymity i.e. a person's ability to remain unknown to others and to be able to 'blend into the masses'. Many people believe that the deployment of biometric systems threatens this ability to be anonymous [85] because of the speed with which such systems can identify a person (a few seconds) and the difficulty of faking biometric samples (in comparison to making up a false telephone number or address) [85].

Scope Creep

Scope creep in a biometric system will occur when the information (the template) gathered is used for other reasons than it was intended for [66 ,84, 85]. Prabhakar, Pankanti and Jain [84] divide scope creep into two areas: function creep and application creep.

Function creep

Function creep implies that the biometric is not used for it initial purpose of identification, but rather for some other function. For example, it is theoretically possible to determine a person's medical health from their fingerprint (if it has a certain malformation) [84, 85] and some medical practitioners believe that the iris and retinal can also give an indication of certain medical illnesses [85].

Application creep

Application creep is when a biometric is used for identification, but not for the purpose it was initially gathered for and could lead to unwanted identification [84]. The biometric information of the user could also be sold to third parties [85] since the enrolled digital data could easily be copied and/or replicated [85]. These third parties could then use the information in their applications for identification purposes.

The big brother effect

Since biometrics provides us with the ability to identify a person a lot of people fear that the government or an organisation in charge of a database containing their biometric data will be capable of tracking their every move [66, 85]. A fear heightened by the possibility of covert recognition [84] — where a person's biometric is captured without their knowledge. An example of possible covert recognition would be using facial recognition in public places [84] — where the person's biometric is visible for all to see. Readers interested in facial recognition and the privacy issues relating to it can refer to the work of Bowyer [86].

Stolen Biometrics

One of the problems with biometrics is that a compromised or stolen biometric cannot be easily replaced or disabled [84]. You cannot simply re-issue someone's finger in the same way a credit or bank card can be and, consequently, people are particularly concerned about identity theft [66, 84], be it through replay of samples or the reproduction of the biometric.

Having established the main privacy concerns, ways of solving these issues can be explored. The following section suggests some initial ways of preserving user privacy.

Privacy: what to do?

How to address these very real privacy concerns? Perhaps the first observation to make is that the model outlined during this discussion cannot function without the user's certificate and private key. This suggests that, so long as an individual keeps their private key and certificate secure, it will be extremely hard for their biometric template to be stolen. This leaves the potential scope creep and big brother effect of having a single organisation in charge of the central biometric database.

Woodward [85], Prabhakar, Pankanti and Jain [84] describe methods that can be used to try and address these information privacy issues. The aforementioned authors do not, however, look at technical solutions, but rather the following regulatory measures as ways of assuaging users that their data/information will be kept private:

- Legal enforcement by the government — Government can implement laws to prohibit the sharing or selling of biometric information to third parties [84, 85]. One example could be the European Union legislation against sharing biometric identifiers and personal information [85].
- Assurance of self regulation [84] — the organisation gathering the biometric data can assure the users that they follow a set of ethical guidelines when working with their data. Woodward [85] suggests the incorporation of a Code of Fair Information Practices (CFIP) for biometric data which organisations can adhere to.
- A regulatory body — another solution would be to institute a regulatory body to enforce guidelines for the handling of information relating to biometric data [84].

Once again, a full examination of possible regulatory and technical measures that could be taken to ensure users' privacy is beyond the scope of this discussion. Nonetheless, an initial assessment of the problem suggests that expanding the roles of the bodies required already to manage the Biometric Authorities could be an expedient solution. These controlling bodies are already issuing digital certificates, rating the biometrics and authenticating these ratings, so a third function could be added to their remit: privacy protections. These

authorities could devise a set of guidelines and rules for the handling of biometric data and ensure that the Biometric Authorities maintaining the biometric databases follow these guidelines. If a BA does not follow the guidelines, the controlling authorities could simply revoke its status as an accredited Biometric Authority. A more technical solution could be to add an encryption process to the databases which makes the stored templates unusable to anybody except the holder of the encryption keys (in this case the user).

Conclusion

In this chapter, three elements which could make or break an implementation of the model described in chapter 6 have been discussed. These elements might not be critical for the model to function, but can enhance its security, the trust placed in the outcome of the recognition process, and the overall acceptability of the biometric implementation. The three elements discussed in this chapter where: the rating of the biometric; PKI trust relationships, and information privacy concerns.

Having looked at all the elements required by the model and the general implementation concerns, the following two chapters will examine two possible alterations that could be made to the model to enable it to function in special environments. The two adapted applications reviewed will be online recognition over the Internet and increasing the security of travel documents through biometrics.

Chapter 8 Online payment making use of a Biometric Authority

Introduction

In the preceding chapters, a model was introduced which can be used to incorporate biometric authentication into multiple applications. In these following two chapters possible implementations of the model will be briefly looked at. This chapter will focus specifically on a thin client, online application that can be delivered via the World Wide Web through a web browser, for example, Internet Explorer or Netscape.

Why online authentication?

As mentioned in the introduction chapter of this study, the internet has grown from primarily a research tool for the government, educational and non-profit organisations [62] to a medium that offers great economical advantages. For instance, it is capable of providing us with a means to:

1. conduct transactions over public networks for home shopping and banking [62];
2. use EDI (Electronic Data Interchange) for transactions with trading partners [62, 69, and 70];
3. gather information for market research and other activities [62, 68]; and
4. allow information distribution transactions [62].

Although it has grown into an extensively used commercial tool capable of delivering distributed applications to millions, the main problem faced when trying to make use of the medium is that security concerns were not prioritised when it was initially developed [59, 89]. Yet, now, after such explosive growth, particularly in the commercial arena, security has become a crucial concern [67, 89].

Good security requires strong authentication methods and systems must be able to identify legitimate users [58], but as mentioned in the introductory chapter, traditional authentication mechanisms (i.e. tokens, passwords) are not very effective — particularly in an online environment. Logging onto a website does not 'tell' a web server who you are [59]; it merely allows the web server to ensure that the information it presents is correct. There is nothing to stop a visitor using someone else's name or credit details and the public communication structure used by the internet makes this information easy to come by. The informational transactions are being conducted over a public network and could be subject to eavesdropping [53] by individuals who might use the information to steal a person's identity. A fact attested to by the continued growth of cyber-fraud.

The above problem appears, initially, to only affect the user whose identity has been stolen. So why should institutes and other organisations go to all the trouble, and cost, of incorporating biometric identification into their transaction systems? There are two main reasons why such institutes might incorporate biometric authentication. The first reason is to increase their market share by offering potential customers a trusted environment within which they can safely transact. And the second reason is non-repudiation (non-denial). Non-repudiation, through biometric authentication, will enable the institute to be certain that a user cannot deny the fact that they were the person conducting the transaction in question. A good example of the value and importance of non-

repudiation is in the case of an institute offering an online share management service. A share management service is a system that will allow a user to manage their portfolio (the shares and stocks they own) remotely. Typically, the user will log into his profile using a standard username and password combination (something that can be acquired quite easily). For this example, let us say that the user logged in and decided to buy shares in *Company X*. That night disaster strikes, *Company X*'s factory is lost in a fire and the share price drops dramatically. The user then turns to the company running the online share management system and denies ever purchasing the shares; moreover, he blames them for the system's poor security (since someone else could use his profile to purchase the shares) and initiates litigation against them. Without having authenticated the user biometrically, the online share management company may find it hard to contest the user's denial that they conducted the transaction in question.

What makes online authentication difficult

Before embarking upon a detailed discussion of the model and how to use it in an online environment, the following question requires answering: *what makes web based authentication special or "difficult"?* The following discussion is an attempt to answer this question.

The architecture of web-based operations (see below for details) raises several concerns. The main concern is the fact that it is, in effect, a thin client environment and all of the application's logic (a web site can be viewed as an application) resides on the server. In essence, this means that whenever something happens it will be processed on the server. For example, if a user logs in with a user name and password combination, the authentication is likely to happen on the server. Similarly, if something is purchased, the transaction is likely to be processed by the server. In all fairness, some transactions can be performed by the client browser, the login, for example, could be done on the browser by using a browser-side script language like JavaScript. The results would then be transmitted to the server and the server would continue with its processing. The problem in either instance is that the server needs to be sure of the integrity of the client browser. This is important to try and prevent someone from altering the authentication process and generating a fraudulent positive result or changing the result during submission to the server. In a "passive" distributed environment like the web this can be a difficult process. The environment is called passive in reference to the fact that, once it has served a web page (consisting out of HTML) to the browser, the web server cannot observe the client and/or browser's activity unless the user explicitly submits information back to the server. In other words, the server cannot actively monitor what is happening on the client side.

Why should this prove to be a problem when applied to the biometric authority model discussed previously? Firstly, the web server cannot be sure that the client has adequately authenticated the Biometric Authority (ensured that it is not fake) before continuing with the authentication process. Moreover, the web server cannot be sure that the client actually submitted the sample to a Biometric Authority for authentication in the first place — the client might just produce a fake 'yes' response. And, finally, how can the web server be sure that the response was not altered during transmission from the client browser?

These problems with online recognition suggest an awareness of them should be summarised as a new requirement for our module. The new requirement is as follows: *We need to be able to perform online biometric*

recognition in a manner that allows the web server to trust the response from the authentication process.

Consequently, the model needs to be adapted to allow some of the processing (biometric authentication) to be performed by web server. This seems the most expedient way of helping the web server be sure that the authentication was done correctly and the result it has is not fraudulent. The changes required to produce this adaptation will be examined in the following chapter, alongside some current implementations of online recognition.

Current attempts

Before moving on to a discussion of how biometric authentication can be accomplished through the World Wide Web (WWW) making use of the model, some current, possible implementation scenarios will be assessed. In this study, two distinct cases will be looked at: the fist being Teoh, Samad and Hussain's [89] online system, based on speech recognition, that make use of an ActiveX control. The second will be Everitt and McOwan's [90] Java-based authentication system.

Teoh, Samad and Hussain

Teoh, Samad and Hussain [89] suggest making use of speech recognition for online authentication. Since speech recognition has been discussed previously, the focus here will be on the mechanism used for the client-server interaction during verification (for more information about the enrolment process, refer to [89]). During verification, the user is presented with a web page with an ActiveX control embedded within it. ActiveX is a Microsoft Windows technology which allows developers to plug software modules into their applications [91]. ActiveX technology also allows a developer to embed a software module into a web page. This module can then be loaded in the client web browser and function like a normal application. Consequently, it will have access to the same resources a normal program running on a client's hard drive [59] unless restricted by the security manager (discussed later) of the browser (see [59] for more on web security).

The aforementioned ActiveX control of Teoh, Samad and Hussain, once loaded, displays two random digits. The user of the system then records the way they say the two digits by pressing a record button in the ActiveX control. Once the user's speech has been recorded it is encrypted and sent to the web server, along with the user's information. On the web server side, the response is received by Active Server pages (ASP), which fall into the CGI category (see below). Once the ASP has all the information it requires (user ID, recording etc.), it will invoke the speaker verification module which will authenticate the user. The ASP then makes use of the outcome of the verification process to determine whether it should grant the user access to certain resources.

Everitt and McOwan

Everitt and McOwan [90] suggest making use of a similar technology, which also allows developers to embed programs into web pages, namely, Java Applets. A Java Applet is an embedded Java application that runs within an applet viewer, for example, a Web browser [77]. The authentication mechanism that Everitt and McOwan suggest using is a dual biometric mechanism that makes use of both keystroke dynamics and signature recognition. Both of these inputs are captured by the Java Applet; the keystrokes dynamics are captured making use of the user's keyboard and the signature will be captured making use of the user's

mouse. Once captured, these details are sent to the server for verification. Once verified, the server will determine if it will grant the user access or not.

Having looked at two possible online authentication mechanisms, it is now possible to establish whether either of these mechanisms will be appropriate for the adapted model and what it needs to accomplish.

Problems with current methods

In the above discussion, although the two current implementations work extremely well, the main problem is that both are biometric-specific and, if another biometric system is selected by the user, the ActiveX control or Java Applet would need to be recoded to use the new biometric, for example, fingerprint. As a result, both mechanisms effectively lock the user into using the biometric the developers have chosen. This is the fundamental difference between current solutions and the one under discussion in this chapter since this model needs to be able to give the user the freedom to select any biometric they want.

Establishing the limitations of these current implementations was, nonetheless, important because knowing these — together with the new requirement recently incorporated into the model — it is possible to list the basic elements of an online system. Once listed, it is possible to ascertain what changes need to be made to the model to allow authentication making use of these elements.

Elements of the online system

Before going into the detail of an online biometric system, the main elements required to perform an online transaction need to be analysed. These elements can be seen in Figure 8-1 and include:

1. Institute requiring authentication;
2. Web browser on a Home/office computer through which the application will be delivered;
3. Communication network;
4. Biometric Authority client side elements; biometric sensor, certificate and client module pool;
5. Biometric Authority;
6. Certificate pool;
7. And, finally, cross-browser software which will allow the web-based application to request authentication from the client module pool through the web browser is required.

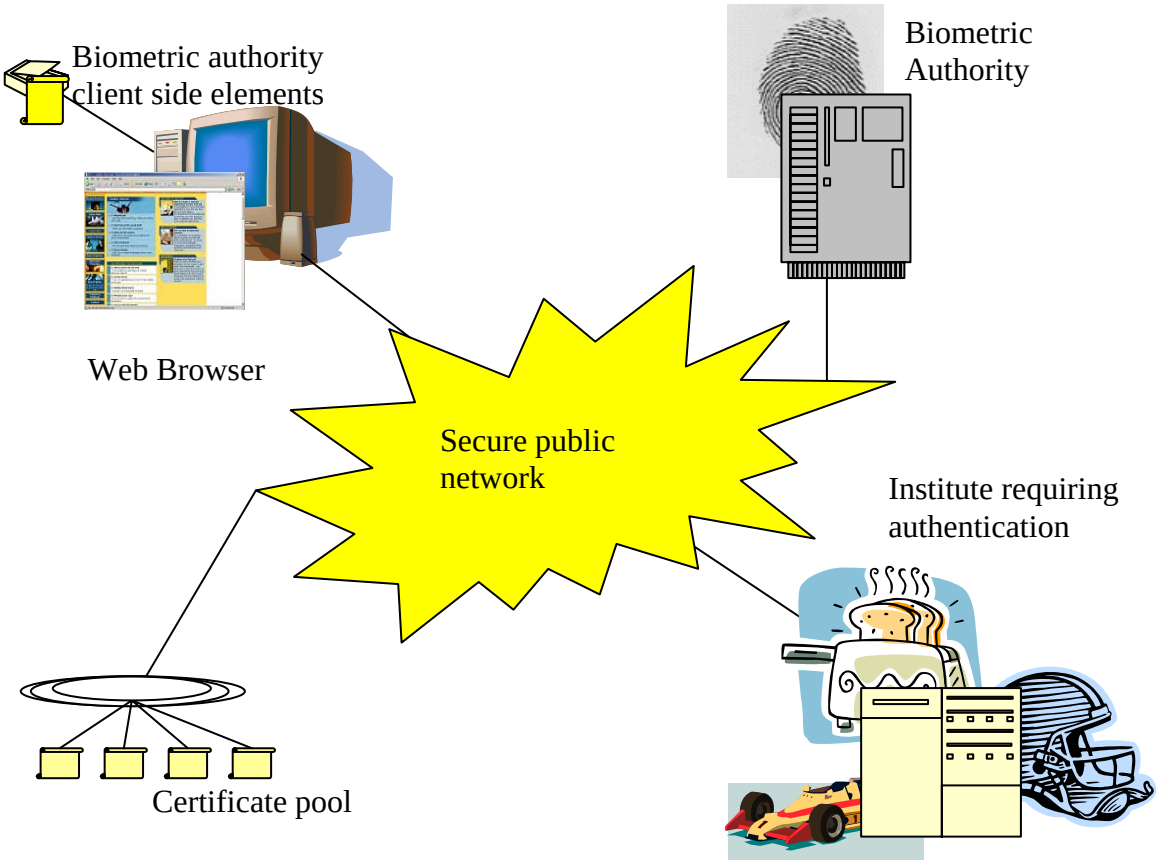

Figure 8-1 Generic Model for online authentication

Institute requiring authentication

The first component in the generic online transaction model is the institute requiring authentication. This institute will be an organisation supplying a service and/or product. The way this institute will interact with their clientele will be through the World Wide Web by making use of a web sever. The web sever will present information to the user through a web browser (see below). The user can now browse through all the services and/or products the institute provides and when the user wishes to perform a transaction (for example purchasing a DVD) the user will send a request to the web server through the browser. Once the server receives the request, it will process the request and display the results to the user as described in the following section.

Web server

In the above process the web server needed to accomplish two main activities: format data for display to the user and process data for transactions. The way the web server accomplishes this is by making use of web programming languages. The main languages used will be HTML (Hypertext Markup Language — used to create web documents [62, 76]) and other, dynamic languages that fall under the Common Gateway Interface (CGI — a program residing on a web server containing dynamic information which it can format into HTML and pass on to the web server and, by extension, the client [62]). CGI allows developers to perform dynamic operations like displaying database information to a user or processing a user's transaction. A number of different languages can be used during CGI development, for example, Visual Basic, Visual C++, Tcl, Perl etc. [62].

Web Browser on the home/office computer

The second component is the web browser on the client PC. The web browser will be the user's interface, receiving data from the server and displaying it for the user. A typical HTML form can be vied in Figure 8-2. In the figure, the two parts of the HTML form can be viewed. The top part is the HTML Code which is delivered from the web server to the web browser. The bottom part is an example of how it could be displayed to the user. The web browser will thus receive the HTML code and format it into a display for the user.

```
<html>
        <head>
        </head>
        <body>
                <form method="post" action="proFrm.asp" name="frmDemo">
                        <input type="text" name="product"><br>
                        <input type="text" name="price"><br>
                        <input type="submit" name="s" value="Submit">
                </form>
        </body>
</html>
```

HTML Code

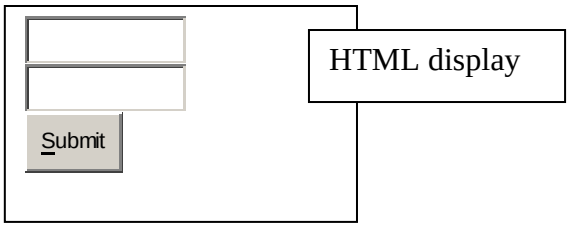

Figure 8-2 Typical HTML form

In Figure 8-2, the HTML code contains an input box for the product and one for the price. When the user hits the submit button the information in the form will be transported to the web server or, more specifically, the proFrm.asp page, which is a dynamic web page which will process the data in the form on the server.

Communication network

All of the above communications between the web server and browser will be conducted through the World Wide Web making use of the hypertext transfer protocol (HTTP). HTTP is an application-layer protocol used to communicate web multimedia and documents through the World Wide Web between the web browser and web server [62, 76].

Biometric Authority client side elements

The fourth component will be all the Biometric Authority's client side elements. This will include the client module pool (with the modules), the BA certificate and the biometric sensor.

Biometric authority

The fifth element is the Biometric Authority as discussed previously.

Certificate pool

The sixth element will be the certificate pool, also, as discussed in previous chapters.

Browser Software (Plug-in)

The final element needed will be the client browser software that will be used to communicate with the client module pool (as exemplified by the two current implementation examples used earlier). The application within the web browser will need to capture the biometric sample. This software, a plug-in for the web browser, will perform the following tasks:

1. Manage the user certificate — The plug-in will ascertain the location of the user's certificate server, the username under which the certificate was stored and the location of the user's private key (in order to decrypt the certificate since it is stored in an encrypted format on the certificate pool, as mentioned in the previous chapter).
2. Communicate with the client module pool — The plug-in will issue the commands to the client module pool for authentication.

Adapting the model for the World Wide Web

Having established what makes online authentication difficult or 'different', and the basic elements, it is now possible to start adapting the original model to cater for this special environment. The main change is that the submission of the template for authentication will be performed by the web server and not the client module pool; in other words, once the web browser plug-in (mentioned above) has captured a biometric template it will transmit the template to the server. The server, in turn, will transmit the template to the relevant Biometric Authority for authentication.

Now that the elements have been established and adapted, it is necessary to start examining how the various parts will interact with each other for maximum efficiency, synergy and robustness.

The main things required to achieve this harmony are:

1. adaptation of the HTTP protocol;
2. addition of some new HTML Tags;
3. addition of a new command to the client module pool.

Online biometric authentication

HTTPB

As mentioned above, the first aspect requiring attention is the adaptation of the HTTP protocol. The reason for this adaptation is to allow the browser, via the plug-in, to setup the right environment and all the elements for authentication. One example of an alteration of the HTTP protocol is the use of HTTPS where the uniform resource locator[7] (URL) starts with an https://. What this does is to indicate to the web browser that it needs to establish a secure connection with the web server by making use of SSL [58].

For the purpose of this study, the alteration to the protocol will be known as HTTPB (where the B stands for Biometric). If a URL starts with httpb:// it will

[7] A URL is the term used for the identifier of a web site or web page [62], examples of URL's are http://www.google.com, https://www.amazon.co.uk, https://10.0.0.2/index.asp

be an indication to the web browser that a secure connection needs to be established where user authentication will be achieved using a Biometric Authority. When the web browser receives such an indication it will first check to see if it has the HTTPB plug-in installed (the HTTPB plug-in is the browser software mentioned above). If the plug-in is not installed, the web browser will inform the user and prompt them to download it from an appropriate location. If the plug-in is installed, temporary control will be given to the plug-in. The plug-in will then retrieve the user's certificate from the certificate pool indicated in the plug-in's configuration. It will then use the HTTPB address provided to connect to the certificate pool and the username to extract the appropriate certificate. Once it has the certificate, it will decrypt it using the private key of the certificate. Using the decrypted certificate, the plug-in will authenticate the client to the server (via the certificate) and the server to the client (the web server will also be authenticate to ensure it is a valid commerce server). After authentication, a secure "tunnel" can be created between the web server and the browser, a possible protocol for this secure tunnel can be SSL in combination with the server's digital certificate and the client's certificate.

Once this secure tunnel has been created, the plug-in can submit information about the user and the Biometric Authority to the web server. With this information, the web server can connect to the Biometric Authority and authenticate that it is a valid BA; it will also authenticate itself to the Biometric Authority. Once the web server and Biometric Authority are confident they are dealing with valid systems, the communication channel will be completed with an additional secure "tunnel" being created between the two.

With the two secure tunnels in place (between the web browser, web server and Biometric Authority), the plug-in can now allow the client module pool to interact with the Biometric Authority (through the web server) to:

1. retrieve the appropriate client module if it is not installed; and
2. request the random key for signing the biometric template (see the discussion of the model for more info on this process).

In the above discussion, the incorporation of a new protocol to setup all the elements and environment for authentication has been examined. It has also been mentioned that within this environment the browser and browser plug-in will interact with the client module pool. In the following section, the reader will be introduced to a new HTML tag which will allow this interaction to take place.

New HTML tags

In this section, a possible solution that will allow the web browser to communicate with the client module pool will be proposed. The client module pool will, in turn, communicate with the biometric sensor (fingerprint, iris, voice scanner etc.).

At first glance, this interaction might not appear that difficult, but it is complicated by the built-in browser security managers. A means of interaction which will not compromise the security managers must be established. A security manager is a tool built into a web browser to try and protect the user's PC from malicious applications delivered through the web. Refer to [59] for further information about malicious ActiveX controls, java applets, as well as the various security managers like the java sandbox.

Another problem is the fact that there are a multitude of different browsers on the market including Microsoft IE, Netscape, Mozila etc. and the software must work on all of these different browsers.

The way to overcome both of these security and compatibility issues is by using the browser plug-in mentioned previously. These plug-ins will most likely be developed by the suppliers of the browsers and in such a way that they will allow a web page to interact with them. The plug-in will then be allowed to 'step out' of the browser environment (leaving behind the restrictions of the various security managers) and interact with the client module pool directly. The way such plug-ins will function and step out of their corresponding browser environments is a discussion perhaps best left to the browser experts like the Netscape and Internet Explorer development teams. This study will concentrate on how the plug-in is activated and how it will interact with the client module pool and web server.

The key to how the browser will activate the plug-in will be the structure of the web page. As mentioned previously, a web page is constructed from HTML and this means that the problem will be solved at the web development level. The main problem the developer will face is the use of different Biometric Authorities. Another problem for the web developer will be security: how can they ensure the security of the transaction being conducted? The solution to the first part of the second problem is the plug-in. The W3C standards body will have to agree on a standard HTML tag which can indicate to the browser that any action performed related to that tag must be handled by the plug-in. This will be similar to the Applet tag used in Java (Code fragment 8-1).

```
<Applet code="TestMe" width="200" height="122">
        <param name="zone" value="GMT">
 </Applet>
```

Code fragment 8-1

The Applet tag gives an indication to the browser that anything within this tag should be handled by the Java virtual machine's Applet viewer. The browser then hands control over to the Java virtual machine to perform the task requested by the tag (depending on the security settings) and without concern for the vendor's identity (for more information of Java, Java Applets refer to the exploring JAVA textbook [77]).

An example of what the biometric plug-in HTML tag could look like can be seen in Code fragment 8-2.

```
<Bioscan>
        <BioButton value="Click me to capture Biometric"
        BgColor="red" height="50"
        width = "100">
        <input type=" bioSample" name="bytesam">
        <input type="bioKey" name="key1" value=
        "SK45J9ECS/cyjosHAGgAAAA=="
</Bioscan>
```

Code fragment 8-2

The <bioscan> tag tells the browser that the code in-between must be handled by the biometric plug-in. Within the tag, a few input types have been added – a "biobutton", "biosample" and "biokey". The function of the biobutton will be to place a button on the HTML page which, once clicked, will prompt the plug-in to request a biometric template from the client module pool. The value in the bioKey field will be used by the client module pool to sign the template (see below for more details). Once the template has been received from the client module pool, the plug-in will place the biometrics byte code representation in the

first "biosample" tag it can find. This will then be submitted to the server for authentication (more on this in the implementation section).

Client Module Pool

As mentioned in chapter 6, in the base model the client module pool will be responsible for all the authentication steps: requesting the template from the sensor; signing it with the random key which it received from the biometric authority; transmitting the signed template, and receiving the authentication response from the Biometric Authority.

In an online environment, as discussed previously, some of the functionality must lie on the web server for security reasons. The functions the web server will be responsible for are:

1. requesting the random key from the server and passing it to the plug-in (which, in turn, will give it to the client);
2. transmitting the signed template to the BA server;
3. receiving the signed response and processing it to see if the user was authenticated.

To facilitate the above requirements, an extra command needs to be added to the client module pool. This command will be used by the browser plug-in to pass the random key to the client module pool (CMPOOL) and request a signed template from the client module pool. The new command can be seen in Code fragment 8-3.

```
<clientpoolcommand>
        <clientpoolcommand action="GET_TEMPLATE">
        <secure_key>
                CM3180221-8947-92FD-DDE88DE255E2
        </secure_key>
        <certificate>
                4YAxuFDeJ9ECS/cyjosJV4hAXCSaAAAAGgAAAA==
        </ certificate>
</clientpoolcommand>
```

Code fragment 8-3 The get template command

Once the CMPOOL receives the get template command it will request a raw biometric sample from the scanner (as discussed in chapter 6). Once the raw sample have been received and verified, it will be signed with the secure key. This signed template will now be base64 encoded and handed back to the plug-in — as illustrated in Code fragment 8-4 (please note, the CMPOOL will perform the module install, load etc. as described in the chapter concerning the model).

```
<clientpoolresponse>
        <clientpoolresponse action=" GET_TEMPLATE">
        <template>
                S43FDeJ9ECS/cyjosHAXCSaAAAAGgAAAA==
        </template>
</clientpoolresponse>
```

Code fragment 8-4 The get template response

In the above sections the alterations to certain elements of the online environment have been discussed. In particular, the discussion has examined:

1. adapting the HTTP protocol;
2. adding new HTML Tags; and
3. adding a new command to the CMPOOL.

It is important to now look at how all of this will link together for authentication.

Implementation

Having looked at the elements, and required alterations to the elements, it is possible to look at how this will work in a 'true life', online environment.

A user will log onto a website making use of a HTTPB URL, for example httpb://www.mystore.co.ut. Once the user has entered the URL, the web browser will, firstly, resolve the host address of www.mystore.co.ut and then, once the address has been resolved, the web browser will connect to the web server to see if it does exist. Once the web browser has established that the web server does exist it will hand over control to the browser plug-in (if the plug-in is not installed the web browser will prompt the user to install the plug-in). Once control has been handed over to the plug-in, it will setup the environment and a secure tunnel with the server. Once the secure tunnel has been created between the web server and web browser, the web server will create a secure tunnel between itself and the Biometric Authority (see the above discussion for more information on how these tunnels are established).

With the secure tunnels in place and all the players authenticated (web browser through the client's Biometric Authority certificate, and the web server and the Biometric Authority through their certificates), the web server will serve web pages to the user. The user can now browse the website until they reach a page requiring biometric authentication — be it to login to a secure section of the site or to process a transaction. Once the user comes across such a page, the browser will be informed by the "bioscan" tag in the HTML document. As mentioned previously, this bioscan tag will contain a "biobutton" which will place a button on the HTML page. It will also contain a "bioKey" field which will contain the secure random key from the Biometric Authority and be used to sign the biometric template (see chapter 6 for reasoning behind signing of templates). This means that, before the page is server to the web browser, the web server needs to request a random key from the Biometric Authority. Once the key has been received, it will be stored on the web server. The key will then be placed in the bioKey field and the page will be served to the client browser.

In the browser, the user will see a button (generated by the biobutton tag). Once the user clicks on the button, the web browser will inform the plug-in and hand control over to the plug-in. The plug-in will then extract the secure key from the bioKey field. The plug-in will then request a signed template from the CMPOOL by issuing the get template command with the random key and client certificate within it. The CMPOOL will then load the client module making use of the information from the certificate (see chapter 6 for details on how the client module gets loaded). The client module will then request a raw sample from the biometric sensor. When the sample has been received, the features will be extracted from the sample to produce a feature template. This feature template will then be signed with the key and passed to the CMPOOL and, in turn, the plug-in.

When the plug-in receives the signed template, it will place it in the biosample field and then submit the page to the server. The server will then extract the

sample and request authentication from the Biometric Authority by transmitting the signed template to the BA making use of Code fragment 8-5 — this is similar to the command the CMPOOL would have sent to the BA (see chapter 6).

```
<bacommand>
        <bacommand action="AUTHENTICATE">
        <user>
                John Doe
        </user>
        <user_id>
                988223452
        </user_id>
        <btemplate>
                S43FDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </btemplate>
</bacommand>
```

Code fragment 8-5 Authenticate command from client module pool

The BA will then review the validity of the signed template i.e. check to see if it was signed with a valid key which has not expired or been used (see chapter 6 for more detail). Once the server has performed the verification, it will sign the response with the key and transmit it back to the web server see Code fragment 8-6 — this is similar to the response the CMPOOL would have received from the BA (see chapter 6).

```
<baresponse>
        <?xml version="1.0" ?>
        <baresponse action="AUTHENTICATE">
        <user>
                John Doe
        </user>
        <user_id>
                988223452
        </user_id>
        <results>
                43S43FDe/josJV4hAHAAA==
        </results>
</bacommand>
```

Code fragment 8-6 Authenticate response from BA

On reception, the web server will check to ensure that the response (received in base64 encoding) was signed with the session key, which will expire after a set time, and that it was not altered during transmission (using the digital signature). If the response received is 'yes', the web server can then log the user in or process the requested transaction.

Meeting the new requirement

Having looked at the implementation of web-based authentication, using the model, it is important to review the process and ensure the new requirement that was determined at the beginning of this study has been adequately addressed. In other words, has the system been able to perform biometric recognition in such a manner that the web server can be confident of the authenticated response? The three way secure communication pattern outlined above (see the above discussion the secure tunnels) would appear to have satisfied this requirement

because the web browser or client can only communicate with the Biometric Authority through the web server, and the response from the BA is similarly not received or processed by the client, but rather the web server so it can be sure that it originated from the BA.

Conclusion

Online transactions are certainly the way of the future. The 'e-revolution' is happening and banks, along with many other organisations, are being forced to change the way in which they conduct business. As is so often the case, these changing trends have brought online transaction "hijacking" and identity theft with them. These abuses or e-crimes have become commonplace and are likely to continue to increase as the cyber world matures. It seems probable that, before society can fully embrace the advantages offered by this new cyber-world, a more effective means of protecting identities and transactions needs to be implemented and the best way of providing such positive identification at this time is through biometrically-enabled systems.

Chapter 9 Biometric authentication in travel documents

Introduction

This chapter will focus on the implementation of a Biometric Authority within an environment which, while still almost exclusively paper-based, has recently been the centre of much government interest and debate. The implementation in question is machine-readable travel documents (i.e. passports or visas) that are electronically linked to the bearer using a biometric.

Most countries protect the integrity of their borders through strict access control. After the September 11, 2001 attack on the World Trade centre, American and other national authorities began investigating ways of further increasing their security and safety measures in an attempt to prevent future terrorist attacks. Traditionally, access control in and out of a country has been the reserve of ID documents such as passports and visas. However, more and more countries are recognising that more is needed to positively identify an individual in a world where identity theft is rife and forged passports are commonplace. One of the steps countries are taking to improve their identity documents is the inclusion of machine-readable biometrics — to help ensure the document does actually belong to the individual presenting it.

An example of this is the Enhanced Border Security and Visa Entry Reform Act
of 2002 [55] — introduced in the US House of Representatives on December 19, 2001 which states:

"Not later than October 26, 2004, the government of each country that is designated to participate in the visa waiver program established under section 217 of the Immigration and Nationality Act shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable biometric and document identifying standards established by the International Civil Aviation Organization."

Machine-readable travel documents

Currently, the International Civil Aviation Organization (ICAO) is the international authority charged with the task of developing a standard for machine-readable travel documents (MRTD). 1986 saw the formation of a Technical Advisory Group on Machine-Readable Passports by the ICAO. The ICAO describes three types of MRTD [82]:

- A passport which indicates a person is a citizen of the issuing country;
- A visa used to indicate that the issuing country grants a non-citizen the rights to enter the country for a set period;
- Other travel documents which could be issued to non-citizens for travel across borders. An example would be a special purpose identification/border-crossing card.

To be able to incorporate a biometric in the above mentioned documents, the ICAO suggests three different implementation options [82]:

- The biometric will be contained within the document by making use of an appropriate storage medium. For example, a chip, magnetic stripe or 2D barcode;
- The biometric templates will be held by the issuing bodies (for example, a central database at each embassy in the case of foreign countries);
- The biometric will be extracted from a visual element within the document (for example, the photo of the face in the document).

Although storing a biometric within the travel document — option 1 and 3 above — does allow authorities to 'biometrically' link the document to the bearer, this situation is still open to potential compromise, namely, possible reproduction by an unauthorized individual or group. This is because the actual template is stored locally on the document. If a skilful forger can replicate the biometric capturing and storing process — be it through inside help, espionage, or other means — the production of fake identity documents becomes possible because the process is only confirming that the biometric held locally matches the live sample being presented. One can only imagine how easy this process would be if option 3 is used and the biometric template is being extracted from the photo in the passport.

Current chip technologies make it extremely difficult for an individual to tamper or forge the content on the chip. However, in the unlikely event the above scenario does occur, authorities will have to amend their current processes. This would require an extremely costly process of recalling and reissuing passports. Another problem we will be faced by only making use of smartcards is a problem mentioned before – duel enrolment. By making use of a central database before authorities issue a passport to and individual they can check to ensure the person has not enrolled himself under another identity. For these reasons, the second option — a central biometric repository — would appear the more satisfactory. This approach will generate an adequately secure environment (much like a secure chip/smartcard etc) while affording the flexibility to alter the biometric template and capturing/storing processes in the event of a compromise.

By making use of a central database we do however now face the problem of possible loss of privacy by the individual. Although the issue of privacy has been mentioned and discussed previously in this study, it is important to mention once again that a number of processes and procedures will have to be put in place in order to protect the individual's privacy. Since an in-depth discussion of the legal requirements is beyond the scope of this present study, this chapter will concentrate on the implementation side of instituting a Biometric Authority for international border control.

The use of a single international Biometric Authority appears impractical, not only because it will require countries to relinquish some of their autonomy, but because it forces every nation to conform to a standardised biometric implementation — one their citizens might have rejected for sociological, technical, economical or political reasons. Allowing countries to maintain their own national repositories seems to be the solution. However, this does present some problems. Firstly, the port system needs to know which national repository to query and prevent communication with a masquerading repository. Secondly, the biometric repository needs to be sure it is communicating with a valid port system. Thirdly, all communication needs to be safeguarded to prevent sample capture and replay, and also to prevent unlimited access to a large number of raw biometric samples (since these samples could be used to commit identity theft and espionage). And finally, for redundancy purposes, an alternative method needs to exist in the event that a national repository cannot be reached. While some of these issues are easy to address in a more general context, the

autonomy and divergence of the countries participating in the process makes solving them more complex.

Most of the above problems are addressed by the model introduced in chapter 6. As a result, the initial implementation requires little more than tweaking the model to fit into the existing "paper-based" travel documentation environment. Nonetheless, issues such as the offline recognition requirement, which has not been addressed previously, still need to be tackled and some elements of the model require interchanging to introduce more stringent security measures.

Elements of a biometric travel document

The elements for a biometric travel document system can be seen in Figure 9-1. The elements consist of:

1. a border post visitor admin software or port system;
2. the Biometric Authority client-side elements — biometric sensor, client module pool (CMPOOL) and client module;
3. a communication network;
4. a Biometric Authority;
5. the travel document.

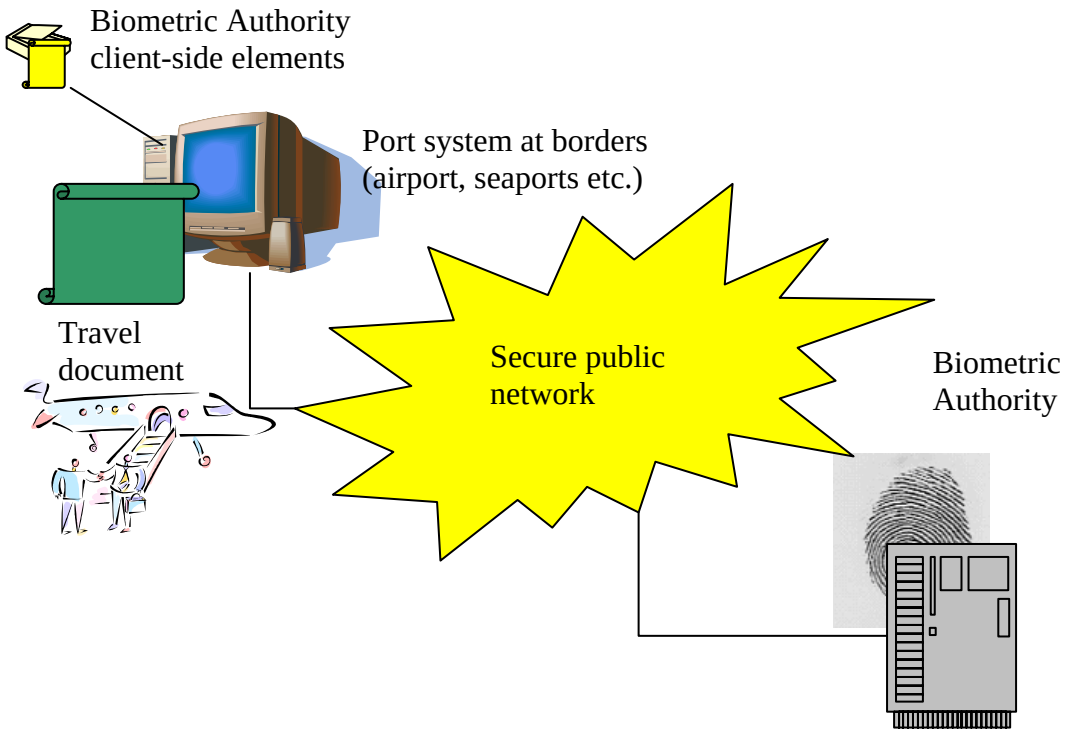

Figure 9-1 Elements of a biometric travel document system

Port system

The port system will be the admin software used by the border post authorities to control visitor movement. The application will be responsible for receiving information from the traveller (by reading their travel documentation) and verifying that the documentation does belong to the individual through biometric authentication.

Biometric Authority client-side elements

The second component is the Biometric Authority's client-side elements. These include the client module pool (with the client modules) and the biometric sensor. In the previous chapter it was noted that the user's BA certificate is part of the client elements, this is still true to an extent, but, in this environment, it forms a more integral part of the traveller's documentation (see below).

Communication network

All of the communication between the port system and the Biometric Authority will be conducted through a combination of private and public networks which need to have an up time of 100%. Since most experts agree that an uptime of 100% is practically impossible, the redundancy measures mentioned earlier (in the event that the repository cannot be reached) become a critical implementation consideration (more on this later).

Biometric authority

The fourth element is the Biometric Authority — as discussed previously.

Travel document

As the main unknown, the main focus of this discussion will be on the travel document, which needs to be electronically linked to an individual using a biometric. In order to accomplish this in conjunction with a central database, the digital certificate — issued to the user by the Biometric Authority — needs to be embedded in the document. Consequently, this environment does not require a central certificate pool, but, rather, each individual traveller will carry their own certificate pool within their travel documentation.

Altering the model for travel

With all the elements identified, it is possible to assess the alterations or tweaks that need to be made to the model in order to meet the requirements mentioned initially. These alterations can be grouped into two main areas: encryption and placement.

The encryption changes will be applied to the digital certificate and, in particular, where the certificate's private key will be held. These changes will be made to both increase security and to facilitate offline authentication in the event that the server cannot be reached.

The second set of changes will be made to the placement of the five sub-sections of the generic model. In chapter 6, the data collection and feature extraction sub-sections were placed on the client and the decision making sub-system and template database on the server. Again, for security reasons, the feature extraction sub-section will be moved to the server (this change will be discussed later).

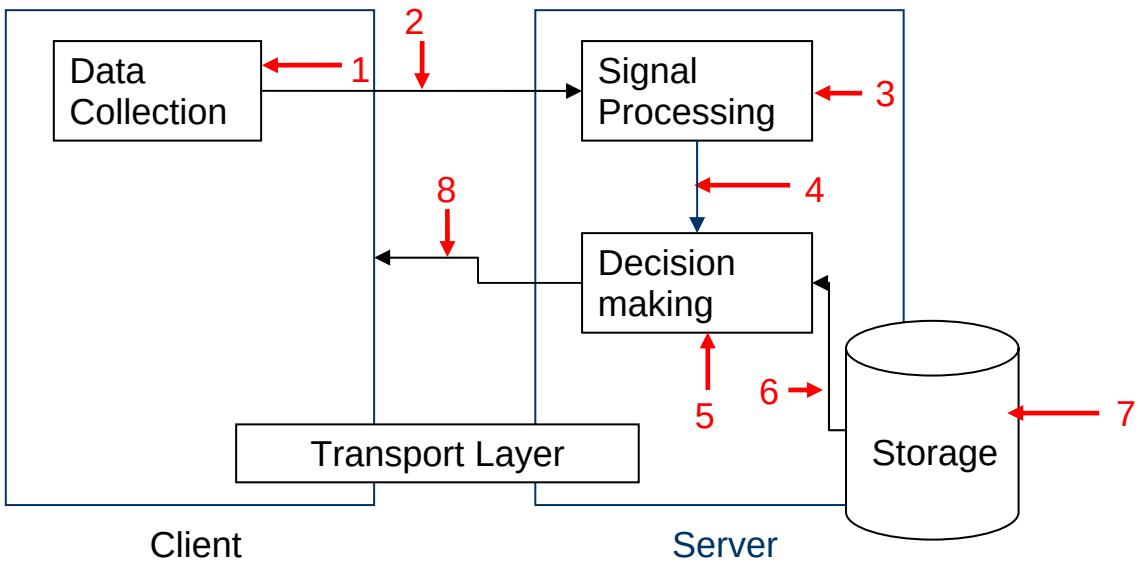

Figure 9-2 New sub-section layout with the security concerns indicated (Adapted from [71, 72])

In Figure 9-2, the sub-system layout and the corresponding security concerns are illustrated. Since most of the security concerns were addressed earlier in this study, the focus here will be on the alterations required for this particular implementation. In particular, number 2 (the transmission of the raw biometric sample to the server), number 3 (alterations to the feature extraction process to produce a fake template), number 4 (alterations to the template in transport to the decision making sub-section) and, finally, number 5 (alterations to the decision making sub-system itself).

Travel document model

This section will start with the required modifications to the traveller's Biometric Authority certificate, followed by the new sub-system arrangement on the server, and will conclude with the client module security enhancements.

User certificate

In the previous chapters, the Biometric Authority certificate was stored and managed by a certificate pool. In the proposed biometric travel document system, there will be no certificate pool because the certificate will be stored on the actual travel documentation. This is because storing the certificate on the document — as illustrated by the traditional, PC-based model outlined in chapter 6 — allows the system to identify both the bearer of the document and the Biometric Authority the document is connected to. Although this is enough information to perform recognition with a Biometric Authority, the certificate must also be able to facilitate authentication if the Biometric Authority is unreachable due to communication problems. For this reason (and others to be discussed later), additional information will be stored on the certificate. As a result, the modified certificate will be referred to as a Document certificate rather than a Biometric Authority certificate.

Document Certificate

A document certificate is an electronic certificate similar to the Biometric Authority certificate discussed in chapter 6 and, in the same way, a large amount

of different bits of information can be stored within the document certificate (DocC). IN this instance, the information will include:

1. Information about the individual — passport number, name etc. — used to identify the individual to the port software.
2. The public key of the private/public key pair generated by the issuing authority when the travel document was produced (the issuing authority will embed the public key within the document and store the private key with the biometric template in its data store — in chapter 6, the user held their private key. This private/public key pair will be used to protect the raw sample during communication (see below for more info).
3. Identification information relating to the data store(s) (multiple data stores can be used for redundancy) — pointing the port software to the appropriate data store.
4. A digital tag identifying which client module to use.
5. A copy of the enrolled feature template — this template will be used in the event of communication failure (solving the offline recognition issue).
6. Supporting information like version numbers of the biometric software etc.
7. A digital signature — all the information in the DocC will be signed by creating a hash of the information and encrypting the hash with the issuing authority's private key [58].

One piece of information not embedded within the certificate will be the rating of the biometric since, in this instance, the user will not be responsible for selecting the Biometric Authority, but, rather, their country; ensuring the effectiveness and usefulness of a particular biometric will be the responsibility of the countries themselves.

Server

The server-side of the passport Biometric Authority consists of two parts: a biometric template database — containing the templates of all individuals enrolled on the BA, and a server-side module — responsible for a number of the operations described in Waymans' generic biometric model [4].

The first operation performed by the server will be signal processing or the feature extraction process. In this adapted module, the reason for locating the feature extraction process on the server (and not on the client module as previously) is for enhanced security. Since this system will become an integral part of a nation's security, it is important to ensure that nothing be compromised. As mentioned in chapter 6, one possible attack on biometric systems is to replace the feature extraction module and produce fraudulent feature templates. With the feature extraction module on the client this would be a much simpler task. Moreover, this arrangement makes monitoring the feature extraction module more difficult because it can be distributed to a number of systems and countries. Moving the feature extraction module to the server greatly increases the system's administrators' ability to protect the module and pick up changes if it is compromised. One possible way to accomplish this could be to regularly audit the module and replace it with an original copy if any anomalies are detected. Also, by moving the sub-section to the server, the template produced by the feature extraction process can be safely transmitted to the decision making sub-section since both are on the same, secure server.

Client module

In the discussion of the document certificate, it was mentioned that the certificate will contain the public key and the Biometric Authority server will retain the private key of the key pair. This is to protect the raw biometric sample being

transmitted from the client module pool to the server for recognition. This protection is achieved by encrypting the raw sample with the public key in the certificate prior to transmission. The biometric server then decrypts the sample with the private key it has stored (no one else has access to the private key) and passes the decrypted sample to the feature extraction module.

An extra command needs to be added to the client module pool (CMPOOL) to support this functionality. This command will instruct the CMPOOL to perform authentication by passing an encrypted raw sample to the server. The command for this process can be seen in code fragment 1.

```
<clientpoolcommand>
        <?xml version="1.0" ?>
        <clientpoolcommand action="AUTHENTICATE_RAW">
        <BA_address>
                www.ba2.co.za
        </BA_address>
        <module_id>
                CM3180221-8947-92FD-DDE88DE255E2
        </module_id>
        <certificate>
                S43FDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </certificate>
        <port_certificate>
                p43FWf9EQA/cyrwer22AXCSaAWWssAAGgA34A==
        </port_certificate>
</clientpoolcommand>
```

Code fragment 9-1 Authenticate command

This command will generate a slightly different reaction from the client module pool than detailed in chapter 6; instead of passing a feature template to the server for recognition, it will transmit a raw biometric sample, but, before it does that it will authenticate the port system to the Biometric Authority so that it is sure it is dealing with a valid port system and not a fake one trying, for example, a denial of service attack. The port system's digital certificate will be placed in the port certificate field in the command.

Implementation

Having reviewed the elements and modifications required for this biometrically-enabled travel document system, it is possible to analyse how these elements will interact when a traveller arrives at a port system.

The first event that will occur when a traveller arrives at a border post is they will be requested to present their travel documentation to the port system. The port system will then read the document certificate embedded within the travel document (it could be stored on either a smartcard, 2D barcode etc. Once the port system has extracted the certificate, it will validate the certificate as detailed in chapter 6. Once the system is happy that it is dealing with a valid certificate, it will give the certificate to the client module pool and request authentication of the person (using the command in Code fragment 9-1).

Once the client module pool receives the command, it will connect to the Biometric Authority and verify it is a legitimate authority (preventing fraudsters from setting up a fake repository which simply generates a 'yes' response to forged travel documentation). Once the Biometric Authority has been

authenticated, the client module will authenticate the port system to the Biometric Authority using the port system's certificate in the command. The traveller's document certificate will be authenticated by the Biometric Authority at the same time. After the authentication, a secure tunnel will be created between the port system and the Biometric Authority. With the secure tunnel in place, the client module will request a random secure key to sign the raw sample with (in order to prevent replay).

Once the connection has been established and the key received, the client module pool will install (if not installed), load and verify the authenticity of the appropriate client module. Once happy with the client module, the client module pool will request a raw sample from the module. The scanner will then capture a raw sample and transmit it to the client module, which will then pass it to the client module pool. The client module pool will then sign it and encrypt it using the public key from the document certificate. This packet will then be sent to the server for authentication.

Upon reception of the encrypted, signed raw sample, the server will extract the traveller's private key and decrypt it. The signature will then be verified using the random secure key (as detailed in chapter 6). Once satisfied with the sample, it will be passed to the feature extraction module and the feature template will then be given to the decision module. The response received will be signed and transmitted back to the client module pool. The response will then be verified for authenticity using the signature (see chapter 6 for more information). The response of the authentication will then be given to the port system using the response in Code fragment 9-2.

```
<clientpoolresponse>
        <?xml version="1.0" ?>
        <clientpoolresponse action="AUTHENTICATE_RAW">
        <certificate>
                S43FDeJ9ECS/cyjosJV4hAHAXCSaAAAAGgAAAA==
        </certificate>
        <success>
                true
        </success>
</clientpoolresponse>
```

Code fragment 9-2 Result packet passed to port system

Conclusion

The threat of terrorism has never been so predominant. As a result, the attitude towards national security has become much more serious and security budgets have been enlarged. Countries are looking for alternative, improved ways of protecting their citizens and this has renewed interest in tamperproof biometric travel documents, often previously considered too expensive.

Among the number of different ways to incorporate a biometric within a machine-readable document, the use of a Biometric Authority (central database) appears the most promising. Although this does not make the system foolproof, it substantially raises the cost (effort) of forgery and can act as an effective deterrent.

The above discussion outlines the establishment of a central data repository which incorporates PKI extensively as a way of raising the cost of

forgery and preventing fraudulent travel documents from being circulated. Although the focus has been on the recognition process, the enrolment process needs to be analysed with equal care. When a travel document is being produced, the architects need to incorporate into the biometric enrolment process a means of preventing individuals from registering multiple identities, much like the process involved in [83] and [3].

Chapter 10 Study Summary

Introduction

We live in an increasingly fast-paced world and the Internet has become an essential tool for many of us. The medium allows us to communicate and interact in new and exciting ways and has had a huge impact on the way we shop, bank, socialise and work. The fact that the Internet now connects millions of people has opened up new commercial opportunities and made it a viable business tool, but it still lacks the security of more traditional approaches. The Internet's academic and research-orientated origins [62] meant that the early developers did not place as much emphasis on security as perhaps they should [59]. The two main security issues — communication and identification — still limit the efficacy of many internet transactions. Although a lot of time and effort has gone into finding solutions for securing communication, for example, SSL, the way internet-based applications (including web sites) identify users is still far from ideal from a security perspective. It was a desire to address this limitation that prompted this study.

Early beginnings

This enquiry began with an investigation into the various means by which individuals might be identified and established there are three main ways (refer to [58]). The first way is by a possession or token (smartcard, digital certificate etc.); the second is by something they know (a secret, like a username/password combination), and the third is through something they are (a physical feature) or something they do in a unique way — this is known as biometrics (examples are fingerprint, voice, iris, etc.).

Further investigation revealed there are also three main problems with identification mechanisms or systems. The first is forgery or 'cracking' — producing a false identification mechanism which will be viewed as the original. The second is loss or damage — this is where an identification mechanism cannot be used because it is lost, forgotten or damaged. The last problem is transportability — where the identification mechanism is either given to another person or stolen. The next step was to assess the various ways of identifying individuals against these problems. The review determined that all the systems are open to forgery and lost or damage, but that biometrics tackle the problem of transportability (summarised in Table 10-1 (repeated from chapter 1)). A finding that suggested biometrics would be the best tool to use.

	Something you have	**Something you know**	**Something you are**
Forgery	Yes	Yes	Yes
Transportability	Yes	Yes	No
Lost/damage	Yes	Yes	Yes

Table 10-1 Comparison of identification techniques

A formal definition of a biometric authentication is the automated identification, or identity verification, of an individual using either a biological feature they possess (physiological characteristic like a fingerprint) or something they do (behaviour characteristic, like a signature) [1]. In other words, to capture a sample of a person's biometric (a fingerprint, iris, voice sample etc.) and compare it to an enrolled biometric template captured previously. By automated,

it means that a computer will handle the decision making process and decide whether the samples match or not.

Armed with this definition, the following problem statement was formulated:

"***How should we implement a central biometric repository which will hold biometric templates and perform the identification step required across multiple applications?***"

Steps towards finding a model to fit the problem

To solve the above statement, the range of biometrics available and how they operate needed to be assessed. As well as establishing how biometric systems function, the enquiry was undertaken to establish what makes a good biometric (i.e. the characteristics of a good biometric). A generic biometric model was discovered and evaluated — see in Figure 10-1 below (repeated from chapter 2).

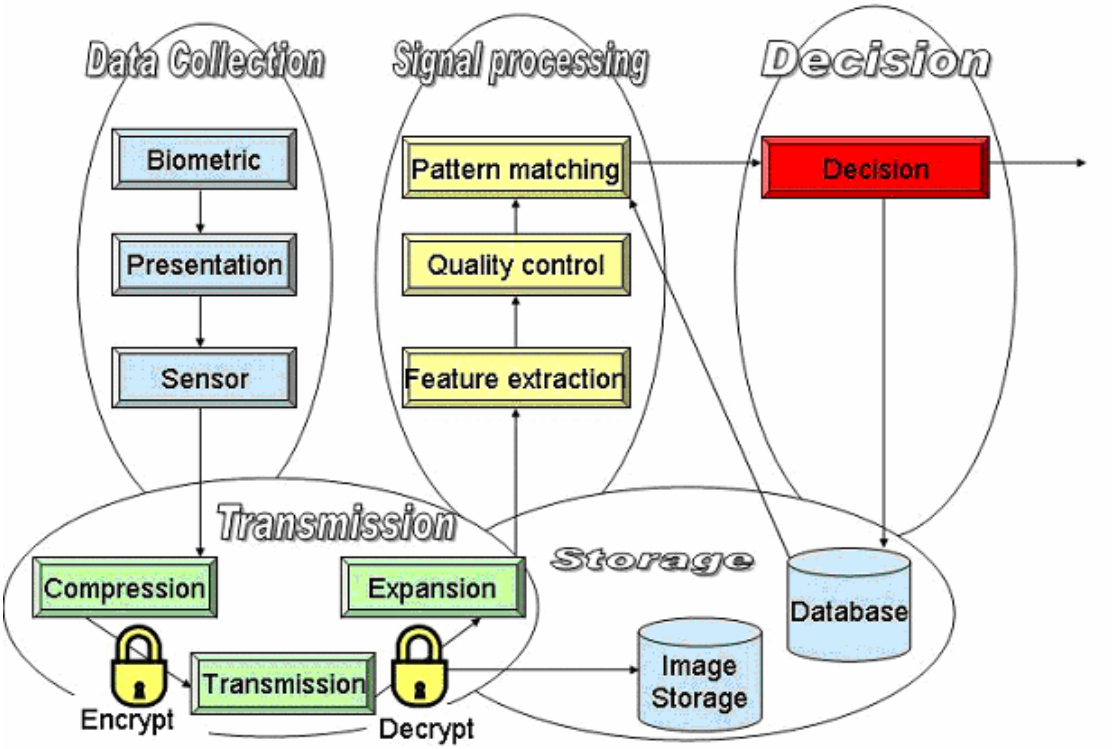

Figure 10-1 Generic model for biometric systems [Adapted from 10] (Refer to the Appendix 1 for a colour version of the figure)

Having established how biometric systems work, a way of determining the effectiveness of a biometric (i.e. its performance and accuracy) needed to be discovered. A detailed analysis of how different biometric systems function helped determine the small differences between them. For the purposes of this study, fingerprint, iris recognition, hand geometry, face recognition, signature recognition, keystroke dynamics and speaker recognition were assessed.

This research revealed a kaleidoscope of solutions and so any external factors that could influence the efficiency and acceptance of a biometric were assessed as well. This phase of the research exposed three main types of external factor: environmental; people and application-specific.

With all of the preliminary and necessary contextual research concluded, a model that would allow one biometric to be integrated into multiple applications was designed. During this process it became apparent that, if designed in a particular way, this model could also solve the issue of how to allow multiple biometrics to be used in one application.

The main components of the model can be viewed in Figure 10-2 and Figure 10-3.

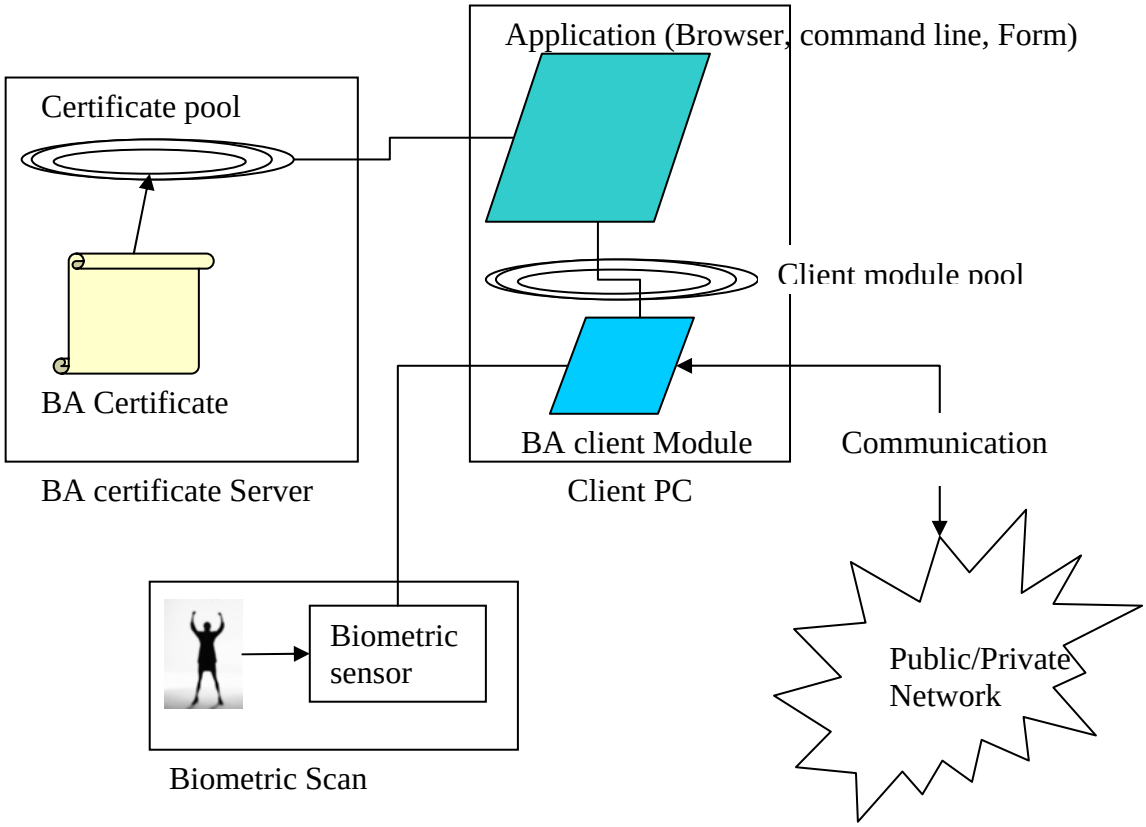

Figure 10-2 Client Side of the Model

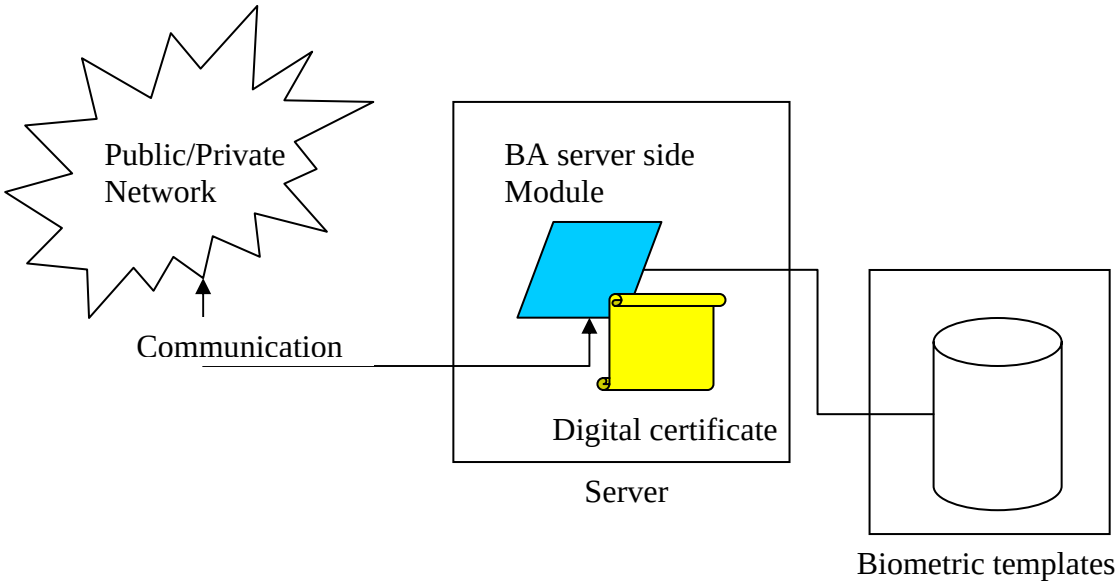

Figure 10-3 Server Side of the Model

The model was designed to work in the following manner: a user enrols their biometric at a Biometric Authority; the BA verifies the person's identity (making use of traditional documents), then captures and stores their biometric template. The BA then issues the person with a Biometric Authority Certificate which they can install on their system. At the same time, the user will receive the certificate's private key (relating to the public key on the certificate). Once enrolled in this manner, the user's application can perform biometric authentication by capturing the user's sample and submitting it to the BA for verification. During this process, the application will make use of the Biometric Authority Certificate to determine which Biometric Authority to use and which client software to use. It will also determine whether the biometric in question is adequate enough to meet the application's needs (using a rating mechanism). Finally, the certificate will be used to secure the entire process (see chapter 6 and 7 for more details).

Once the basic model had been designed, it was possible to look at adapting it for two special applications. The applications were a thin client application, for example, the Internet (chapter 8) and biometrically-enabled travel documents (chapter 9).

Having looked at what was discussed during this study, the following section will briefly outline what was not assessed and why.

Excluded from the study

During this study, a number of different features of biometrics and the model were reviewed, but there are a few aspects of the field that were not

The first aspect that was not examined in detail was the biometric enrolment process since the model's main function was that of recognition. An important point to note is that recognition cannot ensure that a specific identity belongs to a person; it can simply verify that the biometric sample and identity presented at a particular time is the same as the one presented during enrolment. Proper, controlled enrolment — where the identity of a person is verified before enrolment — will be crucial.

The second important factor that was just touched on and not examined in detail was privacy. Privacy is a very big concern, especially when the system relies on a central database under the control of one entity.

The third major aspect was the storing of the enrolled templates — the format they are saved in and, in particular, whether or not this format will allow the system to use the template with other biometric algorithms (supplied by different vendors).

Other factors not looked at included:

- possible usage of smart cards in the model;
- the entity responsible for rating the various biometrics;
- the entity responsible for ensuring the CAs work in a controlled fashion;
- the CA model which would be the best for the model.

Future work

As this study of a central database model makes apparent, there are several aspects that can and should be the subject of future studies, and of particular importance amongst these is privacy.

Privacy

One of the areas open to far greater research is that of user privacy — especially with a model that uses a central database. A common fear people have is that, once their biometric sample has been enrolled with an organisation, the organisation in question will be capable of using it to steal their identity. As a result, there is plenty of scope for developing a comprehensive privacy statement to try and allay such fears. There is also a need to look at more technical ways of trying to protect the user's privacy. Of particular interest is the possibility of developing a matching algorithm that makes use of encrypted templates. A potential solution could be to encrypt the templates at the time of enrolment with a secret key (called key A) before storing them. Then, when the user submits a template for authentication, it is also encrypted using another secret key (called key B). Key A and key B will be generated in such a way that they are a unique pair and an authentication of two templates will only work if the enrolled template is encrypted with the one and the submitted template is encrypted with the other. If only the user has access to these keys, it could help ensure that the organisation storing the templates is unable to use them fraudulently. Things to consider for this research include:

- Generation of the unique key pair
- How will the encryption function?
- How will the matching algorithm function? This will require an examination of:
    - Matching encrypted templates;
    - Performance implications when matching encrypted templates;
    - How will the matching be affected by the encryption — especially since no two samples (or templates) are ever exactly the same (matching is based on statistical averages)? This problem arises because all biometrics, physiological and behavioural, are affected by the behaviour of individuals. For example, a user is unlikely to always place their finger on a fingerprint sensor in exactly the same way (behavioural difference).
- The level with which the user's privacy is protected.

Conclusion

This study has introduced the possible use of biometrics in a central database environment. This approach allows a single biometric to be used in multiple applications and multiple biometrics to be used in one application. Aside of individual method preferences (whether you prefer to use your iris or finger etc.), using biometric authentication holds many advantages over traditional authentication mechanisms like tokens or passwords. These advantages make it highly likely that, once reliable biometric systems are readily available at affordable prices and the issues preventing acceptance, like privacy concerns, have been addressed adequately, the use of biometrics will grow rapidly and become an increasingly central part of our daily lives, replacing inferior alternatives like tokens and usernames/passwords.

Bibliography

[1] Wayman J.L., Alyea L., **Picking the Best Biometric for Your Applications,** National Biometric Test Center Collected Works, vol. 1, J. L. Wayman, Ed. San Jose, CA: National Biometric Test Center, 2000, page 269 - 275

[2] Wayman J.L., **Biometric Identification and the Financial Services Industry,** National Biometric Test Center Collected Works, vol. 1, J. L. Wayman, Ed. San Jose, CA: National Biometric Test Center, 2000, page 263 – 266 & Congressional Testimony of May 20, 1998

[3] Wayman J.L., **Biometric Identification Technologies in Election Processes-Summary Report,** National Biometric Test Center Collected Works, vol. 1, J. L. Wayman, Ed. San Jose, CA: National Biometric Test Center, 2000, page 253 - 261

[4] Wayman J.L., **Fundamentals of Biometric Authentication Technologies,** Proc. Of CardTech/SecurTech Conference, CardTech/SecurTech, Chicago, USA, 1999, page .81 - 101

[5] Mansfield T., Kelly G., Chandler D., Kane J., **Biometric Product Testing Final Report,** Centre for Mathematics and Scientific Computing National Physical Laboratory Issue 1.0, 19 March 2001

[6] Pankanti S., Bolle R.M., Jain A., **Biometrics: The Future of Identification,** IEEE Computer Special Issue on Biometrics vol. 33, No. 2, February 2000, page 46 - 49

[7] Erik Bowman, **Everything You Need to Know About Biometrics,** Identix Corporation, January 2000, http://www.ibia.org/EverythingAboutBiometrics.PDF.

[8] Pankanti S., Prabhakar S., Jain A.K., **On the individuality of fingerprints,** IEEE Transactions on Pattern Analysis and Machine Intelligence vol. 24, issue 8 , August 2002, page 1010 - 1025

[9] Wayman J.L., Reinke R.E., Wilson D.L., **High quality speech expansion, compression, and noise filtering using the sola method of time scale modification,** Twenty-Third Asilomar Conference on Signals, Systems and Computers, 1989. vol. 2, October 30 - November 1 1989, page 714 - 717

[10] Wayman J.L., **A generalized biometric identification system model,** Conference Record of the Thirty-First Asilomar Conference on Signals, Systems and Computers, 1997. vol. 1 , November 2 - 5 1997, page 291 - 295

[11] Daugman J., **High Confidence Visual Recognition of persons by a Test of Statistical Independence,** IEEE Transactions on Pattern analysis and machine intelligence, vol. 15, no. 11, November 1993, page 1148 - 1160.

[12] Wayman J.L., **Evaluation of the INSPASS Hand Geometry Data,** National Biometric Test Center Collected Works, vol. 1, J. L. Wayman, Ed. San Jose, CA: National Biometric Test Center, 2000, page 33 - 40

[13] Jain A., Ross A., Prabhakar S., **Fingerprint Matching Using Minutiae and Texture Features,** Proc. of Int'l Conference on Image Processing (ICIP), Thessaloniki, Greece, October 7 - 10 2001, page 282 - 285

[14] Jain A.K., Prabhakar S., and Ross A., **Fingerprint Matching: Data Acquisition and Performance Evaluation,** MSU Technical Report, TR99-14, 1999, http://web.cps.msu.edu/TR/MSUCPS:TR99-14

[15] De Ru W.G., Eloff J.H.P., **Enhanced password authentication through fuzzy logic,** IEEE Expert, vol. 12, issue 6 , November - December 1997 page 38 - 45

[16] Öden C., Erçil A., Yıldız V.T., Kırmızıta H., Büke B., **Hand Recognition Using Implicit Polynomials and Geometric Features,** Proceedings of SIU '2001, May 2001, page 614 - 619
[17] Jain A.K., Ross A., Pankanti A., **A Prototype Hand Geometry-based Verifcation System,** Proc. of 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), Washington D.C., March 22 – 24 1999, page 166 - 171
[18] Gupta G., McCabe A., **A Review of Dynamic Handwritten Signature Verification,** Technical article Department of Computer Science, James Cook University Townsville, Qld 4811, Australia, September 1997, http://www.cs.jcu.edu.au/~alan/Work/HSV-Lit_rev.ps
[19] Herbst B., Coetzer H., **On an off-line signature verification system,** Proc. of the 9th Annual South African Workshop on Pattern Recognition. (DM Weber, BM Herbst and JA du Preez eds), 1998, page 39 - 43
[20] Al-Abbas R., **A prototype system for off-line signature verification using multilayered feedforward neural networks,** Minor thesis, RMIT, Department of Computer Science, Melbourne, March 1994, http://www.cs.rmit.edu.au/~vc/papers/abbas-mbc.ps.gz
[21] Deng P.S., Liao H. M., Ho C.W., Tyan H., **Wavelet–based Off–line Signature Verification,** Computer Vision and Image Understanding, vol. 76, no. 3, 1999 page 173 - 190
[22] Sabourin R., **Off-Line Signature Verification by Local Granulometric Size Distributions,** IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 9, September 1997, page 976 – 988
[23] Justino E.J.R., Yacoubi A.E., Bortolozzi F., Sabourin R., **An Off-Line Signature Verification System Using HMM and Graphometric Features,** Fourth IAPR International Workshop on Document Analysis Systems, (DAS 2000), Rio de Janeiro (Brazil), December 10 - 13 2000, page 211 - 222
[24] Jain A.K., Griess F.D., Connell S.D., **On-line Signature Verification,** Pattern Recognition, vol. 35, no. 12, 2002, page 2963 - 2972
[25] Wessels T., Omlin S.W., **A Hybrid System for Signature Verification,** IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN'00), vol. 5, Como, Italy, July 24 - 27 2000, page 5509 - 5514
[26] Munich M. E., Perona P., **Camera-Based ID Verification by Signature Tracking,** Proc. of the 5th European Conference on Computer Vision EECV'98, Freiburg, Germany, June 1998, page 782-796
[27] Munich M.E., Perona P., **Continuous Dynamic Time Warping for translation-invariant curve alignment with applications to signature verification,** Proc. of 7th IEEE International Conference on Computer Vision, vol.1, Korfu, Greece, September 20 - 27 1999, Page 108 - 115
[28] Ross A., Jain A., Reisman J., **A Hybrid Fingerprint Matcher,** Proc. of 16th International Conference on Pattern Recognition (ICPR), Quebec City, vol.3, August 11 - 15 2002, page 795 - 798
[29] Britto, A.S., Sabourin R., Bortolozzi F., Suen C.Y., **Recognition of Handwritten Numeral Strings Using a Two-Stage Hmm-Based Method,** International Journal on Document Analysis and Recognition, special issue on multiple classifiers for document analysis applications, vol. 5, 2003, page 102–117
[30] Monrose F., Rubin A.D., **Authentication via keystroke Dynamics,** Proc. of the Fourth ACM Conference on Computer and Communication Security, Zurich, Switzerland, April 1997, Page 48 - 56
[31] Monrose F., Rubin A.D., **Keystroke Dynamics as a Biometric for Authentication,** Future Generation Computing Systems (FGCS) Journal vol. 16, issue 4 Special issue on security on the Web, page 351 - 359

[32] Beymer D.J., **Face Recognition under Varying Pose,** Proc. Of IEEE Computer Society Conference on Computer Vision and Pattern Recognition CVPR '94, June 21 - 23 1994, page 756 - 761
[33] Wiskott L., Von der Malsburg C., **Recognising Faces by Dynamic Link Matching,** Proc. Int'l Conference on Artificial Neural Networks, ICANN'95, Paris, eds. F. Fogelman-Soulié, J. C. Rault, P. Gallinari, and G. Dreyfus, publ. EC2 & Cie, , October 9 – 13, page 347 - 352
[34] Wiskott L., **Phantom Faces for Face Analysis,** Pattern recognition vol. 30 no. 6, 1997, page 837 - 846
[35] Wiskott L., Fellous J., Krüger N., Von der Malsburg C., **Face Recognition by Elastic Bunch Graph Matching,** In Intellignet Biometric Techniques in Fingerprint and Face Recognition, eds. LC Jaim et al., publ. CRC Press, ISBN 0-8493-2055-0, 1999, Chapter 11. page 355 - 396
[36] Zhao W., Chellappa R., Rosenfeld A., Phillips P.J., **Face Recognition: A Literature Survey,** ACM Computing Surveys (CSUR) archive vol. 35 , issue 4, Year of Publication: 2003 ISSN:0360-0300, December 2003, page 399 - 458
[37] Soong F.K., Rosenberg A.E., **On the use of instantaneous and transitional spectral information in speaker recognition,** IEEE Trans. Acoustics, Speech and Signal Processing, vol. 36, no. 6, June 1988, page 871 - 879
[38] Sonng F.K., et al., **A vector quantization approach to speaker recognition,** AT&T Technical Journal, vol. 66, March - April 1987, page 14 - 26
[39] O'Shaughnessy D., **Speaker recognition,** IEEE ASSP Magazine vol. 3, issue 4, October 1986, page 4 - 17
[40] Naik J.M., **Speaker verification: A tutorial,** IEEE Communication Magazine vol. 28, issue 1, 1990, page 42 - 48
[41] Atal B.S., **Automatic recognition of speakers from their voices',** Proc. of the IEEE, vol. 64, no. 4, April 1976, page. 460 - 475
[42] Rosenberg A.E., **Automatic speaker verification: A review,** Proc. of the IEEE, vol. 64, no. 4, April 1976 page 475 - 487
[43] Maes S.H., Navrátil J., Chaudhari U.V., **Conversational Speech Biometrics,** Chapter in "E-Commerce Agents Marketplace Solutions, Security Issues, and Supply and Demand," J. Liu and Y. Ye (Eds.): Springer Verlag, 2001, page 166 - 179
[44] Tisse C., Martin L., Torres L., Robert M., **Person identification technique using human iris recognition,** ST Journal of System Research no. 0, art. 9, July 2003 page 92 - 100
[45] Daugman J., Downing C., **Epigenetic randomness, complexity and singularity of the human iris pattern,** Proc. of the Royal Society, B, 268, Biological Sciences (2001) 268, 2001 page 1737 - 1740
[46] Daugman J., **Biometric Personal Identification System Based on Iris Analysis,** US Patent 5,291,560, March 1 1994
[47] Zhu Y., Tan T., Wang Y., **Biometric Personal Identification Based on Iris Patterns,** International Conference on Pattern Recognition (ICPR'00) – vol. 2, Barcelona, Spain, September 3 - 8 2000, page 2801 - 2804
[48] Kruizinga P., Petkov N., Grigorescu S.E., **Comparison of texture features based on Gabor filters,** Proc. of the 10th International Conference on Image Analysis and Processing, Venice, Italy, September 27 - 29 1999, page 142 - 147
[49] Negin M., Chmielewski T.A. Jr., Salganicoff M., Camus , Cahn von Seelen U.M., Venetianer P.L., Zhang G.G., **An Iris Biometric System for Public and Personal Use,** IEEE Computer no. 2, February 2000, page 70 - 75

[50] Daugman J. **The importance of being random: statistical principles of iris recognition,** Pattern Recognition, vol. 36, no. 2, page 279-291

[51] Collinson M., Wittenberg M., **Labour force dynamics in a rural part of South Africa: the Agincourt sub-district of the Northern Province, 1992 - 2000,** Paper presented at the DPRU/FES conference: "Labour markets and poverty in South Africa", Johannesburg, November 15 - 16 2001

[52] McDonald S., Piesse J., **Rural Poverty and Income Distribution in South Africa,** Paper prepared for the 37th Annual Conference of the Agricultural Economics Association of South Africa, "Agricultural Economics, Farm Management and Agribusiness: combining strengths and stretching the frontiers". Klub Mykonos, Langebaan, Western Cape, September 28 - 30 1999

[53] Pfleeger C.P., **Security in computing second edition,** ISBN 0-13-337486-6 Prentice Hall PTR

[54] Davis D., **High-Tech passport spark stiff competition,** Card technology 8(4) April 2003 page 22 - 24

[55] **Enhanced Border Security and Visa Entry Reform Act of 2002** PUBLIC LAW 107–173 May 14 2002, (116 STAT. 554)

[56] Mont M.C., Pearson S., Bramhall P., **Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services,** Trusted Systems Laboratory HP Laboratories Bristol HPL-2003-49 March 19 2003, http://www.hpl.hp.com/techreports/2003/HPL-2003-49.pdf

[57] Pato J., **Identity Management: Setting Context,** Trusted Systems Laboratory HP Laboratories Cambridge HPL-2003-72 April 8 2003, http://www.hpl.hp.com/techreports/2003/HPL-2003-72.pdf

[58] Von Solms S.H., Eloff J.H.P., Eloff M., Smith E., **Information security First Edition,** First impression 2000/01 ISBN 1-919774-39-4 Amabhuku Publications (Pty) Ltd 2000.

[59] Tiwana A., **Web Security,** ISBN 1-55558-210-9 Digital Press An imprint of Butterworth-Heinemann

[60] Daugman J., **Biometric Decision Landscapes,** Technical Report No. TR482, University of Cambridge Computer Laboratory 2000, http://www.cl.cam.ac.uk/users/jgd1000/biomdecis.pdf

[61] Wayman J.L., **Error Rate Equations for the General Biometric System,** IEEE Robotics & Automation Magazine, vol. 6, issue 1 , March 1999 Page 35 - 48

[62] Lawrence E. Corbitt B., Tidwell A., Fisher J., Lawrence J.R., **Internet Commerce Digital models for Business,** ISBN 0 471 34027 8 John Willy & Sons

[63] **BioAPI Specification Version 1.1** March 16, 2001 Developed by The BioAPI Consortium

[64] Wayman J.L., **Large-Scale Civilian Biometric Systems - Issues and Feasibility,** National Biometric Test Center Collected Works, vol. 1, J. L. Wayman, Ed. San Jose, CA: National Biometric Test Center, 2000, page 139 - 158

[65] Wayman J.L., **A Definition of "Biometrics",** National Biometric Test Center Collected Works, vol. 1, J. L. Wayman, Ed. San Jose, CA: National Biometric Test Center, 2000, page 21 – 23

[66] Woodward J.D. Jr., Webb K.W., Newton E.M., Bradley M., Rubenson D., **Army Biometric Applications: Identifying and Addressing Sociocultural Concerns,** ISBN: 0-8330-2985-1 MR-1237-A, © 2001 RAND

[67] Jutla D., Bodorik P., Hajnal C., Davis C., **Making business sense of electronic commerce,** IEEE Computer , volume 32 , issue: 3 , March 1999 Page 67 - 75

[68] Anandarajan M., Simmers C., Igbaria M., **An exploratory investigation of the antecedents and impact of Internet usage: an individual perspective,** Proc. of the Thirty-First Hawaii International Conference on System Sciences , vol. 4 , January 6 - 9 1998, page 22 - 30

[69] Mei Qi, **Impacts of EDI on the supplier,** 2001. PICMET '01. Portland International Conference on Management of Engineering and Technology, vol.2, July 29 – August 2 2001 page 50 - 59

[70] Mak H.C., Johnston R.B., **Leveraging traditional EDI investment using the Internet: a case study,** 1999. HICSS-32. Proc. of the 32nd Annual Hawaii International Conference on System Sciences, vol. Track5 , January 5 - 8 . 1999

[71] Jain A.K., Uludag U., **Hiding Biometric Data,** IEEE Transactions on pattern analysis and machine intelligence, vol. 25, no. 11, November 2003 page 1494 - 1498

[72] N.K. Ratha, J.H. Connell, and R.M. Bolle, **An Analysis of Minutiae Matching Strength,** Proc. Third Int'l. Conf. Audio- and Video-Based Biometric Person Authentication, June 2001, page 223 - 228

[73] Kotsakis E., Bohm K., **XML Schema Directory: a data structure for XML data processing,** Proc. of the First International Conference on Web Information Systems Engineering, 2000 vol. 1 , June 19 - 21 2000 page 62 - 69

[74] Wu P., **Using plain base32 ASCII-compatible encoding in the local part of E-mail addresses,** Proc. 2002 Symposium on Applications and the Internet, 2002. (SAINT 2002) 28 January 28 - Febuary 1 2002 page 214 – 219

[75] **RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies**

[76] Shay W.A., **Understanding Data Communications and Networks Second edition,** ISBN 0 – 534 – 95054 –X Brooks/Cole Publishing Company a division of International Thomson Publishing Inc.

[77] Niemeyer P., Peck J., **Exploring JAVA second Edition,** ISBN 1-56592-271-9 Published by O'Reilly and Associates Inc.

[78] Younglove R.W., **Public key infrastructure. How it works,** Computing & Control Engineering Journal, vol. 12, issue 2, April 2001, page 99 - 102

[79] Perlman R., **An overview of PKI trust models,** IEEE Network, vol. 13, issue 6, November –December 1999, page 38 - 43

[80] Suaste E., Leybon I G., Leija L., Sossa H., **Virtual environments for clinical analysis, visualization and simulation of congenital nystagmus,** IEEE International Conference on Systems, Man and Cybernetics, 1995. 'Intelligent Systems for the 21st Century'., vol. 5 October 22 – 25 1995, page 4662 - 4664

[81] Singh S., Mishra R., Arango N.A., Deng Jian Min, Behringer R.R., Saunders G. F. **Iris hypoplasia in mice that lack the alternatively spliced Pax6(5a) isoform,** PNAS vol. 99 no. 10, May 14 2002 page 6812 - 6815 published online before print as 10.1073/pnas.102691299

[82] ICAO TAG MRTD/NTWG - **Biometric deployment of machine readable travel documents** Technical Report Version 1.9 19 May 2003

[83] Wayman J.L. **Philippine Social Security System Inaugurates Huge Civilian ID Card/AFIS** System National Biometric Test Center Collected Works, vol. 1, J. L. Wayman, Ed. San Jose, CA: National Biometric Test Center, 2000, page 169 – 171 (Originally published in "Biometrics In Human Services User Group Newsletter" #12, 1999)

[84] Prabhakar S., Pankanti S., Jain A.K., **Biometric recognition: security and privacy concerns,** IEEE Security & Privacy Magazine vol. 1, issue 2 , March - April 2003 Page 33 – 42

[85] Woodward J.D., **Biometrics: Privacy's Foe or Privacy's Friends?** Proc. of the IEEE, vol. 85, no. 9, September 1997, page 1480 – 1492

[86] Bowyer K.W., **Face Recognition Technology: Security versus Privacy,** IEEE Technology and Society Magazine, vol. 23, issue 1, 2004, page 9 – 19

[87] Tilton C.J., **An emerging biometric API industry standard,** Computer , vol. 33 , issue 2 , February 2000 page 130 – 132

[88] **Interface Specification Human Authentication - Application Program Interface (HA-API) Ver 2.0**

[89] Teoh A., Samad S.A., Hussain A., **An Internet based speech biometric verification system,** The 9th Asia-Pacific Conference on Communications 2003. APCC 2003. Vol.1, September 21 - 24 2003 Page 47 - 51

[90] Everitt R.A.J., McOwan P.W., **Java-based Internet biometric authentication system** IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25 issue 9 , September 2003 Page 1166 – 1172

[91] Gurewich N., Gurewich O., **Teach yourself visual basic 5 in 21 days** Fourth Edition Sams Publishin ISBN: 0-672-30978-5

Appendix 1

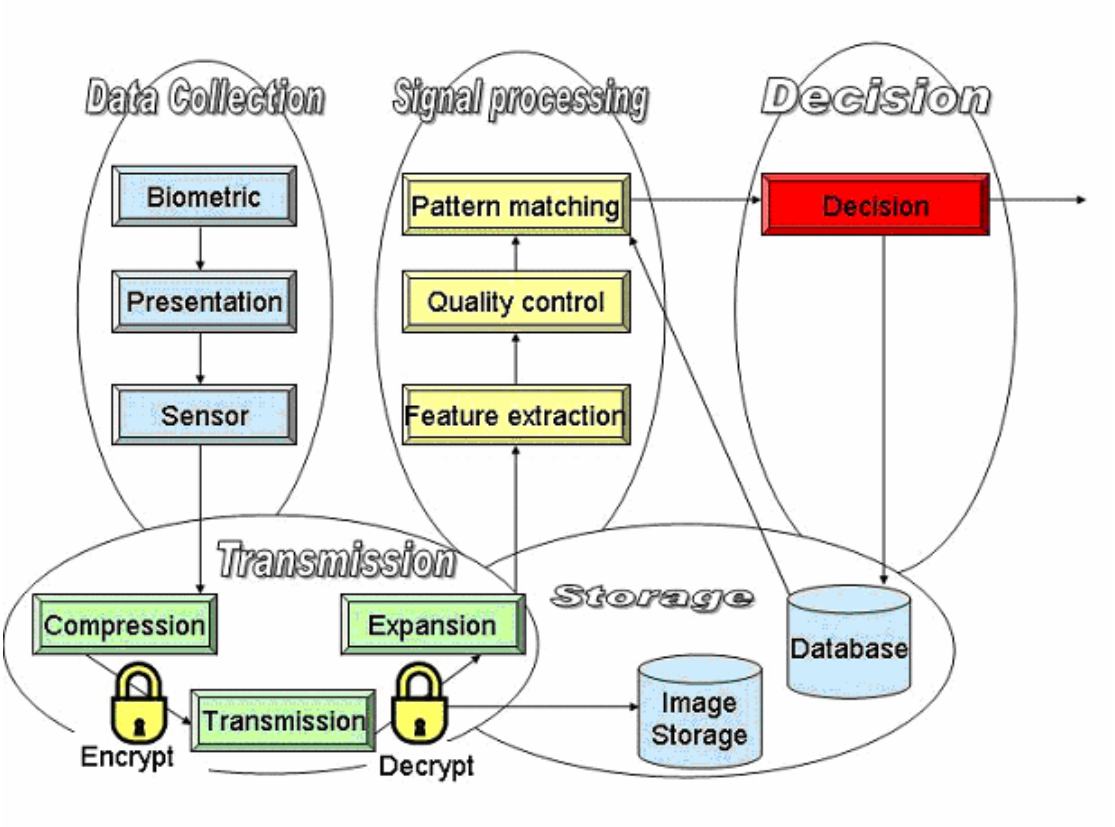

Figure 2-3 Generic model for biometric systems [Adapted from 10]

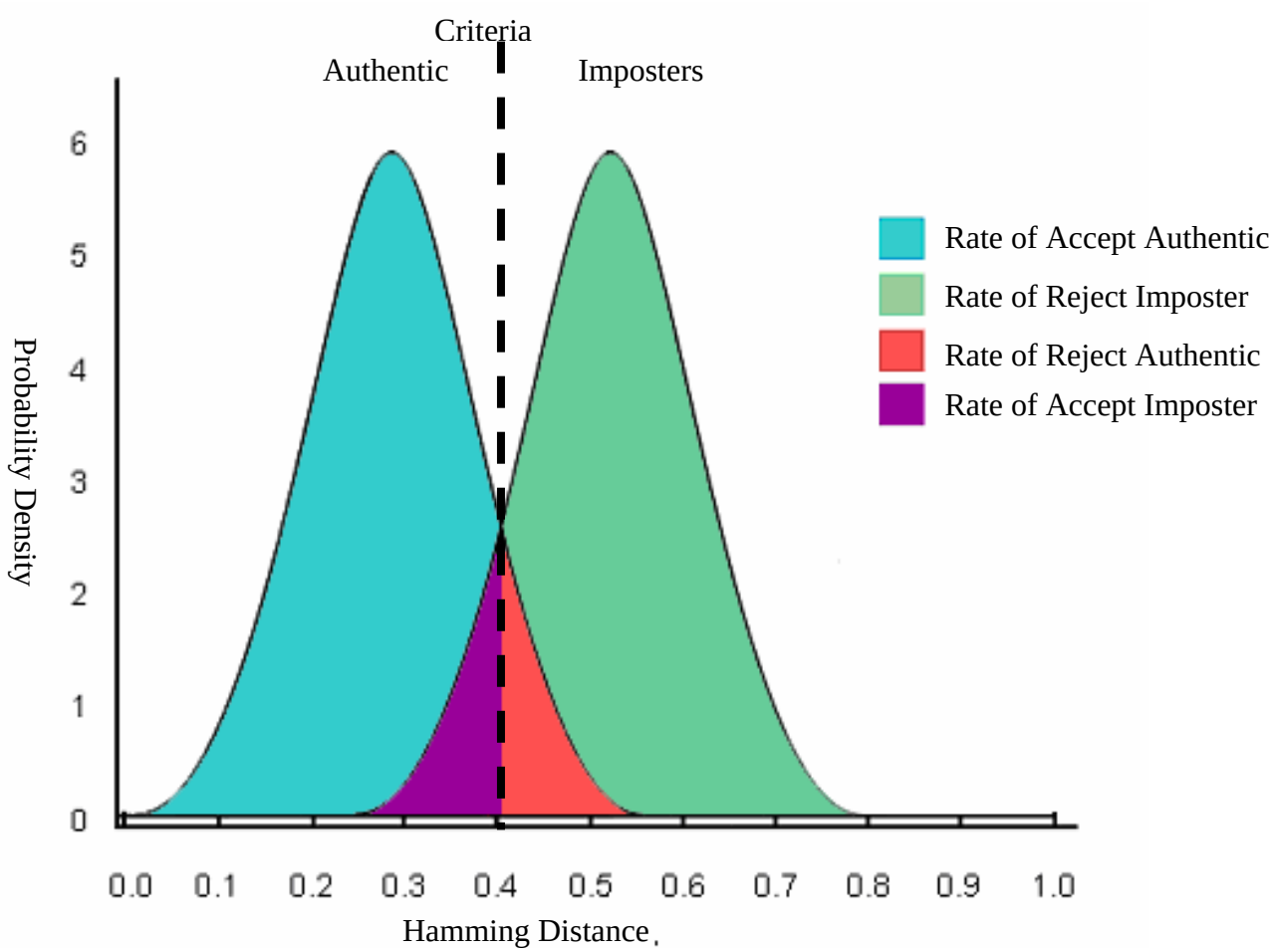

Figure 2-4 Neyman-Pearson formalism for decision under uncertainty. Adapted from [11, 60]

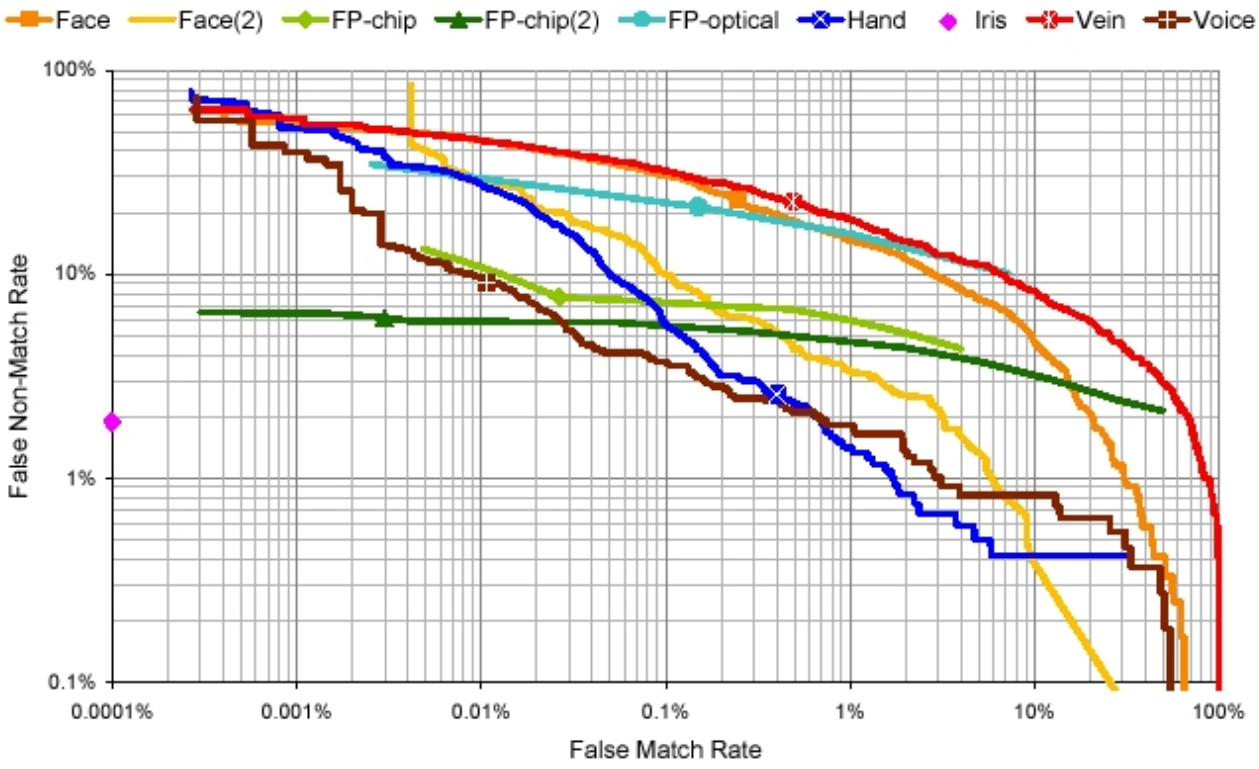

Figure 2-5 False accept and false reject trade off. FP-chip = Fingerprint chip, FP-chip(2) = Fingerprint chip 2, FP-optical Fingerprint optical, Vein= Vein pattern. (The lower and further left on the graph, the better the performance) [5] © Crown Copyright 200x. Reproduced by permission of the Controller of HMSO.

Figure 3-2 A fingerprint gathered using a solid-state sensor with the minutiaes marked in red [13]. Reprinted under permission [13].

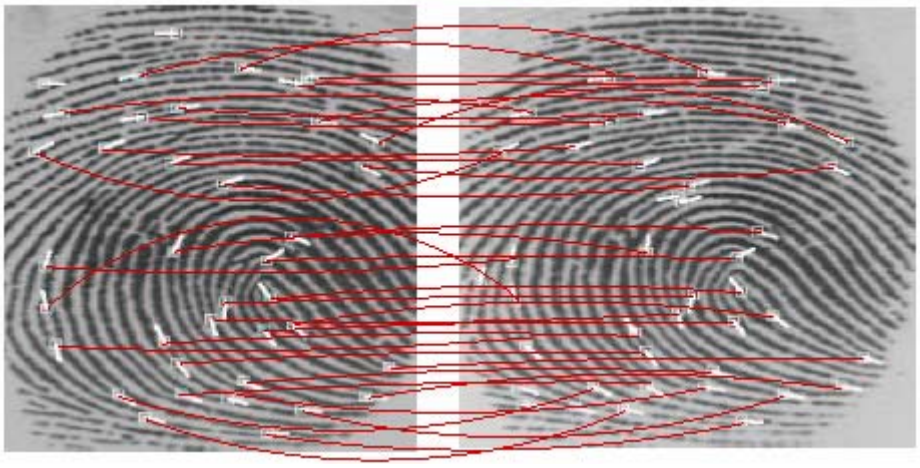

Figure 3-4 Minutiae matching between two different fingerprint templates [8]. Reprinted under permission [8].

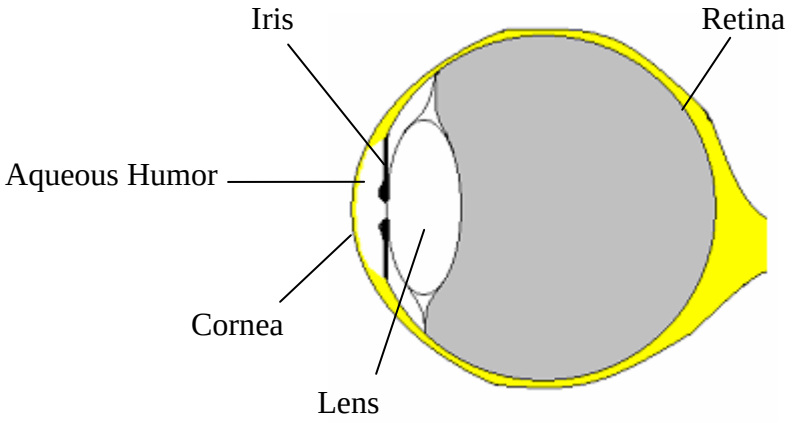

Figure 3-7 The human eye

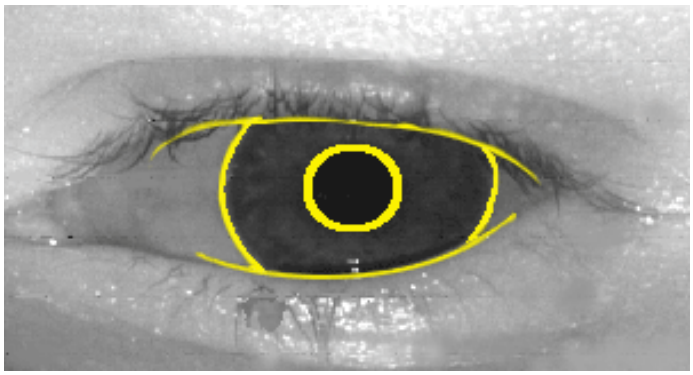

Figure 3-8 The boundaries located during the iris search phases

Figure 3-10 Points indicating possible references the system will identify during geometric feature extraction

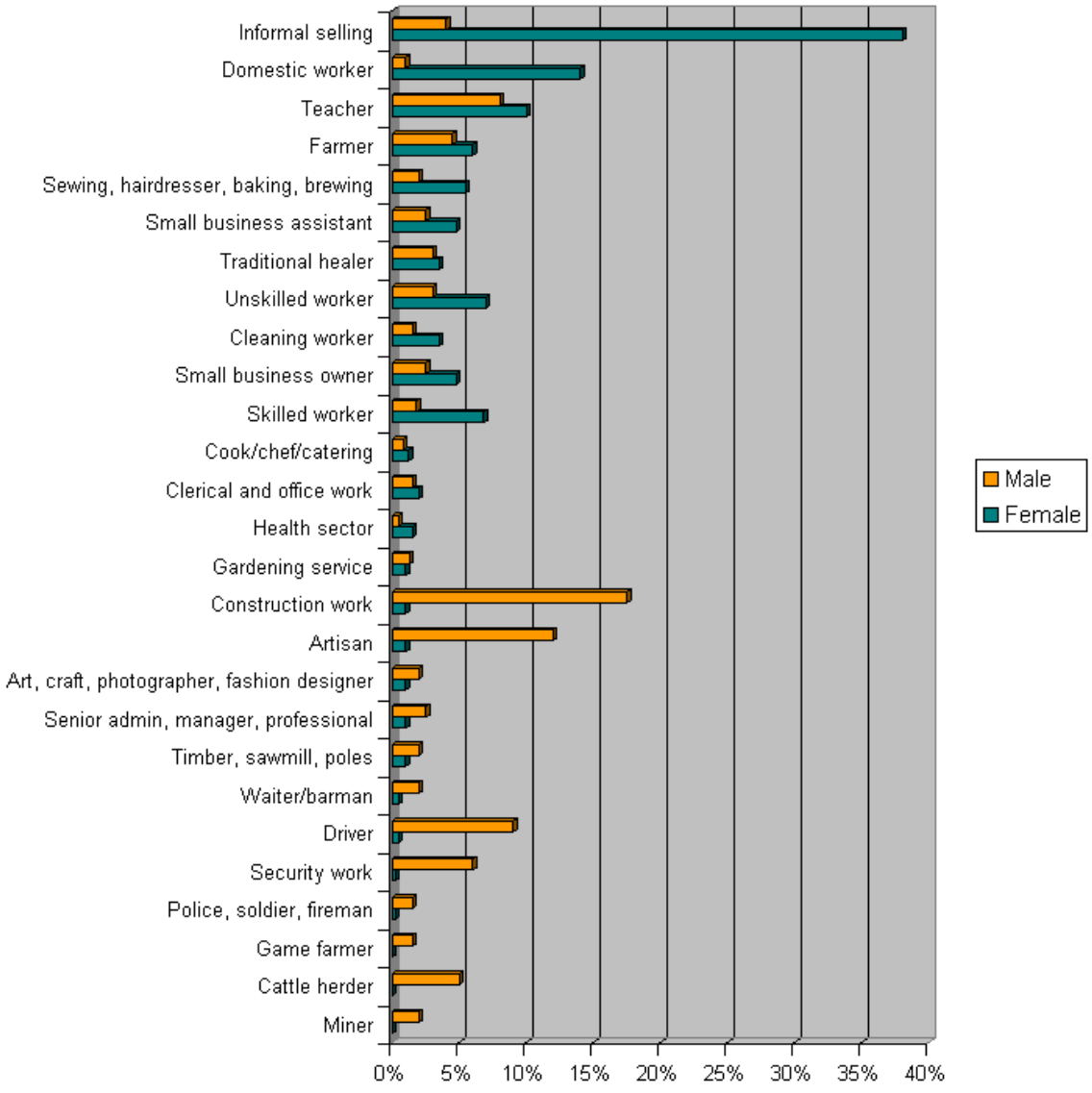

Figure 5-1 Different type of work perform by rural residents in South Africa (adapted from [51])

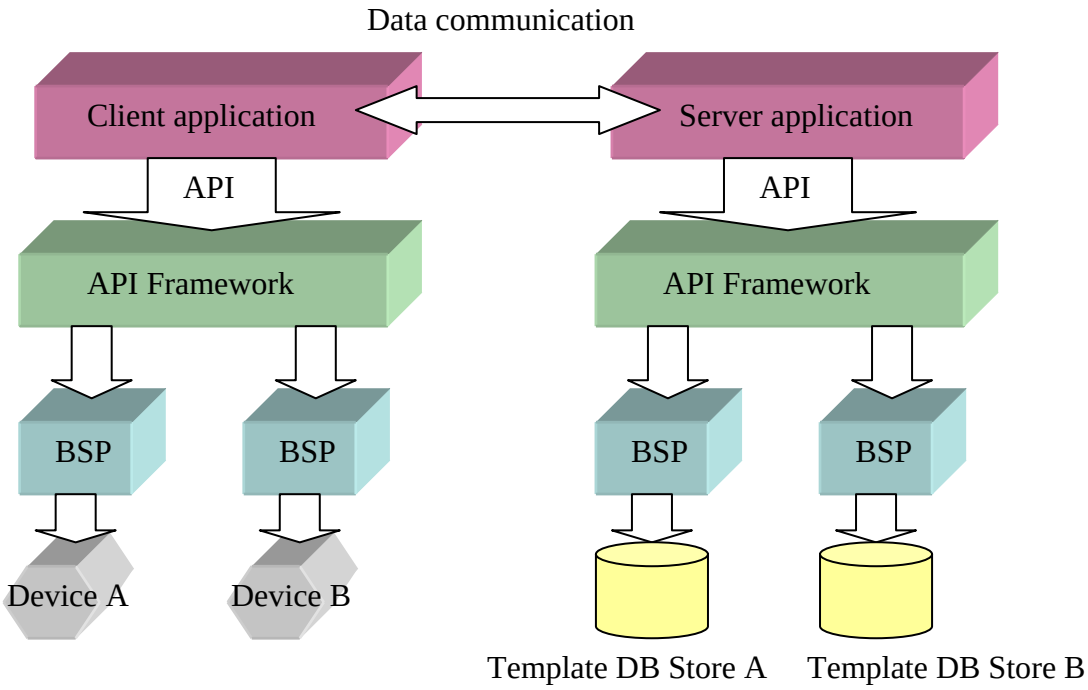

Figure 6-1 Client/Server biometric System implementing BioAPI adapted from [64 and 88]

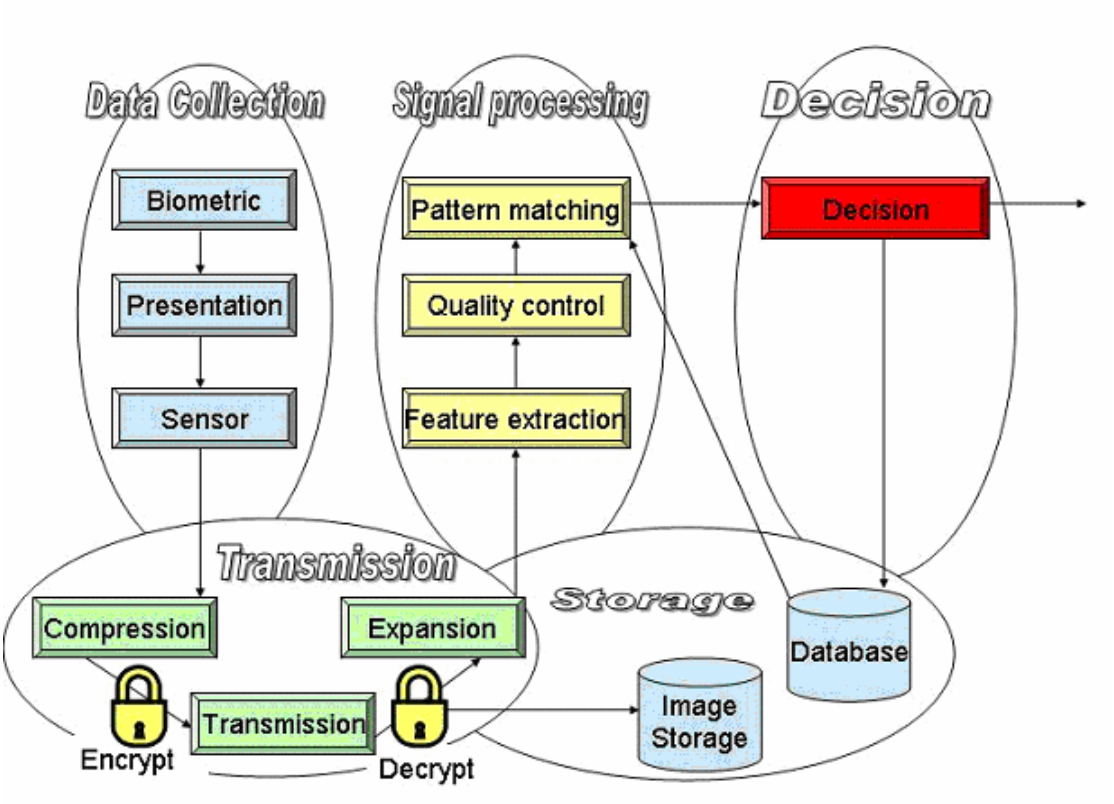

Figure 10-1 Generic model for biometric systems [Adapted from 10]