19

DISTRIBUTED AUTHENTICATION TO PRESERVE PRIVACY THROUGH SMART CARD BASED BIOMETRIC MATCHING

A DISSERTATION

SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE,

FACULTY OF SCIENCE

AT THE UNIVERSITY OF CAPE TOWN

IN FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE

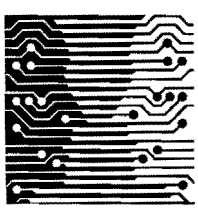
By

Michael Andrew Nelte

November 2000

Supervised by

Dr. Andrew Hutchison



Abstract

A weak point in many otherwise secure systems is the *authentication* of the *individual* claiming to be a particular user. This operation is fundamental to all security related decisions. If an incorrect authentication decision is made, access control, integrity, confidentiality and non-repudiation may all be compromised. Traditionally, authentication has relied upon knowledge of a secret, typically a password. This can be strengthened by the use of a *biometric*, which provides a unique personal identifier. In previous works and existing commercial systems the most common approach has been to store biometrics centrally. This raises a number of fundamental privacy issues.

This thesis focuses on *privacy* concerns, specifically those relating to the storage and use of biometrics. These concerns result from the fact that biometric information is unique. This uniqueness makes the biometric a very strong identifier increasing the possibility that it could be used to monitor an individual's activities. An expert can extract considerable information from a biometric scan, ranging from the age or gender to whether the individual has certain diseases.

This work presents a biometric solution, using the *fingerprint*, which protects the individual's privacy. In this system the individual is not required to relinquish control of biometric data, since a template is extracted from the fingerprint and stored on a *smart card*, which remains in the possession of the user. This smart card has a procedure installed on it to perform a comparison of the resident template and a template obtained from a fingerprint scanner. In this way the template never needs to leave the card, which can authenticate the owner via a secure communications protocol to many applications, including an ATM or banking network, and Internet shopping sites.

The system designed and implemented for this work extracts a set of minutiae from a fingerprint. This set of minutiae, which forms a template of the fingerprint, is installed onto an SLE44C160S smart card, along with a comparison routine. The template on the card forms a basis for comparing future scans to verify the possessor's identity. Effectively, the biometric data needed for authentication is stored in a *distributed database*, with each fingerprint template on a smart card and under

the control of the possessor. The template, which is securely stored on the smart card, can never be removed from the card.

The card can participate in an authentication operation by verifying that a presented fingerprint matches the template stored on it. This matching is performed on the card to eliminate the requirement to remove the template from the card. A matching algorithm was designed and implemented to provide this part of the presented solution.

Results were obtained by experimenting with the implemented solution. These tests verified that the *accuracy* and *timing* of the system were acceptable for real-time authentication. The effect on the accuracy of comparing different levels of information about each minutia was also examined. It was found that using just the position of the minutiae produced equal acceptance and rejection error rates of approximately 40%. By including the other characteristics of the minutiae, in particular the direction and type, this error could be reduced to 5.6%. The results were improved when an *enhancement algorithm* was applied to the fingerprint and *classification* information was used. The addition of the classification information in the comparison reduced the equal error rate to 1.6%. The time required for the complete authentication process is in the region of five seconds.

It has therefore been demonstrated that it is feasible to store a fingerprint template on a smart card. This system performs the fingerprint comparison on the card in real-time thereby countering the privacy objections of individual who wish to retain control over their biometric data.

Acknowledgments

I would like to thank the following people:

- Dr. Andrew Hutchison, my supervisor, for the advice and helpful suggestions.
- Professor Pieter Kritzinger for his valuable input and guidance as the head of the Data Network Architectures (DNA) Research Laboratory.
- Professor Tim Dunne for assisting with and providing direction for the statistical analysis.
- THRIP, NRF, Telkom and Siemens for their funding that made this project possible.
- Dr. Colin Tebbutt at Prism Payments Technologies for providing the specialty equipment needed for this research.
- David for sharing his wealth of experience in fingerprints systems.
- Bill Hunter for assisting me with the porting of the matching algorithm to a smart card.
- Cecily Roos for proofreading this disertation.
- The DNA boys for all the support provided.
- Our departmental system administrators for ensuring that our project ran smoothly.
- The department secretaries for the smooth administration throughout the year.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

Authentication of individuals by a computer system is a common process that has a number of vulnerabilities. The combination of a *username* and a *password* has become the prevalent method of authenticating personal identity. This combination is often used to verify a user to a personal computer or workstation. The combination of username and password is also typically used to authenticate individuals to a network or Internet site. Many sites of this nature require high security levels, for example banks or stockbroking firms. A username/password combination requires both public knowledge (the username) and private knowledge (the password) to perform authentication. For many systems this combination provides an acceptable level of security. The risk incurred through an incorrect authentication needs to be measured against the cost of increasing the security to prevent it. Thus an acceptable level of security must be selected.

A higher level of security in personal authentication requires a *token* and a *password.* The token could be a bankcard with a magnetic strip, a smart card, or any other physical device that forms part of the authentication process. There are many examples of this type of authentication, which include using a bankcard at an Automatic Teller Machine (ATM), combined with a Personal Identification Number (PIN), or some access control systems. Sometimes just the possession of the token is considered proof of identity; even the possession of a credit card is often presumed to indicate the correct user. This provides authentication through the user having a possession (token) and private knowledge (password). This method of using a password or PIN and/or a token is the most common method to identify individuals to computer systems [35].

The difficulty posed by the above systems is that it is possible for passwords to be lost, guessed or stolen. It is estimated that about 25% of people write their PIN on their ATM cards [19]. There are

companies where the majority of users still use their default password, which is often the same as the username, after having been with the company for extended durations. It would not be challenging to guess these passwords. There are attacks that exist which are capable of revealing large numbers of passwords belonging to users of a system. These attacks could be based upon weak algorithms or flaws in the implementation of these algorithms. This can be illustrated with an example of a local company that has Windows NT on their computers. The administrator ran l0phtcrack[1] to check the security of the passwords. Within seconds L0phtcrack found about 100 out of 270 passwords using a modified dictionary attack. A further 100 accounts were cracked by alphanumeric brute-force when left to run for nine hours. L0phtcrack is a freely available point and click program downloadable from the Internet. Even a novice user would be able to use it to acquire passwords. Knowledge-based systems can only determine whether the individual requesting authentication possesses the specific knowledge, not whether they are who they claim to be [19].

The use of a possession as proof of identity can be forged in some cases. If the token used is contactless and uses a radio link to communicate then there is a possibility that these communications could be eavesdropped and replayed. This communication could then be recorded and played back in a replay attack to gain access to the system. Even if it is a token that requires contact it might still be possible to place a tap on the reading device and allow the reproduction of the token. The use of a token can certainly be used to increase security levels, but if the token can be reproduced then the technique fails.

A higher level of security should require the user to be physically present at the time of authentication. This is superior to other authentication schemes where it is possible that the individual who was authenticated had stolen or 'borrowed' the information required to perform the authentication. A solution to this is to use a *biometric*. Biometrics are considered to be the oldest form of identification [18]. We recognise people by their looks, voice and their signature. Since conventional methods of identification are inadequate, why are biometrics not in more common use? One of the primary reasons is *performance*, which is based upon the accuracy, cost, integrity, and ease of use of a system [34].

A biometric refers to the application of statistical analysis to biological data [48], which could refer to any *biological*, *physiological* or *behavioural* characteristics possessed by an individual. For a biometric to be useful these characteristics should be unique to the individual and difficult to replicate. Among the many biometrics that are currently in use, or experimental use, one finds

[1] http://www.l0pht.com

fingerprints, palm prints, voice pattern, face recognition and signature patterns, retina maps, iris patterns and others.

The use of biometrics has been advocated as the solution to many security problems [16]. There are initiatives to use iris or fingerprint patterns to replace passwords, and since biometric data cannot be forgotten, or shared with others, they are considered to provide more secure solutions.

Bruce Schneier [41], on the other hand, is at least one author who warns that biometrics will not remove all security problems. The use of biometrics will not solve protocol or network security problems. For example, if a protocol is vulnerable to a replay attack, then sending a biometric in place of a password will not prevent the replay attack.

This dissertation focuses on the *fingerprint*. Fingerprints have been used as a reliable means of identification for a long time [27]. The fingerprint of an individual is unique and remains constant with age [32].

Since a fingerprint, as with all biometrics, cannot be replaced or changed it should not be dealt with as a password. A biometric is a unique characteristic and its presence implies the presence of the individual to whom it belongs. Since authentication is required over networks, biometrics need to be transmitted in a secure fashion to reduce the potential for it to be acquired by an attacker and re-entered into the system.

1.1 A New Approach to Fingerprint Systems

Biometrics can be used to improve the accuracy of the authentication process. They improve confidence in the verification of a user's identity, as it is considerably more difficult to present a fingerprint of another user than it is to present their password. The advantage that the biometric solution has over a non-biometric solution is the increased difficulty an impostor has to be authenticated as a valid user by the system. A biometric cannot be forgotten or written down on a piece of paper as can a password. This makes it is difficult for an impostor to masquerade as a valid user.

Fingerprint based biometric solutions have existed for a long time. However, a number of privacy concerns have been raised with respect to using fingerprints in civilian applications. These concerns will be addressed in the following chapter. The approach presented in this dissertation will be based on the use of a fingerprint to authenticate an individual. The fingerprint template will be stored on a smart card to create a *distributed* authentication system. The distribution of the database of

authentication information makes it more complicated for an attacker to acquire private information. Since the fingerprint is stored on a smart card the owner also has complete control over when it is used, while gaining additional security from using a biometric. The smart card would be entirely useless to an unauthorised user if it was lost or stolen, since only the authorised user's fingerprint can authenticate the user in conjunction with the card, and possibly to allow or deny access to other information on the card (for example a private key for signing).

The use of a smart card or token improves the security over that provided by using a username to identify an individual. The reason for this is that if someone knows your username they can attempt to enter the system using that username without your knowledge. If, on the other hand, your smart card is stolen you will notice that it is missing the next time that you try to enter the system and can have it revoked.

The approach taken in this study is to store the template of a fingerprint on a smart card. This fingerprint can never be removed from the smart card protecting the biometric data on it, even if the card is stolen or lost. Rather, the card will have functionality on it to perform the comparison between fingerprints. This will allow a smart card to store private information, including a user identity and digital key, which can only be used when a valid fingerprint is presented. The smart card can store a private key that can only be used to sign data digitally when the card has been unlocked for a session by being presented with the correct fingerprint and so this approach has relevance for digital signing too.

The implementation of an authentication system needs to conform to a number of critical success factors. These factors include the *accuracy* with which an individual's identity can be verified, the *time* that this takes and the ability to securely pass this confidence in a user's identity to other components in a system through the use of a *strong communications protocol.*

This system can improve confidence in the authentication process through the use of a biometric, while preserving the individual's privacy. Biometric authentication performed on a smart card can be integrated into many different systems. Systems that could benefit from biometric authentication range from ATM cash dispensing machines through to the purchase of products via the Internet. A future generation of credit card could have a biometric template stored on it allowing accurate authentication of the owner.

1.2 Dissertation Roadmap

This dissertation describes the privacy motivation for placing the fingerprint comparison process on the smart card with the following organisation:

Chapter 2 shows that the method presented here gives the user of the system complete control over when their biometric information is used to provide authentication. Thus, an individual's privacy can be protected while at the same time a higher level of security can be attained through the use of biometrics.

A brief evolution of the fingerprint and the smart card as well as existing fingerprint based authentication schemes are introduced in **Chapter 3**. The growth and development of these technologies is presented. After this background a general overview of how the system was designed along with the reasoning for these design choices is shown.

The architecture of the distributed fingerprint verification system is shown in **Chapter 4**. This chapter places the different components of the system in their respective positions. It shows a high level overview of the system and how these components interact with each other. The processes that occur on the smart card are positioned relative to the other components.

Chapter 5 explains how the test system was implemented. The different sections of the implementation each had their own set of challenges that needed to be overcome. This chapter then explains how these different sections interact with each other to provide the complete solution.

The algorithms used in the process, along with the reasoning as to why specific algorithms were used, and how they had to be modified and optimised to make them suitable for use with a smart card, is shown in **Chapter 6**. The smart card has specific restrictions on the size and heat generation allowed by the embedded microchip. These result in limited computing resources requiring all procedures that are installed on the card to be optimised in both CPU and memory requirements. The choice and the development of the algorithms is explained along with how they are modified. A matching routine was developed to compact the matching code to fit onto a microchip processor.

The system is examined and the accuracy and time are analysed and logical conclusions are deduced. Testing and analysis of the results obtained from this system are presented in **Chapter 7**. Performing batches of comparisons between fingerprints and recording them produced these results, which were compared against the results obtained from other batches of comparisons with different parameters. A database of fingerprints obtained from NIST was used for obtaining these results. The analysis

of these tests shows how the parameters can be modified to produce optimal results. The tests also show how the inclusion of different sections of the algorithm can improve the accuracy. These empirically obtained results are compared with the results obtained from a statistical model of the system.

Chapter 8 lists possible future extensions and areas of research that have potential for further development and research based upon the work in this dissertation.

Chapter 9 contains the conclusions of this study.

Chapter 2

Privacy Motivation

"The right to privacy is one of our most cherished freedoms." W.J. Clinton[1].

This chapter explores the privacy aspects relating to the maintenance and storage of personal information, specifically those pertaining to the use of biometrics. There are unique privacy concerns surrounding the use of biometrics that need to be confronted and dealt with. Some of these issues are the results of poor public education and misinformed perceptions. Others, although less well known to the general public, could still conceivably diminish an individual's personal privacy.

Many systems need to maintain private information on each user in order to operate correctly and efficiently. These systems range from a bank maintaining customer records to an operating system storing lists of users. The private information utilized in these systems is supplied to them for specific purposes. E.g. the bank needs to have your address so that it can send you statements.

This private information is stored in databases, and is normally supplied voluntarily by the users with the implied understanding that (unless explicitly agreed to) it will not be used for purposes other than that for which it was supplied, for example in the legal system a lawyer cannot be ordered to divulge information in a court of law that was acquired in private consultation with clients. The law has a built-in safe guard protecting the privacy of the client — thus allowing the client and the lawyer to talk freely with each other. The European Union issued a directive in 1995 on *On the protection of individuals with regard to the processing of personal data and on the free movement of such data* [7]. The United States of America has the *Federal Privacy Act of 1974* [8]. The United

[1] from the commencement address of W.J. Clinton at Morgan State University, Baltimore, MD, 18 May 1997.

Kingdom has the *Data Protection Act from 1984 revised in 1998* [6]. All of these acts specifying how personal information can be used and exchanged.

In the same way, any system that accesses private information should implement safe guards preventing this information from being utilized in ways not originally intended. Thus if the bank has your address they should not sell your address to direct marketing companies since that is not what you gave it to them for. Sometimes the small print obtains implicit permission.

Additionally the owner of the information should retain control over how and for what it is used. In many countries there are phone directories published by telecommunication companies. These directories contain the address and phone numbers of each person that is part of the telephone network in the selected area. But each individual should be able to specify how much information about them they would like to have in the directory — from having an unlisted number to just the name and number to in addition including the address.

Design principles that protect the clients' privacy should be adhered to. These aim to ensure that private information is only used for the purposes for which it was originally supplied. The owner of the information should still retain complete control over when and how it is used. Thus any system that stores and utilizes an individual's private information should respect the privacy of the information. To ensure that the information is afforded the privacy that it should be, the system must maintain appropriate security standards and have appropriate procedures preventing unauthorised access. Depending on the level of security required it might need to maintain logs of the access to the information and unauthorised attempts to access the private information should be reported.

Procedures should be implemented to give the user control over the information. If the information is incorrect and needs to be updated or modified then the user should be able to follow a procedure to correct the information. The client should be educated on how to use the procedures to control how his private information is used. If there are uses for the information outside of that which it was originally intended for then the client should be consulted before the private information is used. Utilization of private information for additional purposes should by default be treated as "opt out". Thus, unless an individual specifically allows such use of the information then the use of the information should be prohibited.

2.1 Privacy Issues of Biometrics

One of the primary concerns about using a fingerprint to authenticate an individual in commercial applications is the privacy concern. There is the concern that by using a biometric you are reducing the privacy of an individual. There are a number of both perceived and legitimate concerns regarding how the usage of a biometric can affect an individual's privacy. These concerns are addressed in the following sections:

2.1.1 Loss of Anonymity and Autonomy

A good biometric should be unique to each individual. When an individual submits a biometric sample then information is divulged that is truly unique to the individual.

While a biometric is an accurate identifier it is not the first, nor is it the only, identifier used to match or locate information about an individual. Names and numerical numbers like our identity number can also be used. However the claim of a specific name or number does not guarantee that the correct user supplied it. On the other hand the presentation of the correct biometric does guarantee the presence of the particular user.

2.1.2 Invasive Aspects of the Information

Biometric information does sometimes contain latent medical information about the owner. This information might be sold or otherwise distributed if it is stored in a centralised database. There is ongoing research on how to extract more information from biometric scans.

Invasive information might be obtained. It is possible that some biometric recordings might record more than just sufficient information for identification. There might be information about the person's health and medical history. Studies indicate that even a person's fingerprint might disclose medical or hereditary information about the person [57].

A fingerprint contains a large amount of information about the person to whom it belongs. If the hands and fingers are regularly used for manual labour then the fingers and hands develop stronger and larger muscles. This influences the circumference of the fingers, increasing the distance between adjacent ridges on the finger. Office workers on the other hand tend to have a much finer ridge structure.

Trained forensic expert can generally identify from a fingerprint the gender of the owner, along with a few clues as to the occupation and ethnic group. Some occupations regularly expose the fingerprint to chemicals that cause a smoothing of the fingerprint region. Other occupations that involve heavy use of the hands might leave the fingerprint region scratched or scarred.

Examination of the retina or the iris by a medical professional might be able to determine diseases like diabetes, arteriosclerosis, and hypertension [57]. A picture of the face could be enough evidence for a medical doctor to be able to detect skin diseases along with a number of other diseases. With face comparison one would expect the relative positions of eyes, nose, mouth and other features to be used in the comparison, rather than the texture of the skin. A medical practitioner would rather use the texture of the skin to provide a diagnosis. Thus as is often the case different features are of interest to perform a comparison and to extract additional knowledge from the data.

It is clear that it is possible for trained professionals to gain information from biometrics that was not originally intended when a sample was submitted for use with a system. This makes it even more important that any biometric data captured for use with a system is securely stored and not distributed without the owner's permission.

2.2 Protecting the Individual's Privacy with Biometrics

It is not obvious that residual anonymity beyond that remaining after other activities will be lost through the use of biometrics. There is normally a reason why a person's identity is required and it is normally in their best interest that they are identified accurately. An example of this is withdrawing money from an automated cash-dispensing machine. The use of biometrics themselves do not erode privacy. However the way in which they are used could, just as other information might.

It is thus of utmost importance when designing and developing a system to ensure that it will respect the individual's privacy. It should be possible to demonstrate this to those resisting the use of the fingerprint.

Some people think that the storage and use of your fingerprint could be used to track your movements. It is unlikely that using a fingerprint will infringe much more upon the residual privacy of an individual than a password would. However since the fingerprint would remain the same across multiple databases it might allow some extra tracking, if multiple databases are linked together — but if they could be linked on the fingerprint then they could probably also be linked on a username.

The aim of using a fingerprint in place of, or in addition to, a password for personal authentication would be to increase the individual's privacy. Data could be stored, and access to it protected, through a biometric. The biometric cannot be guessed and is much more difficult to forge and replicate by an attacker — making it more difficult to assume a fake identity and masquerade as another user.

If the system allows users to authenticate themselves over a network then it is highly unlikely that attackers will attempt to make their fingerprint appear like someone else's. Rather they would attempt to acquire a digital copy of the fingerprint and surreptitiously inject it into the system via the network [18]. Using a biometric should strengthen at least the authentication section of the protocol without introducing any additional security vulnerabilities.

Even though the use of a biometric is unlikely to create a weak link in a protocol the biometric should still be securely protected. Particularly if the fingerprints are to be stored centrally in a database, the database needs to be secure. Otherwise that database might fall into the hands of the wrong people. And unlike a pass phrase that can be replaced your fingerprint cannot be replaced.

The system can be designed to store enough information to use a template to identify the individual, but not enough to be able to inject into the system to cause a match if it is acquired. For example a template of the biometric can be stored in the database, but the system can insist on a live scan as the acquisition process. Then, even if people do manage to surreptitiously acquire the electronic template of your fingerprint, they should still be unable to use it.

It would also be preferable if the fingerprint did not need to be stored in a large database. Rather a system where the fingerprint, or some representation of it, was stored on a smart card and all the comparison was performed on the card would be superior. This should both alleviate the need to store a central database of fingerprint information and give the user complete control over how and when his fingerprint is accessed. This should satisfy most users.

All the same the more control an individual has over the use and protection of his biometric data the more likely that he will accept the system as secure. The privacy of an individual must be protected.

Critics will still compare the use of biometrics to Big Brother and the loss of individual privacy. The pro biometric community stresses the greater security and the improved service that the technology provides [57]. There are valid arguments for and against biometrics and while biometrics may pose certain privacy issues these issues can be adequately addressed.

In many countries the government is taking an interest in biometrics. They would like to use biometrics to improve the delivery of services while at the same time decreasing the costs and level of fraud [55]. However the very personal nature of a biometric does still raise concerns about its potential impact on personal freedoms. The delivery of services by a government requires positive identification to prevent multiple persons from using a single identity, and negative identification to prevent a single person from using multiple identities.

In the system proposed here in this dissertation, a template of a fingerprint is placed onto a smart card. This template does not store the original fingerprint, but only the information extracted from it. There is not enough information stored in the template to be able deduce any invasive information about the user. But even if there were this should still not be an issue, as the template can never leave the card. This can be achieved by performing the comparison process on the card.

The individual who has possession of the smart card then controls the physical access to the card. And even then only the person with the correct fingerprint can use the smart card. If the print is stored on the card then there is no need to have a central database to verify the identity of an individual and by having the comparison on the card there is never a need to remove the fingerprint template from the smart card. Since control of the print resides with the subject and no central store exists, the implementation of such a model would have to ensure that the fingerprint could be correctly associated with the individual to whom it belongs by additional information.

This should be able to provide a highly secure method to authenticate an individual. And the use of the fingerprint if implemented correctly should even increase the privacy of the user.

It appears that there is a big opportunity for biometrics and digital certificates since certificates profess to offer a "higher" level of authentication, but they still rely on the knowledge of a password — and worse still they are controlled on the client side and may not pick up multiple guessing attempts in the same way that a server would notice this guessing activity. The password can be replaced with a fingerprint.

2.3 Summary

Individuals' privacy should be protected. There are many systems that utilize personal private information. These systems should ensure that the privacy of the information utilized is respected and maintained. The laws of a country should enforce this safeguarding of private information.

Private information stored in databases should be used only for the purposes for which it was gathered. Additionally the owner of the information should have the ability to update it and correct it, if needed, along with control over how it is used. All uses other than that for which information was originally supplied should require permission from the owner. This should prevent the abuse of personal information.

There are a number of privacy issues that relate specifically to biometrics. There are concerns that the use of biometrics in commercial ventures will have the potential to infringe upon an individual's privacy. Some of these concerns are groundless and based on hearsay while others are legitimate concerns. The issues arise from the uniqueness of biometric information. This uniqueness can be thought to cause a loss of anonymity or autonomy — however it is unlikely that a biometric can be used to track individuals any more than non-biometric information.

The other aspect that can affect the privacy is the latent information that could be stored in biometric data. There have been studies that show that fingerprints might reveal medical or hereditary information. Medical experts can detect some diseases from the examination of iris or retina scans. However the information that is extracted from the biometric and stored might not be sufficient to extract this latent information.

The system described in this dissertation implements a biometric based authentication system, but one that preserves the privacy ideals outlined in this chapter.

Chapter 3

Background

This chapter provides background information about biometrics and particularly about the fingerprint. This chapter explains how the fingerprint has been used and how they are used to identify an individual. It deals with classification schemes and comparison methods. The uses and the limitations of biometrics are also explored. Existing biometric solutions are presented and the work done in this dissertation is located in this context.

Smart cards are introduced to show how they have been used to improve the security in authentication systems. The background to the smart card is explained and the different categories of smart cards are described. The evolution of the interlinking of smart cards and biometrics is expounded. Limitations and advantages of using a smart card technology are explored.

3.1 Biometrics

There have been major advances and research into biometric systems in recent years [30]. The two main focuses of this research have been in the authentication or verification of a user's identity and identification of an individual. Authentication involves proving that a person is who they claim to be. The other major focus has been in the identification of an individual [13] from a biometric. Any biometric characteristic of an individual, whether physical, physiological or behavioural can be used for the purposes of identifying them.

There are many biometrics in use today. These include fingerprints [12, 38], face recognition [15, 58], hand geometry [19], voice recognition [5], signature recognition [34], iris scans [56, 26], retina

scans [56] and typing patterns [18]. Each of these methods has different advantages and disadvantages associated with them, along with respective performances. Some, for example face recognition and iris recognition, can be performed passively [35] or without needing the user to perform any specific activity, while others like hand geometry require the user to carry out specific activities, like touching a scanner.

A biometric should satisfy the following requirements [12, 30, 20]:

- *Universality*: The biometric should be one that is possessed by every person.
- *Uniqueness*: The biometric needs to be unique to an individual. This ensures that there are sufficient differences between different individuals to allow a system to discern the difference. For example most face recognition systems struggle to differentiate between identical twins.
- *Permanence*: The feature should be invariant with time. It should not vary according to the condition under which it was captured [37].
- *Collectability*: It must be possible to quantitatively measure the trait. There needs to be some representation of the biometric that can be stored for later retrieval and comparison purposes.

If a particular biometric cannot be used alone to fulfil these requirements in a given system then it could be combined with another biometric. The combination of a second biometric can increase the accuracy and improve the performance of the system. One such system which makes use of multiple biometrics, BioID, is presented by Frischholz and Dieckmann [9]. It uses face, voice and lip movement for identification. The recent emergence of standard biometric API's [49] has simplified the process of replacing one biometric identifier with another or combining multiple biometrics.

There are a number of other characteristics specific to the method and representation used with a particular biometric that need to be considered before it becomes feasible to use it as a means of authentication or identification. These issues include [19]:

- *Performance*: The performance of a system is important. If the system needs to be used in real-time then speed becomes an important factor. The accuracy of the comparison can also affect the usefulness of the system. Along with these, the robustness, resource requirements and any other operational or environmental factors need to be considered that can affect its performance.

- *Acceptability*: The extent to which people are willing to accept a particular system will impact on its success. For example if people need to look into a bright light to have a picture of their retinas scanned they probably will not like the system and consequently will not use it either. It should ideally cause minimal change to people's current routine in order to be accepted.

- *Circumvention*: How easy is it to fool the system? If all that is needed is a photo of the person then the system is useless as a photo can be covertly obtained. The system should be resilient and able to withstand fraudulent impersonations. It also should have counter measures to resist circumvention.

Different biometric technologies can be compared on their accuracy and performance. The main methods of comparing the accuracy of biometric solution are:

- *False Acceptance Rate* (FAR): The FAR specifies the ratio of successful attempts by invalid users, where a FAR of x/y means that on average x out of y attempts which should be rejected will be accepted.

- *False Rejection Rate* (FFR): The FRR specifies the ratio of unsuccessful attempts by valid users, where a FRR of x/y means that on average x out of y attempts which should be accepted will be rejected.

- *Equal Error Rate* (EER): The EER is the error rate where the parameters are adjusted such that the FRR = FAR.

These values are accepted as the accuracy metrics by which biometric systems are judged [38] and ideally they should be very close to zero.

Whether a biometric could be used for a personal authentication depends upon whether the biometric is universal, unique, permanent and collectable. The performance criteria, the operating environment and the acceptability affect the choice of the most appropriate biometric technologies for a particular application [43]. The combination of all of these criteria can be used to determine the suitability of technologies for particular systems.

Biometrics can be used either for purposes of authentication or identification. In an authentication system the biometric is used to confirm that a supplied identification is correct. An identification system seeks to determine the identity of an individual bases on a supplied biometric. This thesis concentrates mainly on authentication or verification systems.

3.2 Fingerprints

> "The main reason for the popularity of the fingerprint as a form of identification is that the fingerprint of a person is unique and remains invariant with his/her age." [32]

The biometric with the most widespread usage is the fingerprint. There have been commercial identification systems based on the fingerprint since the early 1960s [34]. The price of fingerprint scanning equipment used to be in the range of $1000 to $2000 for a single scanner. These optical scanners would have been about the size of half a loaf of bread. Today the new solid state scanners cost less than $100 and are the size of a postage stamp [33]. The low cost of these scanners has greatly increased the use and availability of fingerprint technologies and as a result it has become feasible to have a fingerprint scanner built into a workstation.

Until recently fingerprint systems have predominantly been used in forensic applications for investigating criminals. The uses have, and still are, the subject of leading-edge research. The fingerprint has been found to remain constant for a person. The abundance of research into the use of fingerprints has yielded a number of viable algorithms for their electronic storage and comparison — yielding a very high degree of personal verification accuracy.

3.2.1 Early Evidence of the Fingerprint

Some of the earliest evidence of ridge detail has been found on the hands and feet of humans on the 4000-year-old mummies from ancient Egypt. The hands and feet of these mummies have been examined and there is evidence of a ridge structure on them [27].

The scientific study of fingerprints began in the late sixteenth century as cited in [12], with Nehemiah Grew, an English plant morphologist being the first person to study and describe the ridges, furrows and pores on the hands and feet. In 1684 he published the first fingerprint research. Besides writing on the subject he also published some accurate drawings of the ridge patterns on the fingers and areas of the palms. Along with the drawings his writings described the use of the ridge structure and pore structure. However, the foundations of modern fingerprint technologies date back to the late nineteenth century with the work of Sir F. Galton and E. Henry. Fingerprints, the first biometric to be used as a method of identification, have been actively used as a method of verifying an individual's identity for about 100 years.

While many solutions exist they are all *centralized* in nature. One exception to this, which has emerged in recent months, is a combined development by Gemplus and Veridicom. Simultaneously to the work towards this thesis they developed a system that performs Veridicom's fingerprint matching algorithm on a Gemplus smart card [36].

Prior to the early 1980s the task of comparing two fingerprints was performed manually [29]. In the early 1980s the first experimental systems were developed and since then the comparison process has been further automated.

3.2.2 Description and Function of the Fingerprint

There have been many developments in the applications of fingerprints. Most of these have occurred in the last several hundred years. To understand the history of the fingerprint some basic knowledge from *dactyloscopy*[1] should be understood.

The inside surfaces of the hands, from the fingertips to the wrist, and the bottom surfaces of the feet, from the tips of the big toe to the rear of the heel, are covered with minute ridges. A cross section of the skin in these areas has a corrugated appearance. These ridges and furrows frequently curve, particularly on the fingertips and toe ends. The ridges have sweat pores along their entire length. Thus when an article is touched the sweat runs along the entire length of the ridge and leaves an exact impression of the ridge structure. This is very similar to how an inked rubber stamp leaves its impression on a sheet of paper [27].

The ridges and furrows fulfil three functions:

- *Exudation of perspiration*: The sweat pores occur along the length of the ridge structure at approximately equal distances. The furrows between the ridges provide channels for the sweat to disperse.
- *Tactile facility*: The ridge structure provides a facility with which to perceive touch.
- *Provision of a gripping surface*: When the sweat is excreted from the pores it can flow into the valleys between the ridges. This allows the finger to continue to grip surfaces even while sweating. This is similar to how a tire has ridges and valleys to move water off the road and still provide a surface with which to grip. The ridges are raised areas on the surface of the skin. They improve the ability to grasp objects with minimal slippage [29].

[1] the practice of using fingerprints to identify someone

3.2.3 Fingerprint used for Personal Identification

Every person in the world has a pattern of ridges and furrows on their fingerprints. Using these ridges and furrows of fingerprints provides a method of identification that can be used to uniquely identify an individual. This is based on two facts. The first of these is that no-one has ever found a sequence of ridge detail on the hands or feet that is identical to the ridge detail of another individual [27]. The second of these is that the ridge structure remains constant with age after an individual has reached maturity [32]. There have been many instances of a person trying to change or destroy the ridge details of their fingers. In most of these instances the ridge structure has still been recognisable. Galton, as cited in [12], went further to say that the *minutiae* provide discriminating features that are *unique* and *permanent.* There is evidence to suggest that the pore structure of the fingerprint is also unique and invariant allowing it to be used in the comparison of fingerprints [38].

A study by Galton examined the details that reside in fingerprints. He examined the fingerprints morphologically and carried out experiments on different age groups within different races. From his work two important conclusions can be deduced. The first of these is that a fingerprint is permanent in preserving its characteristics from the birth to the death of an individual. The second of these is that the fingerprints of an individual are unique. Even identical twins have different fingerprints. This has been the fundamental building block upon which research has been performed in the twentieth century.

There are many different minute details that can be distinguished on a fingerprint. Galton's study introduced the concept of minutiae as the discontinuities in the ridge pattern. John Berry [27] identifies seven basic ridge characteristics which he considered to be the most important varieties in ridge detail. These basic characteristics are shown in Figure 3.1. All of these characteristics, also referred to as *minutiae*, can be represented as variations and combinations of the *ridge ending* and the *ridge bifurcation*, which are the first two characteristics illustrated in Figure 3.1.

Along with these minutiae, fingerprints also contain special features called core and delta points. The core point is generally defined as the topmost point on the innermost curving ridge. This can also be thought of as the point of greatest curvature in the ridge structure. The delta points are where the ridge structure has a curvature away from itself. An example of these is shown in Figure 3.2.

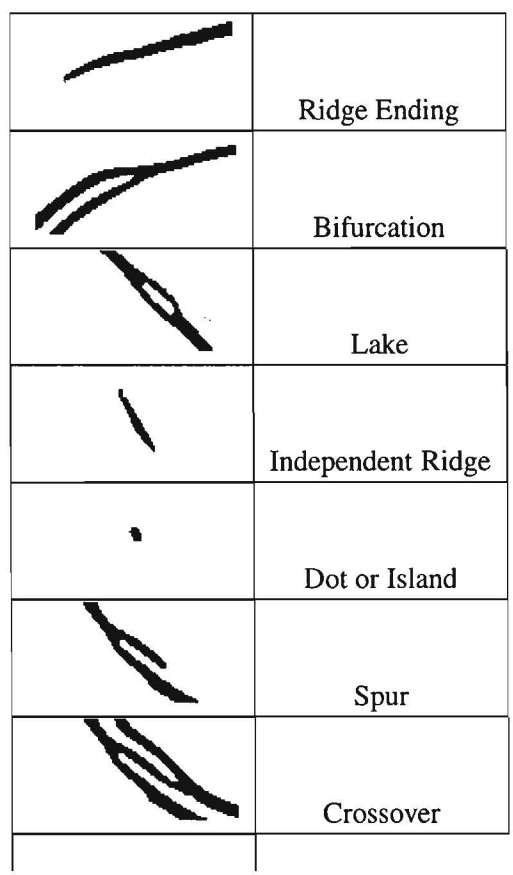


Figure 3.1: Ridge characteristics.

Figure 3.2: Singular points, illustrating the core point (O) and the delta points (A).

3.2.4 Fingerprint Classification

A major step forward in fingerprint research was the development of fingerprint classification schemes. A method of classification allows a large database to be searched for a fingerprint by only performing the comparison on a subset of the database. One of the first such methods developed was the brainchild of Sir Edward Henry, the *Henry System*, which is now effectively used in many countries. His system became operational in Scotland Yard in 1901 [27]. The Henry System is also in use in fingerprint bureaus in, amongst others, South Africa, Australia, Greece, Canada, and the United States. The Henry System is still an integral part of most identification systems [12].

The ridges and furrows on the last joint of the fingers and toes form patterns. These patterns can be classified into many different categories. One method of classification divides fingerprints into four groups. These groups are illustrated in Figure 3.3. The Henry system splits the loop class into two classes. The loop shown in Figure 3.3 would be designated as a left loop. The Henry system has a separate category for right loops..

Figure 3.3: Basic fingerprint patterns.

3.2.5 Manual Comparison of Fingerprints

Many different methods for manually comparing two fingerprints have been proposed and tried. The first group of methods attempt to align the two fingerprints graphically. One fingerprint might be placed on a semitransparent film and then superimposed over the other.

There are also methods that divide the images up into a grid of squares. These grids need to be aligned on the two prints and the corresponding cells are compared for a match. Other methods locate ridge characteristics in a fingerprint and then produce a polygon of these minutiae. The polygon of these minutiae needs to match for the two fingerprints to match.

The *Conventional Method* is the oldest and most accurate method used when comparing two fingerprints. Identification is based on ridge characteristics and their unit relationship with other ridge characteristics. This method differs from the other methods as it does not use the spatial positioning of the characteristics, but rather it uses the relationship between the characteristic and all other ridges in the print. This method allows matching even when there has been considerable distortion of the captured print.

3.2.6 Automated Fingerprint Identification Systems

Manual fingerprint identification is a tedious time-consuming process that can only be performed by trained professionals [12]. In the early 1960's efforts were initiated in the United States, France and Great Britain towards automating the comparison process. These efforts were stimulated by the development and commercial availability of the computer. Lee and Gaensslen [27] stated that this technology was intended to assist or even replace much of the labour intensive process of classifying, searching and matching fingerprints.

The automated methods for comparing fingerprints are based upon the methods used when performing a manual comparison. These methods also use the minute details or minutiae shown in Figure 3.1.

The minutiae can be represented in Cartesian coordinates as an (x,y) pair along with α, the angle of the ridge relative to the primary axes. This is illustrated in Figure 3.4. Lee and Gaensslen also show that a set of sufficient size of these minutiae will produce a unique record. Extracting a set of minutiae from the fingerprint reduces the fingerprint comparison problem to a point-matching problem. The early work that tried to match two sets of minutiae revealed difficulties in the process.

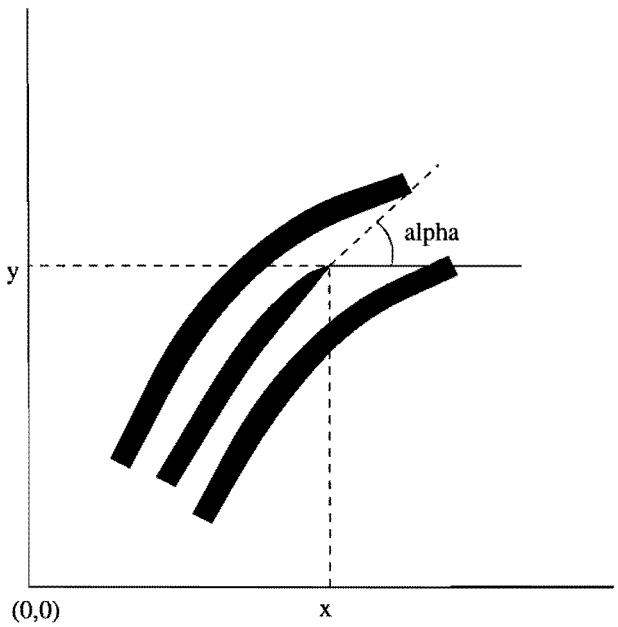


Figure 3.4: A co-ordinate system for minutiae.

These difficulties are direct results of the fact that two scans of a finger are never produced at the same orientation and position relative to the co-ordinate system. Along with this Lee and Gaensslen also indicate that the distortion of a scan differs from scan to scan.

The pattern of the ridges remains constant for an individual once they have reached maturity. This pattern consists of the varying thickness and the curvatures of these lines, which is unique to a particular finger.

The process of performing automated matching is based on the techniques used for manual matching. These techniques all use the fact that the biological principles of fingerprints are well established. These principles can be summarised as [31]:

- Individual epidermal ridges and furrows have different characteristics for different fingerprints.
- The configuration types are individually variable, but they vary within limits which allow classification.
- The configurations and minute details of individual ridges and furrows are permanent and unchanging.

Since the configuration of the minute details is unchanging we may use this configuration to perform the matching. This configuration is unique to a particular finger.

3.2.7 Limitations/Problems of Fingerprints

Fingerprints are used in the identification and verification of an individual's identity. As they are a biometric one would hope that the accuracy of the verification process would be significantly greater than that of non-biometric solutions. There are instances where this happens, although there are also many cases where the use of fingerprints is not the appropriate biometric or method for authentication.

As the fingerprint has been used for a long time many advances have been made in its applications and a multitude of difficulties have been overcome. All the difficulties that are mentioned here have caused problems in real companies and contributed towards the verification system being rejected in favour of a system that does not use the fingerprint. However, there are also example cases of companies that have managed the implementation of the system correctly and overcome or completely avoided these problems.

Identification systems can be split into those that have an operator present at all times when the system is operational and those where the system needs to be able to operate independently of any operator intervention. An Automatic Teller Machine would fall into the latter category, whereas a system that verifies that the correct individual is collecting their pay cheque will probably have an operator monitoring the system. Any system that has an operator monitoring the system can have the operator override the system. However, systems that do not have an operator present when the system is in use need to have more complex procedures for coping with system failures.

Accuracy and Reliability of the Matching Algorithms

Computers are now used around the world to maintain large databases of fingerprints for the purpose of identifying individuals. These computers certainly do not have a 100% accuracy in the matching process. When a fingerprint expert manually searches through a small set of fingerprint cards to determine if a sample print is from the individuals that produced the card then he will consider his work to be 100% accurate. He will state categorically that the fingerprint is or is not a match. On the other hand when the computer performs a match and returns the result there is not a 100% confidence in the result [27].

Most of the automated matching systems use a system involving the minutiae acquired from the fingerprint. They store these minutiae in some format thereby reducing the complexity of fingerprint matching to that of a point-matching problem. Unfortunately there is a lack of reliable minutiae extraction algorithms and a difficulty in quantitatively defining a match between two sets of points [20]. All available minutiae detection algorithms result in spurious minutiae.

A primary difficulty in performing the comparisons accurately results from variations in the biometric itself, as well as variations in its presentation [34].

Resistance to Fingerprints

Traditionally fingerprints have been used, and still are associated with the identification of criminals, since they are considered to be valuable physical evidence in forensic science [27]. They have traditionally been, and still are, used to trace and identify criminals. Due to this fact there is a lack of acceptability for fingerprints by a typical user [19]. This has given the fingerprint a stigma and causes some apprehension with usage among civilians. Many individuals think that if their fingerprints are stored in a database that they might be used against them in an invasion of privacy (as discussed in Chapter 2). There is also the perception that the fingerprints will be used to track an individual's movements outside of the intended purpose for which the fingerprint was initially requested. Fingerprints are already required in many places to obtain a driver's licence or a passport. There has been some resistance to the use of the fingerprint in these systems.

Despite the obvious strengths of biometrics there are still negative preconceptions [34]. The lack of clear information about how and when biometrics may be used can lead to ill-informed regulations, which could be overly restrictive to businesses [25]. There are a number of organisations such as the International Biometric Industry Association (IBIA) and the Biometric Consortium that have been formed to regulate and implement safeguards to prevent the misuse and abuse of biometrics. They also have policies to protect the confidentiality and integrity of databases containing biometric data.

There might be individuals that refuse to be registered by the system for some reason. Sometimes these people refuse because they have a criminal record and are afraid that the records will be turned over to the police and sometimes they refuse for other personal reasons. They might just consider it an invasion of their privacy. Many law-abiding citizens are reluctant to allow their fingerprints to be stored in any electronic database. In their minds there is the distinct possibility that their fingerprints could fall into the wrong hands and that they could be used to invade privacy. The existence of a web

site entitled "Fight the Fingerprint"[2] illustrates how many individuals want to prevent others from having access to their fingerprints. This privacy issue can be solved through the use of distributed storage on smart cards, as this dissertation will proceed to demonstrate.

Long Search Time

A large amount of computational resources are required to perform automatic fingerprint identification [19]. Another difficulty with the fingerprint arises from the lack of efficient search algorithms. It is not known how to order a database of fingerprints consistently. At best a search would have to be a brute force on a significant portion of the database. Implementing a classification scheme can substantially reduce the segment of the database that needs to be checked. However, the whole of the class must be compared against the print being searched for.

This can be a very time consuming way to search through many thousands or even millions of fingerprint records when a comparison of a single fingerprint can take one second. The Verid Fingerprint recognition webpage[3] advertises that their system performs a verification in less than one second, performing a single fingerprint comparison.

Missing Fingerprints

The fingerprints of a small fraction of the population are unsuitable for matching due to genetic, aging, environmental, or occupational reasons [19].

Fingerprints vary widely in pattern and in quality. There are many activities that may cause deterioration or even complete smoothing of the fingerprint. Although the fingerprint does regenerate to the same pattern unless extreme damage has been caused, there are many professions where the fingerprint is routinely damaged. These work environments seldom allow the fingertips sufficient chance to regenerate to their optimal level.

Some forms of manual labour, particularly those where the hands are used for heavy labour can cause the central region of the fingerprint to rub off and become flat. This central region of the fingerprint is the region that is usually used as the predominant section of the print for purposes of alignment and comparison. When this section of the fingerprint is non-existent or non-usable that individual cannot reliably be authenticated based on their fingerprint.

[2] http://www.networkusa.org/fingerprint.shtml
[3] http://www.tssi.co.uk/products/finger.htm

Fingerprints can also deteriorate if the fingers are exposed to certain chemicals, which can cause the sections of the fingerprint to become flat. Acids and bleaches among other chemicals have this effect. This results in the same set of problems that result from heavy labour.

This smoothing of the fingerprint is not permanent. If the finger is given the chance to recover outside of the influences that caused it to flatten in the first place then it will recover to the identical pattern as before.

There is also a fraction of the population that either does not possess the biometric or the biometric is unusable [34]. Some people have lost either a finger or hand and don't have their fingerprints. Other people could have exceptionally damaged prints rendering their fingerprints useless for purposes of identification.

Diversity of Characteristics

There is a wide variety in the fingerprints of individuals. Some have clearly defined ridges, while others have a much smoothed ridge structure. The distance between ridges varies with many hereditary traits of the user.

The large variety is not inherently a problem, although in some systems it is. This is due to the fact that many systems have been developed in the United States of America or in Europe where they have used a database sample containing predominantly European male prints. The difference between the profiles of the population that many systems are designed on and the population that comprise the actual users can cause problems. The accuracy of a system is sensitive to the target population. To have a successful implementation utilizing fingerprint technology one needs to understand and evaluate realistically the technology in the context of the target application and the target population [34].

Some systems use the distance between the ridges to detect if a region of the print is actually part of the fingerprint. If the range were not sufficient to cover all ethnic and gender differences then there could be a section of the population with which the system does not work well.

There could also be systems that use a smoothing or blurring filter in the detection process. This step will help to remove small noise artefacts. If however the ridge structure is very fine, then it could cause neighbouring ridges to merge into one single unrecognisable structure. Many systems have some form of smoothing in the process to remove noise and to minimise the effect of sweat pores.

The wide variety in the fingerprints can actually be a good thing if it is correctly handled. The greater the variety the greater the discriminating power between fingerprints. Thus if it is handled well it will actually increase the accuracy of an authentication.

Print Quality

There are a large number of anomalies that occur naturally in a fingerprint [27]. These range from stretching through to rotation of the fingerprint. Distortions may be found in a fingerprint as a result of pressure and the shear forces involved in rotation.

When the finger is scanned differences in the pressure or movement while the scanning is occurring could also cause a distorted image to be inaccurately captured. These distortions can introduce *apparent* dissimilarities in two prints from the same finger.

In fingerprints there is commonly some error or noise in the scanned image. Sometimes the correct pattern of the print is obscured by this noise. Often the signal-to-noise ratio of inked fingerprints is of a very poor quality [27]. Poor quality prints can be a direct result of the conditions that the prints were acquired in. Some of these conditions are listed below.

1. *Dry fingers*: Depending on the type of scanner the moisture content of the finger has a large effect on the quality of the final print obtainable from the scanner. With many scanners a dry finger often produces a poor quality print. A simple method that can be used to illustrate this difficulty is to place a finger on a clean glass. Then rub the same finger dry and repeat the process. There will be considerably less of a mark on the glass from the dry finger. There are many climates where there is either a dry winter or dry summer and large sections of the population have dry hands. There are systems that struggle to recognise people half of the year or simply do not work for half the year. A climate different from one where the scanner was developed and tested could cause problems.

   Some scanners are more resilient to changes in the moisture content of the finger. This is a result of the fact that the different scanners use different methods to scan the fingerprint. They might be using pressure, moisture content, optical methods or electrostatic charge as the specific quality that gets measured to detect the ridges.

2. *Dirty fingers*: People who work with coal as in coal power stations get the fine coal dust all over their hands. This fine coal dust clogs up the troughs between the ridges resulting in a

fingerprint scan that comes out smooth. The scan is then useless for electronic comparison purposes.

3. *Dirty scanners*: There are companies that expect a fingerprint scanner to work magic once it is installed. They expect it to last indefinitely completely maintenance free. However, every time a finger in placed on the scanner it leaves a grease residue. Over time this accumulates on the scanner and can interfere with the accuracy of the scanning process.

4. *Orientation*: The finger could be scanned at a different orientation from the one at which the reference was captured. There are comparison algorithms that can compare rotated scans accurately. The rotation can however easily cause the user to scan a different section of the fingertip, which could result in too little overlap to perform an accurate comparison.

5. *Translation*: Different positions of the finger in different scans would cause a different area of the finger to be scanned. This translation needs to be accommodated.

6. *Pressure*: Differences in the downward pressure of the finger during the scan can result in spatial scaling of the fingerprint. These differences also affect the contrast between ridges and troughs, particularly if the prints are acquired with the inked method [12].

7. *Shear transformations*: There could be different amounts of shear transformations exerted on a finger while it is scanned.

8. *Partial contact*: Partial contact with the scanner results in only a section of the print being scanned. Long fingernails sometimes interfere with the scanning procedure. They sometimes grow down and around the front of the finger as illustrated in Figure 3.5. Even if they are straight they could get in the way and affect the scanned region. It is not always possible to enforce fingernail length on the users of a system and they will blame the system if it does not accept their fingerprints.

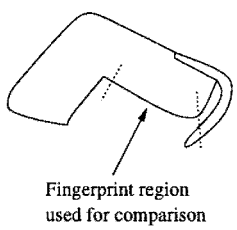


Figure 3.5: The last joint of a finger with the fingernail growing around the front of the finger.

Some people have arthritis in the hands and have stiff fingers preventing them from straightening their fingers. They might be unable to straighten the finger anymore than the finger depicted in Figure 3.5. This prevents them from placing the correct region of the finger on the scanner resulting in a poor quality scan that is often unusable and unrecognisable.

9. *Skin disease*: Some diseases can affect the fingers resulting in large areas of it being unusable for comparison purposes [12].

10. *Quantity of ink*: The ink used in manual acquisition of the print. An over or under inking of a finger will result in a poor quality print.

These factors all affect the quality of the fingerprint that is acquired for matching purposes. The combined effect of these can cause two fingerprints originating from the same finger at first to appear to be extremely different. To overcome these factors many of the manual fingerprint-matching techniques use the number of ridges between two minutiae as the measure of *distance* between them. This ridge count is often used in preference to the special count in manual comparisons. It is however somewhat one-dimensional as the ridges tend to run parallel to each other rather than in a crosshatch pattern. Thus the ridge count provides very good measurements in the direction perpendicular to the ridge structure, while providing poor measurements in the direction parallel to the ridge structure. It can also be difficult to accurately determine the ridge count automatically, particularly in poor quality images.

Long Enrolment Time

Often the enrolling process for a fingerprinting system involves acquiring many scans of an individual's fingerprints to generate a base template. This base template needs to be of the best possible quality to ensure that the matches against it can be of an acceptable accuracy. To achieve a fit as close as possible to the perfect base template, most systems perform many processing steps on the image before reaching the final result. This produces a long enrol time, which can be a problem if large groups of people need to be enrolled sequentially.

The event of having large groups of people being enrolled at the same time is likely to occur regularly in many systems. If a new authentication module is integrated into the system then all the users need to be enrolled. Educational institutions will have regular intakes of students and many companies have policies of recruiting new employees in batches. These scenarios will all require group enrolments.

Proxies

The idea of using a biometric is to ensure that the person claiming an identity can be verified as that person. Unlike the system that uses a PIN or password to verify a username, other people cannot borrow your finger. This can sometimes be a problem. For example if you need a fingerprint to log on to a computer network but you are ill, you cannot give your finger to a trusted friend and then change it the next day as you could with a password. This also happens with pension schemes. Many of the people on pension schemes are not in a position, due to health reasons, to collect their pensions personally on a regular basis. They can often appoint a proxy to collect the pension in their place. This is an extra complexity that needs to be tackled in many biometric systems.

There are subtle features that need examination if proxies are to be enabled. One of the main reasons that pension schemes are keen on using a fingerprint is to reduce fraud — a pensioner dies, but is not cancelled from the system and the pension is still collected. Using the pensioner's fingerprint would ensure that she is still alive. But as it is not always possible for the pensioner to be present physically due to health reasons, proxies are needed. However allowing a proxy nullifies the predominant reason for implementing fingerprint authentication unless it is implemented in conjunction with other controls.

3.2.8 How Fingerprints can be Used

It is still a difficult task to *identify* an individual based on their fingerprints and there is much room for improvement. This is not yet viable for real-time identification, but *verification* of a user's identity using the fingerprint is viable. The user will just need to make a claim as to who they are and then supply a fingerprint supporting this. Only an individual who is registered with a system, which is only verifying his identity rather than identifying who he is, would be able to use it. This makes it very difficult to track a person's movements except where he voluntarily identifies himself.

Fingerprints are very difficult to forge [40]. There is no anecdotal evidence of forgery using modern fingerprint scanners. Modern fingerprint scanners can detect many properties about the finger in addition to acquiring the fingerprint itself. These properties allow the fingerprint scanner to determine whether the finger being scanned is a living finger and can be used to ensure that a valid user is physically present for the system to operate.

The use of modern live scan fingerprint capturing equipment should be able regularly to produce a high quality scan usable for comparisons. From these prints it is possible to extract a set of

minutiae for use in the comparison process. Extracting these points and then comparing them can be performed in reasonable time in automated systems. Various authors have described many different types of minutiae. However these classes of minutiae can all be described in terms of ridge endings and ridge bifurcations. A typical finger will contain between 50 and 150 minutiae on the complete fingerprint. And in automated systems it is generally assumed that 10 points matching is sufficient to establish identity, since a pair of fingerprints that are identical, yet come from two different fingers has never been found [12].

3.3 Smart Tokens

> "A smart card is ... the size of a conventional credit card, and it has an electronic microchip embedded in it. The chip stores electronic data and programs that are protected by advanced security features." Gemplus[4].

3.3.1 What is a Smart Token?

The term *smart token* refers to a number of different technologies, all of which provide portable information storage. A number of different types of smart cards are available on the market. The most common of these look very similar to a credit card in appearance, but offer considerably more functionality. All smart cards provide some form of secure data storage and most new cards support a number of additional services, such as encryption.

The most common type of smart card is the memory card consisting of a non-volatile memory chip that stores data. A typical example usage of these cards is for phone cards. These cards do not have any processing power on them. Some people do not consider these cards to be smart cards, however since some authors treat them as smart cards they have been included in this discussion.

The other "smarter" smart tokens have a builtin microprocessor embedded into the card allowing the card to provide a wide range of additional functionality, ranging from the ability to manage a file system on the card to the encryption and decryption of private sensitive data. These microchip cards can be conceptualised as a small processor, with secure private memory and secure non-volatile storage space. These cards are not full computers, and can only be of use when connected to another computer via a smart card reader.

[4] http://www.gemplus.com/basics/what.htm

A number of standards exist for the design and implementation of smart cards. Of these one of the more common is the ISO 7816 standard, which defines the physical specifications of the card, along with its behaviour under various operating conditions. This standard specifies the size and the positioning of the various components of the card. The card needs to be resistant to ultra-violet light, x-rays, magnetic fields, static electricity, and should to be flexible enough to not crack after being bent 1000 times. These constraints on the card have direct implications on the microchips that can be used. The silicon used in the chip cannot be too thick, as it would then crack if bent. These physical constraints provide challenges to the design of fast microchips for the cards.

3.3.2 Evolution of the Smart Card

Many early cryptographic systems had some form of protection against the seizure of key material. Naval code books were weighted; rotor machine setting sheets were printed using water soluble ink; and some one-time pads were printed on cellulose nitrate, so that they would burn rapidly if ignited [21]. These forms of secure hardware were a precursor to the smart card.

These systems relied on the vigilance and trustworthiness of the operator and were often captured in surprise attacks [2]. Modern cryptographic equipment has been designed with a view to prevent tampering. An example of this is the VISA Security Module commonly used in banks to generate and check the personal identification number (PIN) with which customers authenticate themselves to the automatic teller machine. These modules use a safe to store a computer that generates the PINs. If the safe is opened or tampered with then the contents of the computer are erased [52]. The idea is to protect the customer by preventing the bank's programmers from gaining access to the customer's PINs and the keys that protect them [1].

As early as 1961 the first electronic-based cards were developed and patented. It was not until 1974 that this technology was first used commercially. A French journalist, Roland Moreno invented a circuit-based memory ring that could be used for secure payments. A bank consortium, Le Groupement des Cartes Bancaires realised the potential, but requested that the design be placed on a bankcard rather than on a ring. Moreno then approached the French company CII-Honeywell Bull to mass-produce the cards.

Michael Ugon, an engineer at Bull suggested that an integrated microprocessor chip be used, as this would improve the security. The banks agreed and in October 1980 the first microprocessor bankcards were patented and produced. Soon thereafter both Philips and Schlumberger released

their own standards for such cards. Microprocessor cards slowly started to gain acceptance in French banking and pay TV.

After retail trials the banks adopted Bull's design, as it was open ended and provided better security. Since then smart cards have come to be used for many different applications. These include the electronic purse in open and closed payment schemes, debit and credit cards for banking, identification cards, driving licences, health care, access control, cellphones, and loyalty cards along with many others. For the last three to four years microchip cards have been booming in the GSM phone SIM and electronic purse applications.

Some countries are now using smart card for their credit cards. These cards have a PIN stored on them, which is used to verify the use of the card. These credit-card sized devices contain an embedded microchip consisting of a CPU, RAM and ROM. There are many different applications where smart cards are now used — most of them are in access control, electronic commerce, personal authentication and privacy protection. However there has been limited analysis of the security risks and threats particular to the smart card [42].

The additional security provided by secure hardware should be such that it is difficult for an intruder to observe or partake in any information exchange. The communications between the different pieces of tamper resistant hardware are not necessarily secure unless they are all combined into a single unit of tamper proof hardware.

The most common form of secure hardware is the smart card. Most smart cards have a program loaded in the ROM when they are produced. However, we are seeing more cards that have an application loader in the ROM. This allows the development of multi-application cards with applets in the EEPROM. These smart cards are produced with a bootstrap loader installed on them. This allows the reader to load data or programs onto the smart card and to interrogate different memory locations on the card. These applications on the card can have complete control over the access to the RAM on the card.

From this large range of different applications all utilizing smart card technology the idea was conceived of using a single smart card that could be loaded with all of these programs. Thus the concept of the multipurpose smart card originated.

Along with this growth and development in smart cards, the processing power and the memory storage that is provided by these cards has dramatically increased. This is still adhering to the stringent requirements placed on the physical size and flexibility of the microchip on the card. The

very first microchip cards came with an 8-bit processor and a few bytes of RAM. The cards have progressed a long way since then. The power of modern cards can be illustrated with the SmartJ [45] card. This card contains a 32-bit RISC processor with a peak performance of 40 MIPS. The card was specifically designed to support multiple Java applications on a single card.

Smart tokens can be differentiated into groups depending on the type of reader that they interface with. This would divide smart tokens into two groups — those that require contact with the reader and those that interface via radio frequencies with a contactless reader.

3.3.3 Contact Cards

These are credit card sized cards that contain a small microchip on the front edge of the card. The chip size is limited to about $25mm^2$, typically $5mm \times 5mm$ attached to a contact area of about $10mm \times 10mm$. This card needs to be placed in a smart card reader and the microchip needs to be in physical contact with the reader for it to be usable. This contact allows an electrical signal to be transferred between the reader and the card, thereby driving the card. Contact cards do not have their own power supply, but rely upon the reader to power them.

Memory and microprocessor cards are slowly replacing the more traditional swipe cards. For this reason they often have a magnetic strip to facilitate the transition between these two technologies. The International Organisation for Standardisation (ISO) has defined the exact layout of the contact region of the microchip in the ISO 7816 standard. This standard also places size and flexibility restriction upon the microchip.

Memory Cards

Memory cards act as a storage facility. About half of memory cards are disposable and can be discarded once their task is completed [53]. These cards have been in production for about 15 years and because they are both simple and in high demand they are relatively cheap to manufacture.

Memory cards can be differentiated into two groups. The first group is *simple memory cards*. These can store about 2K of data. Magnetic swipe cards can store at most 0.2K of data. However these cards provide minimal security, since the memory is not protected from reads. *Protected memory cards* are similar to the simple memory cards, but their memory can only be accessed through the use of a secret key. These are a viable option for an electronic purse.

Microprocessor Cards

Microprocessor cards contain a small processor embedded on the front of the card. This provides an enhanced functionality allowing higher security levels and finer control. On-card processing facilities allow the execution of encryption algorithms or other security features. These cards have an operating system executing on the microchip and require software to be developed to enable them to support a wide range of cryptographic and security applications.

The microchip consists of the processor along with three types of memory. The first type of memory is the Read Only Memory (ROM), which stores the operating system. This memory is initialised at the time of card creation and cannot be modified by the cardholder. The ROM can vary from 1K or 2K up to 64K. The second is the Random Access Memory (RAM). This is a workspace for the programs loaded on the card and is typically from 64 bytes to 1024 bytes. The third type of memory is the Electronically Erasable Programmable Read Only Memory (EEPROM), which is non-volatile memory used to store persistent data.

3.3.4 Contactless Tokens

Contactless smart cards do not need to be in physical contact with the reader. Many different technologies are used to power contactless cards. These technologies can be divided into those that are *active* and those that are *passive*. The active cards have their own power source (usually a battery) while the passive cards derive their power from the current produced by converting radio frequency energy, which is emitted from the card reader. They have an embedded antenna to allow them to communicate with a reader. Contactless cards are normally driven by transmissions from the reader.

With contactless cards there are additional complexities arising from the need to supply power to the cards without resorting to an embedded battery. Instead, the card is powered by a different radio-frequency electromagnetic wave from that which carries the data. The microchip needs to include circuits to extract power from the receiver carrier wave in addition to all the components of the contact cards. For practical and economic reasons, the chip should require no external components other than a small printed antenna coil that can be easily assembled in a micro-module [46]. There are also a number of security issues linked to contactless cards, since their signals are broadcast via radio signals and therefore are easier to eavesdrop.

3.3.5 Difficulties with Smart Tokens

Smart cards are intended to provide a tamper resistant environment in which small applications can execute in the privacy of the card's microchip. Increasingly many systems are now relying on this tamper resistance of the smart card in preference to other security devices. Unfortunately this reliance on the integrity of the card is sometimes misplaced, as many of the older cards have been broken [2]. In most of those cases this is not a fault of the hardware, but rather a subtle flaw in the communications or security protocol. Attacks can be attempted over a range of possible angles, ranging from trying to remove layers of the microchip to examine the charge under a microscope and thereby determine the state of a bit, to the more common replay attacks.

Part of the inherent complexity of developing systems that make use of smart card technologies result from the nature of the microchip being split from the other components of the system. The microchip in the card is essentially a CPU and memory device with no dedicated means of communicating with the outside world. Thus the smart card is "handicapped". For the card to communicate with the outside world it needs to communicate via a smart card reader — which is external to the card. This can make the design and use of smart cards riskier than similar systems based on self-contained computers [42]. For example if there is a subverted reader which notifies the user that $1,00 has been charged to their card, while in actual fact $2,00 was charged to the card there is no way for the owner of the card to verify this except by using another reader.

One of the primary purposes for utilizing a smart card is to provide a secure storage area for a small amount of private information. The hardware and the software embedded on the card needs to be able to protect this information, whether it is a private key or biometric information. The card needs to be resilient to the attempts of a subverted reader to extract this information. All this needs to occur with the card in its own isolated cocoon with its only communication line through the reader — with the card having no way of notifying the user if sensitive information is requested from the card.

If smart card is lost or stolen it might take days or even weeks before the owner realises. The thief could even try reverse-engineering the card to defeat the tamper-resistance [2]. A smart card is usually designed to be accessed with a PIN. If n incorrect PINs are entered then the card would become locked. However if the time for a successful verification is less than the time for an incorrect PIN then it could be possible to abort the transaction before the card registers an incorrect PIN. Thus brute force and a careful timing attack might be able to recover the PIN. Other attacks could include fault analysis [4, 3] and side channel attacks such as power or timing analysis [23, 24, 22]. It is therefore advantageous to store the information on the smart card securely in an encrypted format.

If an attacker takes a card into a laboratory containing highly sophisticated equipment, he might attempt to duplicate or to modify the information on the card. Depending on the circumstances this could circumvent security mechanisms. If for example the information on the card was secured with a PIN or a fingerprint and the attacker was able to replace the PIN or fingerprint on the card then this would allow him to impersonate the valid user. A good system needs to be able to prevent the cards from being duplicated and/or modified by an attacker. These subtle attacks can involve the use of fake and modified cards running rogue software, with the intent of subverting the protocol between card and terminal [28].

3.3.6 Why Smart Tokens are Used

Smart cards have some interesting and unique aspects that need to be considered and correctly handled. Manufacturers and developers are slowly gaining a better insight into these complexities as the design of the cards is improved, both at the hardware and at the software layer. As these known attacks are prevented the security and effectiveness of the card is increased.

Cryptography is an essential component in modern information systems. It helps to provide accountability, fairness, accuracy and confidentiality and can be used to reduce fraud and assure the validity of financial transactions. It can prove your identity or protect your anonymity. Cryptography needs to be used in conjunction with secure hardware. A smart card or smart token can provide an affordable secure hardware suitable for cryptographic applications. The system needs to be designed as an integrated unit since two programs with similar features could have vast differences in their security levels and very different subtle security flaws. An experienced cryptographer can tell the difference — so can a thief [39].

A smart card can be used to provide a personalized security token. The microchip makes it considerably more powerful than a swipe card. It provides both access control to the information on the card and can execute small, embedded programs. If for example a swipe card is stolen and the thief tries to use it the card might get locked out by the system after five attempts. However the card still contains private information about the user's account. Compare this to the use of a smart card. If five false attempts are made to use the smart card it can both lock the card and destroy all sensitive information that it holds. In other words, the control has been delegated to the card.

One would like to have a secure tamperproof-operating environment in which it is impossible for an attacker to gain access. Schneier [39] points out that subtle flaws can render any security system

vulnerable to attack. When designing a security system one needs to consider all possible security risks carefully. To increase the level of security one needs to conduct a thorough examination of the possible security flaws and then design systems without them. At the same time one must not introduce new security holes.

3.3.7 Security of the Smart Card

A microchip card contains a small processor and memory, which together can be treated as an object. The memory cannot be accessed externally from the card. The only way that information can be transferred with the card is by sending it messages and receiving responses. Like all objects, the card only understands the set of messages defined for it, providing it with measures to manage its data.

Smart cards are intended to provide a physical level of security to prevent direct access to their memory. The smart card consists of a small microprocessor with memory, (both volatile and non-volatile). The ROM of the card has an operating system installed on it at creation time. The Siemens SLE44C160S, which was used, comes with an operating system loaded in the ROM that provides functionality to install software on the card. This program loader supports only a single program on a card. When it loads a program it erases all data previously in the EEPROM and RAM, before installing replacement software. This provides sufficient protection to prevent modified cards from accessing previous data stored on the card. If the card is modified or reused then all the data, which was on it, is destroyed.

Attacks exist that utilise micro probing to examine the chip and read the contents off of it. These attacks either use an electron microscope to examine the state of the memory or they use micro-probes to eavesdrop on the bus. To prevent micro probing the chips have reduced feature sizes and consist of multiple layers making it difficult to gain physical access to the bus. The communications on the bus are encrypted to render them useless even if eavesdropped.

A second class of attacks comprises the side-channel analysis of the card. These attacks, which monitor the power consumption and timing, have been successful against some of the original smart cards. Random wait states and the addition of noise to the power consumption are features many cards now have to prevent side-channel analysis. Side-channel attacks are one of the most difficult attacks to prevent as they utilize implementation peculiarities to gain information. For example, the timing of a failed and successful authentication could possibly indicate whether it was a success or failure before the transaction completes.

The third group of methods attack flaws in the protocols to gain access to the contents of the card. The protocols that the card participates in are usually small. These protocols should be adequately tested before a product is released to remove flaws from them. The security of smart cards has increased as weak points are identified and removed thereby enhancing the protection that the card is able to offer.

3.3.8 Integration of Fingerprints with Smart Cards.

One of the potential security flaws of passwords and PIN codes is that they are vulnerable to being stolen or guessed. Many people write their passwords down and there is also the possibility of a brute force attack being developed. The need for passwords can be removed if one uses a biometric instead of a password.

Such a system can be designed to incorporate the security principles of privacy. This system could be designed so that each individual requires a unique user name associated. This username would be stored on a smart card along with a biometric template for authentication. The verification information could require a password or PIN in addition to the biometric.

One of the primary concerns many individuals have with a civilian use of the fingerprint is who will have access to the fingerprint and what it will be used for. Will it only be used for the specific purpose for which it was given or will it be used for other unspecified purposes? By placing the fingerprint onto a smart card this should give the user complete control over how and when the fingerprint is used, while at the same time enhancing the level of security attainable through a biometric solution.

3.4 Summary

There are many biometrics that are being used or experimented with for personal authentication systems. These biometrics range from fingerprints through to DNA scans. Each biometric has its own set of advantages and disadvantages, but all of them need to satisfy a number of requirements to be useful. They need to be universal, unique, permanent and collectable. Along with these the algorithm used needs to have an acceptable level of performance. The system should be as non-invasive as possible such that it is acceptable to the public and it should be difficult to circumvent.

Biometric technologies can be compared on the FAR and FRR. The Equal Error Rate (EER) is the adjustment of the match parameters such that the FAR equals the FRR. These measures of the accuracy along with other performance characteristics can be used to determine the suitability of a technology for a specific purpose.

The fingerprint is the most widely used biometric. This is the pattern of ridges and furrows that cover the tips of the fingers and toes, giving them a corrugated appearance. These ridges and furrows allow the fingertips to perspire while maintaining a tactile and gripping facility.

Fingerprints contain minutiae, which can be used for the comparison. These minutiae are located at the ridge endings and the ridge bifurcations. Macro characteristics of the fingerprints can be used to aid in the alignment of fingerprints. Macro characteristics include the classification and location of the core and delta points. Manual fingerprint comparison is based on the matching of minutiae.

There are a number of difficulties with digital fingerprint comparisons that need to be dealt with and overcome to provide a good system. These difficulties include complexity of accurately extracting the minutiae, particularly from images of degraded quality. The print quality is influenced by factors ranging from the moisture content to the cleanliness of the finger and scanner. Some people have a perception that fingerprints can be used to infringe upon their privacy. There is no highly accurate scheme for indexing fingerprints requiring long search times to locate a print in a database. Fingerprints have a wide variety and occasionally they are missing from an individual.

Smart cards provide a tamper resistant hardware that can be used for the storage and comparison of fingerprints. Most smart cards conform to the ISO 7816 standard specifying the size, flexibility and resilience of the cards.

Smart cards are replacing the swipe cards for many applications. Smart cards have been in use as telephone cards for a number of years already. The simplest smart cards are just a memory card, while the more complex ones contain a microprocessor. Typically the microprocessor has a combination of RAM, ROM and EEPROM along with an eight-bit processor executing at clock speeds of 3.5 - 5 MHz.

There are still a number of difficulties with smart cards. There have been attacks on smart cards that have broken most of the early cards. However the manufactures of the cards are using the information gained from these attacks to improve the design making it increasingly more difficult to access the card without the valid authentication. Most of these attacks are not however on the hardware of the card, but rather on the protocols used in the communications between the card and reader.

Smart cards have been used in conjunction with fingerprints to provide personal authentication. Fingerprint comparisons had not yet been performed on the card itself at the time of this research, even though Gemplus have now placed comparison routines on a card. Previous system just used the card to store a fingerprint template. The fingerprint template was then transferred to a computer to perform the comparison. This combination does not prevent an attacker from acquiring the template off of the card.

Chapter 4

Architecture and Design

Authentication of a user's identity is a difficult but crucial task in many contexts. Traditionally the use of a username and a password or Personal Identification Number (PIN) has sufficed as proof of identity. However passwords and PIN numbers can get lost, stolen, or guessed. Thus to overcome this difficulty it is preferable to use a biometric. The fingerprint is used although it is possible to use a different biometric, or combination of biometrics in place of the fingerprint.

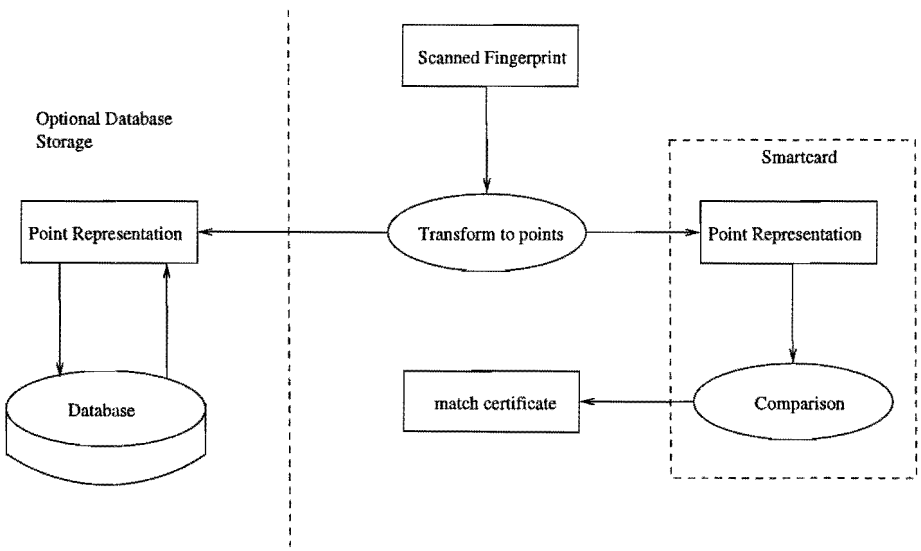


Figure 4.1: Overview of the fingerprint authentication of an individual performed on a smart card.

The conceptual overview of the architecture of the system developed is shown in Figure 4.1. In this diagram there is a high level overview illustrating the processes involved in the authentication of an

individual. This begins with the acquisition of the fingerprint image and ends with a final decision of whether the fingerprints are a match or not. The scanned image is passed through a series of transformations that extract a set of minutiae. These minutiae are each points with an associated direction. Sets of these minutiae are stored on a smart card for use as a template to compare against the set extracted from the input fingerprint. These points could also be stored in a database — but this does introduce extra security issues.

The output from the comparison process is a *match certificate*. This match certificate is returned from the smart card if a fingerprint successfully matches the print stored on the card and should only be used internally to the system to allow a transaction.

4.1 System Requirements

Before any system can be designed and developed there are a number of criteria and constraints that should to be examined. For the system that was developed in this dissertation a number of key issues were examined. These issues are similar to the ones one would expect for any authentication system, although they are presented specifically as they apply to a biometric system for the personal authentication.

4.1.1 Security/Accuracy

When a username/password pair is used to verify an individual's identity the pair needs to be securely stored for purposes of comparison. A number of operating systems encrypt the password file. This password file is sometimes shadowed, which prevents hackers from reading it even in the encrypted format. Somehow the passwords of all the users of a system need to be stored, while at the same time access to the passwords needs to be prevented except for authentication purposes. For minutiae to be used a template of the fingerprint needs to be stored along with the username. This template also needs to be stored such that it can only be accessed for comparison purposes.

One does not require an exact match to consider two fingerprints to have originated form the same finger. This makes it more difficult to determine if two fingerprints originated from the same finger compared with the exact match used in password verification. With fingerprints one determines the correlation between the prints and then uses a confidence level to determine whether to declare them as a match.

These confidence levels are used to specify the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) of the system. The FRR is the percentage of the attempts to validate a user where the correct user is rejected by the system. The FAR describes the percentage of attempts attempted by an incorrect user where she is authenticated as being the correct user.

In the ideal system both the FRR and the FAR would be zero. In practice there are some false positives and some false negatives in any system, just like a password is sometimes correctly guessed, or incorrectly entered. There is a correlation between the FAR and the FRR. Tightening a parameter to reduce the error margin in false acceptance would have the counter affect of increasing the chance of a false rejection.

In the system discussed in this dissertation, the fingerprint template is placed onto a smart card. All comparison of the fingerprint will then be performed on the card itself, removing all reasons for allowing the template to leave the card. By delegating the decision process concerning the match between fingerprints to the card the specialized risks incurred from the use of smart cards are reduced. The card should be unusable to all people except the authorised user. Any data stored on the smart card and protected by the fingerprint should remain private even when tampered with in a fully equipped laboratory.

4.1.2 Efficiency/Performance

An effective authentication system should be quick. The amount of time allowed depends on the application and frequency of the authentication process. For an Automated Teller Machine the maximum that a user would consider acceptable would be about three seconds. For logging on to a computer the whole process could take up to about five seconds and still be acceptable. The performance requirements for a system can also have an effect on the accuracy of the matching process. There are enhancement algorithms that can be applied to a fingerprint, which will reduce the FRR and the FAR. These algorithms are typically CPU intensive slowing the whole process.

To migrate the point comparison step of the matching process onto a smart card will require that it is a highly efficient algorithm in terms of both CPU and memory requirements. The point-matching algorithm has been examined and modified specifically to reduce space and time to allow it to operate on a smart card. The smart cards available for this project have 256 bytes of RAM and an eight-bit CPU operating at speeds in the range of $3.5 - 5$ MHz. This is at least 100 times slower than a modern PC.

4.1.3 Redundancy and Robustness

A system must be robust. It should contain measures to ensure that the system can function correctly under adverse conditions. For any system that authenticates individuals one can safely assume that there will be attempts to hack into the system. These attackers will attempt to impersonate other valid users to gain unauthorised access. They will attempt to stress the system beyond its breaking point.

Thus any system developed for personal authentication that protects sensitive information should be designed to be resilient under extreme pressure. It should be robust enough to cope with most events that could happen. There should to be some redundancy in the system to accommodate system failures. If a network link goes down then the system should ideally still be able to function in an acceptable fashion. The system should be able to cope with errors and recover from these errors. Performance should gradually degrade under a loss of resources rather than a complete sudden failure.

How does the system perform under stress? Is there enough redundancy designed into the system to provide robustness for it to recover after a failure? Can the system recover from errors and seamlessly continue by utilizing alternate methods?

4.1.4 Scalability

Many systems in current operational use were designed and implemented for a limited number of users. Over time the number of users for these systems has increased resulting in a gradual degradation of performance in these systems. Systems, even when they are designed for only a small company's use, should still be designed based on the scalability principles.

The system needs to be designed to cope with large numbers of users. Currently systems that identify a user based on a fingerprint take a long time when a large database needs to be searched. Those systems have trouble scaling to cover large numbers of users as the search is $O(n)$. There are no search algorithms for a database of fingerprints that are $O(\log n)$. Systems that use a username and a fingerprint are capable of scaling to include large numbers of users, however if the search can be performed on a username then it can be found in $O(\log n)$ time.

4.1.5 Offline/Online

Some systems are designed to only operate when they are online. These systems include most database systems. They are unable to operate if they are unable to contact the database server. Very often though the system could be authorised to allow limited transactions to proceed even without authorization from the database. Sometimes the only reason to access a particular database is to validate a user's identity.

How efficiently and effectively will the system perform offline, or does it need to be online? One would like the system to work efficiently offline thereby making it more robust and reliable under failure. Does an authentication server need to online be to authenticate an individual?

Placing the fingerprint template onto a smart card allows the authentication to be distributed and thus performed without the need for any network access. This should allow a system to operate offline thereby increase the robustness and scalability of the system.

4.2 System Overview

As previously mentioned this dissertation is concentrating on the processes from the acquisition of a fingerprint scan through to the final decision of whether they originated from the same finger. The last step will be performed on a smart card, while the initial preparation phases, which are used to extract the minutiae set, can be executed on a workstation.

4.2.1 Choice of Smart Cards for this Work

For this work the Siemens SLE44C160S smart card was chosen. This card has 16KB ROM, of which 1KB is used for the operating system on the card. The ROM is written at the time of card creation and cannot be changed after that. This work does not use the ROM. There is 16KB of EEPROM, which was divided into two 8KB blocks. The one block was used for data and the other for code. This division can easily be changed. The card has 256 bytes of RAM.

The SLE44C160S card contains sufficient resources for the purposes of the work. For additional developments to this work the SLE66CX160S card, with its crypto-processor, would add the ability to sign data with the RSA algorithm using 1024-bit keys in less than one second. Triple-DES can be implemented on either of these cards requiring less than 100ms for the required computation to create a digital signature.

4.2.2 Data Representation

The system developed made use of the Siemens FingerTip fingerprint scanner to acquire digital fingerprint images. These images contain an intensity field representing the ridge structure. Each pixel is an eight-bit value. Low values indicate a ridge with the fingertip closer at that pixel to the scanner. This initial intensity image is used as the input for the matching process. From this image a usable representation of the fingerprint is extracted as it is passed through a number of transformations. These can be seen in Figure 4.2.

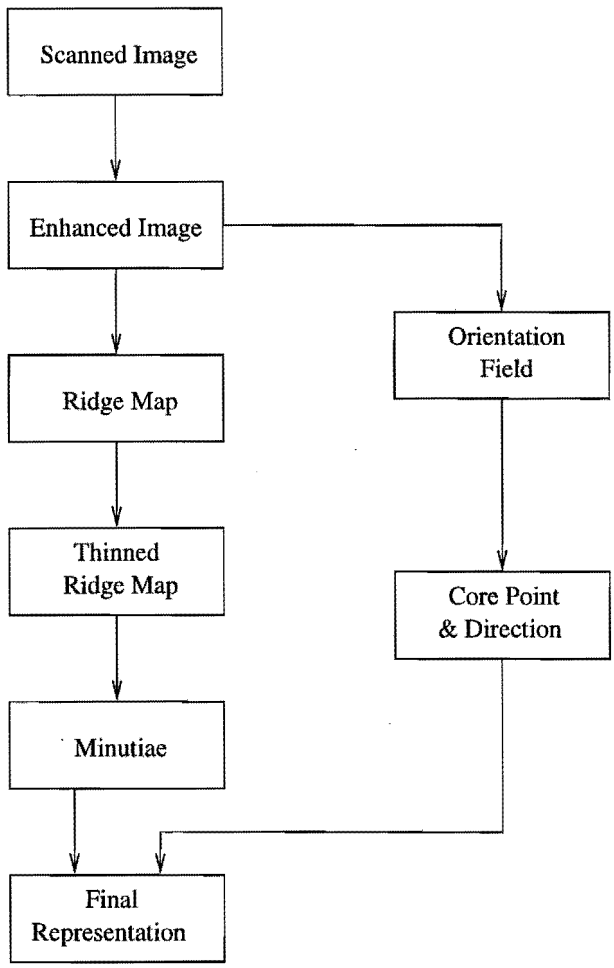


Figure 4.2: An overview of the transformations of the fingerprint.

For the purpose of testing the system it also can take as input an image of a fingerprint from a database. This image can be injected into the system in place of the image acquired from the scanner. It will only be used for test purposes, but it will allow the system to be compared against

other systems that utilize fingerprint technologies. There are a number of standard databases that can be utilized for this purpose. For this research the fingerprint databases from National Institute of Standards and Technology (NIST) were used.

The input image, from either the scanner or the database, is passed through a number of steps. The first of these stages is the enhancement stage, during which the random noise is reduced and the ridge and trough structure is sharpened.

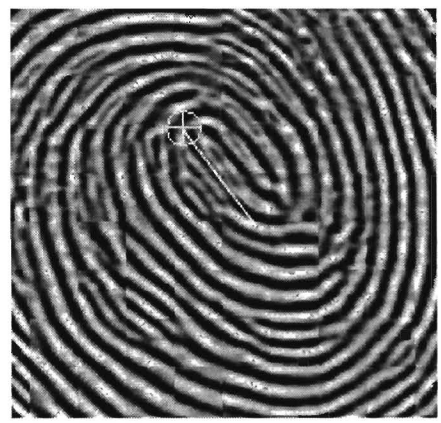


Figure 4.3: The enhanced fingerprint showing the core and the direction.

This process produces an enhanced, smoother pressure field of the fingerprint. This enhanced image is used as the input to construct an orientation field and a ridge map (see Figure 4.2). The orientation field indicates the dominant directions of the ridge structure. From the orientation field the core point is extracted and a direction associated with the print is determined. This direction and core point can be used in the alignment of two scans from a finger. In Figure 4.4 the orientation field with the core point and direction superimposed over the orientations is illustrated. This core point is overlaid onto the enhanced fingerprint image in Figure 4.3. The core point is defined as the point of sharpest concave curvature of the ridge structure. All fingerprints should have a single unique point that fits this description.

A ridge map needs to be produced from the enhanced fingerprint as illustrated in Figure 4.2. The ridge map is a two-colour image of the fingerprint splitting the image into ridges and troughs. The ridges are then further processed to produce a thinned ridge map, which simplifies the extraction of the minutiae by thinning each ridge to a single pixel in width.

From the thinned ridge map a set of minutiae are extracted. These minutiae are comprised of both the endpoints of the ridges and the ridge bifurcations or forks in the ridges. These minutiae have

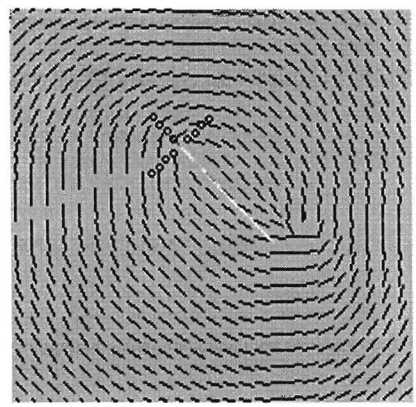


Figure 4.4: The orientation field of a fingerprint with the core and direction superimposed on it.

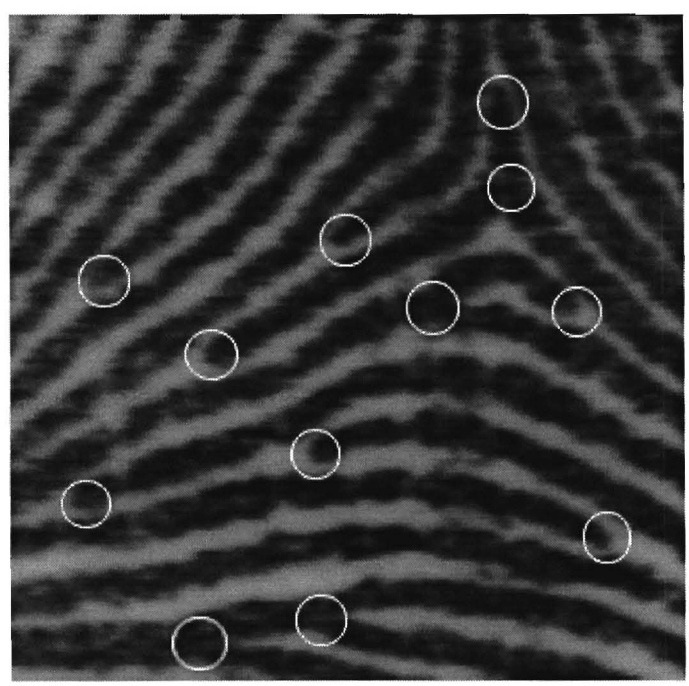


Figure 4.5: Minutiae from an enlarged section of a fingerprint.

been highlighted with circles superimposed over the original scanned image in Figure 4.5. They are used as the basis of the fingerprint representation that is stored. Only these minutiae need to be compared to determine whether or not the prints are a match.

The minutiae are then converted from Cartesian coordinates (x, y) to polar coordinates (r, θ). The direction (α) of the ridges from which the minutiae were extracted along with other characteristics of the minutiae are recorded together with the position of the point. This information is needed to perform the matching step.

4.2.3 Matching Process

The procedure described in Section 4.2.2 produces a set of minutiae. These minutiae can either be stored as a template for later comparisons or they can be compared with a previously recorded template of minutiae.

If used as a template they would be placed onto a smart card. This set of minutiae needs to be compact in size. The reduction of size in the stored representation is necessary since the Siemens smart cards that are used have only 256 bytes of RAM and 16 KB of Electrically Erasable Programmable Read Only Memory (EEPROM). This set of minutiae can then be stored in the EEPROM of the smart card and reduces space requirements from 256 KB needed for an image scan of size 512 x 512 with an 8-bit intensity resolution, to less than 512 bytes. In effect the matching problem has been reduced to a simple point-matching problem.

The 256 bytes of RAM create a constraint on the size and complexity of the matching algorithm. The desire to perform the matching process on the smart card was a critical factor in the decision to use a set of minutiae as the representation.

The matching process is performed on the smart card. By performing the match on the smart card the template of the fingerprint never needs to be removed from smart card. This gives the cardholder complete control over the use of her fingerprint. She can then choose exactly when she wants to verify herself using her fingerprint and other people cannot access or remove the representation of the fingerprint from the card. The fingerprint does not need to be stored centrally in a database.

4.3 Summary

The authentication process can be divided into two main sections — those that need to be performed on the smart card and other subsidiary processes. For security and privacy reasons the minutiae comparison procedure needs to be placed on the smart card. The set of minutiae can be extracted before being sent to the smart card without any loss of privacy since the fingerprint must be scanned into some intermediate area prior to sending it to the card. The process starts with the acquisition of a fingerprint image from a scanner. This image is then transformed into a set of minutiae, which are then sent to the smart card for comparison against a template stored on the card.

Systems implementing this authentication process need to fulfil certain performance requirements to be useful. The comparison of fingerprints needs to have a sufficient level of accuracy for it to be able to provide a secure authentication solution. The comparison needs to be efficient to allow it to be used for real-time verification. As with all security systems there needs to be sufficient robustness and redundancy to make it difficult for an impostor to masquerade as a valid user. The distributed database created by storing the fingerprints on smart cards allows the systems be very scalable and to operate offline.

Chapter 5

Implementation

The process of verifying a user based on his or her fingerprint presents a number of challenges. For this system the main challenges were to compress the fingerprint representation and matching routines to allow it to be implemented on a smart card. Many of the algorithms were modified in order to rise to these challenges.

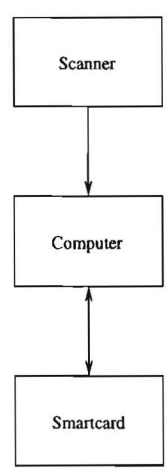


Figure 5.1: An overview of the physical separation of the components in the authentication process.

The whole process has been split into three sections which are shown in Figure 5.1. The first of these sections is the acquisition of the fingerprint image. In this section the fingerprint would be acquired from a live scan device. For testing purposes, however it can be replaced with a fingerprint image, which has been extracted from a database.

The second phase extracts from the original input image a much smaller template of the fingerprint.

This template is created through a number of processing stages to finally produce a set of minutiae. The extraction of the template would occur on the computer or workstation.

The third stage uses the template created in the second phase. This representation is then either stored on the smart card or compared against the template already stored on the smart card. The comparison in this stage occurs entirely on the card. The results of the comparison are returned to the controlling computer.

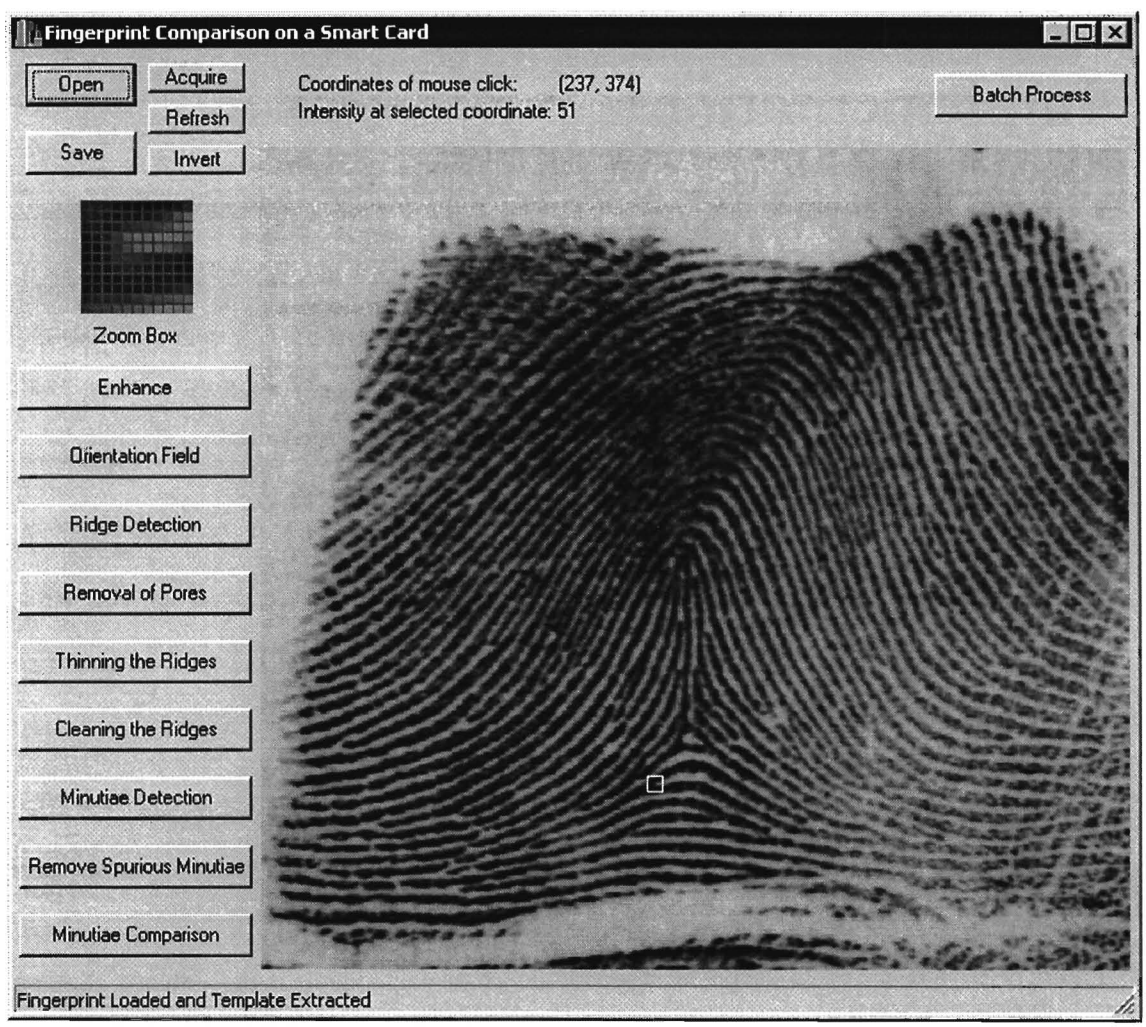


Figure 5.2: A screen shot from the implementation showing the main window.

A screen shot of the main window of the system that was developed is shown in Figure 5.2. This window has buttons in the top left corner to *load*, *save* or *acquire* a fingerprint scan from the Finger-Tip scanner. Just below these buttons is an area to display a zoomed in view of the area highlighted

with a little white square around it. This area can be selected with the mouse from the main fingerprint display. The text above the fingerprint displays the coordinates and the intensity at the selected point. At the right of the window a button has been placed to bring up the batch-processing window. The buttons below the zoom box allow the user to control and monitor the stages in the template extraction algorithm.

The "Orientation Field" button opens up another similar window providing a display of the orientation field. This additional window has buttons to allow the user to locate the core and valid regions of the fingerprint along with providing the ability to calculate the quality of the fingerprint.

The "Minutiae Comparison" button opens up another new window. This window contains a few buttons to allow sets of minutiae to be compared both on the workstation and on the smart card.

5.1 Acquisition of the Fingerprint

In this, the first stage of the process, a fingerprint needs to be acquired. It can be either inputted from a scanner as would happen when the system is deployed, or it could allow input from a database for test purposes.

5.1.1 Fingerprint Scanner

A FingerTip sensor from Siemens was used for the research towards this dissertation. The FingerTip scanner is a small unit of dimensions $18mm \times 21mm \times 1.3mm$ with a scan region of $11.288mm \times 14.36mm$. The scan region consists of a sensor array of 224×288 cells. The sensor works by means of a capacitor feedback sensing circuitry. The pixels of the sensor are pre-charged. The charge of the pixel is then transferred to a sampling capacitance. If a finger is placed on the chip, the surface of the skin acts as a counter electrode. The varying distances of the finger from the sensor surface due to the ridges and troughs produce different capacities for ridges and troughs.

The FingerTip scanner can be connected to a computer via an Extended Parallel Port (EPP). The total time required for an image capture is less than 100 ms [44].

5.1.2 NIST Fingerprint Database

To allow for the performance testing of the system the NIST Special Database 4 Fingerprint Database was used. This database contains 2000 pairs (4000 fingerprints) of 8-bit grey scale images of randomly selected fingerprints. Each of these prints is a 512 X 512 pixel image in a flat file format with a small header at the beginning of the file. These images were acquired from inked impressions and then scanned in at a resolution of 500 dots per inch [54].

Each pixel of the prints requires 8-bits or one byte of storage. A fingerprint from this database requires 262144 bytes of storage without the header. This is clearly considerably more than could be stored on any smart card currently available.

5.2 Extraction of a Template from the Fingerprint

The template extracted should contain some information about the general structure of the fingerprint as well as the minute details needed to perform a comparison accurately.

The general information about the fingerprint extracted could include some sort of classification. The more categories of fingerprints provided the better. In addition, fingerprint alignment information can be extracted by examining the complete print. This would be stored with the template on the smart card.

The minute details of the fingerprint also need to be extracted. These minutiae allow fingerprints to be compared at a very fine level of detail. The differences between fingerprints at the fine level are more pronounced than at the more general coarse levels. This set of minutiae, along with features of each minutia, will comprise the remainder of the template of the fingerprint.

The process of acquiring this information from the fingerprint requires that a number of processing stages be applied to it. These stages start from the scanned image and eventually produce the set of minutiae and classification information.

It is important to extract the features as accurately as possible. There is the possibility of a few spurious minutiae being detected. False minutiae should be reduced, while at the same time it should attempt to locate all of the correct minutiae accurately.

The main stages in the extraction of a template from the fingerprint are listed below. The effects of each of the these stages in the algorithm is reflected in the main fingerprint display area in Figure 5.2,

except for the ridge detection, which utilizes its own window, and the minutiae comparison that is performed from another window.

- Enhancement
- Orientation Field
- Core Point Location
- Valid Region Detection
- Quality of Fingerprint
- Ridge Detection
- Removal of Pores
- Thinning the Ridges
- Cleaning the Ridges
- Minutiae Detection
- Removal of Spurious Minutiae

The original image was acquired in the process described in Section 5.1 and is used to produce an *enhanced image* using the enhancement algorithm presented by Candela[11]. This enhancement of the fingerprint is intended to reduce random noise resulting from distortion caused by the scanning process. The simplest method is to pass the image through a smoothing filter to cause a slight blurring of the image. This will remove very small inconsistencies in the image. The difficulty with any attempt at enhancement is the possibility of removing valid information. An algorithm has been applied to attempt to strengthen the pronunciation of the ridge structure. This algorithm is further explained in Section 6.3.1.

From the enhanced image an *orientation field* is extracted as is explained in Section 6.3.2. The orientation field extraction algorithm is based upon existing algorithms. This orientation field is used to calculate the *core point* and a *curvature index* for the fingerprint. The author developed an algorithm to locate the core point, which is further described in Section 6.3.3. The enhanced image is also used to determine the classification of the fingerprint.

The image that was acquired from the fingerprint scanner is rectangular in shape. Very often part of this image is not in the fingerprint. In the screen capture displayed in Figure 5.2 a fingerprint is displayed in the lower right of the screen. This fingerprint does not use the full area available. Thus it is necessary to be able to locate the *valid region* of the scan. For this the orientation field can be used. The author's algorithm used to locate the fingerprint in a scanned image is explained in Section 6.3.4.

Sometimes scanning produces images of very poor quality. These might result from finger movement during the scanning process or even the lack of a finger when the scan occurred. It is thus important to be able to determine whether a fingerprint was actually presented and whether the scan can be used. The algorithm shown in Section 6.3.5 uses the valid region and the orientation field to calculate a *quality* factor of the fingerprint.

Ridges are extracted from the valid region of the scan. These ridges are extracted using the author's algorithm presented in Section 6.3.6 from the enhanced image and the orientation field.

The ridge map that is produced has small holes in some of the ridges. These holes are from the sweat pores that are on the ridges. Scans that are at resolutions of 500 DPI do not have enough resolution to be able to identify sweat pores reliably. For this reason the *sweat pores* need to be *removed.* The algorithm that was used to do this is explained in Section 6.3.7 and is based upon the algorithm presented by Megdal [29].

After removing the pores from the ridge map it is thinned to produce a *thinned ridge map.* This contains all ridges, each a single pixel in width. Section 6.3.8 describes how the ridge are thinned.

The thinned ridge map might still contain a few short spikes or bridges. Often these are artefacts remain from previous errors in the scanned image. It is therefore desirable to remove these spurs from the ridge map to produce a *cleaned ridge map.* This cleaned ridge map is created by applying the algorithm in Section 6.3.9, which is based upon the algorithm presented by Megdal.

From the thinned and cleaned ridge map a set of *minutiae* are extracted. These minutiae are extracted by examining the structure of the ridges. If the ridges bifurcate or end then the point at which they do this is recorded. This point is then stored in Cartesian coordinates. The core point is used as the centre of the fingerprint and all of the minutiae are converted into polar coordinates relative to the core point. The algorithm used to extract the minutiae from the ridge map is shown in Section 6.3.10.

Unfortunately the minutiae detection process occasionally detects spurious minutiae. An attempt is made to *remove* the majority of these *spurious minutiae* without removing valid minutiae. This

process has a similar set of hazards to the enhancement stage. If the decision to remove a minutia is too lenient then many valid minutiae might be removed, while if it is too stringent then it won't do much good. The algorithm to remove the spurious minutiae is explained in Section 6.3.11.

5.3 Initial Template of the Fingerprint for Smart Card

This template of the minutiae of a fingerprint needs to get transferred to the smart card where it will serve as the basis for matching fingerprints in the future. The minutiae are converted to polar coordinates for storage on the card. The use of polar coordinates simplifies the comparison process.

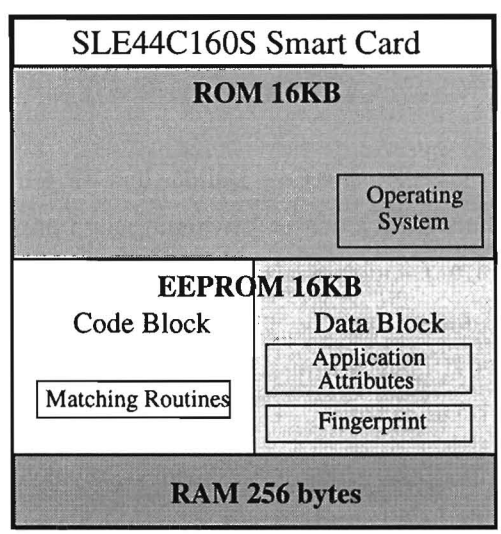


Figure 5.3: The layout on the smart card.

The SLE44C160S smart card used for this implementation has 16KB of ROM and 16KB of EEPROM. The EEPROM is divided into a data block and a code block each of 8KB. The template of the fingerprint uses 516 bytes of the EEPROM on the card. This means that over 7KB remains in the data block, which is enough, for example, to accommodate a 1024 bit private key and/or subject identification information as required by specific applications. The card was read with the "Chipdrive intern" card reader [50].

5.4 Comparison of Fingerprint Performed on the Smart Card

Due to the nature of smart cards — they have small amounts of processing power and small amount of RAM. The matching algorithm therefore needs to be highly efficient both memory and speed.

If the classification of the fingerprint does not coincide with the classification of the print on the card then the print is rejected as incorrect. Similarly if the curvature at the core of the print is too different from the template print then it can be rejected as belonging to different fingers. This should considerably reduce the number of false prints where the minutiae need to be compared.

Extracting a set of minutiae from the fingerprint reduces the remainder of the matching process to that of a 2-d point-matching problem. Since the core has been located on both the template and the finger provided one could implement a highly efficient algorithm. This algorithm is described in detail in Section 6.4, which was developed by the author to reduce the memory and CPU requirements.

5.5 Summary

A system was developed in C++ using C++ Builder that implemented concepts presented in this dissertation. The algorithms, which consist of existing algorithms with extensions developed for this project, are described in Chapter 6. The system was developed to demonstrate the viability of performing fingerprint matching on a smart card. The complete process was modelled from the acquisition of fingerprint images from a FingerTip scanner through to the comparison of the biometric templates on a smart card.

From an implementation perspective the process can be divided into three sections. The first of these sections interacts with the fingerprint scanner through a parallel port to acquire the fingerprint. The ability to save and load images from file was added to the system to facilitate the testing of the separate components.

The second section of the implementation extracts a set of minutiae from the scanned image. This section passes the scanned image through a number of processes to produce a set of minutiae with reasonable accuracy. These minutiae are compared in the third phase of the process. This system allows the comparison of the minutiae to be compared either on a workstation or on a smart card.

Smart card software was developed that performed the comparison of the fingerprint minutiae on the card. This software handled the transfer of the biometric template between the computer and the

card. Once this software was loaded into the EEPROM of a smart card the card could then be loaded with a biometric template. The smart card accepted a second set of minutiae to compare against the template installed on the card. The security of the card was such that all biometric information that was transferred to the card could not be read off of the card.

Chapter 6

Fingerprint Comparison Algorithm

A fingerprint consists of a pattern of ridges and troughs, as was explained earlier. These ridges and troughs curve to form a pattern that is unique to a finger; even identical twins have different fingerprints. The pattern consists of the varying thickness and curvature of these ridges and troughs. A counter example has never been found showing two different fingerprints from two different fingers to have a matching pattern.

In addition to this the pattern created by the ridges and the troughs of the fingerprint remains constant throughout an individual's lifetime. This allows us to use the pattern of the ridge structure along with any information that can be extracted from it in personal identification.

This unique pattern formed on the fingertips contains a set of minute details. The configuration of these minutiae forms a pattern that is also unique to a particular finger, providing a richness of information. This set of minutiae can be extracted from a fingerprint and used in comparisons. Most automated fingerprint matching systems use the minutiae set as the basic data to compare fingers.

At an even finer level of detail the fingerprint contains sweat pores on the ridge structure. These sweat pores are also thought to provide a unique pattern that can be used for comparison. However since these pores are smaller than the ridges they need a higher resolution scan to be reliably extracted from the fingerprint.

At a slightly higher level the curvature pattern of the ridges can be examined to extract classification information. This information is general information about a given fingerprint. It is however not unique to a fingerprint, but rather divides the fingerprints up into a number of classes. This

information can be used to complement the information stored in the set of minutiae representing a fingerprint.

6.1 Feature Selection

Fingerprints contain a rich store of information in the pattern of the ridge structure. This pattern on the fingerprint is composed of a series of curved ridges and troughs. Each ridge has a series of sweat pores extending along its length. It is the sweat from these pores that leaves an impression of the fingerprint on surface touched by it.

The most obvious features of the fingerprint to use for the comparison stage are the ridges themselves. They can be used, but it is not a simple task to compare a set of ridges. For this reason many other features have been examined and studied to determine whether they are suitable to uniquely identify an individual.

The ridges are thin curved regions of the fingerprint that are raised above surrounding region. These ridges run in an almost parallel fashion with troughs separating them. Along the length of a ridge there are pores in an almost regular fashion. The ridges have a start point and an end point. These are known as ridge endings. Sometimes ridges that are next to each other combine and continue as a single ridge. These are known as ridge bifurcations. There are numerous other minute features about the ridge that could be listed, some of which are shown in Figure 3.1. However, most of these can be represented as combinations of the ridge ending and ridge bifurcation. For example a short ridge is just two ridge endings.

A third feature set that can be used to determine the match between two fingerprints is the pore structure [47]. The pores are smaller features and require a higher resolution scan to detect them accurately. They are also numerous and can be used to provide an accurate comparison.

These different features are not by any means unrelated to the others. The pores are on ridges and the ridge ending and ridge bifurcations are also on the ridges. These features can be used separately or combined together to provide a more accurate match.

Most electronic fingerprint comparison methods use a set of minutiae as this reduces the comparison from an image comparison down to a point comparison problem, and since the configuration of the minute details is unchanging we may use this configuration to perform the matching. This configuration is unique to a particular finger. This thesis has focused on minutiae matching techniques.

6.2 Minutiae Matching Technique

The most common method used in the digital comparison of fingerprints uses the minutiae as the main features in the comparison. In this dissertation I have concentrated on the minutiae matching techniques. These minutiae are extracted from the input image. The scanned image of a fingerprint is at a resolution of 500 pixels per inch and is in the form of a 256-colour grey scale image, where the intensity of the shade of grey is used to differentiate the details of the ridges and the troughs. This input image needs to be passed through a number of processing stages to extract the set of minutiae.

Figure 6.1: The core point of a fingerprint along with the alignment direction of the fingerprint.

The *core point* as illustrated in Figure 6.1 can be used as a reference point for the fingerprint. The core point can be thought of as the *centre* of the fingerprint. This core point along with the direction associated with it is used in the alignment of two fingerprints to facilitate the comparison. This direction is the direction of the ridge structure at the centre of the ridges that have been folded back on them. If there is no such structure then the ridge on which the core was located is examined. This ridge has two directions leaving the core point. The middle direction between these two ridge-directions is then taken as the direction at the core point. This direction is used to perform an approximate alignment of the fingerprints for the minutiae comparison.

The minutiae are calculated from the original fingerprint in the standard Cartesian coordinate system using the core point as the origin for the Cartesian plane. The coordinates of these minutiae are then converted into polar coordinates. Each minutiae can then be represented as a tuple (r, θ) with coordinates for the radius and the angle respectively to capture the positional information. All of the minutiae are converted into polar coordinates to simplify the minutiae-matching algorithm.

Each minutia has a position in polar coordinates. This position is shown relative to the core point for a single minutia in Figure 6.2. Along with this positional information about the minutiae there is also a wealth of information that can be gathered about the minutiae. This other information is critical to the comparison process as it greatly increases the accuracy of the matching algorithm.

This information varies from minutiae to minutiae and includes as the main features the direction of the minutiae. This is the direction of the ridge that the minutia was extracted from. Other features could include the type of minutiae or the number of ridges between it and its nearest neighbour.

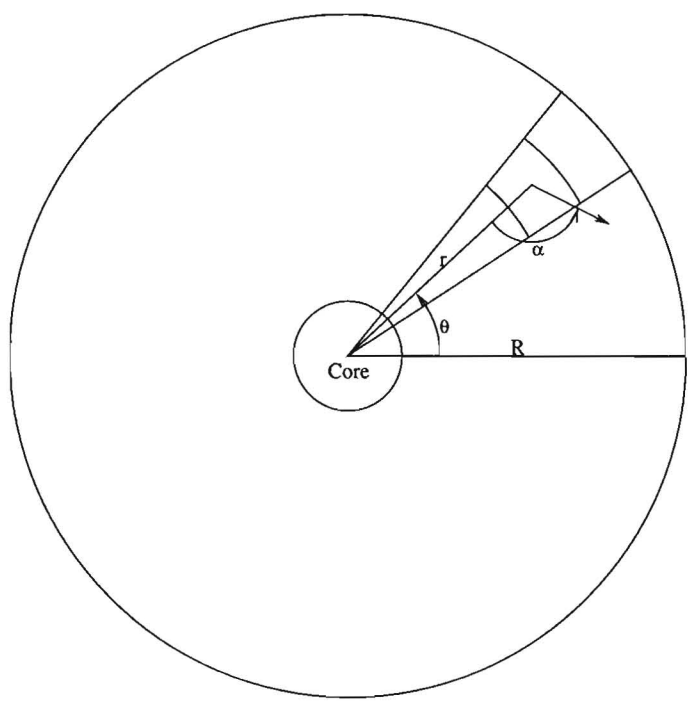


Figure 6.2: A minutia illustrated in relation to the core point.

Figure 6.2 illustrates a single minutia. This figure further shows a circle of radius R which is the radius of a larger circle that is used to define the maximum region of the coordinate space. $R = 256$ has been chosen to provide a suitable maximum area for minutiae detection bases on the expected

size of a fingerprint. A smaller inner circle is indicated on Figure 6.2 surrounding the core region. This circle indicates a small region that is not used for minutiae detection as small variations in the position of a minutia inside this circle can have a large impact on the polar coordinate. The region between these two circles is retained to extract minutiae. All the rest of the area of the fingerprint is discarded, which is usually only a small area.

Along with each point a direction α is stored as is illustrated in Figure 6.2. The direction was calculated from the orientation of the ridge on which the minutia was located. The direction along with other properties of the minutiae can be used in the comparison process. The only other feature that has been examined in this dissertation is whether the point on the fingerprint associated with a minutia represents a ridge ending or a ridge bifurcation. These features can be compared to determine whether a particular pair of minutiae from two fingerprints match each other.

The sets of minutiae extracted from the fingerprint image are each stored along with all their specific information. Comparing these sets of minutiae then compares fingerprints. For a comparison between fingerprints to be considered a success a particular number of these minutiae needs to match between two sets of minutiae. Thus for a minutia to match a particular point from another fingerprint image it needs to match on the radius (r), the angle (θ), the direction of the minutiae (α), and whether it is a ridge ending or ridge bifurcation.

Each scan of a fingerprint will acquire the fingerprint slightly differently. Therefore the comparison cannot be implemented as an exact comparison, as the relative positions and features of each minutia can vary. There may also be some pairs of minutiae that do not match even when the two scans originated from the same finger. There could be a few spurious minutiae, which have accidentally been included in the list of minutiae associated with the finger. These are the results of distortion and noise, which sometimes prevent minutiae from being accurately detected. In Table 6.1 the arrangement of minutiae from two scans of a finger are compared. The two columns are from two different scans of the same finger. The shaded regions illustrate the minutiae that have been detected in the image. These minutiae can be divided into two groups — those that were correctly detected and those that were spuriously detected. The alignment of the columns shows the minutiae that match between the scans.

To overcome this difficulty a pair of points is considered to match on position if they occur within some pre-specified distance in the polar coordinate system. Along with position matching the minutiae also need to match within a specific tolerance for the direction of the minutiae (α) and they must

Scan 1	Scan 2
Valid Minutiae	Valid Minuitae
Missed Minutiae	Valid Minuitae
Valid Minutiae	Missed Minutiae
Missed Minutiae	Missed Minutiae
Spurious Minutiae	Spurious Minuitae
	Spurious Minuitae
Spurious Minutiae	

Table 6.1: Arrangement of minutiae.

both have originated from a ridge bifurcation or from a ridge ending. The more stringent the tolerance the fewer false points will match. At the same time we suspect that a minutia which should have matched might be declared a non-match if the tolerance is too tight. If the tolerance is too relaxed then the chances of declaring a false match for a pair of minutiae also increases.

The algorithm used to perform the comparison can be split into two main sections. The first of these creates a template of the fingerprint from the input image. This template contains the set of minutiae along with the classification information. In the second stage this template is compared against templates created from other fingerprint images. If these templates match then the original fingerprints should have originated from the same finger.

6.3 Minutiae Extraction

An original scanned image is shown in Figure 6.3. As the different processing algorithms are applied to the data a number of global characteristics are produced as by-products of the algorithms. These are recorded along with the set of minutiae for use in the comparison stage.

The process of extracting the salient information from the fingerprint has different stages. Each of these different stages has been included in the complete process either to create the template or to improve the quality of the final template produced.

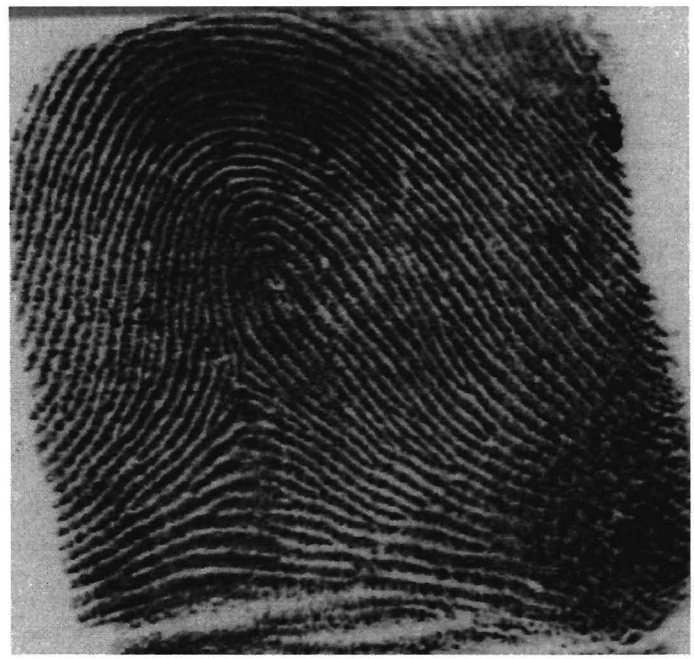


Figure 6.3: The scanned fingerprint image.

6.3.1 Enhancement

The scanned fingerprint needs to pass through a number of different stages to extract the final set of minutiae. The first step in this process is usually an enhancement stage. This stage is included as the first part of the process as it should improve the accuracy of each minutia that is finally extracted.

The purpose of an enhancement is to improve the quality of the image so that the following steps in the process will be able to execute more accurately. With this aim the enhancement step attempts to reduce minor inconsistencies on the ridge structure. These could be the artefacts of the pores, but since the pores are not used in this comparison an attempt is made to remove or lessen the effects of them.

The other reason for including the enhancement stage is that it is possible to use ridge information to enhance the ridges and valleys. One would like this to close small gaps in the ridge structure. For any enhancement to improve the final result it needs to remove more inaccuracies in the image than it introduces. Thus it is important that the enhancements are not over applied.

The first processing step applied to the fingerprint attempts to eliminate or reduce the affects of noise and distortion in the image. The simplest method reducing noise effects is to use a smoothing filter.

The smoothing filter removes small irregularities. A typical smoothing filter for this purpose is the Sobel smoothing filter as shown in Figure 6.4. A 5 x 5 Sobel filter could also be used to increase the blurring. However it is important not to use too large a filter as this could then cause adjacent ridges to merge into each other. Rather one would like to reduce the effects of the pores in the ridge structure and correct errors in scanned image. The smoothing filter will improve the accuracy of the set of extracted minutiae.

1	2	1
2	4	2
1	2	1

Figure 6.4: A 3 x 3 Sobel Filter.

The first and simplest method of removing minor inconsistencies in the image is to apply a smoothing filter over the image. This will have the effect of blurring the image slightly. This should remove many rough edges from the ridges that could have been detected as short ridges spikes along with reducing the affects of the sweat pores. One would expect the smoothing to have a noticeable effect on the accuracy of the final set of minutiae. However it does not improve the accuracy as much as one would like it to.

Using a simple smoothing filter does not utilize all the information that could be used. There is a wealth of directional information that can be gleaned from the fingerprint at a higher level, without looking at the minute details. Enhancing the print in the direction of the local orientation of the ridge structure would bridge short gaps in the ridge structure of the print. Very often these short gaps would have been the result of errors in the scan at that region. This enhancement also allows for a larger region of the fingerprint to be used in the minutiae detection process.

There are other methods of enhancing the image that improve the ridge structure. These methods use the known ridge structure and assume that the nearby ridge structure will possess a similar orientation and ridge spacing. Each area of the image can then be enhanced at the approximately correct orientation and ridge spacing for it. This should significantly improve the ridge detection routine.

Candela et al [11] present an enhancement algorithm which uses the ridge orientation and ridge spacing to improve the ridge structure. It should enlarge and improve the quality of the usable region of the fingerprint.

This algorithm divides the input image up into a sequence of squares, each 32 x 32 pixels in size.

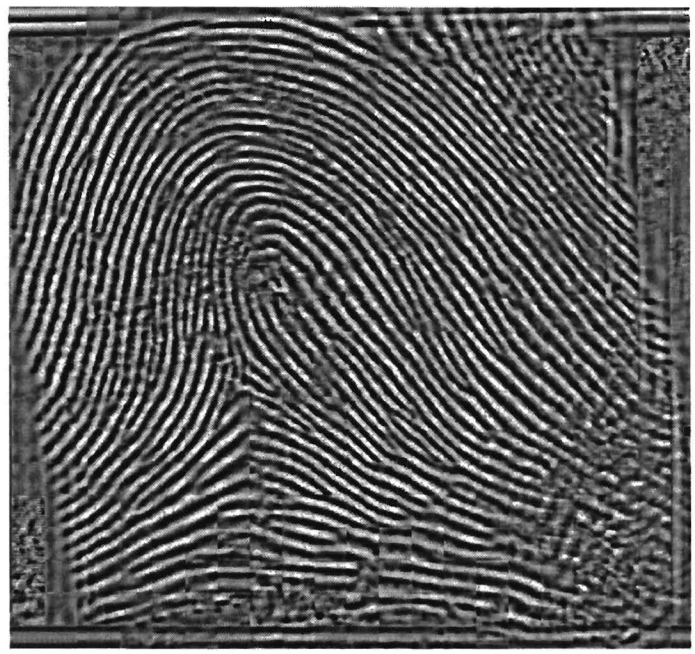


Figure 6.5: The enhanced fingerprint image.

These squares are overlapping such that the central 24 x 24 pixels cover the image in a non-overlapping fashion. This overlapping of the squares is necessary to reduce the edge effects that are introduced at the cell boundaries.

The enhancement routine is sequentially applied to each these squares. As it is applied to a cell the 32 x 32 square is used to determine the parameters, but only the central 24 x 24 pixels are extracted to produce the enhanced image. The results of the enhancement are illustrated in Figure 6.5.

The enhancement converts the spatial representation to a frequency representation using a fast Fourier transformation. The frequency representation is passed through a non-linear function which increases the useful information relative to the noise. The reverse fast Fourier transformation is then applied to convert the frequency information back into spatial information.

6.3.2 Orientation Field

The enhanced image is used to create an orientation field for fingerprint. At each point in the orientation field the orientation should be tangent to the direction of the ridges. This orientation information can be used to improve the accuracy of the ridges in the following stages.

6		7		0		1		2
5		6	7	0	1	2		3
		5				3		
4		4		C		4		4
		3				5		
3		2	1	0	7	6		5
2		1		0		7		6

Figure 6.6: The pattern of directions used to determine the orientation field.

The method used to determine the ridge orientations calculates an orientation at each pixel. These orientations at the pixel level are calculated as one of eight possible directions. These eight directions are depicted in Figure 6.6.

The direction at a pixel is calculated by examining each of the eight discrete directions. These are examined by placing the centre, C, of the grid in Figure 6.6 on the pixel and then summing the pixels along each direction, $s_i, i = 0..7$. If C is in a valley the smallest slit s_i would be in the direction of the ridge structure. Otherwise if C is on a ridge then the largest slit s_i would be on a ridge and represent the direction of the ridges. Comparing C to the surrounding pixels can be used to decide if it is on a ridge or in a valley.

$$C > \frac{1}{32}\sum_{i=0}^{7} s_i \tag{6.1}$$

This (6.1) can be used to decide whether to use the smallest or largest slit in deciding the direction. This is effectively using a localised threshold to differentiate between ridges and troughs. This does provide a better result than using a single threshold value for the whole image as it takes the gradual fluctuations of brightness in the fingerprint into account.

However this only uses the centre value and does not use the whole slit thus making it sensitive to short breaks in the ridge structure. The whole slit can be used to determine if it is on a ridge by checking if the average of the slit sums is greater than the average of the minimum and maximum slits.

$$\frac{1}{2}(s_{min} + s_{max}) > \frac{1}{8}\sum_{i=0}^{7} s_i \tag{6.2}$$

(6.2) uses the minimum and maximum values for the slits. One would expect one of these to be an outlier if the pixel falls either on a ridge or in the valley. On the ridge the minimum slit would be small causing the average of the slits to be larger than the average of the minimum and maximum slits. Similarly if the slit were in a valley then the maximum would be large causing the average to be less than the average of the minimum and maximum slits.

$$4C + s_{min} + s_{max} > \frac{3}{8}\sum_{i=0}^{7} s_i \tag{6.3}$$

(6.1) and (6.2) can be combined together to form a weighted average. This weighted average should calculate a more accurate orientation than either of the parts separately. (6.3) is simply a weighted average of (6.1) and (6.2), with the first one weighted twice the second.

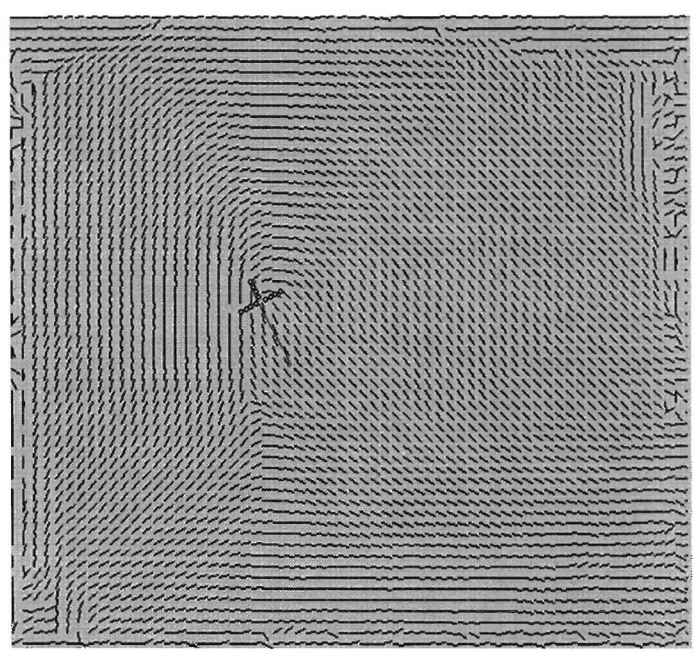


Figure 6.7: The orientation field with the core point marked.

This produces an orientation field at the pixel level. This orientation field however contains many small perturbations and inconsistencies. Thus rather than utilize the orientations at the pixel level these orientations can be averaged over small squares.

This averaging process should remove most of the minor inconsistencies in the orientations field, at least if it originated from a fingerprint. The averaging process converts the direction at each pixel into a vector format comprising an x and a y component.

The fingerprint region is split into squares. For each of these squares a direction is calculated. The direction uses the vector directions of each of the pixels in the square. The x component of the square is the sum of the x components of each pixel in the square. Similarly the y component is also calculated.

This summation of the components should result in short vectors where there are large inconsistency in the pixel vectors and long vectors where there is a high consistency in the pixel directions. The length of this vector can be used as an indication of the accuracy of the orientation at a given point. These orientations are then smoothed to improve the consistency between adjacent squares. The orientation field that results from this process is shown in Figure 6.7. These vectors can be converted to angles.

6.3.3 Core Point Location

The orientation field is used to calculate the location of the core point. The core point can be defined as the point of sharpest concave curvature in the ridge structure of the fingerprint. The orientation field can be used as an approximation of the ridge structure.

Every fingerprint should contain a single point that satisfies the criteria of a core point. This core point is needed in the minutiae comparison stage since it is the primary data for the alignment.

Figure 6.7 illustrates a core point overlaid on the orientation filed. The core point location detection routine uses a template of what it expects the core point to look like. This template is overlaid on the orientations and rotated until a best match is found.

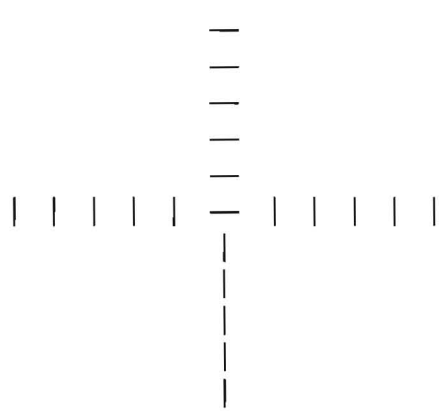


Figure 6.8: The template of size five that is used to determine the core point.

There are two templates that are used to locate the core point. The first of these is shown in Figure 6.8. This template is used when the lower half can be matched very accurately. Loops and whorls and tented arches are likely to match this template as they have a very sharp curvature at the core with the ridge orientation forming an almost straight line away from the core as it leaves the core area on the lower. This results from the ridge structure reaching the core and then almost folding back on itself. This template was matched in Figure 6.7. Here the "tail" of the template can be seen to align with the orientation at the core.

Sometimes, particularly in fingerprints of type arch, the fingerprint does not contain a feature that the "tail" of the template can match. In these instances an alternate template can be used. The second template is shown in Figure 6.9.

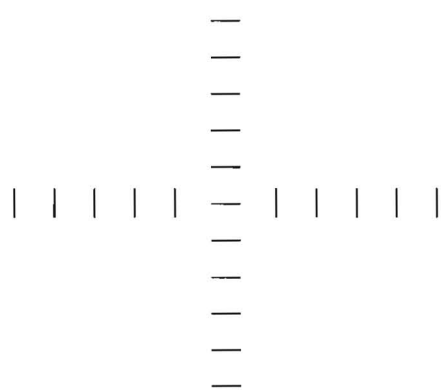


Figure 6.9: The secondary template of size five that is used to determine the core point.

This second template does not require the folding over of the ridge structure that is needed to form an orientation almost perpendicular to those just above them in the fingerprint.

The reason for choosing these templates is that if there is a loop or a whorl in the fingerprint then the lower tail of the first template will attach to the top of this macro feature of the print. If however the fingerprint is of type arch then there is not any section of the print with which the lower tail can align. Rather the section of greatest curvature in the ridge structure is located. This point will occur in the central point of an arch structure.

The comparison of the template and the orientation field returns a *curvature index* for the point at a given orientation. This curvature index is determined be summing the absolute differences between the orientation in the template cells and the orientation of the ridges. The curvature index is calculated at different positions in the fingerprint. The position of minimum of these is chosen as the core point. The curvature index is found to be fairly consistent for the core point of a finger.

This process is repeated at different resolutions starting at coarse resolutions and repeating the process on finer resolutions on a small area surrounding the position of the coarser resolution. It was found that averaging the orientation field into blocks in the sequence of sizes 16 x 16, 8 x 8 and 4 x 4 produced good results. It was also necessary to get a rough estimate of where the core point should be to avoid using minor fluctuations to locate a core point erroneously. The area surrounding the estimated core point was then resampled at a finer level of detail. This allowed the core point to be determined to within 4 pixels of its true position.

The core point found has been shown in Figure 6.7. This Figure also shows the orientation of the template relative to the orientation field that created the best match. The orientation of the template can be used in the alignment of fingerprints in the final stage of the comparison process.

6.3.4 Valid Region Detection

The consistency of the orientation of the ridges can be used to determine which sections of the image are from a fingerprint. Adjacent ridges are almost parallel. This correspondence between ridges can be used to locate the valid region. The orientations calculated outside of the fingerprint region would have random orientations varying widely within a small area.

The orientation field, O, where each element represents the orientation of the ridge structure in a small square of the fingerprint can be used. An array of the valid regions, R, needs to be created and initialised at the same size as the orientation field.

The magnitude of the direction vector, d, is evaluated for each block in position (x,y) of the orientation field. If this magnitude is less than some pre specified constant, d_{min}, then the cell is marked as invalid in R.

$$|d| < d_{min} \tag{6.4}$$

The absolute magnitude of the direction vector is compared against d_{min} in (6.4). This measures the consistency of the orientation inside the square that d was extracted from. If all the pixel orientations had aligned then d would be large, otherwise d would be small.

These orientation blocks are then compared to the surrounding blocks to determine the level of consistency in the ridge orientation. Summing up the differences in the orientation of the surrounding

cells compared to the cell in question does this. If this summation is greater than some maximum difference, *maxd*, then the square should be marked as invalid.

$$maxd < \sum_{i=x-size}^{x+size} \sum_{j=y-size}^{y+size} min(abs(O[x][y] - O[i][j]), 360^o - abs(O[x][y] - O[i][j])) \quad (6.5)$$

In (6.5) the smallest possible change between the angle of orientation in one square and the surrounding squares is summed up. Thus for example the difference between 358^o and 6^o is 8^o. The complete algorithm can be seen in Figure 6.10.

Initial step:
    initialise R to indicate all regions as valid
for each square **do**
    if $|d| < d_{min}$
        or $maxd < \sum_{i=x-size}^{x+size} \sum_{j=y-size}^{y+size} min(abs(O[x][y] - O[i][j]), 360^o - abs(O[x][y] - O[i][j]))$
    then
        Mark square as invalid
    end if
end for
end

Figure 6.10: Algorithm to determine valid region.

The algorithm presented in Figure 6.10 examines each square in the orientation field. Based on this information it then calculates the valid region of the fingerprint.

This algorithm does sometimes incorrectly mark regions of the fingerprint as invalid and it sometimes misses regions that it should mark. To handle this, small regions surrounded by invalid regions should be also marked as invalid. Valid regions can be treated in the same way. The algorithm indicates regions of sharp curvature as invalid regions. This is not a problem since these regions are small in area compared to the whole valid region. Figure 6.11 indicates the region of valid fingerprint. It has indicated a small section of the central region to be invalid. This is a side effect from sharp curvature of the ridges in that region. It was decided to not remove these regions as most of the small region of invalid area inside the fingerprint region result from smudges or otherwise poor quality images in the local region.

Figure 6.11: The valid region of the fingerprint.

6.3.5 Quality of Fingerprint

Input images vary in quality from very good to very poor. Images of high quality will work well with most systems and produce very accurate results, but the poorer the quality of a fingerprint, the less the chance that it could be used successfully for a match. This makes it important to be able to calculate a quality factor quantitatively. There are a number of different methods that can be used.

In this dissertation the quality of the fingerprint was calculated by examining the valid region of the fingerprint. For the fingerprint to be accepted as valid input for the rest of the process the valid region needs to be of sufficient size. A quality factor is calculated by calculating the ratio of the valid region to the complete fingerprint region.

The fingerprint region can be reduced by up to 25% of the image region on each side. This is to allow for the fact that often the fingerprint does not occupy the whole region of the scanned area. There is a limit in the amount that it can be reduced to prevent it from becoming too small. Inside this reduced area the ratio of valid region over the total area is calculated. This ratio needs to be sufficiently low to be satisfied that the print contains sufficient accurate information to use for matching purposes. If the quality factor that is calculated is too low to be of use then the fingerprint is rejected. A very low quality factor indicates with a high probability that what was scanned was

not a fingerprint, or that the finger was in motion during the scanning.

6.3.6 Ridge Detection

The enhanced fingerprint image is still in a 256-colour intensity image. From this image the ridges need to be detected to produce a 2-colour image of the ridges and valleys between them. There are different methods of extracting the ridge structure from the intensity image.

The first of these methods is to use a simple threshold to split the image into two colours. This can be improved with the second method by using an adaptive threshold to take local perturbations on pressure and intensity into account. The third method uses orientation information by making the assumption that ridges are more likely to occur in the direction of the ridge orientation than perpendicular to it.

In the first of these methods a simple threshold is calculated from the image. The minimum and the maximum values in the image can be found and the mean of these values is used. This gives an approximate of the median of the image. Ideally the median of the image would be used to cause half of the image to be labelled as ridge and the other half as valley.

This was found to produce a poor result since the simple threshold is sensitive to local perturbations in the intensity of the fingerprint image. These perturbations could have been caused by the variations in pressure of different regions of the finger on the scanner. This could cause whole sections of the fingerprint to be incorrectly calculated as ridge or trough, making it impossible to select a good threshold that works throughout the whole image.

One method of overcoming the local variations is to use an adaptive threshold to divide the image. To do this the image is divided into squares. These squares could be of size 32 x 32. In each of these squares the threshold value is calculated using the same method as used in the global threshold, but it would only be applied to a particular square. This method adjusts to the fluctuations of intensity in different areas of the fingerprint. However this method still struggles to correctly determine the ridge structure in areas of smudging and in poor quality scans.

The third method that was used to find ridges uses the orientation field as well as the enhanced fingerprint. The predominant direction of the ridges is assumed to be parallel to the direction of the orientation field. This process of deciding if a pixel is part of a ridge examines the pixels in short segments in the direction of the orientation field.

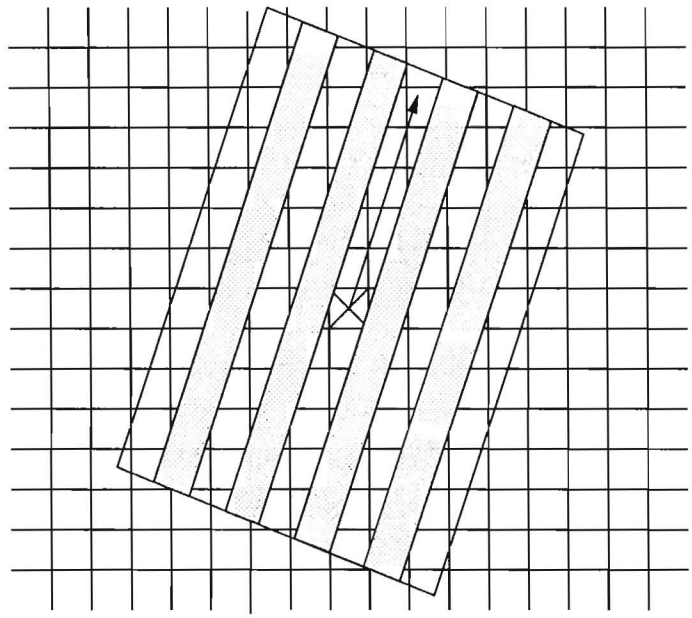


Figure 6.12: The pipes overlaid on the image.

Pixels need to be split into those that occur on the ridges and those that occur in the valleys between the ridges. The calculation to determine whether a pixel is on a ridge or not places a set of *pipes* over the image centred at the pixel as illustrated in Figure 6.12. These pipes are aligned in the direction of orientation. The average value for a pixel is then calculated for each of these pipes.

The average of these pipes is used as a threshold. This average is an adaptive threshold over the image coping with fluctuations in intensity. The average pixel value in the central pipe is compared against the threshold value to decide whether the pixel is on a ridge or in a valley. If the pipe containing a pixel is above the threshold then the pixel is marked as part of a trough, otherwise it is part of a ridge.

The length and the number of pipes used affects the accuracy of the ridges produced. A sufficiently wide area needs to be covered by these pipes, so that at least the width of one ridge and valley pair is covered. Spanning a ridge and a valley should ensure that the average is a fair estimate dividing the image into about equal amounts of ridge and valley.

The use of pipes in calculating the ridges greatly reduces the effects of the pores in the ridge structure, although it does not completely remove them. These pipes will also be less likely to record short breaks in a ridge incorrectly. This gives a fairly reasonable ridge structure and is sensitive to local perturbations in intensity. These threshold values can be recorded and passed through a

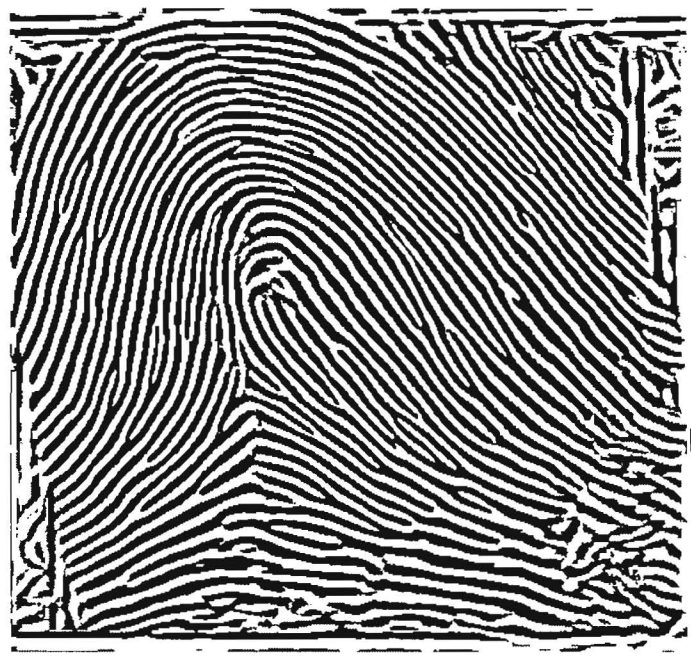


Figure 6.13: The ridges of the fingerprint.

smoothing filter instead of being used directly. This results in the ridge map shown in Figure 6.13. The invalid regions calculated in the previous section are shaded. The valid region has produced a clear ridge map.

6.3.7 Removal of Pores

There are sweat pores that naturally occur within the ridge structure. These pores can be used in the comparison process, but they require that the scan be performed at a much higher resolution than that used in this dissertation. They are not used in the comparison process presented here and therefore it is desirable to remove them to prevent them from being incorrectly detected as minutiae.

7	0	1
6	C	2
5	4	3

Figure 6.14: The eight connected pixels surrounding a pixel.

It is not necessary to remove the pores since many of them will have been removed by the enhancement stage and the method of ridge detection. Using an adaptive threshold to calculate the ridges

would have left many more pores in the image, but there will still be some pores remaining. These pores can still leave loops in the ridges. Removing these pores will improve the thinned ridges produced in the next stage.

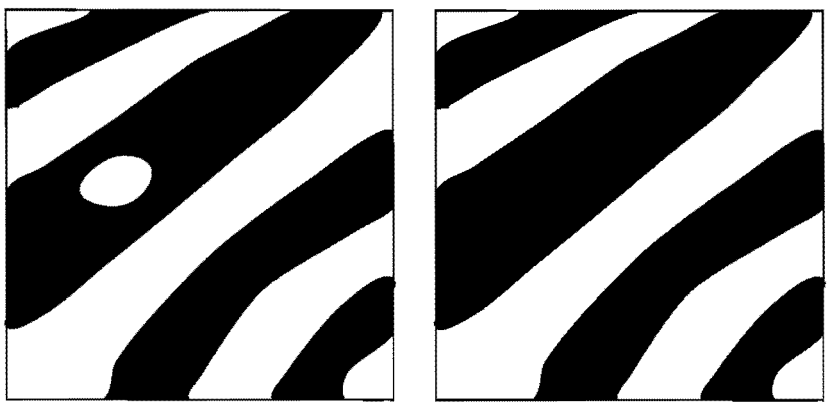
```
for each pixel in image do
    if pixel not on a ridge
    then
        if pixel adjacent to a ridge
            then
                set direction d such that
                    the pixel in direction + 7 mod 8 is a ridge
                    and the pixel in direction is a non-ridge pixel
                while area of marked pixels < a threshold
                        or pixel already marked
                    mark the pixel as visited
                    move in direction d
                    increment d mod 8
                        until pixel in direction d is not part of a ridge
                end while
                if looped back to a marked pixel
                    then found a hole
                    Fill in hole
                end if
        end if
    end if
end for
end
```

Figure 6.15: Algorithm to find holes in the ridges.

The holes are located using the ridge map. Each pixel in the ridge map is examined. If it is not part of a ridge it is then tested to determine whether it is part of a hole. If it is part of a hole then the hole is filled.

The sweat pores are first located by an examination of the ridges. This process examines every pixel in the image to determine whether it is on a ridge edge. If it is on the ridge edge then the edge is followed to decide if the edge is a pore.

In Figure 6.14 the eight pixels surrounding a pixel are shown. They are numbered starting from 0 in a clockwise direction. These eight directions are used to trace the edges between the ridges and



A pore The pore removed

Figure 6.16: Removal of pores.

non-ridge regions. A direction d is chosen such that the pixel in that direction is a ridge pixel. This direction is incremented modulo eight until the pixel in direction d is *not* a ridge pixel. The position is moved in this direction. This process is repeated while recording the minimum and maximum x and y coordinates.

The process ends when the edge loops back on itself to form a closed hole or the difference between the minimum and maximum x or y coordinate of the edge is large enough to indicate that it is not a hole, but rather an edge between a ridge and valley. If it ends by detecting a hole then the hole is filled and the process continues at the next point in the fingerprint.

The algorithm to detect and remove holes is shown in Figure 6.15. This algorithm is applied to the ridge map to detect and remove the pores. The application of this algorithm is shown in Figure 6.16. This example shows an enlarged section of the ridge structure that contains a pore. The edge of the pore is then traced and the pore removed. This process should clean the ridge structure and reduce substantially the number of remaining pores and hance reduce the number of spurious minutiae detected.

6.3.8 Thinning

The thickness of the ridges can vary considerably in a fingerprint. These differences result from differences in the pressure exerted during the scanning process and variations in the threshold used to distinguish between the ridges and the valleys. Thus the apparent width of the ridge varies. It is therefore desirable to eliminate the ridge width information. The other advantage of thinning

the ridge structure to a single pixel in width is that it greatly simplifies the process of detecting the minutiae.

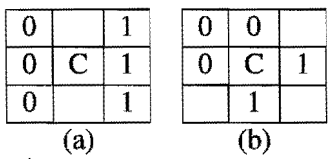


Figure 6.17: Possible configurations of pixels to form a ridge edge.

The first step in the thinning of the ridge map locates the edges of the ridges. The edges of the ridges are identified by a chain of ridge pixels with a chain of non-ridge pixels adjacent to it. Once this edge of the ridge has been located then the ridge needs to be examined to determine whether it is more than a single pixel wide. If it is, then the edges need to be marked as such and removed.

Figure 6.17 shows two 3 x 3 configurations that can be used to locate ridge edges and the pixels that need to be removed. These two templates can be rotated to produce eight different templates. If any of these eight configurations of cells are found in the ridge map then the pixel that is at the centre of the configuration can be marked for deletion. The process is repeated until all the ridges are a single pixel in width.

An equivalent result can be obtained through a different process that counts the length of the chains of ridge pixels and non-ridge pixels in the pixels adjacent to a ridge pixel. The algorithm shown in Figure 6.18 shrinks the ridges from both sides until a single 8-connected ridge structure remains. In an 8-connected line each pixel forming the line is attached to its neighbours by a minimum number of pixels surrounding it. The eight pixels surrounding it are illustrated in Figure 6.14. This process of shrinking the ridges was chosen as it minimises the impact of small local perturbations in ridge width and direction. If the local perturbations are not minimised then many spurious short ridge spikes can occur as the image quality degrades.

The algorithm uses as input the ridge map that has had the pores in it removed and produces as output an 8-connected thinned ridge map. The algorithm does a number of passes over the ridge map and on each pass it shrinks the width of the ridges by one pixel from each side. This process is repeated until no more modifications need to be made.

The first stage examines the ridge map and marks all the pixels on the edges of ridges. This process of detecting the pixels on the edges of the ridges examines every pixel. Then based on the eight pixels surrounding the pixel it is either marked as a ridge edge of left as it is.

```
for each pixel in ridge map
    if pixel on a ridge
    then
        r = length of chain of ridge pixels
        n = length of chain of non-ridge pixels
        if n ≥ 3
        then
            if r ≥ 3 and (r ≥ 4 or n ≥ 4)
            then
                mark pixel
            else if chain chains of non-ridge pixels rounds a corner
                        and opposite corner has the same configuration as Figure 6.17(b)
            then
                mark pixel
            end if
        end if
    end if
end for
end
```

Figure 6.18: First phase of algorithm to shrink the ridges from the edges.

In Figure 6.17 the possible configurations of pixels are illustrated that could form a ridge edge. In these configurations 1 represents a ridge pixel, while 0 represents a non-ridge pixel. The *C* indicates the pixel being examined. These configurations can occur in any of the four configurations formed by rotating them by either 90^o, 180^o or 270^o, thus producing eight possible edge conditions. From these configurations of pixels a method presents itself of detecting these configurations by counting the maximum number of ridge pixels forming a chain, along with the maximum length of the chain of non-ridge pixels around the central pixel, *C*.

```
for each pixel in ridge map
    if marked as on edge of ridge
    then
        set pixel as non-ridge pixel
    end if
end for
end
```

Figure 6.19: Second phase of algorithm to shrink the ridges from the edges.

The length of a non-ridge chain must be between three and five. If the length of the ridge chain is three or more then the central pixel is marked as on an edge. Otherwise, if the non-ridge chain rounds a corner as illustrated in Figure 6.17(b), then the two pixels next to the opposite corner pixel must be checked. Pixels that have been marked as on the edge of a ridge are not counted in the chains for other pixels. This algorithm is presented in Figure 6.18.

The algorithm has so far located all the pixels on the ridge edges. These pixels must be deleted and marked as non-ridge pixels. The rest of the process to delete these pixels from the ridge structure is presented in Figure 6.19.

The process of detecting the edges of the ridges and then shrinking the ridge needs to be repeated until no more pixels are marked in the section shown in Figure 6.18. This final output of this algorithm is shown in Figure 6.20.

6.3.9 Clean the Thinned Ridges

The thinned ridge structure sometimes contains short branches or spikes in it. These spikes would cause spurious minutiae to be located. These are artefacts of the thinning process and not genuine

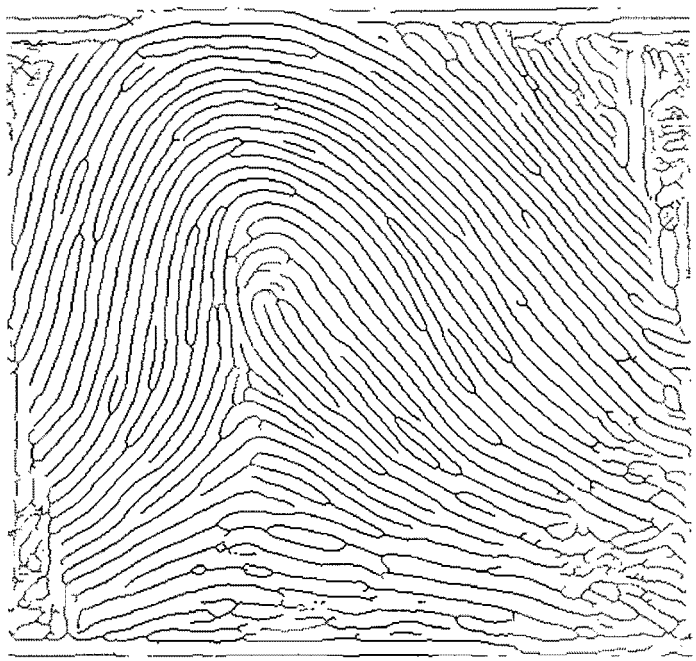
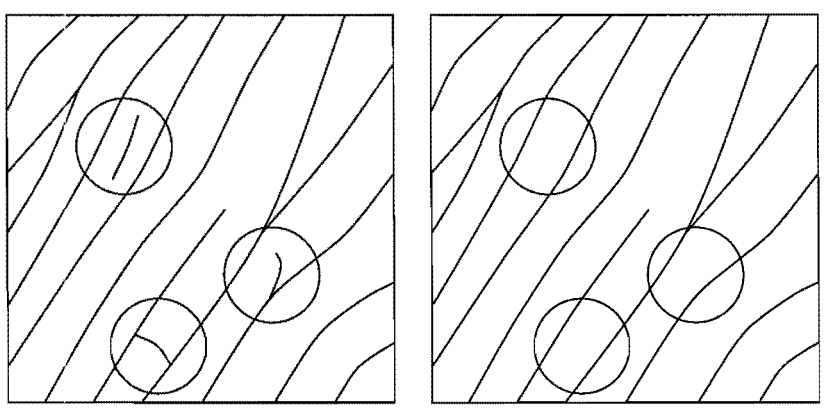


Figure 6.20: The thinned ridges of the fingerprint.

features of the fingerprint. The overall accuracy of the set of minutiae would be improved if these ridge spikes were removed.

The cleaning process uses the thinned ridge map as input. Short ridge segments are located and then removed. This produces a thinned and cleaned ridge map, which should improve the accuracy of the minutiae detection process.



(a) Example spikes and branches (b) Cleaned ridges

Figure 6.21: Removal of short spikes and branches.

In Figure 6.21(a) an enlargement of the thinned ridge structure is shown. In Figure 6.21(b) the cleaned ridge structure is shown. The algorithm to clean the ridge structure examines each pixel that is on a ridge. If it is part of a ridge then it is tested to determine whether it is ridge ending or a ridge bifurcation.

```
for each pixel in ridge map do
    if end of ridge or intersection of ridges
    then
        direction = 0
        length = 0
        repeat
            while pixel in direction not on a ridge
                direction = (direction + 1) mod 8
            end while
            move active position in direction
            direction = (direction + 5) mod 8
            length = length + 1
        until ridge end or ridge intersection encountered and length ≤ maxlength
    end if
end for
end
```

Figure 6.22: Algorithm to remove spikes and branches from the thinned ridge map.

Each of the ridges is then traced up to a predefined length. If the end of the ridge is encountered or another ridge is intersected before reaching the pre-specified limit then the ridge segment is identified as a ridge spike and removed.

The ridges are traced in a similar manner to the way the edges of the pores were traced in the pore removal. The eight directions illustrated in Figure 6.14 are again used as the basic directions. Figure 6.22 shows the algorithm used to trace the short ridge spikes and ridge braches.

When a short segment is found and identified as an artefact of the previous processing stages then it is removed using the same algorithm as is used to trace the ridge segment and each pixel is then marked as a non-ridge pixel.

6.3.10 Minutiae Detection

The minutiae detection process uses the cleaned and thinned ridge map to locate the minutiae. This should produce a set of minutiae that can be used in the comparison of fingerprints. This set should be unique enough to be used as the primary feature set for comparison.

The minutiae extraction then becomes a simple process of detecting the minutiae from a thinned ridge map. Each pixel in the ridge map is examined. If it is on a ridge then the number of neighbouring ridge pixels is counted. If there is only one neighbouring ridge pixel then that pixel is at a ridge end. If there are two pixels then it is in a ridge and if there are more than two pixels neighbouring it then it is a ridge bifurcation.

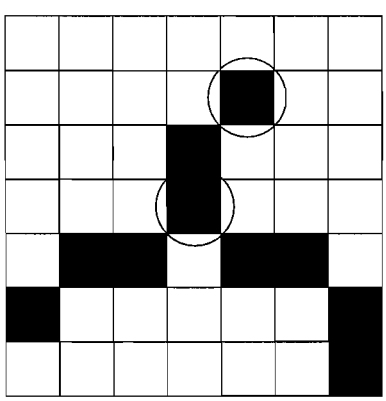


Figure 6.23: An enlargement of the thinned ridge pixels of a fingerprint.

In Figure 6.23 the pixels in the thinned ridge map are shown in enlargement. On the ridges the number of pixels surrounding a ridge pixel is two if it is on a ridge segment. At the ridge end, which has been circled only one pixel, is adjacent to it. At the ridge bifurcation, which has also been circled we can see that there are three adjacent pixels.

In Figure 6.24 each of the minutiae is shown. When the minutiae are detected the ridge on which they fall is followed for a short distance. The method of tracing the ridge is the same method used to trace a ridge in the cleaning of the ridge structure. For a ridge ending this ridge is traced for ten pixels to determine the direction of the minutia. For a ridge bifurcation all the paths are traced and the one that is most different from the other two is chosen as the direction.

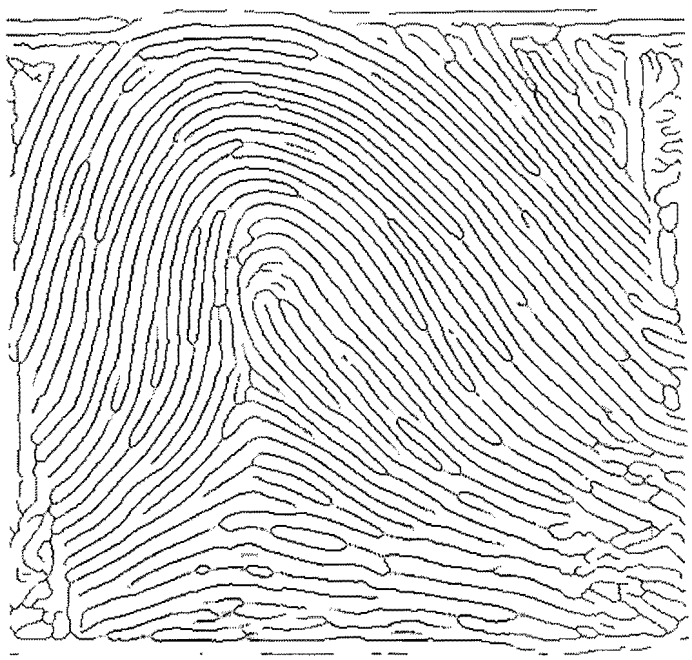


Figure 6.24: The minutiae detected overlaid on the thinned ridges of the fingerprint.

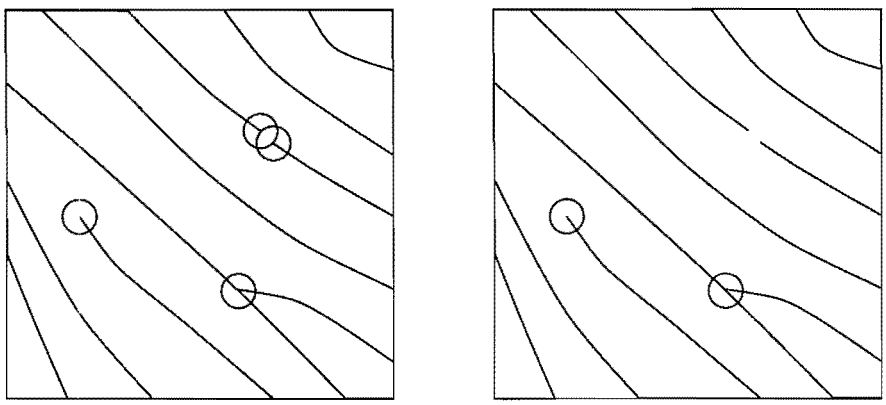
6.3.11 Removal of Spurious Minutiae

The set of minutiae that was produced in the previous step can now be used in the comparison process. Unfortunately there are sometimes extra minutiae that have been acquired in the process that are spurious. If possible it would be desirable to remove these spurious minutiae. The difficulty is in determining which minutiae are accurate.

The algorithm presented here uses the small area surrounding a minutia to decide if the minutia is valid or not. All other minutiae on this area are located. If there are no other minutiae in this area then the minutia is assumed to be valid.

If the minutiae in the surrounding area appear to have a random direction associated with each one there is a great probability that they are spurious. If they align in direction then they can be married into a single minutia. The minutiae that were produced in the previous stages are examined to determine if any of them are false. If they are found to be false then they are removed. In Figure 6.25(a) an example of false minutiae caused by a short ridge break is shown. In Figure 6.25(b) the spurious minutiae have been removed.

The algorithm to remove false minutiae stores all the minutiae in a two dimensional array at their



(a) Some minutiae caused by a short break (b) The spurious minutiae removed

Figure 6.25: Removal of spurious minuitae.

location. This array is scanned for minutiae. For each minutia in the array a small section of the array surrounding the minutiae is examined. If any minutiae are located in this section then all of these minutiae along with minutiae in the centre are either removed or welded together into a single point.

This does have the possibility of falsely removing correct minutiae, but most of the time it will remove the minutiae generated by the presence of short ridge spikes, short ridges, and short ridge breaks. Most of the features that it does remove are artefact of noise in the scanned image or the algorithms used in the previous steps. Thus it will predominantly remove spurious minutiae.

6.4 Minutiae Comparison

The minutiae extraction stage produces a set of features that can be used to uniquely identify a finger from the fingerprint. This set of features needs to be compared reliably against other feature sets to determine whether or not they originated from the same finger.

Two sets of minutiae need to be compared to decide if they originated from the same finger. This process needs to be orientation independent and needs to tolerate distortions of the fingers. One can also expect the sets of minutiae to contain some spurious points and to have missed some correct points. The comparison of these sets of minutiae is shown in Table 6.1.

In designing the point comparison algorithm in this thesis, the two main objectives were to optimise the comparison in terms of *speed* and in terms of *memory*. There were very specific criteria to which

the matching routines needed to adhere. The memory requirements had to be restricted to 256 KB of RAM. This is because the smart cards used for this research only contain 256 KB of RAM. The template of the fingerprint also needed to be limited in size. There is a storage space on the smart card of 8 KB in the form of EEPROM memory. This does place some limits on the size of the template, but it did not appear that this would be a problem with respect to a point representation. Another constraint was the speed of the microchip on the smart card, which runs at speeds of 3.5 to 5 MHz. This is in the order of magnitude of 100 times slower than a modern PC.

The minutiae comparison routine makes use of the core point as a reference point in each print. It is adjusted to the origin and all the points are then converted into polar coordinates. This helps to simplify the matching process.

The matching process examines each coordinate from each set of points to determine whether there is a match on that point. First the distances from the core points are compared. These need to match within a tolerance. If they match on distance then all the other properties except for the angular coordinate of the pair of minutiae are compared. If all of these properties match, then the angular coordinate is used.

The calculation of the matching angle between the pair is recorded. This difference in angle is the angle required to rotate one set of minutiae to allow the pair of minutiae in question to match. This angle is used as the index into an array of all possible angles. This angle position in the array is then incremented. An examination of this array for a peak value indicates the rotation angle of best match along with the number of minutiae that match at that angle.

This is an $O(n^2)$ algorithm as every point needs to be compared with every other point to see if they match. It can be improved to an $O(n)$ algorithm by ordering the minutiae. The minutiae can be sorted on the radius from the core point. This sort can be performed in $O(n)$ time by implementing a "bucket sort" as the possible values of the radius are discrete and of a limited range.

The comparison of the sorted lists of minutiae can be performed in $O(n)$ time. This is done by maintaining indices into the two arrays of the minimum possible position, which could cause a match on radius of the point. This effectively limits the minutiae that need to be compared to those that could match on the radius.

6.5 Summary

The fingerprint is comprised of a pattern of ridges and troughs that curve to form a pattern. These unique patterns remain constant throughout an individual's lifetime providing a biometric that can be used to identify or verify an individual's identity.

There are a number of different possible features on the fingerprint that can be used in the comparison process. The first of these features is the ridge structure itself. This can be used to provide a highly accurate comparison, but it is difficult to implement ridge comparisons on a computer. The second method is to use minutiae. These minutiae are the fine details of the ridge structure. They occur at the points of ridge endings and ridge bifurcations. The comparison of the minutiae is the most common method of digitally comparing fingerprints. A third method is to use the pore structure of the print. These pores occur on the ridges in an approximately regular fashion.

This dissertation focuses on the techniques that utilize minutiae as the basis for the comparison process. The comparison of the minutiae is the most common method of digitally comparing fingerprints and is based upon the methods used in manual fingerprint comparison techniques. The algorithms used in the comparison process can be divided into two sections. The first extracts a set of minutiae from the fingerprint while the second compares this set of minutiae with another set of minutiae.

The process of extracting a set of the minutiae uses a scanned image as input. From this input image an enhanced image is generated. The enhancement stage is intended to improve the accuracy of the minutiae. Orientation vectors are extracted from the enhanced image, which are used to locate the core point and determine the fingerprint region and the quality of the image. A two-colour image is extracted from the enhanced image using the orientations in the orientation field as the expected ridge direction in their respective region of the image. These ridges are cleaned to remove the effects of the sweat pores, since they are not used in the comparison process. The cleaned ridge structure is thinned to a single pixel in width to aid the minutiae detection process. This thin ridge structure is despurred to remove short ridge ending and short ridge spikes that usually are side effects of the algorithms used.

From the thinned ridge structure a set of minutiae is extracted. These minutiae are located at the ridge endings and the ridge bifurcations. A number of characteristics are calculated for each minutia. These are needed to allow accurate comparisons to be performed. The set of minutiae that are calculated are examined to remove any that could be considered spurious.

The minutiae detection process attempts to acquire an accurate set of minutiae. It is however impossible to consistently extract the same set of minutiae. This is a direct result of the differences in the area and orientation of the print along with the other factors that reduce the quality of the scanned image. The combined effect of these factors is that the two sets of minutiae that are compared will have some different minutiae and the accuracy of the characteristics of the minutiae might vary.

The comparison stage uses the set of minutiae in polar coordinates with the core point as the origin. These sets of points can be efficiently compared on a smart card. The complete set of minutiae extracted from a finger is stored in a format that uses 516 bytes. This makes it suitable for storage and comparison on the smart card.

Chapter 7

Testing and Analysis

In the research towards this dissertation a system was developed to implement and test the ideas presented. This chapter describes how the ideas were tested and analysed. All the results presented in this chapter are from the system developed by the author.

The first performance characteristic that was tested is the *accuracy* of the system. The accuracy of the fingerprint matches was one of the primary aims in the development and implementation of these ideas.

Along with the accuracy the *timing* of the authentication process needs to be analysed to determine whether it is suitable to provide real time authentication. The timing was an important requirement in the development of the ideas, since the intended use of the ideas was to provide real time verification of an individual's identity through the use of a smart card and their fingerprint.

7.1 Accuracy

The accuracy of a system is a primary concern when determining its suitability for the desired purpose [43]. We therefore need to calculate the accuracy. The system should also be examined for weak points. If the system allows users to authenticate themselves over a network, then it is highly unlikely that they would attack the system by attempting to make their fingerprint appear as someone else's fingerprint. Rather they would acquire a digital copy of the fingerprint and attempt to inject it surreptitiously into the system via the network [18].

A complete personal authentication system should be able to verify two things in order to be successful. Firstly it needs to verify the *freshness of the scan* from which the fingerprint originated (i.e. that the biometric was actually scanned from the person at the time of verification) Secondly, it needs to determine whether the fresh biometric *matches a master template* that is stored on file [18]. Biometrics are not secrets. Fingerprints are left on everything that you touch, while face or iris patterns can be observed every time that you can be seen. Thus you also need to be able to verify the freshness and the owner's identity of the scan.

The analysis of the *accuracy* of the fingerprint matching routines is examined first *statistically* and then *empirically*. The statistical analysis seeks to predict the degree of coincidence between two random sets of points. This coincidence can then be used to predict the probability of fingerprints from different fingers incorrectly being declared a match. We require the probability of a chance false match to be very small before the converse proposition is assumed and the fingerprints are declared a match.

The statistical analysis can predict the number of minutiae that are expected to coincide between different fingerprints. This can be used as a guide to determine a threshold level of minutiae that are required to match before the fingerprints are declared as a match. If the fingerprints originated from the same finger then one would expect there to be a high level of coincidence between the minutiae extracted from them.

The empirical analysis uses pairs of matching fingerprints and executes batch comparisons to determine the FAR and FRR. The empirical determined FAR is then compared to the predicted FAR.

7.2 Statistical Analysis of FAR

One would like for any pair of fingerprints from the same finger to have a large number of minutiae matching, while at the same time one would prefer pairs of fingerprints from different fingers to have very few points matching. The statistical model developed here attempts to predict the frequency of falsely declaring a match between non-matching prints.

In comparing fingerprints only the minutiae need to be compared. The minutiae will be assumed to have about equal probability of occurring in any position on the fingerprint. To simplify the process the circle of radius R will be treated as if it is split into a number of cells each with an equal probability of having a minutia in it. Although the probability of a minutia appearing in an

outside segment might be larger due to the fact that the area of an edge segment is larger, there is often a counter-weighting phenomenon of more minutiae per unit area in the inner bands. Thus the presumed equivalence of probabilities for each cell might be a reasonable approximation, which could be the subject of later optimisations. It will also be assumed that each cell will have *at most one minutia* in it. The implementation does not guarantee that there will not be two minutiae in the same cell, however the chances are negligible as there is some post processing on the minutiae to prevent them from occurring too near to each other. If two points are within a certain distance of each other then they are married together to form a single minutia and are treated as such.

In order to determine whether two fingerprints originated from the same finger we need to compare the two sets of minutiae. If sufficient minutiae from the two sets match then they can be assumed to have originated from the same finger. The question to ask is how many points need to match for us to be 99% confident that the prints are from the same finger. To answer this question we will examine the case where the minutiae are compared at a particular orientation.

By making the assumptions that all N cells are equally likely to be filled by one minutia the number of the minutiae that are expected to match can be modelled by the hypergeometric distribution [51]. N is dependant on the maximum radius of the circle R.

$$P(\textit{common minutiae}|N,m,n) = \frac{\binom{n}{r}\binom{N-n}{m-r}}{\binom{N}{m}} \tag{7.1}$$

where, N = total number of cells in the fingerprint other than the core.
n = the number of minutiae in the reference fingerprint. $n \leq N$
m = the number of minutiae in the fingerprint being compared. $m \leq N$
r = the number of points that match. $r \leq \min\{m,n\}$

This fixes the probability for the coincidence of r cells chosen for possible matching from the n occupied cells *matching due to chance alone*. This formula does not take the orientation α or the *character* (bifurcation or ridge ending) of the minutiae into account. Intuitively we would expect that low values of r would be associated more frequently with non-matching prints and high values of r to be associated more frequently with matching prints. To determine the FAR the probability

of at least x cells coincidently matching is needed. This probability can be calculated by summing (7.1) up from x through n.

$$P(\textit{at least } x \textit{ common minutiae}|N,m,n) = \sum_{r=x}^{n} \frac{\binom{n}{r}\binom{N-n}{m-r}}{\binom{N}{m}} \tag{7.2}$$

If orientation α is independent of basal direction θ and of radius r then adding the direction of the minutia into the comparison can be thought of as reducing the chances of a match for a particular cell by the ratio of the range of acceptance divided by the full revolution. Even if α is not completely independent it would still be expected to have some selective power to remove false matches. The addition of α in the comparison process has the effect of increasing N. i.e. $N = N(R,\alpha)$

The other characteristic that is recorded with each minutia is the type — or more specifically whether it is a ridge ending or a ridge bifurcation. In the simplified case one can assume that the probability of each ridge feature is equal. This assumption would effectively double the size of N. i.e. $N = N(R,\alpha,t)$

This argument illustrates the probability of x or more pairs of minutiae matching coincidently from different fingerprints at a preset orientation. However since the approach thus far assumes a particular orientation for each fingerprint to be chosen without any bias of how many minutiae. This approach needs to be generalized to allow one image to rotate at any angle. The best matching angle would be the angle used for the match. The secondary print needs to be allowed to rotate to any angle with respect to original print. As it does this rotation the maximum match is taken as the match between the two prints. Allowing rotation will increase the number of coincidental matches.

7.2.1 Example

N represents the total number of cells into which the print can be divided. This number can be approximated by the number of angular subdivisions multiplied by the number of divisions of the radius. These subdivisions need to be large enough to ensure that the majority of points that should match do, while at the same time ensuring that minutiae from different fingers do not match. If the angular coordinate is split into 16 segments each of 22.5^o and the radius is also divided into 16

bands each of 16 pixels, then the total area would be divided up into 256 distinct regions giving $N = 256$. For simplicity we will assume all regions to be equally likely.

If $n = 100$, $m = 100$ and $N = 256$ then from Equation 7.2 $x = 49$ yields $P(x) = 0.01$ with a 1% chance of a match declared on the basis of $x \geq 49$, if chance only is operating (i.e. the fingerprints are from a distinct pair of fingers). Similarly $x = 59$ yields $P(x) = 0.000001$, with a chance of order 10^{-6} that randomly chosen fingerprints will yield the signal $x \geq 58$ which we choose (reasonably, but in fact falsely, in this scenario) to indicate a match.

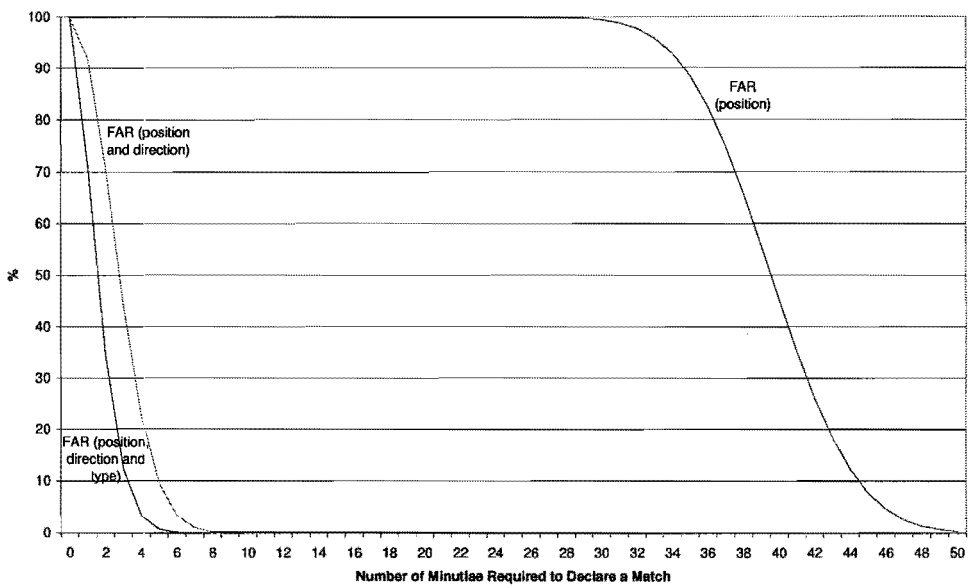


Figure 7.1: The FAR that is predicted by the hypergeometric distribution.

The example has been presented to illustrate that *using just the positions of minutiae is insufficient to match fingerprints accurately*. The number of random points that coincide on just position would require far too many points to match. The graph in Figure 7.1 shows the high FAR when just position is used to compare minutiae. Fortunately there are characteristics about minutiae that can be recorded such as the type of minutiae and the angle, α that the ridge from which the minutia was acquired, was directed.

Thus if α is independent of the location of the minutia and the range of acceptance is 22.5^o then dividing a single revolution by α can be conceptualised as further subdividing each cell into another 16 parts. This division would reduce the chance of a coincidental match involving α between a pair of minutiae to $\frac{1}{16}$ the chance without α. In the previous example, N would increase from 256 cells up to 4096 cells, assumed equally likely.

Now $x = 8$ in (7.2) with $N = 4096$ yields $P(x) = 0.01$ so that $x \geq 8$ can be used to signal a match. Were there no match of the prints by pure chance, then $x \geq 8$ will occur less than 1% of the time. Similarly if we are more strictly taking $x \geq 13$ as the signal for a match, since $P(x \geq 13) = 0.000001$, then the chance of a false match is less than 10^{-6}. This additional requirement has achieved a significant reduction in the number of minutiae required to match in order to achieve the desired accuracy. The improvement and corresponding reduction in the FAR is shown in Figure 7.1.

The other characteristic of each minutia that was recorded was whether it was a ridge ending or bifurcation. This information can be used to strengthen the matching procedure. The effect would be to further subdivide each cell into two cells resulting in a total of $N = 8192$ possible cells (assumed equally likely) in a fingerprint. This increase in the number if divisions of the area would reduce the minutiae required to declare a match to 5 and 9 with FAR of 10^{-2} and 10^{-6} respectively. Using all three of these characteristics one would expect almost 30% of random fingerprints to have 0 matching minutiae and most prints to match few point coincidently.

Using the type has the effect of reducing the FAR. This is illustrated in Figure 7.1 where the effect on the predicted FAR of using different amounts of information in the comparison of minutiae is shown.

7.3 Empirical Analysis of FAR and FRR

The empirical accuracy of the system was measured by running batch comparisons on sets of fingerprints from a database and recording the rate of matching. The batch comparison could either compare all the fingerprints that were supposed to match, or those that were not supposed to match. The fingerprints from the NIST Special Fingerprint Database 4 were used as test fingerprints.

In the implementation of the ideas presented in this dissertation a facility to run batches of comparisons was included. This batch feature was used the accuracy and timing of sections and the complete authentications process.

7.3.1 Description of the Procedure to Test FAR and FRR

All the tests recorded the accuracy of the matching process when just the position (r, θ), or the position and direction of each minutiae (r, θ, α) or the position, direction and type of each minutiae (r, θ, α, t) was used for comparison.

The FRR is the percentage of *valid users* that are *rejected* by the system. The FRR is compared to the number of minutiae required for the fingerprints to be declared a match. In this testing different fingerprints originating from the same finger are compared.

In contrast the FAR is the percentage of *successful attempts by invalid users*. Tests to determine the FAR empirically used fingerprints originating from different fingers and recorded the results.

The tests in the remained of this chapter examine the FRR and FAR relative to the number of points that are required to match for the pair of prints to be declared a match. This experiment is repeated using various sets of characteristics of a minutiae pair to consider them a match.

These experiments execute a batch of fingerprint comparisons and output a list of how many fingerprints pairs have a given number of minutiae matching. This list would have the layout of Table 7.1.

Exact number of minutiae matching	Number of distinct comparisons
0	m_0
1	m_1
2	m_2
⋮	⋮
127	m_{127}

Table 7.1: The results generated from a batch fingerprint comparison recording how many pairs matched.

The sum of all fingerprints that match is the total number of comparisons that are performed in a particular test batch.

$$Number\ of\ comparisons = \sum_{i=0}^{127} m_i \tag{7.3}$$

The results illustrated in Table 7.1 can be used to calculate the ratio of comparisons that are falsely declared a match. This calculation involves the total number of all the comparisons that had at least n minutiae matching, divided by the number of comparisons in the batch.

$$acceptance\ ratio = \frac{\sum_{i=n}^{127} m_i}{Number\ of\ comparisons} \tag{7.4}$$

The same results can be used to calculate the rejection rate. The comparisons that are rejected as

not having sufficient minutiae matching are those that have less than n minutiae matching. This rejection ratio can be calculated as $1 - acceptance\ ratio$ or

$$rejected\ ratio = \frac{\sum_{i=0}^{n-1} m_i}{Number\ of\ comparisons} \tag{7.5}$$

The FAR can be determined by calculating the acceptance ratio on a batch of fingerprint comparisons that should be rejected by using (7.4). The FRR is determined when (7.5) is applied to the results of a batch where pairs of matching fingerprints are compared.

The empirical testing of the FAR an FRR of this system starts with the simplest system and then proceeds to show how the addition of sections of the algorithm and the modification of the tolerance parameters affect the accuracy of the matching process.

The results from these tests are presented in the remainder of this chapter. They were intended to test the effect of varying the algorithm and parameters used by it. The following tests were performed and the FAR and FRR recorded:

- Compare the use of different amounts of information in the matching of minutiae.
- Compare the effect of allowing the orientation between the fingerprints to vary.
- Examine the effect of varying the tolerances in matching minutiae.
- Compare the inclusion of enhancement stage in the minutiae extraction algorithm.
- Examine the effect of using classification information in the comparison process.
- Examine the effect of the quality of the fingerprint scans.
- Examine the effect of classification when quality fingerprint scans are used.

In these tests a minutia is treated as a 4-tuple specifying its position and characteristics.

$$(r, \theta, \alpha, type) \tag{7.6}$$

where, $r =$ the radius of the minutiae from the core point.
$\theta =$ the angular component of the polar coordinate specifying the position.
$\alpha =$ the angle specifying the direction of the ridge from which the minutiae was extracted.
$type =$ the type of the minutiae. (bifurcation/ending)

The 4-tuple shown in (7.6) shows the characteristics that define a minutia. The radius, r, has a range of (0..128). Both θ and α specify angles. For these angles the units are $\frac{360}{256}^\circ$. This effectively divides the full revolution into 256 units. The type of minutiae is either a ridge ending or a ridge bifurcation.

7.3.2 No Rotation

The simplest method presented here uses an orientation calculated from one fingerprint to align it with another fingerprint. The first comparison examines the effect of using different characteristics of minutiae in the comparison process.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels;
Tolerance of $\theta = 11 \times \frac{360}{256}^\circ$
Tolerance of $\alpha = 13 \times \frac{360}{256}^\circ$

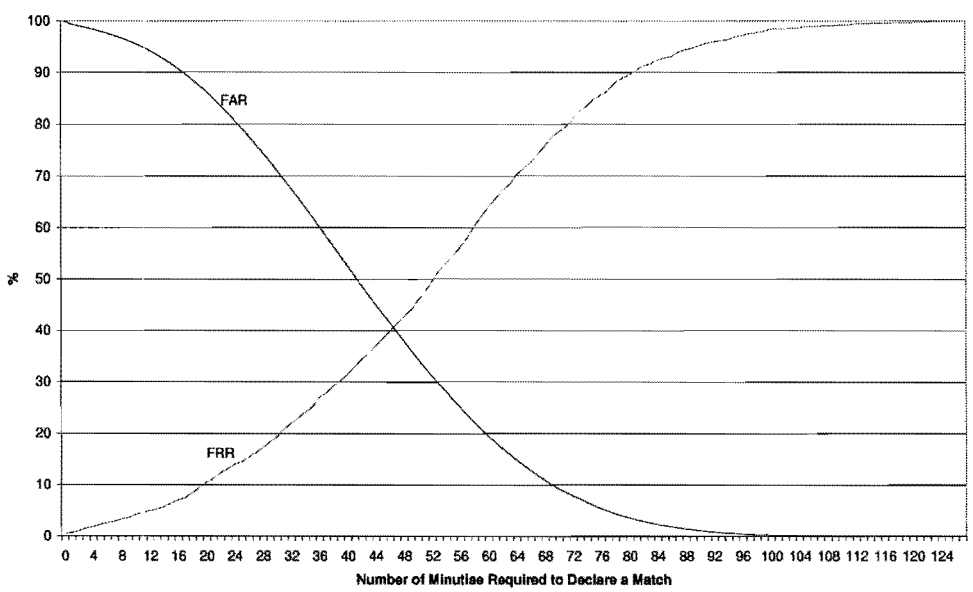


Figure 7.2: The FRR and FAR when only position is used to match minutiae.

Comparing the sets of minutiae extracted from the fingerprints produces the following results.

The first test produces an equal error rate (EER) of about 40%. This EER is the point where the FAR is equal to the FRR. The results of the first batch of comparisons uses only the position, or the

first two coordinates in the 4-tuple representing a minutia to determine if a pair of minutiae matches. The FAR and FRR have been graphed in Figure 7.2.

It is undesirable for this many points to match between fingerprints from different fingers. It is therefore necessary to use more than just the position of the minutiae in the comparison. The direction α of each minutia can be included in the criteria for deciding whether a minutiae pair matches.

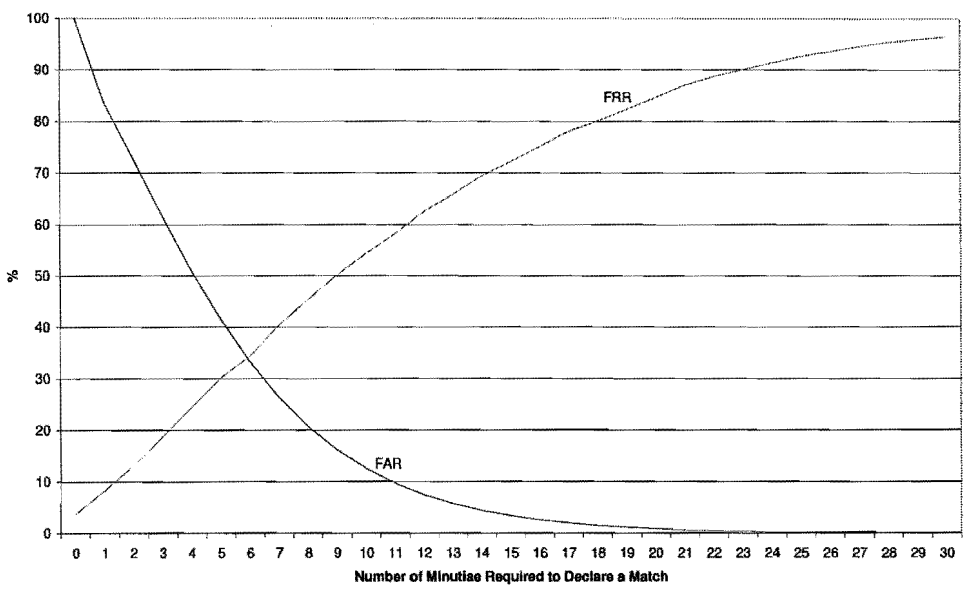


Figure 7.3: The FRR and FAR when position and alpha are used to match minutiae.

In Figure 7.3 the FRR and FAR are graphed when both the position and the direction α are used to compare minutiae. The new information has the effect of reducing the number of minutiae matching between both matching and non-matching pairs of fingerprints. It does cause a larger reduction in the number of minutiae that are declared to match yet originate from different fingerprints. Its inclusion in the matching process does reduce the associated error rates and is therefore desirable.

In addition to the direction, α, the type of each minutia can be included in the criteria for deciding whether or not a pair of minutiae matches. One would expect this to reduce the FAR further while not increasing the FRR substantially.

Figure 7.4 shows a graph of the FRR and FAR for fingerprint comparisons performed using type, direction and position to decide if a pair of minutiae matches. Unfortunately the inclusion of the type here has also increased the FRR while reducing the FAR resulting in little change in the EER. The use of the EER in comparing methods assumes that the FAR and FRR are weighted equally. In

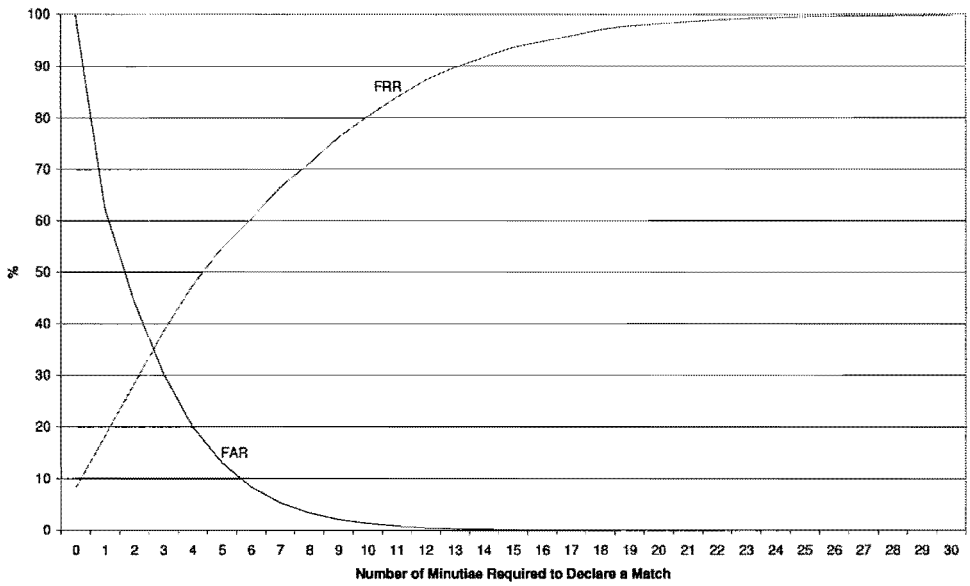


Figure 7.4: The FRR and FAR when position, alpha and type are used to match minutiae.

practice the FAR would most likely have a greater weighting.

This test has empirically shown that using the *position alone is insufficient* to differentiate between the sets of minutiae extracted from different fingerprints. Further more this test has shown that the inclusion of more characteristics about a minutia reduces the FAR and therefore the number of minutiae required to declare a match. This finding is in agreement with the results produced by the statistical model and as expected there is a corresponding increase in the FRR when the same number of minutiae is used to declare a match.

7.3.3 Limited Rotation

Each fingerprint has a core point that is located near the centre of the fingerprint. The ridge information at this point can be used to determine the orientation of the fingerprint. This orientation might not be completely accurate, therefore it is desirable to allow some rotation between the pair of fingerprints being compared. It is not necessary to allow complete rotation. Rather the rotation can be limited to a certain range.

This test attempts to determine how much rotation should be allowed for an optimal matching process. The complete set of 2000 pairs of fingerprints is used in this test. The FAR is calculated by attempting to match non-matching pairs of fingerprints and the FRR is calculated by attempting

to match matching pairs. In the calculation of the FAR 7 996 000 comparisons are performed and for the FRR 2000 comparisons are made. This batch of comparisons is repeated with different tolerances in the maximum amount of rotation allowed between the pair of prints. The number of minutiae n, in a fingerprint is ignored in these tests. The only factor used in deciding if the prints match is whether a minimum number of minutiae match and not the number of minutiae in each print.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels;
Tolerance of $\theta = 11 \times \frac{360}{256}^\circ$
Tolerance of $\alpha = 13 \times \frac{360}{256}^\circ$
Tolerance in the rotation ranging in $[0..100] \times \frac{360}{256}^\circ$
A match is declared if 10 minutiae match.

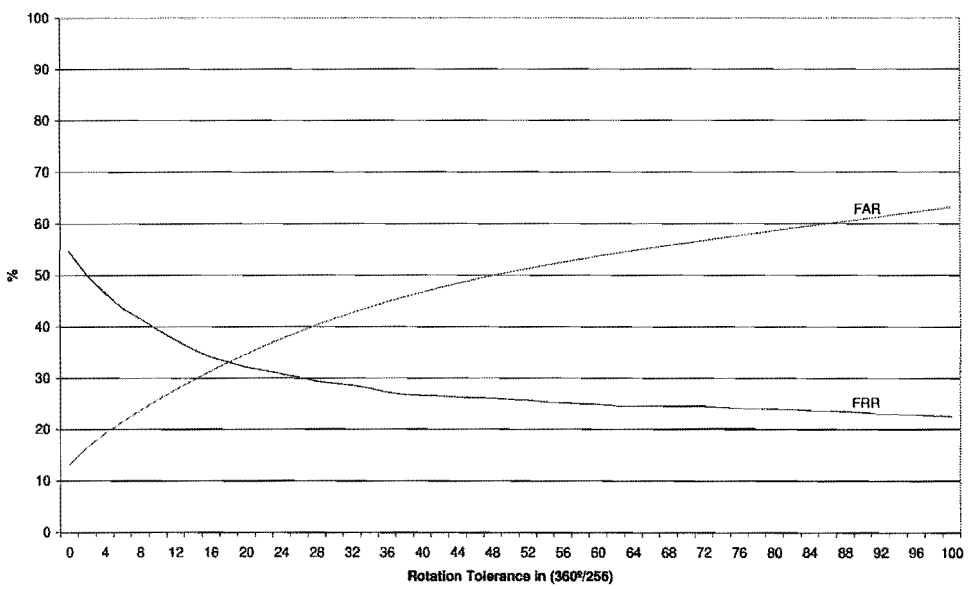


Figure 7.5: The FRR and FAR when the rotation between fingerprints is varied.

For the batch of comparisons used to calculate the FAR and FRR ten minutiae matches were used to signal a match. The complete 4-tuple representing a minutia was used to compare a pair of minutiae.

The maximum rotation allowed between the calculated orientations of the two fingerprints was started at 0° and incremented in units of $2 \times \frac{360}{256}^\circ$ until it reached $100 \times \frac{360}{256}^\circ$. For each of these

increments the batch process was executed to calculate the FAR and the FRR. The results from these batches was plotted as a graph in Figure 7.5 to allow comparison between the tolerance in the rotation and the respective error rates.

From the graph in Figure 7.5 one can see that the FRR decreases as the tolerance is increases. Unfortunately the FAR increases as the tolerance is increased. From the graph it looks as if allowing the fingerprint to rotate by about $20 \times \frac{360}{256}^{\circ}$ gives a good balance. Below this point the FRR decreases rapidly, while after this point the FRR decreases gradually indicating that this is about the maximum error in the orientation calculation. The FAR continues to increase as this tolerance is increased. The tolerance should thus be restricted to minimise the error rate.

7.3.4 Varying the Matching Tolerances

Each minutiae detected in the fingerprint is recorded as a 4-tuple describing the location and characteristics of the minutiae. In the comparison of a pair of fingerprints these tuples of minutiae are checked to identify a correspondence between them. The number of pairs of minutiae, (with one minutia from the one and the other minutia from the other fingerprint), which match on the all of the characteristics of the 4-tuple is used to indicate the probability that the fingerprints originated from the same finger.

This set of tests examines the tolerances within which the minutiae need to match to be designated as matching. They need to allow some tolerance in the matching since there is a level of inaccuracy in extracting them. These tests seek to determine the optimum values for the tolerances.

Radius Tolerance

The first value in the 4-tuple (7.6) of characteristics representing a minutia is the radius, r, in polar coordinates. There is a level of error in the extraction of the position. This error could be the result of smudges or interference in the input image or error in the location of the core point. Whatever the reason the comparison process needs to cater for a limited level of error. This test has been designed to examine the effect of changing the tolerance with which the radius is matched.

Batches of comparisons are performed and the results recorded. These batches are repeated with varying tolerances used in the matching of the radius component of the minutiae.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of r ranging in [0..100] pixels
Tolerance of $\theta = 11 \times \frac{360^\circ}{256}$
Tolerance of $\alpha = 13 \times \frac{360^\circ}{256}$
Tolerance in the range of rotation = $20 \times \frac{360^\circ}{256}$
A match is declared if 10 minutiae match.

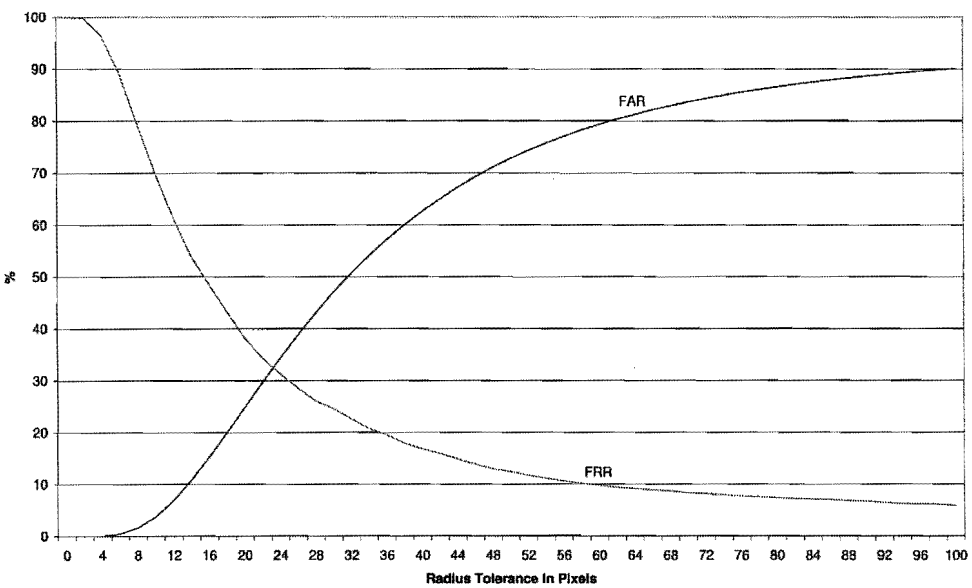


Figure 7.6: The FRR and FAR when the tolerance in matching the radius is varied.

The complete 4-tuple representing a minutia was used to compare a pair of minutiae and ten minutiae matches between a pair of fingerprints was used to declare the fingerprints from the same finger.

From the graph in Figure 7.6 it appears that the tolerance in the radius should be in the range of $10 - 20$ pixels. For values less than this value the FRR decreases rapidly, while the FAR does not increase as rapidly. On the other hand for values greater than this value the FRR does not decrease at the same rate as the FAR increases.

Choosing a tolerance in this range appears to produce the best results by minimising the error rates. For the remainder of the tests the tolerance used for matching the radius has been chosen as 11 pixels. This tolerance seems to perform with a balance between the FAR and FRR.

Tolerance in θ

The second value in the 4-tuple (7.6) of characteristics representing a minutia is the angular coordinate, θ. This coordinate will also have an associated level of error that will be similar to the error of the radius. This error will be similar to the error in the radius as the same Cartesian coordinates were used and converted to polar coordinates.

This test was developed to determine the optimum tolerance in θ. The batch process was repeated with different tolerances in matching θ and the results recorded. These results indicate the effect of varying the tolerance on the FAR and FRR.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels
Tolerance of θ ranging in $[0..100] \times \frac{360^\circ}{256}$
Tolerance of $\alpha = 13 \times \frac{360^\circ}{256}$
Tolerance in the range of rotation $= 20 \times \frac{360^\circ}{256}$
A match is declared if 10 minutiae match.

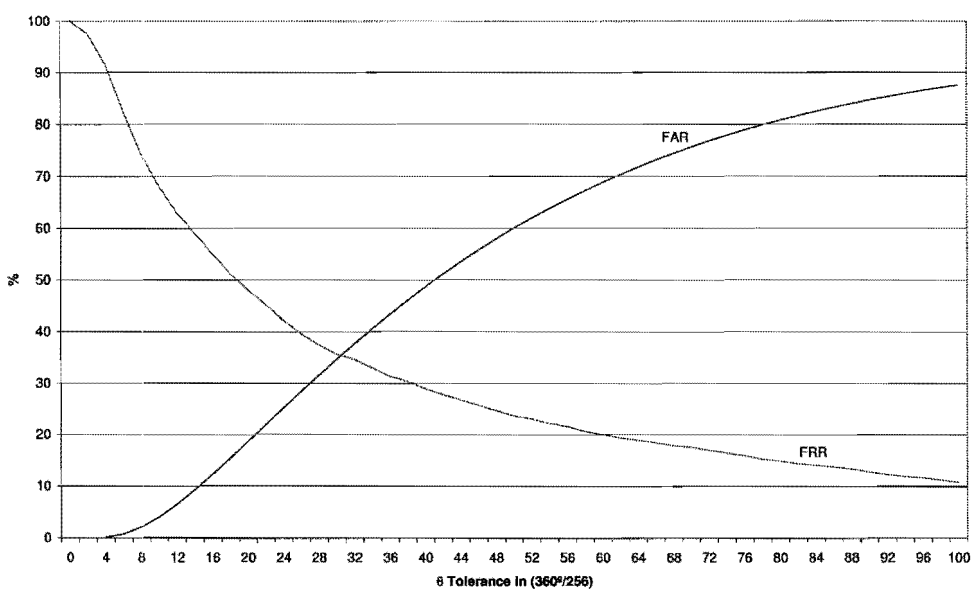


Figure 7.7: The FRR and FAR when the tolerance in matching a pair of minutiae on θ is varied.

The complete 4-tuple representing a minutia was used to compare a pair of minutiae and ten minutiae matches between a pair of fingerprints was used to declare the fingerprints from the same finger.

The graph in Figure 7.7 shows that FRR decreases rapidly as the tolerance for the angular coordinate θ in the comparison is increased. This indicates that there is a measure of error in the detection process of the minutiae. Thus this error needs to be catered for in the comparison process. The FAR also increases as this tolerance is increased making it undesirable to make it any larger than is absolutely needed. From the graph it appears that a tolerance of between $10 \times \frac{360}{256}^\circ$ and $20 \times \frac{360}{256}^\circ$ gives a best result.

Tolerance in α

The third value in the 4-tuple (7.6) of characteristics representing a minutia is α, the direction of the ridge from which the minutiae was extracted. The extraction of this attribute also has a certain level of error. This test runs batches of comparisons with the same set of fingerprints varying the tolerance in α between batches and recording the results.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels
Tolerance of $\theta = 11 \times \frac{360}{256}^\circ$
Tolerance of α ranging in $[0..100] \times \frac{360}{256}^\circ$
Tolerance in the range of rotation = $20 \times \frac{360}{256}^\circ$
A match is declared if 10 minutiae match.

The complete 4-tuple representing a minutia was used to compare a pair of minutiae and ten minutiae matches between a pair of fingerprints was used to declare the fingerprints from the same finger.

The graph in Figure 7.8 shows how the FRR and the FAR change as the tolerance in the minutiae matching process changes. As the tolerance on α increases the FRR decreases and the FAR increases. It appears that tolerance of between $12 \times \frac{360}{256}^\circ$ and $20 \times \frac{360}{256}^\circ$ produces a good result.

7.3.5 Enhancement

There is an enhancement stage in the algorithm that was not applied in the previous tests. This enhancement sharpens the scanned images before any of the extraction algorithms are applied.

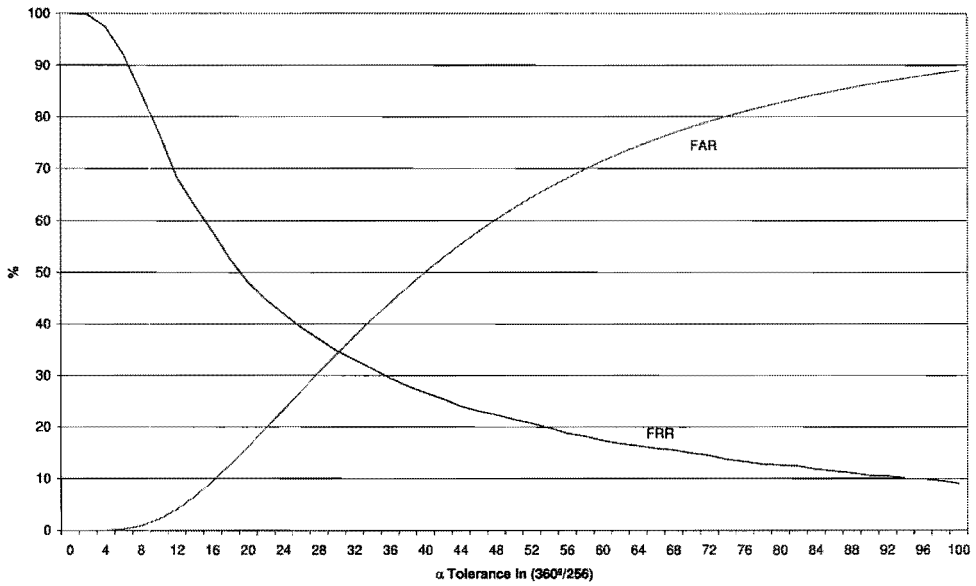


Figure 7.8: The FRR and FAR when the tolerance in matching the α is varied.

This stage can be added and then compared with the results produced without it. The criteria used in the previous sections that produced the best results have been used except that an enhancement of the fingerprint images has been added to the beginning of the minutiae extraction process.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels
Tolerance of $\theta = 11 \times \frac{360}{256}^{\circ}$
Tolerance of $\alpha = 13 \times \frac{360}{256}^{\circ}$
Tolerance in the range of rotation = $20 \times \frac{360}{256}^{\circ}$

The enhancement stage improves the accuracy and reduces the EER to less than 30%. This reduction indicates that there was considerable error in the determination of the position and characteristics of the minutiae in the previous stage of the testing and that the enhancement reduces this error. The corresponding results are depicted in Figure 7.9.

7.3.6 Classification

All of the previous tests used only the minutiae in the comparison process. It is however possible to use global features of the fingerprint in the comparison process. One would expect and prefer these

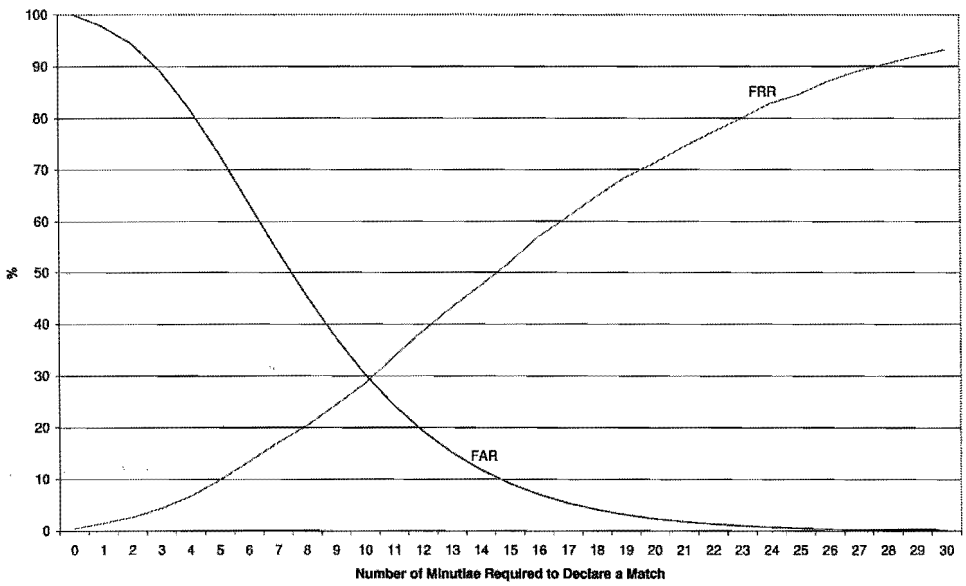


Figure 7.9: The FRR and FAR when the enhancement stage is used.

to reduce the FAR without increasing the FRR.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels
Tolerance of $\theta = 11 \times \frac{360}{256}^{\circ}$
Tolerance of $\alpha = 13 \times \frac{360}{256}^{\circ}$
Tolerance in the range of rotation = $20 \times \frac{360}{256}^{\circ}$

The classification that is based on the Henry system is used to divide the prints into classes. This will prevent a large section of the prints from matching. The other global feature that was used in this test is the curvature index. This curvature index represents the curvature of the ridges at the core of the fingerprint, and needs to match within a small tolerance. In Figure 7.10 the classification information rejects about 91% of the fingerprints that should not match before even comparing a single minutiae, but it also rejects 17% of the valid matches. Using a minimum level of 9 points to declare a match rejects over 99% of non-matching fingerprints.

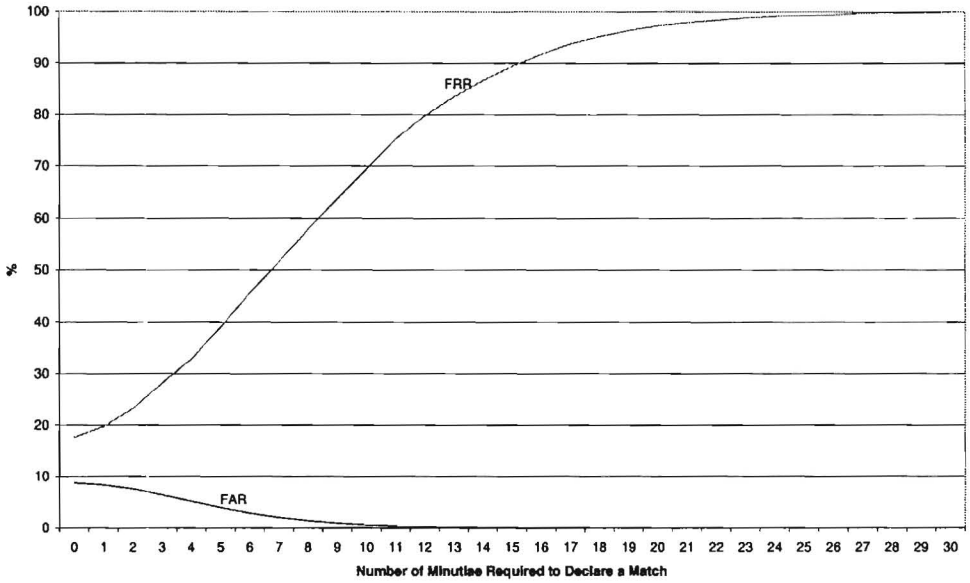


Figure 7.10: The FRR and FAR when the classifications are used.

7.3.7 Quality Fingerprints

In the previous tests it was shown that the FAR could be reduced to less than 1% if 10 points are used to declare a match. Unfortunately the FRR that corresponded to this FAR is larger than was desirable. It was conjectured that this inadequacy was due to the poor quality of some of the fingerprints in the database. To test this hypothesis 200 pairs of good quality images were visually selected from the database.

Figure 7.11 shows a sample fingerprint of good quality, while Figure 7.12 shows a sample fingerprint of poor quality. The poor quality fingerprints are difficult to match against anything and cause the FRR to become large, but have little affect on the FAR precisely because they are unlikely to match anything.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels
Tolerance of $\theta = 11 \times \frac{360}{256}^\circ$
Tolerance of $\alpha = 13 \times \frac{360}{256}^\circ$
Tolerance in the range of rotation $= 20 \times \frac{360}{256}^\circ$

Figure 7.11: An example of a good quality image.

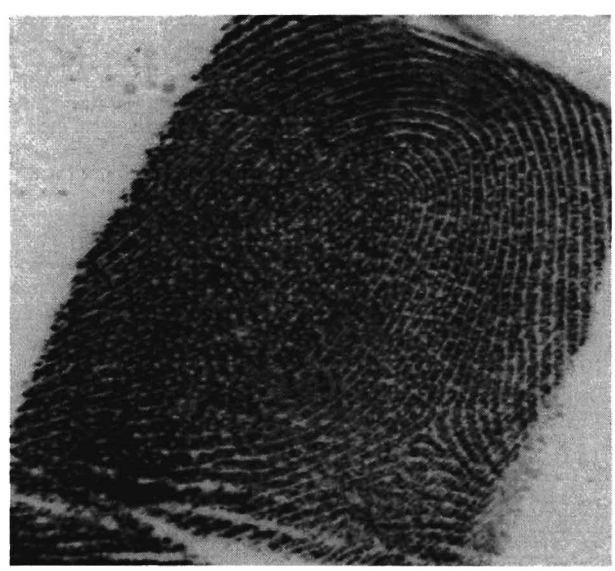


Figure 7.12: An example of a poor quality image.

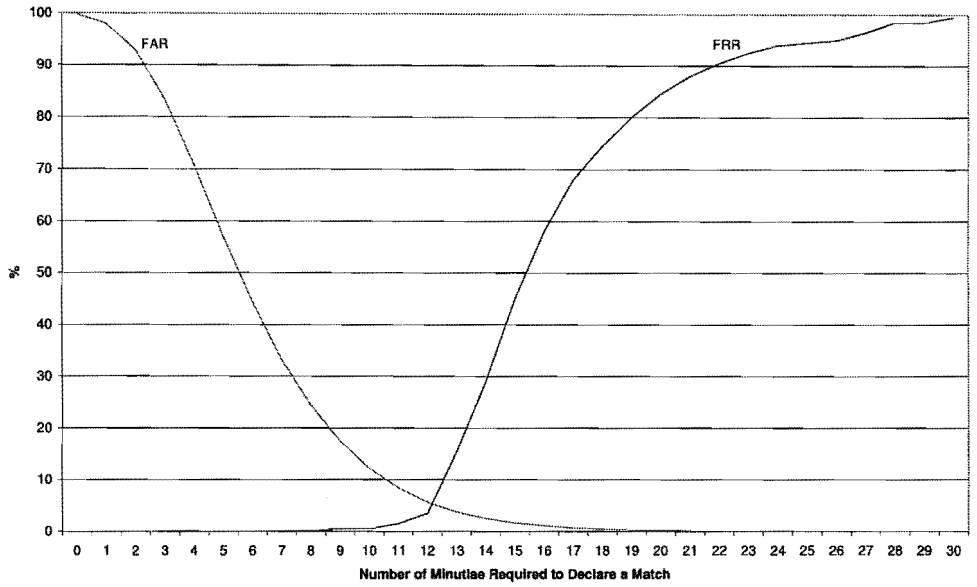


Figure 7.13: The FRR and FAR when quality fingerprints are used.

The complete 4-tuple representing a minutia was used to compare a pair of minutiae, and no classification information was used in the comparison process.

The results from the tests using the quality images are presented in Figure 7.13. These show a significant improvement in the accuracy of the comparison process. There are a significantly larger number of minutiae that match between a pair that should match. The graph in Figure 7.13 shows that the FRR decreases compared to the poor quality images without having much effect on the FAR.

The results with the quality images have an EER of 41% if only position is used to compare minutiae. If position and α is used then this EER drops to 8.8%. It is then further reduced to 5.6% if the type of the minutia is also used. This indicates that the more characteristics that are used the better the accuracy of the matching process.

7.3.8 Quality Fingerprints with Classification

As in the tests with the complete database, global features of the fingerprints can be used to compare the fingerprints before they are compared on the minutiae.

The tolerances used in deciding if a pair of minutiae match for this test are:

Tolerance of $r = 11$ pixels

Tolerance of $\theta = 11 \times \frac{360}{256}^{\circ}$

Tolerance of $\alpha = 13 \times \frac{360}{256}^{\circ}$

Tolerance in the range of rotation $= 20 \times \frac{360}{256}^{\circ}$

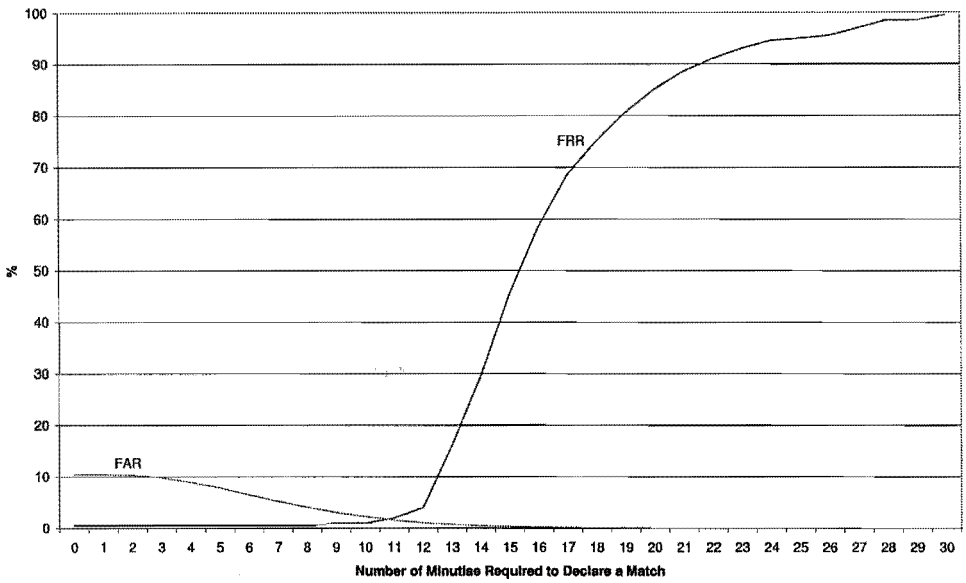


Figure 7.14: The FRR and FAR when quality fingerprints are matched with classification information.

The complete 4-tuple representing a minutia was used to compare a pair of minutiae and all the classification information was used in the comparison process. This is similar to the test performed on the whole database described in Section 7.3.6.

Figure 7.14 shows the results of using global characteristics of fingerprints to improve the comparison process. This reduces the EER to about 1.5%. A poor quality image will tend to increase the FRR, but have little effect on the FAR [38].

7.3.9 Consolidation of the Accuracy Analysis

The accuracy of the matching process has been found to improve when certain sections are included in extraction and comparison of the minutiae.

Table 7.2 shows how the EER changes when the whole database is used, compared with the set selected on their quality. This table demonstrates the effect of allowing rotation and using differing

	Complete Database EER		Selected Pairs EER	
Match on	No Rotation	Full Rotation Allowed	No Rotation	Limited Rotation Allowed
Position	41.40	43.35	36.58	41.34
Position, θ	34.25	34.30	14.11	8.81
Position, θ, α	35.36	32.10	11.51	5.64

Table 7.2: Comparison of the equal error rates.

amounts of information to perform the minutiae comparison. This table clearly demonstrates the effect of using additional characteristics about each minutia for the comparison. On reasonable quality fingerprints the EER is reduced by about 80% by the utilisation of the direction associated with each minutia. This is further reduced by about 35% with the inclusion of the type. Additional characteristics can be extracted for each minutia and used in the comparison to reduce these error rates.

Algorithmic Stages	EER
Basic	35.36
Enhancement	29.65
Enhancement and Classification[1]	17.60
Quality Set with Enhancement	5.63
Quality Set with Enhancement and Classification	1.56

Table 7.3: Comparison of the equal error rates with different sections included in the comparison algorithm.

The algorithm used to extract the minutiae can include different sections in the algorithm. Table 7.3 shows how the EER is reduced when the enhancement stage is included improving the accuracy of the minutiae extracted. The classification information further reduces the EER. The affect on the high quality fingerprints is also shown in Table 7.3.

[1]The FAR and FRR do not cross in this case. The larger of the two was used as the EER. In this case the FRR is 8.74 and the FAR is 17.60

7.4 Curvature Index Consistency

The core point of each fingerprint is located at the point of greatest concave curvature. A number can be extracted at this point representing the curvature of the ridge at this point, which can be used as an indexing mechanism for the fingerprints. The difference in the curvature index between the matching pair of fingerprints was calculated. Ideally this difference should be small allowing it to be used as an approximate index.

7.4.1 Without Enhancement

The first test was performed on the entire set of 2000 fingerprint pairs. The range of values calculated for the index is from about two up to about nine. The absolute difference between the indexes calculated for each of the fingerprints in the pair was recorded. This difference was used to determine whether it could be used as a rough index and how far the search area of each side would need to be.

Mean	0.97
Variance	0.73
Standard Deviation	0.85
Median	0.75

Table 7.4: The difference in the curvature index from matching fingerprints.

The results in Table 7.4 show that 50% of the matching pairs have a curvature index less than 0.75 apart. The variance is quite large as a result of a few outliers as a result of prints with a large difference in the index.

7.4.2 With Enhancement

The same test was repeated, but this time the fingerprints were enhanced before they the curvature was calculated.

The results in Table 7.5 show that 50% of the matching pairs have a curvature index less than 0.70 apart. The variance is still on the large side.

The inclusion of the enhancement stage has made an improvement in the accuracy of the results. The mean difference has decreased along with the variance in the difference.

Mean	0.91
Variance	0.62
Standard Deviation	0.79
Median	0.70

Table 7.5: The difference in the curvature index from matching enhanced images.

7.4.3 Quality

The test was repeated with the same set of quality fingerprints selected to test FAR and FRR. In this test the fingerprints were enhanced before the index was extracted.

Mean	0.26
Variance	0.03
Standard Deviation	0.17
Median	0.25

Table 7.6: The difference in the curvature index from quality fingerprints prints.

The results in Table 7.6 show that on quality fingerprints the mean difference, along with the variance in this difference, in the curvature index calculated from matching fingerprints substantially decreases. Half of the pairs have a difference of less than 0.25.

7.5 Timing

The performance of a system needs to meet have specific criteria for it to be a viable option. In the system tested here the timing is of critical importance. The timing of the system needs to conform to constraints to ensure that a system can be used in real time.

The process of identity verification can be divided into a number of stages. This first of these stages is the process of acquiring the image from the scanner. The total time required for an image capture is less than 100ms [44]. The second stage in the process is the extraction of a set of minutiae. The third stage is the comparison of the minutiae. The timing for the second and third stages have been tested and recorded.

7.5.1 Minutiae Extraction

The process of extracting a set of minutiae and the corresponding characteristics about each minutia has been recorded. The minutiae extraction was performed on a computer with an Athlon 600 MHz processor.

Mean	3.4s
Variance	0.1s
Standard Deviation	0.32
Median	3.4s

Table 7.7: The time taken in seconds to extract a set of points from a fingerprint.

Figure 7.7 shows the time taken to extract a set of minutiae from a fingerprint. This minutiae extraction process is the main contribution to the time taken to perform a comparison.

7.5.2 Matching On the Smart Card

The second stage is the comparison of the minutiae. This stage can be divided into two sections. The first copies the second set of minutiae to the card and the second compares it to the set already on the card.

Mean	1.7s

Table 7.8: Time in seconds to copy a set of minutiae to the smart card.

Table 7.8 shows the times taken to transfer the set of minutiae to the smart card. This time is largely due to the time taken to store the minutiae in EEPROM, which is a time consuming step. No variance is presented, as it is negligible compared to the time of 1.7 seconds taken to copy the minutiae across to the card.

Mean	0.026s

Table 7.9: Time to compare minutiae on the smart card.

The results in Table 7.9 show the time required to match two sets of minutiae on a smart card. The variance in the time was negligible. Combining the copying to the card and the comparison could

reduce the time since the write to EEPROM would then be avoided. This combination was not implemented since the times are within the acceptable range.

7.5.3 Matching On the Computer

In addition to testing the time for comparison on a smart card, the time needed for a comparison on the computer was recorded. Computer comparison time would be used if the comparison routine were used to search through a database.

Mean	0.00012s

Table 7.10: Time to compare minutiae on the computer.

The results in Table 7.10 record the time required to perform the matching routines on a computer with an Athlon 600 MHz processor. On the same machine if the classification information is used to do a quick reject of non-matches then over 70000 comparisons are performed per second.

From these results one can show that the complete authentication process from the moment the smart card is inserted into the reader and the fingerprint is scanned until the moment when it is either declared to be a match or non-match takes about five seconds. By implementing additional optimisations this process can be reduced to about three seconds.

7.6 Summary

The accuracy and the timing of a real-time system are critical to its success. In this chapter these performance metrics of the system designed and implemented by the author have been tested. Both statistical analysis and empirical testing are presented here. Accuracy results were summarised in Table 7.2 and Table 7.3. These results showed that using additional characteristics about each minutia reduced the error. Additionally the inclusion of the enhancement stage and the use of the classification information improved the accuracy of the verification.

A statistical model was developed to predict the level of false acceptance. The set of minutiae extracted from a fingerprint was expected to have a high level of coherence with other sets of minutiae extracted from the same finger, while one would expect a very low level of coherence between sets of minutiae extracted from different fingers.

The statistical model assumes that the set of minutiae extracted from a scan can be treated as a random set of equally likely points. This structure can be modelled with a hypergeometric distribution, where the fingerprint is divided into a number of regions, each of which can have a single minutia in it. An attempt to match this with another scan will have the potential for a minutia to be in the corresponding region by chance. When this coincidence happens then the minutia is counted as being a match. The statistical model is able to predict the FAR when the rotation between the fingerprints is kept constant.

The empirical testing and analysis records the results from executing batch comparisons. These comparisons show that using just the position of the minutiae for comparison is insufficient to produce accurate results. The addition of direction decreases the FAR, but increases the FRR. The net effect, however, is to reduce the overall error. The addition of minutia type did not reduce the error rates significantly, on the original set of fingerprints. It did however reduce the EER by about half when operated on better quality scans. This effect shows that scan quality has a large effect on the FRR.

The effect of varying the amount of rotation allowed between fingerprints was also examined. It was found that allowing a small amount of rotation decreased the FRR significantly, although allowing more than about $20 \times \frac{360^o}{256}$ had minimal effect on the FRR. Allowing rotation did increase the FAR, but the FRR decreased more notably for small rotations. A similar effect was noticed by allowing the tolerance between minutiae to vary, which would cause minutiae to be declared as matching.

Inclusion of an enhancement stage in the minutiae detection algorithm was then tested. This was found to reduce the EER by about 5%. There was in addition a significant reduction in the FRR and a small reduction in the FAR. The use of classification information in the comparison stage was tested and found to improve the accuracy. There was a large reduction in the FAR, but the FRR increased due to the misclassification of a few fingerprints.

Often the inked fingerprints are of a very poor quality, resulting in low signal-to-noise ratios [27]. Poor quality prints can be a direct result of the conditions under which the prints were acquired. Inclusion of the enhancement stage was able to improve the results on poor quality images.

Batch comparisons were performed on a selected set of quality image pairs. 200 pairs of images were visually selected as good quality images. On these fingerprints the tests showed that using just the position to compare minutiae without classification information produced equal error rates of around 40%. Including the direction of the minutiae reduced the EER to less than 10% and using the type of the minutia further reduced this EER to about 5.6%. The addition of classification

information into the comparison process reduced the EER to 1.56%.

In [37] a computer was set up with 40 user accounts, each with an associated fingerprint. A round-robin test where each user attempted to gain access to each of the accounts was then performed. Doing so produced 1600 test queries, of which 40 queries should have been granted and 1560 denied. The FRR was in the range zero to 44% while the FAR was in the range zero to 0.4%. Most of the error in the system originated from poor quality images.

It was shown that the curvature index calculated at the core point could be used to provide a rough indexing scheme into a database. On good quality fingerprints the mean difference in the index between fingerprints from the same finger was 0.26. Thus, if a tolerance of 0.5 were used then most matching fingerprints would still be declared as matching while eliminating most non-matches.

Timing information gathered from the batch comparisons showed that the authentication process is efficient enough to make it a feasible option. The complete authentication process takes about 5 seconds.

Chapter 8

Future Work

The implementation and analysis described in this work demonstrates that performing a fingerprint comparison on a smart card is feasible. This method can be used to enhance the privacy and security of a system. Testing of the implementation showed that the extraction of the minutiae set was the most time consuming part of the authentication process. This aspect could receive optimisations to reduce the time delay that it causes. There are a number of related areas that could be researched further to extend the themes explored in this dissertation. Some of these are presented here.

8.1 Identification from a Central Database

The second phase of the comparison process as described in Section 6.4 was able to compare over 70 000 fingerprints per second on a PC with an Athlon 600 MHz processor. These speeds were only attainable by caching the minutiae in memory. This is feasible because the biometric template is small. This indicates that the system presented here, or some derivative of it, could be used to search through large databases of fingerprints. It might even be possible to search through databases containing over 100 000 prints in real-time.

The search through the database could easily be parallelised to give a large improvement in the throughput of comparisons. The curvature index that was calculated at the core point could be used to provide a rough ordering of the fingerprints. One would expect this heuristic to reduce significantly the search space required to locate matching prints.

8.2 Generation of the Biometric Template

The set of minutiae in this system was created from a single fingerprint. The use of multiple input fingerprints from the same finger could be used to generate a more accurate template of the minutiae. This would also allow the classification of the fingerprint to be performed more accurately. If the different scans are classified into different classes then the predominant class can be used as the primary classification, while a secondary classification can be stored until it is needed. The use of a secondary classification should almost remove the effect of misclassifications from the FRR. The use of multiple scans to generate a template should also produce a more accurate curvature index.

8.3 Protocols Making Use of Distributed Matching

This study has shown that it is feasible to perform the fingerprint verification on the smart card. However there still needs to be a secure protocol to ensure that the authentication is accurate.

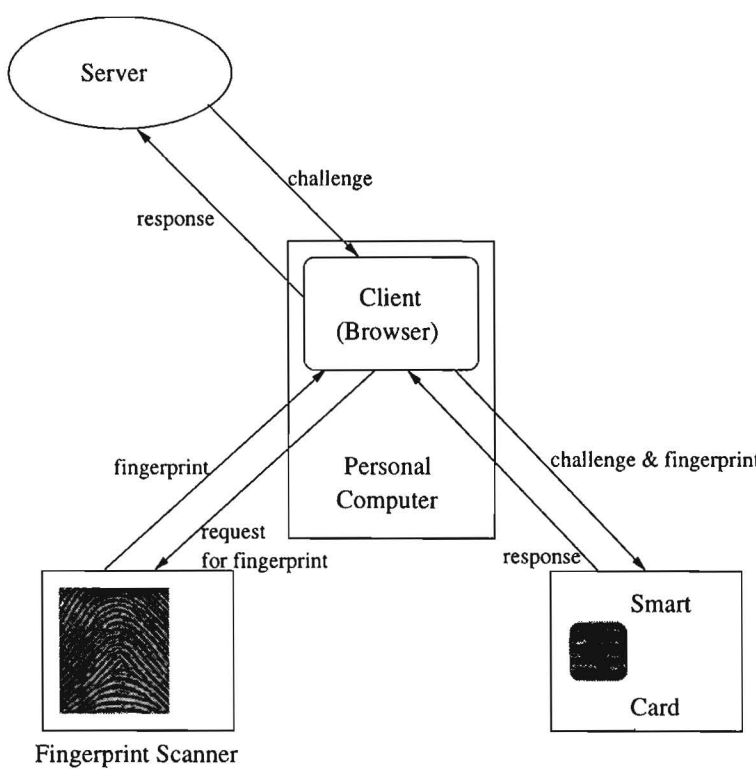


Figure 8.1: A high level representation of the protocol needed to use fingerprints over the Internet.

It would be ideal if a biometric could be used to authenticate a user over the Internet securely. This would require that the protocols used are secure. Figure 8.1 shows a high level overview of how the protocol would be expected to behave. There would need to be a challenge from the server to guarantee the freshness of the response. This system would need to acquire a fingerprint from the scanner to forward to the card along with the challenge. If the fingerprint were accepted as a match by the card then the response would indicate this.

The smart card still stores the fingerprints in a distributed fashion allowing the owner to retain complete control over their biometric data. The comparison should still also be performed on the card. This protocol might be something along the lines of a server sending a challenge, possibly a timestamp, through to an Internet browser. The browser would initiate a fingerprint scan at the PC. The template extracted from the fingerprint would then be sent to the smart card. The smart card might use a private key to sign the response digitally verifying its identity to the server.

This protocol would need to follow all the major design criteria such that the key stored on the card and used to sign the verification process would be protected from unauthorised access. The challenge from the server needs to include a timestamp or nonce to ensure the randomness necessary to prevent replay attacks. Additionally the implementation needs to withstand side channel attacks that monitor the power consumption or timing. The major difficulty in this protocol design would be the limitations with respect to what can be performed in reasonable time on the card with its limited processing capabilities.

8.4 Using other Biometrics for the Smart Card Matching

The smart card has limited CPU and memory resources. These provide challenges complicating the process of performing the match on the card. Other biometrics could replace the use of the fingerprint in this implementation. The same approach can be taken and privacy goals solved in the same way. Questions, which remain though, are how large templates are for other biometric techniques and whether they will fit on smart cards. Rapid increase in the capacity of cards suggests that this will be viable in the near future.

8.5 Embedding a Biometric Sensor into a Cellular Phone

The system developed here stores a fingerprint template on a smart card. Since most GSM and other mobile phones contain a smart card anyway, (the Subscriber Identification Module (SIM)), increases in card capacity should also permit use of distributed authentication as proposed in this dissertation on such devices. If this system can be built into a cellular phone it could be used to perform the authentication in e-commerce systems.

8.6 Using an adaptive Error Tolerance

The error tolerances of the paramaters could be adaptive. The use of Cartesian and polar coordinates influences the error that is tolerated when a fixed tolerance is used in matching minutiae. Using an adaptive tolerance might improve the accuracy of the verification process. There are however stringent computational limits on the algorithms when one uses a smart card.

Chapter 9

Conclusion

In many otherwise secure systems the authentication of the individual is a weak point in the security. Authentication is fundamental to all other security related decisions, since an incorrect authentication would compromise access control, integrity, confidentiality and non-repudiation.

Currently the primary method of authentication uses a password with a username or token. There are a number of difficulties with the use of a password. It could be guessed or stolen, allowing illegitimate access to sensitive information. Many systems that are operational have a difficulty in authenticating the user reliably.

No one can guarantee 100% security, but the risk can be reduced to an acceptable level. Fraud exists in current commerce systems: cash can be counterfeited; cheques altered and credit card numbers stolen. However, these systems are successful overall as the overall benefits outweigh the losses — the risks are considered acceptable. A system using a template of a fingerprint stored on a smart card with a secure communications protocol can provide a secure form of authentication, which can then be used for financial transactions. The security provided will be considerably higher than that currently employed in ATM transactions.

Strong cryptographic systems can withstand targeted attacks up to the point where it becomes easier to get the information some other way. Computer programs, no matter how good, cannot prevent an attacker from going through someone's garbage to find passwords that have been written down. However, the security risk caused by the careless activities of a valid user with their password can be eliminated if they no longer need to use a PIN or password, but rather a biometric.

Additionally it is important that the granularity is appropriate to the application. Even the best

authentication will not ensure non-repudiation if the subjects can leave their workstations for half an hour and someone else can impersonate them from their workstations in their absence. For this reason it is standard to require a re-authentication every time that a new transaction is conducted. This is one method to reduce the risk.

Biometrics provide a method to authenticate an individual with a very high accuracy. With modern equipment it is possible to acquire digital scans of sufficient resolution to allow many different biometrics to be used for authentication. However there have been a number of privacy concerns raised with respect to the use of biometrics to identify individuals in civilian applications.

The aim of this research was to investigate the privacy concerns of using biometrics and to develop a solution that used biometrics for authentication, which at the same time preserved the individual's privacy. The scope of the system was constrained by the need for it to be able to use inexpensive equipment to authenticate an individual reliably in real-time.

Investigation of the privacy of the biometric showed that since a biometric is a unique attribute of an individual, many individuals do not want to relinquish control over its use to a third party. There is also the perception that it will be used to track the individual's activities. This is mainly due to the extensive use of biometrics, (particularly the fingerprint), in forensic research associated with a criminal investigation.

The other less well-known concern with biometric scans is that they contain information. They could be used to gain invasive knowledge about the individual. There is a wealth of information stored in a biometric scan concerning the owner's medical history. For example a picture of the face can indicate the presence of skin diseases and even the fingerprint can provide clues towards the owner's gender, age and occupation.

The approach of this dissertation was to provide the user with a system that would allow complete control of the biometric information to remain with the individual, while improving the security and accuracy of the authentication process through the use of a biometric. In this research the fingerprint was used to provide biometric data with sufficiently unique information to provide an accurate verification of identity. From the fingerprint a set of minutiae were extracted and placed on a smart card as a template. The later verification of the individual's identity was performed on the card, thus removing all reasons requiring any biometric information stored on the card to be removed.

The use of biometrics and smart cards is intended to increase the level of security. For the system to be viable it needs to ensure that that the implementation is efficient and that new security loopholes

are not introduced. With this aim in system development an implementation was demonstrated whereby as much of the verification process as possible is moved onto the smart card, thereby removing the need to be able to access the biometric template externally from the card.

The technology used to produce smart cards has also expanded and improved, resulting in greater security in these cards and making it more difficult to gain unauthorized access to the contents. This, together with the reasonable price of smart cards, results in a cost effective method of achieving a high security authentication.

The system explained in this work can be used to provide authentication for many different applications. The card can store a private key, which is protected by a fingerprint. The physical protection of the card should protect its contents from unauthorised access if secure communications protocols are used. The card in conjunction with a fingerprint can verify a user's identity to an ATM to allow a cash-withdrawal or to an Internet site for e-commerce.

This method of authentication does not require the bank or the Internet site to keep any client's biometric data to authenticate them biometrically. In this way the individual's privacy is protected.

Many users do not want their fingerprints to be stored electronically in databases. This does not cause problems is this system as the fingerprints do not need to be stored in databases, but rather just a template extracted from the fingerprint is stored on a smart card. The use of the smart card is then entirely under the control of the individual. They can have the added security provided by the use of a biometric, yet at the same time they can keep the biometric under their control at all times. This method does not need to do any searches through huge databases of fingerprints and it does not place large demands on network traffic.

A statistical model was developed to predict the FAR. This model assumed that minutiae sets from different fingers could be expected to have very low levels of coherence. The FAR was modelled with a hypergeometric distribution.

The implementation was also tested empirically. These empirical results showed that the minutiae were not always extracted perfectly accurately. The effect of varying the range of tolerance used to declare two minutiae as a match was examined. It was found that a small tolerance produced the best results.

Inclusion of an enhancement stage in the minutiae detection algorithm was then tested. This was found to reduce the EER. There was a significant reduction in the FRR and a small reduction in the FAR. The use of classification information in the comparison stage was tested and found to

improve the accuracy. There was a large reduction in the FAR, but the FRR increased due to the misclassification of a few fingerprints.

On the set of high quality fingerprint scans it was shown that using just position to match minutiae was inadequate as it produced an EER of around 40%. Including the direction of the minutiae reduced the EER to less than 10% and using the type of minutiae further reduced it to 5.6%. The use of classification information decreased the EER to 1.56%.

This would be acceptable for some commercial systems. For many access control systems this would provide a sufficient level of confidence in the user's identity. Particularly when used in conjunction with the fact that the user is in possession of the correct card. For systems like a cash dispensing machine this level of confidence in a user's identity would most likely not be sufficient. For those systems additional information will need to recorded about each minutiae and used in the comparison process.

It has therefore been demonstrated that it is feasible to store a fingerprint template on a smart card. This system outline in this dissertation performs the fingerprint comparison on the card in real-time thereby countering the privacy objections of individual who want to retain control over their biometric data.

Bibliography

[1] R. Anderson. Why Cryptosystems Fail. *Communications of the ACM*, 37(11):32 – 40, November 1994.

[2] R. Anderson and M. Kuhn. Tamper Resistance - a Cautionary Note. *The Second USENIX Workshop on Electronic Commerce Proceedings*, pages 1 – 11, November 1996.

[3] E. Biham and A. Shamir. Differential Fault Analysis of Secret KEY Cryptosystems. *Advances in Crypytology – CRYPTO '97 Proceedings*, pages 513 – 525, 1997.

[4] D. Boneh, R.A. Demillo, and R.J. Lipton. On importance of Checking Cryptographic Protocols for Faults. *Cryptology – EUROCRYPT '97 Proceedings*, pages 37 – 51, 1997.

[5] J.P. Campbell. Speaker Recognition: A Tutorial. *Proceedings of the IEEE*, 85(9):1437 – 1462, September 1997.

[6] Data Protection Act 1998. Her Majesty's Stationery Office, United Kingdom.

[7] Directive 95 of the European Parliament and of the Council On the protection of individuals with regard to the processing of personal data and on the free movement of such data. ECO 291, CODEC 92, European Union, 2 February 1995.

[8] Federal Privacy Act of 1974. 5 U.S.C. Section 552a, as amended, United States of America.

[9] R.W. Frischholz and U. Dieckmann. BioID: A Multimodal Biometric Identification System. *Computer*, 33(2):64 – 68, February 2000.

[10] L. Gong and P.F. Syverson. Fail-Stop Protocols: An Approach to Designing Secure Protocols. In *The Fifth International Working Conference on Dependable Computing for Critical Applications*, pages 44 – 55. Springer-Verlag, September 1995.

[11] G.T. Candela, P.J. Grother, C.I. Watson, R.A. Wilkinson and C.L. Wilson. PCASYS - A Pattern-Level Classification Automation System for Fingerprints. Technical Report NISTIR 5647, National Institute of Standards and Technology, August 1995.

[12] U. Halici, L.C. Jain, and A. Erol. Introduction to Fingerprint Recognition. In L.C. Jain ... [et al.], editor, *Intelligent Biometrics Techniques in Fingerprint and Face Recognition*, International Series on Computational Intelligence, chapter 1, pages 1 – 34. CRC Press, 1999.

[13] L. Hong. *Automated Personal Identification Using Fingerprints*. PhD thesis, Michigan State University, June 1998.

[14] L. Hong, Y. Wan, and A. Jain. Fingerprint Image Enhancement Algorithm and Performance Evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(8):777 – 789, 1998.

[15] A.J. Howell. Introduction to Face Recognition. In L.C. Jain ... [et al.], editor, *Intelligent Biometrics Techniques in Fingerprint and Face Recognition*, International Series on Computational Intelligence, chapter 7, pages 217 – 283. CRC Press, 1999.

[16] Wired Digital Inc. Your Eyes Are Windows to MS. *Wired News Report*, 2 May 2000.

[17] A. Jain, L. Hong, and R. Bolle. On-line Fingerprint Verification. *IEEE Transactions on Pattern Analysis and Analysis and Machine Intelligence*, 19(4):302 – 314, 1997.

[18] A. Jain, L. Hong, and S. Pankanti. The Uses of Biometrics. *Communications of the ACM*, 42(8):136, August 1999.

[19] A. Jain, L. Hong, and S. Pankanti. Biometric Identification. *Communications of the ACM*, 43(2):91 – 98, February 2000.

[20] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle. An Identity-Authentication System Using Fingerprints. *Proceedings of the IEEE*, 85(9):1365 – 1388, September 1997.

[21] D. Kahn. *The Codebreakers*. Macmillian, 1967.

[22] J. Kelsey, B. Schneier, D. Wagner, and C. Hall. Side Channel Cryptanalysis of Product Ciphers. *ESORICS '98 Proceedings*, pages 97 – 110, 1998.

[23] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman. *Advances in Cryptology - CRYPTO '96*, pages 104 – 113, 1996.

[24] P. Kocher. Differential Power Analysis. *http://www.cryptography/com/dpa*, 1998.

[25] K.L. Kroeker. Biometric Organisations. *Computer*, 33(2):57, February 2000.

[26] M. Negin ... [et al.]. An Iris Biometric System for Public and Personal Use. *Computer*, 33(2):70 – 75, February 2000.

[27] H.C. Lee and R.E. Gaensslen. *Advances in Fingerprint Technology*. Elsevier, 1991.

[28] J. McCormac. *European Scrambling Systems*. Waterford University Press, 1996.

[29] B.B. Megdal. *VSLI Computational Structure Applied to Fingerprint Image Analysis*. PhD thesis, California Institute of Technology, Pasadena, California, February 1983.

[30] S. Miller. Vital Signs of Identity. *IEEE Spectrum*, 31(2):22 – 30, February 1994.

[31] A. Moenssens. *Fingerprint Techniques*. Chilton Book Company, London, 1971.

[32] N.Ratha, S. Chen, and A Jain. Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images. *Pattern Recognition*, 28(11):1657 – 1672, 1995.

[33] L. O'Gorman. Practical Systems for Personal Fingerprint Authentication. *Computer*, 33(2):58 – 60, February 2000.

[34] S. Pankanti, R.M. Bolle, and A. Jain. Biometrics: The future of identification. *Computer*, 33(2):46 – 49, February 2000.

[35] A. Penland and T. Choudhury. Face Recognition for Smart Environments. *Computer*, 33(2):50 – 55, February 2000.

[36] S. Percetti. Gemplus implements Veridicom's fingerprint matching algorithm on a smart card. *http://www.gemplus.com*, 24 February 2000.

[37] P.J. Phillips, A. Martin, C.L. Wilson, and M. Przybocki. An Introduction to Evaluating Biometric Systems. *Computer*, 33(2):56 – 63, February 2000.

[38] A.R. Roddy and J.D. Stosz. Fingerprint Features - Statistical Analysis and System Performance Estimates. *Proceedings of the IEEE*, 85(9):1390 – 1421, September 1997.

[39] B. Schneier. Why Cryptography is Harder than it Looks. Counterpane Systems, 1997.

[40] B. Schneier. Biometric: Uses and Abuses. *Communications of the ACM*, 42(8), August 1999.

[41] B. Schneier. Crypto-Gram. http://www.counterpane.com/crypto-gram-0005.html, May 2000. Counterpane Internet Security, Inc.

[42] B. Schneier and A. Shostack. Breaking Up Is Hard To Do: Modeling Security Threats for Smart Cards. *First USENIX Symposium on Smart Cards*, February 1999.

[43] W. Shen, M. Surette, and R. Khanna. Evaluation of Automated Biometrics-Based Identification and Verification Systems. *Proceedings of the IEEE*, 85(9):1464 – 1478, September 1997.

[44] Siemens. *Fingertip CMOS Chip and System*, December 1998.

[45] STMicroelectronics. Instant Java for your smartcard. *http://www.st.com/smartcard*, 1999.

[46] STMicroelectronics. Contactless Smartcards Come of Age. *http://www.st.com/smartcard*, 2000.

[47] J.D. Stosz and L.A. Alyea. Automated system for fingerprint authentication using pores and ridge structure. Department of Defence, Ft. Meade, MD 20755-6000.

[48] D Thompson, editor. *The Concise Oxford Dictionary Ninth Edition*. Oxford University Press, 1995.

[49] C.J. Tilton. An Emerging Biometric API Industry Standard. *Computer*, 33(2):130 – 132, February 2000.

[50] *CardServer V2.02 Technical Documentation*, February 1998.

[51] L. Underhill. *Introstat*. Juta and Company Ltd., 1987.

[52] VISA. *VISA Security Module Operations Manual*. VISA, 1986.

[53] Price Waterhouse. Technology forecast, 1998.

[54] C.I. Watson and C.L. Wilson. *NIST Special Database 4 Fingerprint Database*, March 1992.

[55] J.L. Wayman. Federal Biometric Technology Legislation. *Computer*, 33(2):76 – 80, February 2000.

[56] R.P. Wildes. Iris Recognition: An Emerging Biometric Technology. *Proceedings of the IEEE*, 85(9):1348 – 1363, September 1997.

[57] J.D. Woodward. Biometrics: Privacy's Foe or Privacy's Friend. *Proceedings of the IEEE*, 85(9):1480 –1492, September 1997.

[58] J. Zhang, Y. Yan, and M. Lades. Face Recognition: Eigenface, elastic Matching, and Neural Nets. *Proceedings of the IEEE*, 85(9):1423 – 1435, September 1997.

Index