Enhancing authentication accuracy using fingerprint image quality

Lim, Eyung

2007

Lim, E. (2007). Enhancing authentication accuracy using fingerprint image quality.
Master's thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/39182>

<https://doi.org/10.32657/10356/39182>

Enhancing Authentication Accuracy Using Fingerprint Image Quality

Lim Eyung

School of Electrical and Electronic Engineering

A thesis submitted to the Nanyang Technological University
in fulfilment of the requirement for the degree of
Master of Engineering

2007

Acknowledgements

I would like to express my sincere gratitude to my advisors, Professor Suganthan, Dr. Toh Kar Ann and Dr Eng How Lung for their patience, support and motivation. I have picked up a lot of technical skills as well as knowledge from this very fruitful journey. Without them, the thesis could never be completed.

In addition, I would like to thank Prof. Ser Wee and colleagues in Centre for Signal Processing, for their kind assistance in any way for the past five years for my problems in academics, work and life. I am grateful to Centre for Signal Processing for granting me with the permission to take up this Master of Engineering programme on a part-time basis.

Last but not least, I would like to acknowledge love and encouragement from my family members. They are the motivation for me to take part in this Master programme.

Table of Contents

Acknowledgements	I
Table of Contents	II
Summary	VI
List of Figures	VIII
List of Tables	XI
1. Introduction	1
1.1 Need for Biometric Authentication	2
1.2 Fingerprint Biometrics	4
1.2.1 Popularity of Fingerprint Biometrics	4
1.2.2 General Concepts in Fingerprint Biometrics	6
1.2.3 Common Problems in Fingerprint Biometric Systems	9
1.3 Fingerprint Image Quality	11
1.3.1 Motivation and Problem Statements	11
1.3.2 Use of Fingerprint Image Quality	12
1.3.3 Scope of the Project	14
1.4 Contributions of this Thesis	14
2. Literature Review	16

2.1 Automatic Fingerprint Authentication Systems (AFIS)	16
2.1.1 Minutiae-based Methods	18
2.1.2 Non-minutiae-based Methods	22
2.2 Fingerprint Image Quality Measures	23
2.2.1 Background	23
2.2.2 Direction-based Method	26
2.2.3 Sinusoidal Method	27
2.2.4 Other Methods	28
2.3 Summary	28
3. Pattern Classification Tools	29
3.1 Self-Organizing Map (SOM) with Learning Vector Quantization	30
3.2 Radial Basis Function Neural Network	33
3.3 Naive Bayes	35
3.4 Support Vector Machine (SVM)	39
3.5 Reduced Multivariate Polynomial (RMP)	40
4. New Quality Measures	42
4.1 Uniformity	43
4.2 Orientation Certainty	45
4.3 Signal-to-Noise Ratio	48

4.4 Curvature	50
4.5 Summary	51
5. Experiments	52
5.1 Databases	52
5.1.1 Database Setup	53
5.1.2 Database Set	56
5.2 Quality Assignment and Fingerprint Matcher	57
5.3 Subjective Quality Evaluation	58
5.3.1 Background on Subjective Quality Evaluation	58
5.3.2 Experiment I: Automatic Quality Classification Guided by Subjective Quality Level	59
5.3.3 Experiment II: ROC Performance of Subjective-quality enabled Fingerprint Matcher	61
5.4 Matcher-based Quality Evaluation	63
5.4.1 Background on Matcher-based Quality Evaluation	63
5.4.2 Experiment III: ROC Performance of Matcher-based-quality-enabled Fingerprint Matcher	64
5.5 Experiment Results for Quality Automatic Classification (Experiment I)	67
5.5.1 Results	67
5.5.2 Observations	70

5.6 Experiment Results for Subjective-quality-enabled Fingerprint	
Matcher (Experiment II)	70
5.6.1 Results	70
5.6.2 Observations	75
5.7 Experiment Results for Matcher-based-quality-enabled Fingerprint	
Matcher (Experiment III)	76
5.7.1 Results	76
5.7.2 Observations	86
5.8 Summary of Results	86
6. Conclusions	88
6.1 Project Flow	88
6.2 Quality Measures	89
6.3 Subjective Quality Evaluation	89
6.4 Matcher-based Quality Evaluation	90
6.5 Some Concluding Remarks	90
6.6 Recommendation for Future Work	91
Bibliography	92

Summary

While awareness for security arises under terrorism threat of today, deployments of automated biometric systems are getting popular everywhere in the world. An automated biometric system aims to substitute human in performing identity authentication through certain biological characteristics. When an automated biometric system is put in the unsupervised mode, biometric samples with insufficient or contaminated features are expected to cause problems. Nevertheless, many biometric systems of today lack the ability to verify whether the presented samples are carrying valid and sufficient features for authentication. Those samples which are quantified as low in quality, are often the cause for the instability of biometric systems.

This thesis focuses on the fingerprint biometric authentication problem. The objective of the work is to empower an Automated Fingerprint Identification System (AFIS) with the ability to analyze quality level of the captured fingerprint image during registration and query processes. By making use of such quality information in the fingerprint matching processes, we hope to achieve an improvement in the overall matching accuracy.

Quality Measures are first defined within the context. Quality Measures are quality indicators that can be directly computed from the presented fingerprint image. Once computed, the indicators are mapped to a one dimensional quality axis (quality score) by means of classification.

In this work, the mapping from Quality Measures to some values on the quality axis

is approached in two ways. In the first approach, human subjective perception on fingerprint image quality is used as a guiding target for the classification process. The trained classifier should substitute human role in determining the quality level of the presented fingerprint image.

In the second approach, the classification on fingerprint quality is guided by average matching score of a fingerprint image. The philosophy behind the operation is: higher matching score implies that the fingerprint sample carries more valid features with respect to the fingerprint matcher used, and hence better quality relative to this matcher. This is also called matcher-specific quality in this context.

To study the effect of quality analysis on the fingerprint matcher, quality score is used as an additional input to the fingerprint matcher where we call this a quality-supplemented system. TOC performances of the original and the quality-supplemented fingerprint matchers are compared and reported. Our empirical study using a moderate size of data shows that quality-supplemented fingerprint system provides noticeable improvement in terms of Receiver operating Characteristic performance, although a very large margin of improvement is not anticipated.

List of Figures

Figure 1	A Typical ROC Plot with Two ROCs
Figure 2	A General Biometric System
Figure 3	Block Diagram of a Typical Fingerprint Verification System
Figure 4	Types of Minutiae
Figure 5	Thinning Process
Figure 6	A Typical Radial Basis Neural Network Structure
Figure 7	Four Fingerprint Sub-blocks (Uniformity)
Figure 8	Image Object and the 3x3 Mask(Clustering Factor)
Figure 9	mask centered at location (2,2) (Clustering Factor)
Figure 10	mask centered at location (4,4) (Clustering Factor)
Figure 11	A typical texture-like ridge block (Orientation Certainty)
Figure 12	Two full-sized fingerprint images with directions of $\tilde{E}_{max}$ computed for each image sub-block (Signal-to-Noise Ratio)
Figure 13	Signature along $\tilde{E}_{max}$ direction (Signal-to-Noise Ratio)
Figure 14	Image sub-blocks with DFT of the signatures along $\tilde{E}_{max}$ (Signal-to-Noise Ratio)
Figure 15	Image sub-blocks with orientation information (Curvature)

Figure 16	Fingerprint Image Sub-blocks of Different Qualities
Figure 17	Synthetic Fingerprint Images of Different Qualities
Figure 18	ROC with RMP order 6 (Experiment II)
Figure 19	ROC with RMP order 7 (Experiment II)
Figure 20	ROC with RMP order 8 (Experiment II)
Figure 21	ROC with RMP order 9 (Experiment II)
Figure 22	ROC with RMP order 10 (Experiment II)
Figure 23	ROC with RMP Orders 1-6 (Experiment III)
Figure 24	ROC with RMP Orders 1-7 (Experiment III)
Figure 25	ROC with RMP Orders 1-8 (Experiment III)
Figure 26	ROC with RMP Orders 1-9 (Experiment III)
Figure 27	ROC with RMP Orders 1-10 (Experiment III)
Figure 28	ROC with RMP Orders 2-6 (Experiment III)
Figure 29	ROC with RMP Orders 2-7 (Experiment III)
Figure 30	ROC with RMP Orders 2-8 (Experiment III)
Figure 31	ROC with RMP Orders 2-9 (Experiment III)
Figure 32	ROC with RMP Orders 2-10 (Experiment III)
Figure 33	ROC with RMP Orders 3-6 (Experiment III)
Figure 34	ROC with RMP Orders 3-7 (Experiment III)
Figure 35	ROC with RMP Orders 3-8 (Experiment III)

- Figure 36 ROC with RMP Orders 3-9 (Experiment III)
- Figure 37 ROC with RMP Orders 3-10 (Experiment III)
- Figure 38 ROC with RMP Orders 4-6 (Experiment III)

List of Tables

Table 1	ROC Classification Results for SOM with LVQ1 (Experiment I)
Table 2	Classification Results for RBFNN (Experiment I)
Table 3	Classification Results for Naïve Bayes (Experiment I)
Table 4	Classification Results for Support Vector Machine (Experiment I)
Table 5	Classification Results for Reduced Multivariate Polynomial (Experiment I)
Table 6	Optimum Order Selection (Experiment II)
Table 7	Optimum order selection for Matcher-based Quality Evaluation (Experiment III)

Chapter 1

Introduction

Each person in our society has his/her own unique identity. At the same time, we belong to different groups based on some characteristics. Some examples of such characteristics can be nationality, organization, military ranks, residential area and school of study. Such characteristics are always tagged on to one's unique identity such that a unique subject carrying multiple grouping memberships from different grouping criteria. In real life environment, we often rely on unique identity and group memberships in daily interaction.

As an example, consider a situation where a traffic police officer stops a car and request for identification card from the driver. After verifying driver's information through radio, the driver is asked to proceed. In this example, the officer first obtains driver's unique identity from the identification card. This identity is then used to obtain the group membership status of the driver in "law-offending group". The driver is cleared from the "law-offending group" and is thus not detained.

There are many other cases in life whereby we first try to obtain the unique identity of someone, and subsequently make use of some pre-knowledge to determine what the group membership of the subject is, from the identity. The process of uniquely

identifying someone, also known as authentication, must work in a reliable manner for the subsequent decision making to be in order. The work presented in this thesis aims to enhance such authentication accuracy through quality assessment which shall be covered in the following sections.

1.1 Need for Biometric Authentication

The most common and perhaps the most traditional way in authentication, is by an identification number assigned to each person. This number, however, cannot easily be verified against a subject. There are many disadvantages in using an identification document or a password alone. Identification document does not necessarily follow the owner everywhere and can be easily misplaced. On the other hand, the password or Functional Identification Number (FIN) number can be known to unauthorized personnel. Moreover, password can also be easily forgotten especially when there are so many of them to remember. These identities are thus “transferable” which implies that we cannot verify the true identity of the carrier without additional means.

Intuitively, an authentication process can be made more secured if one’s identity is tagged on to one’s physical characteristics. In other words, we can authenticate someone through his personal biological characteristics, which are not transferable and will follow him wherever he goes. Such a process is known as biometric authentication.

Biometrics is the measure of physical or behavioral characteristics of human being. A direct implication from biometric authentication’s non-transferability characteristic is that the authenticated target is the subject himself/herself instead of a

non-living object, such as an identification document. Features such as fingerprint ridges, palm prints, arteries layout, etc. do not change drastically and no misplacement can happen. Subject does not need to remember passwords for different applications and no more passes will be left behind due to forgetfulness.

Biometric Authentication has other advantages other than non-transferability. The biometric features that were applied cannot be forged or reproduced easily. The biometrics applied can be seen as an extensive coding presented in a peculiar way. For fingerprint, the coding can be the unique layout of ridge branches with risen and sunken area on skin surface. We also have iris and DNA recognition technologies which deal with differently structured iris pattern and DNA chain combinations. All these lead to a more secured authentication platform.

With the rapid advancement in technologies, biometric authentication is assisted by devices which allow easy capture of biometrics information with minimum inconvenience to subjects under query. Unlike password authentication which needs the subject to manually key in the remembered password, iris and face recognition system requires only some cooperation from the user in certain posture and information capture is done by some electrical sensing devices. Fingerprinting no longer needs inking for the process to be completed, instead this is done by using a fingerprint scanner which can be easily interfaced with a personal computer. The application of infrared imaging has also made capture of arteries layout a hassle-free process.

Before a biometric can be considered suitable for human authentication, the following aspects have to be justified [1, 2, 3].

- *Universality*: This characteristic should be found on everyone.

- *Uniqueness*: The difference in such characteristic between two different subjects should be distinguishable.
- *Permanence*: The characteristics should not change drastically over time or under different environment.
- *Collectability*: The characteristics should be quantitatively measurable.
- *Acceptability*: People should be willing to use such biometric system.
- *Performance*: this means the achievable authentication accuracy and the resource needed to achieve acceptable accuracy should be within a satisfactory range.
- *Circumvention*: Such a biometric system should not be hacked or tempered with easily.

So far, many biometrics have been utilized for authentication purposes. For physical characteristics we have iris, fingerprint, hand-geometry, palm-print, hand veins, etc. [1]. Other behavioral biometrics include signature, speech, gesture, and so on.

This thesis focuses on fingerprint biometric due to high popularity of the application as well as availability of large fingerprint image databases to us. The quality study can be further extended to other biometrics with some amendments.

1.2 Fingerprint Biometrics

1.2.1 Popularity of Fingerprint Biometrics

Being one of the earliest Biometrics technologies, fingerprint is an easily available identifier for each individual. Inked fingerprint image was captured on national identity card for this purpose. In those earlier days, authentication was done through

manual comparison of captured fingerprints and inked records by trained personnel. Hence, fingerprint could be the most successful authentication technique in those days partly due to the lack of technology for capturing samples of other biometrics.

There are a few factors which contribute to the popularity of the fingerprint biometric technology. As one of the main reasons, the inking method as well as the recent advancement in fingerprint sensor technology has made fingerprinting an easy task to perform with high consistency. Face recognition suffers from posture, expression and illumination problems. One's voice can also change considerably when the subject just awoken from sleep, having a sore throat and so on. It is also practically hard to ask someone to speak totally the same way as he did sometime ago. Fingerprint authentication, however, is relatively more consistent than voice biometrics. Although the quality of fingerprint image is subject to change according to the condition of fingerprint and user behavior, an averaged-quality fingerprint image will allow someone to be authenticated even in the dark or when the subject is ill. Moreover, the fingerprint pattern will not change considerably when someone grows old.

Thanks to the strong computation power available today, fingerprint authentication is almost immediate. This is in contrast to DNA authentication which shall take hours to complete. Being one of the earliest biometrics technologies, fingerprint has gained its user acceptance through its application over years. As one of the major concerns for private companies, a fingerprint sensor is inexpensive. As low as USD100, such a sensor is available to almost everyone.

1.2.2 General Concepts in Fingerprint Biometrics

(i) Verification vs. Identification

Someone is at your door. Looking out of the window, you saw the face of the visitor. By trying to recall the faces of the friends and relatives you know, you finally output an answer, whether you don't know him, and if you know him, what is the name, etc. This is a simple identification process and such a process is one-to-many. In identification systems, a biometric signature of an unknown person is presented to a system. The system compares a new biometric signature with the biometric signature of known individual in databases. From the comparison, the system reports success or failure in identifying this unknown person, together with the identity if the identification is successful [4].

If, however, your mother has told you that the person at the door seems to be Susan. Looking out of the window you reply your mum saying that "Yes, it is Susan" or "No, it is not Susan", this is a typical one-to-one verification process. In verification systems, a user presents a biometric signature and a claim of a particular identity to the biometric signature. The algorithm either accepts or rejects the claim. Alternatively, the algorithm can return a confidence measurement of the claim's validity.

An identification system is generally more user-friendly as it does not need the end-user to produce any document at the time presenting his/her biometric signatures to the system. The system does not have any assumption on the identity of the signatures presented but merely estimates the results based on stored database entries. On the other hand, a verification system will rely on some pre-knowledge on ones identity. Such pre-

knowledge is normally based on an accompanied identification card or document. The authentication time for a verification system is shorter than identification system.

(ii) Performance Evaluation

Any authentication system requires two steps: enrolment and verification. In a fingerprint authentication system, enrolment process requires users to submit fingerprint image samples to the system. The system would then perform feature extraction and generate a template to be stored. Once a user has enrolled in the system, verification can take place. This would involve user submitting his fingerprint image sample to the system for feature extraction and followed by template matching between the newly submitted entry and the users' fingerprint images stored in database. It is important to note that none of the biometrics is known to be completely error free. The implementation of the biometrics system can also be erroneous. Ambiguity and algorithm imperfectness can occur at every stage of the processing. How frequent the system makes an incorrect decision is an important parameter to benchmark systems.

The four basic error rates employed in a fingerprint identification system are summarized below. While a false or imposter matching refers to an unregistered user

- False Acceptance Rate (FAR): The probability that a false match occurs in such a way that an unauthorized user (imposter matching) is erroneously accepted as an authorized user by the system.

- Authentic Acceptance Rate (AAR): The probability that a true match occurs in such a way that an authorized user (genuine matching) is correctly accepted by the system.
- False Rejection Rate (FRR): The probability at which an authorized user (genuine matching) is erroneously rejected as an unauthorized user by the system. Note that $FRR + AAR = 1$.
- Correct Rejection Rate (CRR): The probability at which an unauthorized user (imposter matching) is rejected by the system. Note that $CRR + FAR = 1$.

Genuine matching is referred to the case whereby two fingerprint images from the same finger are compared (matched) against one another. On the other hand, imposter matching is given by matching of two fingerprint images from different fingers. Each of the error rates describes different aspects of matching performance. However, as these performance benchmarks are not independent of one another, system tuning for optimum performance of one error rate could result in poorer performance of another. A graphical representation known as Receiver Operating Characteristics or ROC curves is normally engaged to study and compare overall system performance.

- Receiver Operating Characteristics (ROC) Curve: A curve that plots AAR against FAR. By changing the security setting for a given system, we can obtain various AAR and FAR data points to form the plot. The curve exhibits a monotonically increasing trend which indicates that when the system security setting is lowered to allow more genuine user to be accepted (higher AAR), more imposter will also

be allowed to get through (higher FAR) due to the lowered threshold. On the other hand, when the system is more secured to have low FAR, more genuine user will be rejected erroneously and thus higher FRR. There is thus a trade-off between FRR (1-AAR) and FAR which is more obvious from the ROC plot.

Figure 1 : A Typical ROC Plot with Two ROCs

Figure 1 shows two ROCs plotted in a single diagram. The horizontal axis of the diagram represents FAR and it is normally in logarithmic scale for clearer representation. The vertical axis of the diagram represents AAR. AAR has a monotonically increasing relationship with the FAR and with the increase in system security setting. From the diagram, the blue ROC is always above the one in red reveals that ROC in blue represents a more reliable system. This can be understood by the fact that blue ROC has a better AAR no matter what is the value for FAR. ROC is an effective way of comparing performance between multiple biometric systems.

1.2.3 Common Problems in Fingerprint Biometric Systems

Automatic fingerprint identification system (AFIS) and automated fingerprint verification system (AFVS) are integrated systems that can handle fingerprint enrolment as well as identification/verification with minimum human attention. Enrolment is the process of

adding one's fingerprint record into the database while identification/verification is to perform feature matching between the query image and database entries/entry. Accessing rights to the facilities (e.g. door, computer system, etc.) will be issued according to the matching result. However, the identification as well as verification performance of such system is very sensitive to the quality of the captured fingerprint image. Since AFIS and AFVS are expected to work independently and exposed to potentially large number of users, the fingerprint sensor that is attached to the system is possibly subjected to inappropriate use. This includes the applying of dry, wet or dirty finger on the sensor. In addition, some CMOS type of sensors have problems of residue and background noise. Although optical sensors have generally better image quality, longer capture time makes it likely to capture a partial fingerprint image when a user removes his finger from the system before a complete capture. Aging will also degrades one's fingerprint quality [5]. All of these lead to "poor quality" images being captured. A poor quality fingerprint image is a result of genuine finger that is captured with noise (polluted fingerprint image) or with insufficient information (partial fingerprint image). While residual images generate false features that might be able to gain access from the system, partially detected or highly noisy true fingerprint can cause the false rejection of an authorized user. As a result, the system's performance is degraded. Therefore, it is vital for the AFIS and AFVS systems to gain information on the quality and validity of the captured fingerprint images so that they can work independently in a reliable manner.

1.3 Fingerprint Image Quality

1.3.1 Motivation and Problem Statements

Fingerprint Image Quality Analysis plays the role of estimating the usefulness of fingerprint image captured. Although the relationship between the quality of a query image and its corresponding reliability of matching result returned by an AFIS system is complex, Austin Hicklin [7] found that applying fingerprint quality measure in predicting the probability for failure in matching can be done with some accuracy. On the other hand, fingerprint quality measure has not been widely applied and there are no formal standards for single-finger image quality measurement or quality control [8]. It is thus the objective of this project to establish some methodologies, which are feasible in examining fingerprints' quality. A Fingerprint Quality Evaluation Engine will be developed to automatically evaluate fingerprint image's quality and output a fingerprint *Quality Score*. It is also the motivation of this project to study the effect of such *Quality Score* on fingerprint matching accuracy. The ultimate objective is to enhance the matching accuracy through the inclusion of fingerprint quality information in the matching process.

1.3.2 Use of Fingerprint Image Quality

Following discussion above, it might be feasible to develop a Fingerprint Quality Evaluation Engine (FQEE) to evaluate how suitable the captured sample is for fingerprint matching application. Accuracy of a fingerprint matching application suffers from poor quality captures in both enrolment and identification/verification process. In our case, fingerprint quality analysis aims to predict the matching accuracy of a given fingerprint image. A “higher quality” candidate refers to a captured fingerprint image contributing to higher matching accuracy by carrying more valid fingerprint characteristics during image capturing process. If the image is captured for verification or identification purposes, the candidate should be more inclined to being accepted for the case of true match and to be rejected otherwise. The FQEE evaluates and reports the quality level of a captured fingerprint image by mean of *Quality Score*. When incorporated with an AFIS, such analysis should play a role to filter off low quality images, which will contribute directly to a lower false acceptance rate than the original system. Lower false rejection rate is also achievable by trading-off of false acceptance rate. Other than directly using Quality Score as a standalone quality preprocessing filter to reject low quality images, such a Quality Score can be used as an input to the segmentation algorithm to determine background or low quality area, minutiae detection algorithm to evaluate the confidence level of the extracted minutiae, or matching module to provide additional information for the decision making process. All of the above lead to a more reliable biometric system. A typical diagram representation of quality-enabled biometric system is depicted in Figure 2 below.

Figure 2 : A General Biometric System (Extracted from [6])

The scenarios described above are many-finger-to-one-sensor cases whereby multiple fingers were applied to one particular working sensor to carry out the fingerprint quality evaluation. On the other hand, a one-finger-to-many sensor mode of operation is another model that the same FQEE can be put into use. Under this model, one finger is applied on different fingerprint sensors to evaluate the capturing capabilities of each sensor. A multiple number of fingers used in the evaluation will construct a statistical performance study of fingerprint sensors' capabilities.

1.3.3 Scope of the Thesis

The scope of this thesis is summarized as follows:

- To define several quality indicators that can be directly computed from a given raw fingerprint images. The indicators are known as Quality Measures.
- To implement algorithm that evaluates Quality Measures automatically from the fingerprint image.
- To propose and implement methodologies to map the extracted Quality Measures to Fingerprint Quality Scores
- To study the performance variation of fingerprint matching accuracy with the inclusion of Fingerprint Quality Score in the matcher.

1.4 Contributions of this Thesis

Main contributions of this work are listed as follows:

(i) Development of Novel Quality Measures

From structural and signal point of view of a fingerprint image, four quality measures were defined. Each of the defined quality measures caters for some aspects of the fingerprint quality but each might not work well for all fingerprint images when used alone. By combining all four measures, they give a more comprehensive estimation for the general spread of fingerprint images.

(ii) Proposal of a Subjective Quality Evaluation Scheme

Quality scores were assigned subjectively to each fingerprint image based on human perception. Several classifiers were used to train the mapping between quality measures and quality scores, and results reported with their generality.

(iii) Proposal of a Matcher-based Quality Evaluation Scheme

Matching performance of a given fingerprint sample is estimated using a quality evaluation engine supervised by matching score. 582660 cross-matching pairs from 36 persons, 6 fingers per person and 5 fingerprint impressions per finger are generated and tested to verify the validity of the proposed procedures.

Chapter 2

Literature Review

2.1 Automatic Fingerprint Authentication Systems (AFIS)

Fingerprint matching was carried out by trained personnel in the past. The task can be quite tedious due to detailed structures on the fingerprint surfaces. In the past decades, however, the need for an automatic biometric authentication system has led to the development of an automated fingerprint authentication system.

Figure 3, which is extracted from [9], showcase a typical fingerprint verification system. The whole process starts with fingerprint image acquisition using a fingerprint sensor. The sensor captures digitized format of ones fingerprint image and the image is sent to the processing system (PC or standalone processing unit) for storage as well as further processing. Feature Extraction is the phase to extract useful features for comparison between fingerprint images. The features are normally much smaller in dimension as compared to the size of the entire fingerprint image. This provides a compact version of fingerprint representation which is machine resource friendly. The features should be carefully selected such that the uniqueness of the fingerprint images

was maintained. The reliability of the system is heavily dependent on the effectiveness of feature extraction algorithm. Imperfection in the developed feature extraction algorithm will result in ambiguity between different fingerprint images and thus lowered accuracy.

Figure 3 : Block Diagram of a Typical Fingerprint Verification System

What could be missing from the diagram in Figure 3 is an image enhancement process prior to feature extraction. The enhancement process aims to filter off noise while maintaining ridge and valley structures. Due to its importance, a lot of work has been carried out in the field of image enhancement. Most of the works try to filter off discontinuity along the ridge flow while maintaining ridge/valley interchange pattern orthogonal to the ridge flow. Gabor Filter is often used as an oriented filter to achieve the above mentioned task in many of the previous works [10][11]. Takahiro Nakamura et. al. make use of the fact that ridges are multiple parallel lines and they implement a parallel ridge filter[12, 13, 14, 15, 16] which achieves directional filtering by using a Directional

Filter Bank. There are a lot of other published works on image enhancement using the directionality characteristics [17]-[24].

During the registration process, feature extraction algorithm retrieves the salient features from each fingerprint image and stores each record in the system database. It is also useful to associate each of the records with individual particulars like name, ID, age, etc. When a new fingerprint sample is presented to the system, the same feature extraction process is carried out and the retrieved features are now compared against those in the stored records. The matching algorithm will output a *Matching Score* to indicate the similarity between the two matching targets. Finally, the matching target from the stored records that has the highest above-threshold matching score with the presented fingerprint sample is return as the identified individual. The individual's particulars which are tied to the database record earlier can thus reveal the identity of the subject in query.

Subsections 2.1.1-2.1.3 describe several feature extraction and matching algorithms. The various algorithms are grouped into Minutiae-based, non-Minutiae-based and Hybrid methods.

2.1.1 Minutiae-based Methods

Human experts use “local discontinuities of the ridge flow pattern” to extract salient features and identify fingerprint images [6]. These discontinuities are called minutiae. There are two types of minutiae commonly used, which are namely ridge endings and ridge bifurcations. Figure 4(a) shows a fingerprint minutia which is a ridge

ending point. Ridge bifurcation is illustrated in 4(b) where two ridges merged into one. The most common feature-based techniques rely on minutia matching. The problem then becomes a graph or point pattern matching problem. The method is inspired by manual fingerprint matching procedure. Although approximately 50 to 150 minutiae are present in an image, 10 minutiae matches are generally considered sufficient to determine that the fingerprints are from the same finger.

Figure 4 : Types of Minutiae

In other words, instead of the global ridge-valley flow, any fingerprint image is represented by its 2D minutiae points' distribution in a minutiae-based matching algorithm. Each minutia can be accompanied by its attributes such as type (ending or bifurcation), orientation of the nearby ridges and structure of the nearby minutiae. This information is able to improve matching accuracy. To extract useful minutiae data from a digitized fingerprint image, there are following two main methods.

Binarization and Thinning

Being a traditional method to obtain minutiae data from the original captured image, the algorithm aims to convert the few-pixel-width ridges into a single-pixel width

ridges on a binarized image. Figure 5 (a) shows a digitized capture of a portion of fingerprint image. The algorithm first binarizes the image into “black and white” by using a suitable threshold value or an adaptive thresholding technique [25]. Thinning operation is then carried out to reduce the “thickness” of the ridges bit by bit until a skeletal image is formed. It is then straight forward to obtain minutiae through ridge following algorithm. Thinning is a very computation intensive process and takes up a considerable computation time.

(a) Original Captured Image

(b) Processed Skeletal Image

Figure 5 : Thinning Process

Ridge Tracing

Instead of going through thinning and then ridge following, Jiang *et. al.* [26] and D. Maio *et. al.* [27] use ridge following or ridge tracing algorithm to directly trace the enhanced captured image for skeletons as well as minutiae. There are a few advantages in this method:

- Binarization and Thinning are extremely time consuming and computation intensive.
- Binarization causes loss of useful information.
- Binarization can be erroneous due to different qualities of the captured fingerprint images.

All these factors result in ridge tracing being a faster and more efficient.

After the minutiae data is successfully retrieved, it is now important to identify which fingerprint images were identical. Bebis *et. al.* used an approach based on the Delaunay triangulation for indexing and matching fingerprints [28]. Delaunay triangulation is performed on all minutia points. Each triangulation face is characterized by invariants based on edge lengths and internal angles. An indexing algorithm is then used to determine the best matches in a database. A match is evaluated by finding the similarity transformation that leads to the highest correspondence between the faces of the two fingerprints. The best matches are refined by computing the optimal affine transformation and evaluating the number of matching minutiae.

Ratha *et. al.* matches fingerprints using a fingerprint representation called Minutia Adjacency Graph (MAG) [29]. Edges are formed between minutiae when the distance between them is less than a threshold. Each edge is characterized by the two vertices it connects, by its length and orientation, and by the number of ridges it crosses. Matching proceeds by first attempting to match the star-shaped neighborhood of vertices. Reliable matches obtained with this method are then used to extend the matches with relaxed rules.

Jiang *et. al.* [30] matches fingerprint minutiae by using both local and global structures. The local structures of the fingerprint image describe a rotation and translation invariant feature of a minutia into its neighborhood. This is used to find the correspondence for each of the minutia in a minutia set. The matching process is made elastic by a bounding box to tolerate the deformation during the fingerprint capture

process. Matching certainty level based on the local structure similarity level ensures that the global match presents between two fingerprint images.

2.1.2 Non-minutiae Based Methods

In contrast to the minutiae point based matching, non-minutiae based matching makes a graphical comparison of the two templates and determines a measure of the difference. Non-Minutiae techniques rely on the correlation of image segments for matching. The larger the difference the less likely the prints match.

Koichi Ito *et. al.* uses a Phase-Only Correlation (POC) [31-33] function (or simply a “phase-correlation function”) in a fingerprint matching algorithm [34]. The POC technique has been successfully applied to high-accuracy image registration [35-37] in computer vision domain.

A. K. Jain *et. al.* perform fingerprint matching by using filter-based algorithm. The proposed algorithm uses a bank of Gabor filters to capture both local and global details in a fingerprint as a compact fixed length finger code. The fingerprint matching is based on the Euclidean distance between the two finger codes and hence results in shorter computation time.

There are many other non-minutia image or graph based methods found in [38-41]. Generally speaking, minutiae-based methods do not utilize a significant portion of the richly discriminatory information available from a fingerprint image. Therefore, the uniqueness of the template representation of the fingerprint image is weakened. However, minutiae-based templates do have relatively smaller template size compared to non-

minutiae-based counterparts. This is a direct impact from the difference in point based and graphical/image level based templates. [42] comments that the template size for a non-minutiae based template cannot be easily controlled or compressed as compared to a minutiae based template. The reduction in template size could also contribute to a faster searching speed. Depending on the non-minutiae-based algorithm used, when physical changes like scar or blemish affect the fingerprint region, a new template might be needed. On the other hand, minutiae-based methods are more immune to such changes due to the fact that only a portion of the total minutiae is used for the matching process.

2.2 Fingerprint Image Quality Measures

2.2.1 Background

One of the earliest international efforts in defining biometrics quality comes from BIOAPI consortium[65]. BIOAPI consortium was founded to develop a biometric Application Programming Interface (API) that brings platform and device independence to application programmers and biometric service providers. BIOAPI Consortium has a current group of over 120 companies and organizations. BIOAPI Consortium developed a specification and reference implementation for a standardized API that is compatible with a wide range of biometric application programs and a broad spectrum of biometric technologies. BioAPI Version 1.1 specifications address the objectives of biometric quality as follows:

- The primary objective is to have the quality information to inform the application how suitable the biometric sample is for the purpose specified by the application.
- The secondary objective is to provide the application with relative results (e.g. current sample is better/worse than previous sample).

BioAPI Version 1.1 specifications [6] clearly states that “The performance of biometrics varies with the quality of the biometric data.” as well as “a universally accepted definition of quality does not exist.” The quality score reported are purpose dependent. The purposes can be biometric capture for enrollment/verification, biometric capture for enrollment/identification, biometric capture for verification, etc. In our context, the quality score should estimate the performance of such capture of a fingerprint image in a fingerprint identification system. In other words, a high quality fingerprint image should capture more valid fingerprint features and reflect high matching score in case of true matches and low matching scores in false match cases.

To summarize, fingerprint image quality is an indicator to estimate the accuracy performance of a captured fingerprint image for enrollment/verification, enrollment/identification, verification alone and so on. Notice that the image quality is also matching algorithm dependent. One high quality fingerprint image for a particular matching algorithm can be a low quality one for on another.

BioAPI sets the quality scores in the range of 0-100 with the following interpretation [6]:

- 0-25: UNACCEPTABLE: The biometric data cannot be used for the purpose specified by the application (BioAPI_PURPOSE). The biometric data must be replaced with a new sample.
- 26-50: MARGINAL: The biometric data will provide poor performance for the purpose specified by the application and in most application environments will compromise the intent of the application. The biometric data should be replaced with a new sample.
- 51-75: ADEQUATE: The biometric data will provide good performance in most application environments based on the purpose specified by the application .The application should attempt to obtain higher quality data if the application developer anticipates demanding usage.
- 76-100: EXCELLENT:: The biometric data will provide good performance for the purpose specified by the application. The application may want to attempt to obtain better samples if the sample quality (BioAPI_QUALITY) is in the lower portion of the range (e.g. 76, 77,...) when convenient (e.g. during enrollment).

Despite the need for a quality evaluation engine, quality itself is conceptual and there has not been much effort in defining fingerprint quality and developing evaluation engines. The desire to improve the accuracy of AFISs motivates the need for FQEE. However, different AFISs have different low quality image toleration capabilities. Not only some AFIS will be more immune against low quality fingerprint input image than the others, but each AFIS may also respond differently to different types of fingerprint

image imperfections. Thus, it is nearly impossible to develop a common one-dimensional coordinate system of quality measure for different AFISs.

Researchers approach fingerprint image quality quantification relying on general understanding of image quality and characteristics of fingerprint images. Directional fields formed by ridge and valley structures of a fingerprint image are the main features used in the few on-going and past efforts in the investigations of fingerprint image quality.

2.2.2 Direction-based Method

In [43], Bolle *et. al.* divide a fingerprint image into blocks of pixels. Each block is marked as directional or non-directional by searching for sufficiently large image gradient in some pre-defined directions. The blocks are also determined to be within the foreground or background of the image. Contiguous regions of blocks that are directional in the foreground are selected. The image quality measure is given by the area ratio of the selected contiguous to the total foreground area. A threshold is used to judge if a fingerprint image is of good quality.

Shen *et. al.* [44] applied Gabor filter to image sub-blocks, and concluded that a good quality block with clear repetition of ridge and valley pattern can be identified by the outputs of a Gabor filter bank. The authors make use of the fact that Gabor filter is a directional filter. The concentration of signal strength on one or a few filter bank output(s) implies that there is a strong directional field.

Kang *et. al.* [45] applied direction contrast method in their image quality measure. They applied three underlying ideas to reflect good fingerprints:

- (i) high contrast between ridges and valleys
- (ii) foreground for most of the image area
- (iii) little scar or latency.

The directional contrast method computes gray-value gradient of the image sub-blocks in eight different directions. The existence of a high contrast gradient in one of the eight directions indicates that the image sub-block has higher image quality level.

Three methods above make use of the local orientation information of the fingerprint image. However, as the gray level ridge and valley structure of the fingerprint image contains much more information than the orientation and a fingerprint image exhibits a global smooth ridge flow, the local directional strength alone might not be sufficient to measure the quality of fingerprint images.

2.2.3 Sinusoidal Method

Hong *et. al.* [46] classifies a sub-block in an input fingerprint image as recoverable or unrecoverable region. Classification of blocks into recoverable and unrecoverable categories is performed based on the amplitude, frequency as well as variance that characterize the sinusoidal-shaped wave formed by local ridge and valley patterns. The method evaluates more aspects of the fingerprint image than the previous few methods. The former methods will give a “high quality” score whenever there is a strong localized directional strength. However, as fingerprint sub-blocks are more than just a simple sinusoidal wave, a sub-block that contains minutiae or core will cause the modeling to fail and the sub-block will be reported as unrecoverable or bad block.

2.2.4 Other Methods

Ratha and Bolle [47] proposed a method for image quality estimation from a wavelet compressed fingerprint image. This is beneficial if the image to be processed is in Wavelet-packet Scalar Quantization (WSQ) compressed format. However, in a live automatic fingerprint identification system, the images are not commonly in the WSQ format.

2.3 Summary

Most of the fingerprint image quality analysis algorithms discussed above are based on the directionality characteristics of local fingerprint ridge-valley structures. In addition to that, majority of the methods are relying on single feature from fingerprint image which do not provide a well-rounded analysis. Fingerprint image quality is expected to be multi-dimension as there are various aspects of qualities.

We propose several novel quality measures which analyze the fingerprint image quality in some different ways. By making use of classification tools, we interpret the proposed quality measures into some useful quality performance indexes. The interpreted quality information is then used to enhance fingerprint authentication performance.

Chapter 3

Pattern Classification Tools

Pattern classification tools are applied in this project with the following objectives:

- Quality is multi-dimensional and involves multiple quality measures that describe different aspects of qualities. A multiple inputs single output pattern classification tool combines different quality measures into useful quality score.
- Each quality measure does not increase monotonically with the increase in quality. We need classification tool to map different regions of the quality measure scale to different levels of quality score.
- To include quality score as one of the inputs to the fingerprint matcher, another classification tool is needed to combine inputs from quality score and matching score. The output from this classification tool is the matching results.

Five commonly used classification tools are described in this chapter and are used in this project.

3.1 Self-Organizing Map (SOM) with Learning Vector Quantization (LVQ)

Kohonen developed SOM in the early 1980s [48]. SOM can be visualized as a sheet-like neural-network array that will arrange among itself according to some meaningful nonlinear coordinate system. It is a data visualization technique, which can reduce the data dimensions such that it is easier to be visualized by human in 2-D or 3-D. In addition to reducing dimensions, SOM also groups similar items together. The learning process of SOM is competitive and unsupervised, meaning that no teacher is needed to define the correct output. The cells of the map will become specifically tuned to various input signal patterns or classes of patterns in an orderly fashion through this learning process. The first application area of the SOM was speech recognition, or perhaps more specifically, speech-to-text transformation.

For a two dimensional self-organizing map, all cells within the map are first initialized with a real feature vector

$w(i, j) \in R^n$, where i and j are the indices of the cell locations

$w(i, j) \neq w(m, n)$, $\forall m, n$ and

$i \neq m$ or $j \neq n$.

At the same time, the set of input samples is described by

$x(t) \in R^n$ where t is the index of the sample, or the discrete-time step.

$w(i,j)$ and $x(t)$ have the same number of elements. The initial values of the components of the initializing feature vector $w(i,j)$ may be selected at random or initialized in some orderly fashion.

Any input vector $x(t)$ is now mapped into the location $w_c(i,j)$ which is the nearest according to a distance metric. The winner $w_c(i,j)$, together with its neighboring cells in the map are updated towards the input vector with some weight. The input vectors are presented for a few epochs and the process is summarized below:

An input vector $x(t)$ is compared with all vectors within the map $w(i,j)$. The best-matching cell $w_c(i,j)$ is called the winner.

$$|w_c(i,j) - x(t)| \leq |w(i,j) - x(t)| \quad \forall i,j \quad (1)$$

The feature vector carried by the winner, and a number of its neighboring cells in the map are changed towards the input vector according to the learning principle specified.

$$w_{new}(i,j) = w_{old}(i,j) + \mu(t)\Psi(t)[x(t) - w_{old}(i,j)] \quad (2)$$

Where $\Psi(t)$ is called the neighborhood function, and

$\Psi(t) = 1$, when cell (i,j) falls within neighborhood of the winner node.

else $\Psi(t) = 0$

At the beginning of the learning process the radius of the neighborhood is fairly large, but it is made to shrink gradually during learning process. This ensures that the global order is obtained already at the beginning, whereas towards the end, as the radius gets smaller, the local adaptations of the model vectors in the map will be more specific.

The factor $\mu(t)$ is the scalar gain between 0 and 1, which also decreases during the learning process.

The basic idea underlying SOM learning process is that, for each sample input vector $x(t)$, the winner and the cells in its neighborhood are changed closer to $x(t)$ in the input data space. During the learning process, individual changes may be contradictory, but the net outcome in the process is that ordered values for the $w(i,j)$ emerge in the lattice array.

Unsupervised training process above arranges the cells according to the overall statistical density function of the input. The next phase is to determine the labels of the feature vectors, by presenting our input samples $x(t)$ with known classification, and assigning each cell of the map $w(i,j)$ with class label by majority voting, according to the frequency with which each $w(i,j)$ is closest to the calibration vectors of a particular class.

This Learning Vector Quantization process is a supervised training process functions to pull the feature vectors away from the decision surfaces to demarcate the class borders more accurately. Again, the input vectors are presented iteratively, applying the updating algorithms:

$$\begin{aligned} w_{c,new}(i,j) &= w_{c,old}(i,j) + \alpha(t)[x(t) - w_{c,old}(i,j)] && \text{If } x \text{ is classified correctly,} \\ w_{c,new}(i,j) &= w_{c,old}(i,j) - \alpha(t)[x(t) - w_{c,old}(i,j)] && \text{If } x \text{ is classified incorrectly,} \end{aligned} \quad (3)$$

$$w_{k,new}(i, j) = w_{k,old}(i, j) \quad \text{for } k \neq c.$$

$\alpha(t)$ is a scalar gain between 0 and 1, which is decreasing monotonically in time.

This algorithm tends to reduce the point density of the $w(i, j)$ around the Bayesian decision surfaces. After training, any new input $x(t)$ is classified using the “nearest neighbor” principal by comparing $x(t)$ with $w(i, j)$. $x(t)$ is classified the same as its nearest neighbor from $w(i, j)$.

3.2 Radial Basis Function Neural Network (RBFNN)

An RBFNN is composed of receptive units (neurons), which act as the operators providing the information about the class to which the input signal belongs. Although the architectural view of an RBFNN is very similar to an ordinary feed forward neural network, the hidden neurons of an RBFNN possess basis functions to characterize the partitions of the input space. Each neuron in the hidden layer provides a degree of membership value for the input pattern with respect to the basis vector of the receptive unit itself. The output layer is also comprised of neurons.

Figure 6 : A Typical Radial Basis Neural Network Structure

An RBFNN, as shown in Figure 6 above, can be considered as a mapping of $Rr \rightarrow Rs$. In our context, $\mathbf{P}$ is the input vector and $C_i (1 \leq i \leq u)$ is the center of the network. The output of each RBF unit is as follows:

$$R_i(P) = R_i(\|P - C_i\|) \quad i=1, \dots, u \quad (4)$$

where $\|\bullet\|$ indicates the Euclidean norm in the input space. Usually, the Gaussian function is preferred among all possible radial basis functions due to the fact that it is factorizable. Hence

$$R_i(P) = \exp \left[-\frac{\|P - C_i\|^2}{\sigma_i^2} \right] \quad (5)$$

where σ_i is the width of the i^{th} RBF unit. The j^{th} output $y_j(P)$ of an RBFNN is

$$y_i(P) = \sum_{i=1}^u R_i(P) \times w(j, i) \quad (6)$$

where $R_0=1$. $w(j, i)$ is the weight or strength of the i^{th} receptive field to the j^{th} output and $w(j, 0)$ is the bias of the j^{th} output neuron. The outputs of an RBF neural classifier are characterized by a linear discriminant function. Consequently, the performance of an RBF neural classifier strongly depends on the separability of classes in the u -dimensional space generated by the nonlinear transformation carried out by the u RBF units.

3.3 Naïve Bayes

Naïves Bayes is a simple class-conditional classifier. The main assumption underlying the naïve Bayes classification technique is: the attribute values of an example are conditionally independent from each other. In other words, the probability of observing all the attributes together is their product. This is a very strong assumption and therefore may not be realistic. However, Naïve Bayes classifier can still yield good prediction performance. Frank from Department of Computational Linguistics and Phonetics, Saarland University [49] summarizes the properties of Bayes Classifiers as follows:

Incrementality

With each training example, the prior and the likelihood can be updated incrementally.

Robust to errors.

Combines prior knowledge and observed data. Prior probability of a hypothesis is multiplied with probability of the hypothesis given the training data.

Probabilistic hypotheses

Outputs are not only a classification, but a probability distribution over all classes.

Meta-classification

The outputs of several classifiers can be combined by multiplying the probabilities corresponding to a given class.

Recent interest in Naïve Bayes classifier includes text-categorization and anti-spam filtering [50][51][52].

Bayes Rule

If we have a hypothesis h and data $\mathbf{D}$ which bears on the hypothesis, then:

$$P(h \mid \mathbf{D}) = \frac{P(\mathbf{D} \mid h)P(h)}{P(\mathbf{D})} \quad (7)$$

where,

$P(h)$: independent probability of h : prior probability

$P(\mathbf{D})$: independent probability of $\mathbf{D}$

$P(\mathbf{D} \mid h)$: conditional probability of $\mathbf{D}$ given h :likelihood

$P(h \mid \mathbf{D})$: posterior probability or conditional probability of h given $\mathbf{D}$.

Maximum A Posteriori

Following Bayes Rule above, we can compute a hypothesis to maximize $P(h \mid \mathbf{D})$:

$$\begin{aligned}
h_{MAP} &= \arg \max_{h \in H} P(h \mid D) \\
&= \arg \max_{h \in H} \frac{P(D \mid h)P(h)}{P(D)} \\
&= \arg \max_{h \in H} P(D \mid h)P(h)
\end{aligned} \tag{8}$$

where H is the set of all hypotheses. $P(D)$ can be dropped at the last line of expression above as the probability of the data is constant and independent of the hypothesis.

Maximum Likelihood

We can further simplify the posterior computation by assuming all hypotheses are equally probable, i.e. $P(h_i) = P(h_j)$ for all $h_i, h_j \in H$. The expression of maximum likelihood hypothesis is given by:

$$h_{ML} = \arg \max_{h \in H} P(D \mid h) \tag{9}$$

Naïve Bayes Classifier

For feature vectors that consist of multiple attribute values $(a_1, \dots, a_n)$ and the classification targeting on finite set of classes V , the most probable class V_{MAP} formed by Bayes Rule is as follows:

$$\begin{aligned}
V_{MAP} &= \arg \max_{v_j \in V} P(v_j | a_1, a_2, \dots, a_n) \\
&= \arg \max_{v_j \in V} \frac{P(a_1, a_2, \dots, a_n | v_j) P(v_j)}{P(a_1, a_2, \dots, a_n)} \\
&= \arg \max_{v_j \in V} P(a_1, a_2, \dots, a_n | v_j) P(v_j)
\end{aligned} \tag{10}$$

Now we apply the independence assumption that the attribute values are conditionally independent given the target value:

$$P(a_1, a_2, \dots, a_n | v_j) = \prod_i P(a_i | v_j) \tag{11}$$

and Naïve Bayes classifier is given by:

$$V_{NB} = \arg \max_{v_j \in V} P(v_j) \prod_i P(a_i | v_j) \tag{12}$$

The independence assumption of Naïve Bayes estimates $P(a_i | v_j)$ instead of $P(a_1, a_2, \dots, a_n)$ which greatly reduces the number of parameters. An unseen instance is classified by identifying the class that maximizes the posterior.

3.4 Support Vector Machine (SVM)

While conventional classifiers follow the empirical risk minimization principle (i.e. an error measure based on the training set), Support Vector Machines [57] follows the principle of structural risk minimization. This principle states that good generalization ability can be achieved by minimizing the bound on the generalization error.

Let the data set D , which consists of N data points, be divided into two classes labelled as +1 and -1 respectively. The function that maps the data points to their class labels can be expressed as:

$$f_{SVM}(\alpha, x) = \text{sgn}\left(\sum_{i=1}^N \alpha_i y_i K(x_i, x) + b\right), \quad (13)$$

where $K(x, y)$ is a positive definite symmetric function called the kernel function. $\text{sgn}(\cdot)$ is the sign function and b is a bias estimated on the training set. The parameter α is the solution of the following quadratic programming (QP) problem:

$$\left\{ \begin{array}{l} \max_{\alpha} J(\alpha) = \sum_{i=1}^N \alpha_i - \frac{1}{2} \sum_{i=1}^N \sum_{j=1}^N \alpha_i \alpha_j y_i y_j K(x_i, x_j) \\ \text{with the constraints:} \\ \sum_{i=1}^N \alpha_i y_i = 0 \quad \text{and} \quad 0 \leq \alpha_i \leq C, i = 1, 2, \dots, N \end{array} \right. \quad (14)$$

In non separable case, the constant C must be set to a given value. Choosing a value for C can be done through an empirical search like cross-validation.

The kernel function $K(x, y)$ defines the nature of the decision surface that

separates the data. This function should satisfy some constraints in order to be applicable (Mercer's conditions [58]). A typical and commonly used kernel is the polynomial kernel $K(x, y) = (\gamma x^T y + 1)^d$, where d is a positive integer defining the order of the polynomial, γ is a real number that normalize the inputs. In applying SVM with polynomial kernel, the parameters d , γ , C (so called 'hyper parameters') should be defined (e.g. via cross-validation) before classifying unknown data.

The modification of SVM for multi-class case is done through integrating many single-output SVM classifiers in one-versus-the-rest scheme [58] or pairwise scheme [59]. In our experiments, a SVM Matlab toolbox [60] which has already implemented SVM with polynomial kernel for multi-class case is used.

3.5 Reduced Multivariate Polynomial (RMP)

Grounded on Weierstrass's approximation theorem, the Multivariate Polynomial (MP) possesses the universal approximation capability (see e.g. [61, 62]). A general form of MP is a linear combination of all possible polynomial (product) terms $x_1^{n_1} x_2^{n_2} \dots x_l^{n_l}$ with

$n_1, n_2, \dots, n_l$ vary such that $\sum_{j=1}^l n_j \leq r$. The number r is the degree of the polynomial and K

is the total number of weighting parameters α_j (i.e. the number of product terms).

However, a full multivariate polynomial faces the problem of parameter explosion. The number of parameter, K [62] is given by

$$K = \binom{l+r}{r}, \quad (15)$$

which grows exponentially as l and r increase. In [63, 64], a reduced multivariate polynomial model, which has much less parameters while keeping crucial polynomial terms, was proposed as follows:

$$\begin{aligned} f_{RM}(\alpha, x) = & \alpha_0 + \sum_{k=1}^r \sum_{j=1}^l \alpha_{kj} x_j^k + \sum_{k=1}^r \alpha_{rl} + k \left(\sum_{j=1}^l x_j \right)^k + \\ & \sum_{k=2}^r \left(\sum_{i=1}^l \alpha_r(l+1) + (k-2)l + ix_i \right) \left(\sum_{j=1}^l x_j \right)^{k-1} \end{aligned} \quad (16)$$

The number of polynomial terms in (16) now grows linearly over the degree and the number of inputs under the relationship $K = 1 + r + l(2r - 1)$. To stabilize the solution for least squares error, a regularization can be performed [63]. The criterion function to be minimized is thus:

$$J = \|y - F^T \alpha\|_2^2 + b \|\alpha\|_2^2, \quad (17)$$

where $y = [y_1, y_2, \dots, y_N]^T$ is the target output vector and $F = [f_1, f_2, \dots, f_N]^T$ with f_i being the column vector of all polynomial terms in (16) which is applied to the i -th ($i = 1, \dots, N$) training sample. The estimated output is $\hat{y} = F\alpha$ and the solution for α that minimize J is

$$\alpha = (F^T F + bI)^{-1} F^T y$$

where b is a regularization parameter (b is usually chosen to be a small value, say 10^{-4} [63], for stability and not introducing much bias).

Chapter 4

New Quality Measures

Fingerprint quality is a useful but complex measure. It is a subjective indicator depending on evaluation objectives and decision-making personnel or engines. As an example, human naked eye may classify a low contrast image as a low quality one while most of the fingerprint-matching algorithm has no problem processing the image as long as it exhibits sufficient grayscale variations between ridges and valleys. We will thus approach the fingerprint quality evaluation by looking for fingerprint information content that is meaningful to machine processing. Human intuitive or perceptual “feeling” about quality should not come into the picture as long as machine perceptible fingerprint information is present. Hence, we are left with the problem of determining what kind of valid fingerprint information should be present. Fingerprint images have different sets of local and global characteristics. It is thus necessary to study characteristics from both ends to ensure a more or less complete quality deduction.

4.1 Uniformity

Definition

We define uniformity as the consistency in ridge and valley’s respective gray levels. Four samples of fingerprint sub-blocks with good to bad uniformity are presented in Figure 7 below:

Figure 7: Four Fingerprint Sub-blocks. Uniformity changing from the highest uniformity (Leftmost) to the Lowest uniformity (Rightmost)

Figure 7 shows fingerprint image sub-blocks of different uniformities. For the first image sub-block on the left, there is a fairly constant gray level for ridge/valley regions. There is little noise within ridge region as shown. Second image sub-block contains small patches of noise among ridges, while third sub-block have higher ridge inconsistency (low ridge uniformity) as the ridges are blurred and no clear ridge pattern can be identified. Finally, the rightmost highly “contaminated” image sub-block is regarded as of carrying the lowest uniformity among the four images. The examples above suggest us to relate the level of uniformity to quality measure. We define a parameter below to give a measure on fingerprint image uniformity.

Clustering Factor

Clustering Factor is defined as the degree to which similar gray level pixels cluster in the nearby region. The fundamental philosophy supporting the use of such

measure in our analysis of a binary system is that: The more the clustering of “black” or “white” pixels, the higher the confidence level of such pixels (“black” or white”) to be useful signal, and hence higher image quality. This is in contrast to a pool of randomly mixed white/black pixels, whereby no concrete useful information can be deduced. Otsu method[53] is first applied to obtain an optimum threshold value in binarizing each image sub-block.

Figure 8 shows the binarized Image Object (in our case 60x60 fingerprint image sub-blocks. Sub-blocks of 60x60 pixels were chosen as they contain fairly constant orientation certainty which will ease our analysis in section 4.2) as well as a 3x3 mask used for clustering factor computation. The mask is centered at (2,2) and (4,4) respectively in Figure 9 and Figure 10, overlaid on the image object. The center of the mask moves from (2,2) to (59,59), computing cumulative results for clustering factor. The clustering factors for both black and white pixels were computed. For the mask centered at a black pixel (Value=0), the region covered under the masking area is examined. If more than 4 out of 9 carry the same pixel value (Value=0), a 1 is returned. If less than 4 pixels carry the same pixel value (Value=0), a prorated value is returned ($n*0.2$, where n is the number of pixels carrying the same pixel value). The returned value is accumulated for the whole mask-shifting process with the mask centered at black pixels (Value=0) only. On the other hand, the clustering factors for white pixels (Value=1) is computed by following the same procedure, but centered only on white pixels (Value=1) and counting only the white pixels (Value=1) under the masking area.

Figure 8: Image Object and the 3x3 Mask

Figure 9: mask centered at location (2,2)

Figure 10: mask centered at location (4,4)

The higher the clustering factors, the higher the confidence level of the structure. A lower value indicates somewhat randomly organized structure and hence of low quality.

4.2 Orientation Certainty

As shown in Figure 11, an image sub-block generally consists of dark ridge lines separated by white valley lines of the same orientation. The consistent ridge orientation is therefore one of the distinguishable local characteristics of the fingerprint image.

Figure 11: A typical texture-like ridge block.

The grey level gradient (dx, dy) at a pixel exhibits the orientation and the orientation strength of the image at this pixel. By performing Principal Component Analysis on the image gradients on an image block, an orthogonal basis for an image block can be formed by finding its eigenvalues (only 2 values due to 2-dimensional image) and eigenvectors. The ratio between the two eigenvalues gives an indication of how strong the energy is concentrated along the dominant direction with two vectors pointing to the normal and tangential directions of the average ridge flow respectively.

The covariance matrix $\mathbf{C}$ of the gradient vector for an N points image block is given by

$$\mathbf{C} = E \left\{ \begin{bmatrix} dx \\ dy \end{bmatrix} \begin{bmatrix} dx & dy \end{bmatrix} \right\} = \begin{bmatrix} a & c \\ c & b \end{bmatrix}. \quad (18)$$

$$E\{\bullet\} \equiv \frac{1}{N} \sum_N \bullet$$

where

For the covariance matrix given in (18), the eigenvalues λ can be written as:

$$\lambda_{\max} = \frac{(a+b) + \sqrt{(a-b)^2 + 4c^2}}{2} \quad (19)$$

$$\lambda_{\min} = \frac{(a+b) - \sqrt{(a-b)^2 + 4c^2}}{2} \quad (20)$$

For a fingerprint image block, Orientation Certainty Level (*ocl*) is given by the ratio between $\lambda_{\min}$ and $\lambda_{\max}$:

$$ocl = \frac{\lambda_{\min}}{\lambda_{\max}} = \frac{(a+b) - \sqrt{(a-b)^2 + 4c^2}}{(a+b) + \sqrt{(a-b)^2 + 4c^2}} \quad (21)$$

This ratio gives an indication of how strong the energy is concentrated along the ridge-valley orientation. The lower the value the stronger it is the energy. It is obvious that *ocl* is between 0 and 1 as a & $b > 0$ ($a = (dx)^2$, $b = (dy)^2$ from equation 18).

Similar work has been done in [54] with the objective to determine image field direction by considering the cross correlations of the gradients in x and y directions. Donahue *et. al.* determine the tangential vector of an image pattern by finding extreme values for the minimization function [55]. Here, we extend the work into determining fingerprint image block orientation as well as directly using the ratio between the eigenvectors as an indicator of the certainty level.

4.3 Signal-to-Noise Ratio

High uniformity and orientation level do not indicate a high quality fingerprint image. In addition to possessing uniform structures with strong directional strength ridges and valleys, a good quality fingerprint image exhibits a repetitive/periodic pattern that resembles a sinusoidal/square wave. Following the Principle Component Analysis in section 4.2, Eigenvector $\tilde{E}_{min}$ (corresponding to λ_{min}) points to the direction of ridge/valley flow while $\tilde{E}_{max}$ (corresponding to λ_{max}) to the direction of maximum ridge-valley change (normal to ridge/valley flow direction). Examples of fingerprint images with directions of $\tilde{E}_{max}$ plotted for each sub-section of the images are shown in Figure 12:

Figure 12: Two full-sized fingerprint images with directions of $\tilde{E}_{max}$ computed for each image sub-block.

For each sub-block of image shown above, we can compute a signature along the $\tilde{E}_{max}$ direction, positioned at the center of each sub-block as shown below. The signature will pass through the centre of the image sub-block in the direction of x (or $\tilde{E}_{max}$) as shown in Figure 13.

Figure 13: Signature along $\tilde{E}_{max}$ direction

In the coordinate system of (x, y) as shown above, the signature is computed as below:

$$T(x) = \frac{1}{2r+1} \sum_{k=-r}^r D(x, k) \quad (22)$$

where $D(x, y)$ is the gray level at point (x, y)

The signature of a high quality image is a periodic signal, which can be approximated either by a square wave or a sinusoidal wave. In frequency domain, an ideal square wave should exhibit a dominant frequency with sideband frequency components (sinc function). Sinusoidal wave consists of one dominant frequency and minimum component at other non-dominant frequencies. Thus, we are able to make use of such information in identifying good or bad quality blocks. The existence of one dominant frequency and actual value of the dominant component are two main elements that are useful in quality determination.

Figure 14 shows four fingerprint image sub-blocks with varying quality. Bad quality image in Figure 4(c) can be easily identified by the existence of dominant frequency at very low frequency (<5), which is out of the normal ridge frequency range. On the other hand, Figure 4(d) does not possess obvious dominant frequency, which

suggests that the image is highly contaminated. A 26 points DFT is also presented in Figure 14 as part of the local feature vector.

Figure 14: Image sub-blocks with DFT of the signatures along $\tilde{E}_{max}$

4.4 Curvature

The curvature information within each sub-block is included as a part of the feature vector to be used for training. Although curvature has no direct relationship with fingerprint image quality, it will greatly affect the quality determination process through Orientation Certainty and Signal-to-Noise ratio. For an acutely curved ridge-valley structure (around core point, for example), orientation certainty determination will give a low confidence value. It is also less likely for the signature of such structure to exhibit a periodic sinusoidal or square wave pattern. On the other hand, the curvature within a fingerprint image sub-block should follow a particular trend/pattern. Thus, it is useful to include the curvature information in the training process, not just to identify core region, but also to identify invalid curvature.

The curvature information of an image sub-block is captured by orientations of four quadrants, together with each of their certainty level. Figure 15 shows (a) a normal fingerprint sub-block (b) a sub-block consisting core region and (c) a bad quality image sub-block. Each fingerprint image sub-block is further segmented into four quadrants, with each of the orientation and certainty level computed as in section 4.2. Orientation is useful to distinguish between (a) and (b). Orientation certainty level certainly helps to separate (b) from (c).

Figure 15: Image sub-blocks with orientation information

4.5 Summary

From the four Quality Measures defined above, it is clear that each of the measures will have its own strength. While Uniformity serves to detect concrete or scattered pixels in a fingerprint image sub-block, proper ridge-valley structure with strong directional strength should contribute to a high Orientation Certainty level. On the other hand, Signal-to-Noise ratio checks for repetition in ridge-valley layout and Curvature helps to identify core region which could cause previous three measures to fail. They are complementing one another to provide a complete analysis on fingerprint quality.

Chapter 5

Experiments

5.1 Database

We start off with a database comprising of fingerprint images with a range of qualities to allow the classifier to be uniquely characterized for different quality levels. A qualitatively well distributed database is also suitable test samples to evaluate classification accuracy of the trained classifier. The variation in quality can be due to different fingerprint conditions for example: clean or oily, wet or dry and so on. In addition to that, varying fingerprint placement pressure is also another factor contributing to the variations in fingerprint image quality. While adequate pressure to capture clear and separated ridges is desired, extreme pressure can cause connected adjacent ridges or a very “faint” impression to be captured.

To capture a database comprising different quality images, the database collection should be performed based on the following guidelines:

- The database should be captured over a significantly long period.
- Database must comprise samples from multiple subjects
- The fingerprint image collection should be unguided.

Each of the guidelines above introduces uncertainties in the collected fingerprint image qualities. This helps us to achieve the objective of collecting fingerprint images of varying qualities.

In addition to that, our quality analysis is approached by means of machine learning which requires target samples to be “learnt” by a classifier. For this purpose, we synthesize fingerprint images with “absolute qualities” to be used as training targets for each of the quality groups. While captured fingerprint images can have ambiguity in its quality level, synthesized fingerprint images act as candidates with clear cut quality levels. On the other hand, to evaluate how quality scores affect fingerprint matcher accuracy and to study the altered ROC performance, another database that comprises repetitive captures of multiple fingers from multiple human subject was collected. Repetitive captures of the same fingerprint provides *true match* cases and matching between other fingers provide cases of *false match*. The pre-known true and false match ground truth allows estimation of statistical performance measures for the matching accuracy with/without the addition of quality evaluation process. The database should also be significantly large to cover broad range of fingerprint types for an unbiased study.

5.1.1 Database Setup

The four database sets which will be described in section 5.1.2 were collected through the following means:

a. Fingerprint Image Collection Through Fingerprint Identification System

An Automated Fingerprint Identification System is setup in the Centre for Signal Processing, NTU for daily door access operation. A 500dpi Veridicom CMOS sensor is connected to a PC where fingerprint-matching computation is performed. The captured fingerprint images were stored for both access granted and access denied cases from all users. The system was left unattended and it was collecting for a period of 3 weeks.

The sub-block images were classified manually into four image groups of different quality level, namely Very Good, Good, Bad as well as Very Bad. The general guidelines for manual classification are as follows:

Very Good and Good groups contain images with acceptable quality, where ridges and valleys are clearly differentiated such that a minutiae extraction algorithm is able to operate reasonably well.

Very Good images are “perfect” intuitively while Good images suffer from either one of the following: noisy ridge, noisy valley, or background with residue.

Bad images suffer from serious blurring or residue. The minutiae information cannot be identified for this group of image due to the excessive corruption.

Very Bad images are so heavily corrupted that even basic ridge or valley information can hardly be identified. They can also capture unwanted residue or wet patches in sensor daily operation.

500 image sub-blocks were chosen into the database from each of the image groups, building up a database of 2000 image sub-blocks. Some entries for each of the four image groups were shown below in Figure 16.

Figure 16: Fingerprint Image Sub-blocks of Different Qualities

b. Synthetic Fingerprint Image Generation

We synthesized 48 fingerprint image sub-blocks with different degree of curvature to be included in our training sets. For each of this synthesized image, we added different degree of “pepper and salt” noise to simulate sub-blocks of different qualities. Some samples of the synthetic fingerprint images are shown in Figure 17:

Figure 17: Synthetic Fingerprint Images of Different Qualities

c. Fingerprint Image Collection from Repetitive Captures of Multiple Fingers from Multiple Human Subjects

Thirty-six staff members from Centre for Signal Processing, NTU is chosen as the studied subjects. Each staff member is requested to present his/her thumb, index finger as well as middle finger from both hands on the Veridicom CMOS sensor for image capture. Ten captures were required for each of the finger. The collection was done in the way that single captures for all six fingers were performed for the first round, followed by another round of captures for all six fingers, until a total of ten captures were done for each finger. The way that the fingerprints were collected introduced more variability to the image captures as fingerprint image from the same finger is not captured consecutively. A total of 2160 fingerprint images were collected through this method.

5.1.2 Database Set

Four databases A1, A2, B1 and B2 were constructed through means described above. Database A1 and B1 were used as training samples while A2 and B2 were reserved for testing phase.

Database A1

Database A1 contains 400 images from each of the four quality groups in Fingerprint Collection through Fingerprint Identification System (5.1.1 a). In addition to that, 48 synthesized fingerprint images (5.1.1 b) were added to the database to make up a total database size of 1648.

Database A2

Database A2 contains 100 images from each of the four quality groups in Fingerprint Collection through Fingerprint Identification System (5.1.1 a). The total database size is 400.

Database B1

From 2160 fingerprint samples collected in Section 5.1.1 c, first five samples from each finger grouped as Database B1. Database B1 has a size of 1080.

Database B2

From 2160 fingerprint samples collected in Section 5.1.1 c, next five sample images from each finger were grouped as Database B2. Database B2 has a population of 1080.

5.2 Quality Assignment and Fingerprint Matcher

The first consideration here is regarding how do we quantify or classify the quality level of a fingerprint image. This process provides ground truth to enable machine to automatically estimate the quality level of a presented fingerprint image. The classification outcome can be applied to filter off a captured fingerprint image before it is presented to the fingerprint matcher for access verification. However, such an algorithm can only make good use of cases when fingerprint images are of extreme quality levels as it is practically hard for human to decide what is an adequate quality level to be use for accepting or rejecting an incoming fingerprint image with respect to a particular verification system.

To allow a systematical implementation of quality-enabled fingerprint matching system, we perform a *second level classification* which takes in fingerprint quality score as well as the matching score as inputs to produce the final matching results. As matching score acts as one of the inputs to the classifier, a fully-functioned fingerprint matcher and a considerably large database is needed. The classifier's parameters are first tuned for maximum matching accuracy. The trained classifier will be then tested on a new database to verify the effect of the inclusion of fingerprint quality score. This process does not require a hard quality threshold to be implemented when a classifier with continuous output is being used.

5.3 Subjective Quality Evaluation

5.3.1 Background on Subjective Quality Evaluation

Following the discussion in the last section, providing the system with our view of image quality is the first classification process that automatically groups fingerprint images according to their quality level. Subjective Quality Evaluation indicates that the network training of this classification is done through human supervision. To be more specific, the machine is trained by fingerprint image samples with human assigned quality level. The guidelines for quality level assignment is discussed in Section 5.1.1 a.

Given a simple quality-enabled fingerprint matching scenario below:

- Fingerprint captured by sensor
- System supervisor examines fingerprint samples and rejects low quality ones.

- Survived samples were fed into a Fingerprint Matcher
- Matching Results reported.

Subjective Quality Evaluation intends to substitute the role of system supervisor using a trained machine. A properly trained quality classification network enables the fingerprint matching scenario to operate without supervisor attention.

Experiment I below performs low level classification on quality level and Experiment II performs higher level classification on matching results aiming to combine results from matching and quality scores.

5.3.2 Experiment I: Automatic Quality Classification Guided by Subjective Quality Level

Experimental Background

Section 4 of this thesis provides several qualitative measures for a fingerprint sub-block. To allow the use of the quality level effectively, we need to have a single value representation which combines the information from all Quality Measures in section 4 (*Quality Classification*). Moreover, such a single valued score should be calibrated against the acceptability or quality level of the fingerprint images. This is a typical classification process which takes in several inputs (quality measures) and classifies the subject (fingerprint image sub-block) into its appropriate classes (quality level) based on the inputs.

In Subjective Quality Evaluation, database A1 was used as training samples and the subjectively assigned quality level for each fingerprint image sub-block entry was used as the training target value. The classifier tries to learn the human concept on fingerprint quality providing the multiple quality measures for a fingerprint image sub-block.

Experiment Setup

Database A1 has 1648 fingerprint image sub-blocks with quality ranging from *Very Good*, *Good*, *Bad* to *Very Bad*. We assigned a target value of +2 to sub-blocks with *Very Good* quality, +1 to sub-blocks with *Good* quality, 0 to sub-blocks with *Bad* quality and -1 to sub-blocks with *Very Bad* quality respectively. The quality measures (*QM*), together with the assigned target values from database A1, forms 1648 training samples. The samples were used to train our classifier *C*.

To verify how effective the classifier is trained, Database A2 with 400 fingerprint image sub-blocks is used as test samples. The output from each sample is read by the following formula:

$$\text{Estimated Quality Level(EQL)} \left\{ \begin{array}{ll} = \text{Very Good} & \text{if } \text{floor}(C(FV)+0.5) \geq 2 \\ = \text{Good} & \text{if } \text{floor}(C(FV)+0.5) = 1 \\ = \text{Bad} & \text{if } \text{floor}(C(FV)+0.5) = 0 \\ = \text{Very Bad} & \text{if } \text{floor}(C(FV)+0.5) \leq -1 \end{array} \right.$$

The Estimated Quality Level is then compared with the assigned quality level for each test sample to verify if a correct quality level is estimated.

5.3.3 Experiment II: ROC Performance of Subjective-quality-enabled Fingerprint Matcher

Experiment Background

Following the *Quality classification* from Experiment I, Experiment II aims to investigate how the ROC performance of a fingerprint identification system is affected based on subjective quality.

As the implementation of the Quality Analysis aims to improve the overall matching performance of the fingerprint identification system, we bundle the matching score together with the EQL for each fingerprint image in Database B1 as training sample. For a matching between any two fingerprints A and B, an input vector takes the form of:

$$[MS \quad \overline{EQL} \quad \hat{EQL}] \quad (23)$$

where MS : matching score.

$$\overline{EQL} = \frac{\sum_{k=1}^{18} EQL(k)}{18} : \text{Mean of the EQL for all 9 sub-blocks from fingerprint A}$$

and 9 sub-blocks from fingerprint B.

$$\hat{EQL} = \sqrt{\frac{1}{18} \sum_{k=1}^{18} (EQL(k) - \overline{EQL})^2} : \text{Standard Deviation of the EQL for all 9 sub-blocks from fingerprint A and 9 sub-blocks from fingerprint B.}$$

The output vector of the matching between fingerprint A and fingerprint B is assigned as:

$$[o_1 \ o_2] = \begin{cases} [1 \ 0] & \text{if it is a true match} \\ [0 \ 1] & \text{if it is a false match} \end{cases} \quad (24)$$

Experiment Setup

Database B1 comprises fingerprint images for 36 persons. There are 6 fingerprints observed for each person and 5 fingerprint captures per observing fingerprint (a total of 1080 fingerprint captures). To cross-match these fingerprint images with one another, the total number of matches is given by $\frac{n(n-1)}{2}$ while n is the number of fingerprint images.

This gives a total of $1080 \times 1079 / 2$ or 582660 cross-matching pairs. Equations 18 and 19 are applied on each of the cross-matching pairs and these form the training samples in Experiment II.

Due to the large size of the database we have, we choose the Reduced Multivariate Polynomial (RMP) [56] classifier that is proved to be a good trade-off between accuracy and speed in our previous analysis. To test the accuracy of the trained classifier, Database B2 with 528660 matching pairs is used. The input vector for the test set remains as equation (18) above. The output vector from the classifier provides the classification of the outcome. In equation (19) :

The matching result is **True Match** if $o_1 \geq o_2$ from equation 19. The matching is considered **False Match** if $o_1 < o_2$ (equation 19). A representation of the *Quality Included Matching Score (QIMS)* is given by

$$QIMS = \frac{o_1 - o_2}{o_1 + o_2} \quad (25)$$

The original ROC curve for Database B2 without including quality figure is plotted together with the new ROC curve with addition of quality score (*QIMS*) and the performance variation is studied.

5.4 Matcher-based Quality Evaluation

5.4.1 Background on Matcher-based Quality Evaluation

Subjective Quality Evaluation is supervised by human perception based quality level and does not look at the way machine does. A fingerprint image might “looked bad but information still retrievable” by fingerprint identification system. To look at the same way as a fingerprint identification system, a quality evaluation system based on fingerprint matcher is applied.

Matcher-based Quality Evaluation System looks into how favorable a fingerprint image is viewed by the fingerprint matcher. A better scored match reflects that the fingerprint is of “high quality” in the eye of fingerprint matcher as it has more qualities that the fingerprint matcher requires. In other words, the matching score can reflect the fingerprint quality and it can be used as target value in fingerprint quality training as

depicted in Subjective Quality Evaluation, substituting the subjectively assigned value. However, only true matches were used in the training phase. The reason being for both false match and true unmatched cases to be considered, a badly scored match can be due to difference in minutiae distribution (false match with unknown quality) or low quality in the fingerprint image (e.g. true match but low quality). Their matching score is thus unsuitable to be used as a target value to train a quality evaluation engine as the two cases cannot be effectively differentiated from one another.

5.4.2 Experiment III: Matcher-based-quality-enabled Fingerprint Matcher ROC Performance

Experiment Background

Each fingerprint image in Database B1 is partitioned into 9 sub-blocks with its Quality Measures (QM) Vector extracted (Refer to Chapter 5). The 9 QM Vectors forms 9 input vectors for 9 training samples to the classifier and they share the same target value. The target value is obtained through the following procedure:

- ◆ The fingerprint image has four other correctly matched targets (same person and same finger but different capture).
- ◆ The fingerprint is matched with all other four fingerprint images and the 4 matching scores obtained were averaged. The averaged score is the estimated matcher-based quality score (MBQ).

$$MBQ \text{ for } FS_{i,j,k}(m) = \frac{1}{4} \sum_{k \neq l} Matching(F_{i,j,k}, F_{i,j,l}), m=1,2,\dots,9 \quad (26)$$

Where i : person index

j : finger index

k : capture index

m : sub-block index

$FS_{i,j,k}(m)$: Fingerprint Sub-block m of person i , finger j , capture k .

$F_{i,j,k}$: Fingerprint of person i , finger j , capture k .

$Matching(A,B)$: Returns a matching score of fingerprint A and B .

The procedure is repeated for all fingerprint images in Database B1 and this made up of a total of 9720 training samples. Again, RMP [56] which is reasonably accurate and fast is used to learn the concept.

A trained RMP classifier is able to predict the MBQ value of a fingerprint sub-block once its Quality Measure (QM) Vector is presented. We are now able to repeat what we do for Subjectively Quality Evaluation (Section 5.3.3 Experiment II). In equation (18), instead of EQL , MBQ is included.

$$[MS \quad \overline{MBQ} \quad \hat{MBQ}] \quad (27)$$

Again,

where MS : matching score.

$$\overline{MBQ} = \frac{\sum_{k=1}^{18} MBQ(k)}{18} : \text{Mean of the MBQ for all 9 sub-blocks from fingerprint A}$$

and 9 sub-blocks from fingerprint B.

$$\hat{MBQ} = \sqrt{\frac{1}{18} \sum_{k=1}^{18} (MBQ(k) - \overline{MBQ})^2} : \text{Standard Deviation of the MBQ for all 9}$$

sub-blocks from fingerprint A and 9 sub-blocks from fingerprint B.

Equations (19) and (20) are used.

Experiment Setup

RMP is again chosen as the classifier to performed experiments on Matcher-based Quality Evaluation. There are two training phases of classification process to be gone through. Firstly, provided the Quality Measures for each of the fingerprint image sub-blocks as input vector and the MBQ (equation 21) as output vector, first RMP classifier is needed to learn the MBQ estimation. In the second phase, the MBQ estimation from the first phase is used in a matching pair and input vector is formed using equation (22). The output of the second phase if provided by a match/non-match feature vector as depicted in equation (19). Another RMP is applied to learn the match/non-match judgment.

The training phase depicted above is carried out using Database B1. During the testing phase, Database B2 which has never been presented to the system is used.

5.5 Results for Quality Automatic Classification (Experiment I)

5.5.1 Results

In experiment I, several classifiers were used to compare the performance for *Quality Classification*. The tables in the following sections present the accuracy and recognition/training time under several settings for different classifiers for Estimated Quality Level. 400 fingerprint images from Database A2 with pre-known quality level are presented to test system accuracy.

Self-organizing Map (SOM) with Learning Vector Quantization(LVQ)

Table 1 : Classification Results for SOM with LVQ1

NODE SIZE	LVQ Starting Gain	Train Time(s)	Recog Time(s)	Accuracy(%)
10x10	0.03	491.87	5.03	63.25
10x10	0.1	497.59	5.03	62.75
10x10	0.3	493.77	5.04	63.75
15x15	0.03	1069.80	12.68	59.50
15x15	0.1	1394.60	11.35	62.75
15x15	0.3	1061.70	11.92	65.50
25x25	0.03	2860.60	30.46	61.00
25x25	0.1	2701.70	30.23	63.75
25x25	0.3	2721.00	30.35	65.00
30x30	0.03	3854.30	43.48	63.00
30x30	0.1	3852.80	43.40	63.50
30x30	0.3	3853.40	43.52	59.75

Radial Basis Function Neural Network

Table 2 : Classification Results for RBFNN

Spread of Radial Basis Function	Maximum Neuron	Train Time(s)	Recog Time(s)	Accuracy (%)
0.7	200	729.41	1.282	69.25
0.7	400	2540.60	1.652	69.75
0.7	600	5723.70	2.674	73
0.7	800	10592.00	3.666	70.25
1.0	200	730.57	0.851	72.75
1.0	400	2542.70	1.722	73.5
1.0	600	5758.20	3.405	73.5
1.0	800	10650.00	3.665	74.75
3.0	200	735.64	1.132	73.25
3.0	400	2527.70	1.792	73
3.0	600	5699.70	2.804	72.5
3.0	800	10550.00	3.725	70

Naïve Bayes

Table 3 : Classification Results for Naïve Bayes

Train Time(s)	Recog Time(s)	Accuracy (%)
0.03	21.861	75.00

Support Vector Machine

Table 4 : Classification Results for Support Vector Machine

Gamma	Cost of the constrain violation	Train Time(s)	Recog Time(s)	Accuracy (%)
0.1	0.1	9.75	3.07	62.75
0.1	1	6.16	2.31	73.25
0.1	3	5.43	2.12	75.25
0.1	10	5.24	1.92	77.50
1	0.1	11.40	2.86	57.00
1	1	9.38	2.58	73.50
1	3	9.19	2.56	73.50
1	10	9.17	2.53	73.00
3	0.1	12.97	2.91	35.25
3	1	12.49	2.84	65.50
3	3	12.21	2.79	66.50
3	10	12.23	2.77	66.25
10	0.1	13.46	2.91	26.75
10	1	13.84	2.89	45.50
10	3	13.60	2.84	48.50
10	10	13.58	2.85	48.50

Reduced Multivariate Polynomial

Table 5 : Classification Results for Reduced Multivariate Polynomial

Order	Train Time(s)	Recog Time(s)	Accuracy (%)
1	0.30	0.10	65.50
2	1.43	0.12	72.25
3	1.79	0.12	73.75
4	3.19	0.18	75.00
5	5.02	0.26	75.25
6	7.31	0.25	73.00
7	9.98	0.35	72.50
8	13.90	0.40	72.50
9	17.71	0.44	70.75
10	22.33	0.50	68.25

5.5.2 Observations

Tables 1 to 5 above outlines the classification results as well as training/recognition time for five different classifiers: Self-Organizing Map, Radial-basis Function Neural Network, Support Vector Machine, Reduced Multivariate Polynomial and Naïve Bayes. The performance of the classifiers is seen to be comparable to one another and achieves around sixty to seventy percent accuracy range. It is also worth noticing that Reduced Multivariate Polynomial (RMP) has the minimum training and recognition time with a similar accuracy to other classifiers. We hence RMP in our following analysis which deals with a much larger database.

By achieving a 70+% accuracy in classifying EQL, we are still unsure if this classifier is able to improve the matching accuracy of a Fingerprint Identification System. We will now proceed to include the classifier output into the matching score and observe the change in ROC.

5.6 Results for Subjective-quality-enabled Fingerprint Matcher (Experiment II)

5.6.1 Results

RMP is chosen as the classifier due to its good trade-off in both accuracy and speed. By feeding the RMP classifier output (EQL) into equation (18), we are now able to obtain $QIMS$ (equation 20) to plot the new ROC. To train the input/output vector pair in

equations (18) and (19), we will first find the optimum Polynomial Order that produces the highest accuracy.

Optimum Order Selection

The optimum order selection for the polynomial is done through a 3 fold experiments on the training set. The 2160 MATCH cases and 580500 NON-MATCH cases were distributed evenly into 3 sub-groups with each sub-group containing the same number of the MATCH and NON-MATCH cases. For each polynomial order ranging from 1-10, 3 experiments were carried out to make one of the 3 sub-groups test set and the other two training sets. The accuracies for these 3 experiments were averaged to provide an average accuracy for the classification based on Database B1 alone. The computed average accuracy based on Database B1 is presented in Table 6.

Table 6 : Optimum Order Selection

Polynomial Order	Accuracy in %
1	0.9971
2	0.9976
3	0.9990
4	0.9990
5	0.9991
6	0.9992

7	0.9992
8	0.9992
9	0.9992
10	0.9992

As shown in Table 6, orders 6 to 10 have the higher accuracy of 0.9992 in our Optimum Order Selection process.

ROC Curve

To observe the change in the overall matching capability of the system, ROC curve is used to compare the original ROC as well as new ROC obtained. In Figures 18 to 22 , the upper plot shows match score distribution while the lower plot shows original and new ROC curves. Original ROC is in RED while New ROC is in BLUE.

Figure 18 : ROC with RMP order 6

Figure 19 : ROC with RMP order 7

Figure 20 : ROC with RMP order 8

Figure 21 : ROC with RMP order 9

Figure 22 : ROC with RMP order 10

5.6.2 Observations

Improved in the system accuracy is represented by a new ROC curve that has its AAR always larger than the old ROC curve at any FAR setting. In other words, the new ROC curve should be “above” the old ROC curve anywhere in the plot. However, for polynomial setting from 6 to 10, the system AAR is improved for most FAR settings but it cannot get rid of some crossed over in the ROCs for minor portion of the curve.

Consider Figure 22 when polynomial order is 10 as an example. During High and Medium Security Settings which correspond to High and Medium FAR settings, the new ROC curve is above the original ROC curve. However, when a Low Security Setting is

defined, the new quality enabled system has lower Authentic Acceptance Rate than the original system which means that more “true” user is rejected by the system. A user to such a subjective quality evaluation system has to face a compromised performance in some security setting which is not acceptable in many cases.

The experiment results indicate that good visual preference from human and higher matching accuracy can be two different concepts. In other words fingerprint images that we perceive as good in quality visually might not be a good candidate for the matching system. The phrase “a good candidate” implies that the fingerprint images should be accepted as images from the same finger and rejected from those different finger ones. To link up quality and matching in a more reliable manner, we need to explore a quality analysis algorithm that is closely related to matching process and Matcher-based Quality Evaluation is our proposal.

5.7 Results for Matcher-based-quality-enabled Fingerprint Matcher (Experiment III)

5.7.1 Results

It is worth noting that RMP has an order from 1 to 10. Thus, for the first (the Quality Assignment) phase and second (the Matching) phase, the two RMP used gives a total of 10x10 or 100 different settings. To find the optimum setting for the two RMP, again a 3

fold experiment similar to section 5.2.2 is used on Database B1 and the average accuracy for each of the 100 different settings are reported in Table 7 .

Table 7: Optimum order selection for Matcher-based Quality Evaluation

Quality Assignment Phase Order	Matching Phase Order									
	1	2	3	4	5	6	7	8	9	10
	1	0.997	0.9975	0.9989	0.9989	0.999	0.9992	0.9992	0.9992	0.9992
	2	0.997	0.9975	0.9989	0.9989	0.999	0.9992	0.9992	0.9992	0.9992
	3	0.997	0.9975	0.9989	0.9989	0.9991	0.9992	0.9992	0.9992	0.9992
	4	0.997	0.9975	0.9989	0.9989	0.999	0.9992	0.9992	0.9992	0.9992
	5	0.997	0.9975	0.9989	0.9989	0.9991	0.9992	0.9992	0.9992	0.9992
	6	0.997	0.9974	0.9989	0.9989	0.9991	0.9992	0.9992	0.9992	0.9992
	7	0.997	0.9976	0.9989	0.9989	0.999	0.9991	0.9992	0.9992	0.9992
	8	0.997	0.9974	0.9989	0.9989	0.999	0.9992	0.9992	0.9992	0.9992
	9	0.997	0.9974	0.9989	0.9989	0.999	0.9992	0.9992	0.9992	0.9992
10	0.9897	0.9901	0.9988	0.9988	0.9916	0.9991	0.9991	0.9991	0.9948	0.9919

Table 7 shows the average accuracy for the 3 fold test on Database B1. The row index refers to the RMP order for the Quality Assignment Phase while the column index indicates the RMP order for the Matching Phase.

It appears that the accuracy are similar to one another and the maximum frequency of 0.9992 or 99.92% is reported. 44 different RMP settings were identified to contribute to this maximum accuracy.

ROC Curve

For each of the 44 RMP settings that contribute to the maximum accuracy, we retrain the classifier using database B1 and plot the ROC as well as Matching Score distribution using test database B2. The following diagrams show some of the plots from the 44 settings.

Figure 23 : ROC with RMP Orders 1-6

Figure 24 : ROC with RMP Orders 1-7

Figure 25 : ROC with RMP Orders 1-8

Figure 26 : ROC with RMP Orders 1-9

Figure 27 : ROC with RMP Orders 1-10

Figure 28 : ROC with RMP Orders 2-6

Figure 29 : ROC with RMP Orders 2-7

Figure 30 : ROC with RMP Orders 2-8

Figure 31 : ROC with RMP Orders 2-9

Figure 32 : ROC with RMP Orders 2-10

Figure 33 : ROC with RMP Orders 3-6

Figure 34 : ROC with RMP Orders 3-7

Figure 35 : ROC with RMP Orders 3-8

Figure 36 : ROC with RMP Orders 3-9

Figure 37 : ROC with RMP Orders 3-10

Figure 38 : ROC with RMP Orders 4-6

5.7.2 Observations

For the figures above, the red curves represent the original ROC plots without inclusion of Matcher-based Quality Score while the blue ones are the new ROC plots with Matcher-based Quality Score. As discussed in Chapter 3, improvement in the ROC curve can be observed by the position of the new curve which is higher than the original one. Such improvements can be observed from Figure 23 to Figure 32 as well as Figure 38 above.

Figure 27 and Figure 28 are very good examples of how the inclusion of Matcher-based Quality Score can improve the accuracy of a Fingerprint Identification System. For any setting on the x-axis which is the False Acceptance Rate of the system, the new ROC has a better Authentic Acceptance Rate than the original curve. This indicates an overall system performance improvement. On the other hand, Figure 36 shows case of regional improvement in matching accuracy at the expense of the poorer accuracy at the region of lower FAR.

5.8 Summary of Results

From the above results, Experiment II indicates that there is either marginal or no improvement in the ROC performance for subjective-quality-enabled fingerprint matching system over non-subjective-quality-enabled system even though the best classifier was chosen from the lower level classification processes in Experiment I.

In contrast to that, matcher-based-quality-enabled fingerprint matching system is improved over the original system as suggested in Experiment III.

The enhancement of matcher-based-quality-enabled fingerprint matching system compared to the non-quality as well as subjective-quality-enabled fingerprint matching system suggests the following:

- Fingerprint quality is a useful parameter to determine how reliable a fingerprint image sample is. The quality information can effectively improve the matching accuracy when it is used as one of the input parameters to the fingerprint matcher.
- Subjective quality analysis does not look quality the way fingerprint matcher does. Some quality features are obvious to human perception but they are not important to machine processing for fingerprint matcher. In addition to that, while some fingerprint features seem to be missing from human vision, machine might be still able to process such information from the raw image data.

Chapter 6

Conclusions

6.1 Project Flow

One of the main objectives of Fingerprint Quality Analysis is to improve the matching accuracy of a Fingerprint Identification System. Quality information plays the role to filter off low quality images, which will contribute directly to a lower false acceptance rate. To approach Fingerprint Quality Analysis, the first step taken was to define quality measures to be evaluated. Quality measure is the qualitative information that can be directly retrieved from the fingerprint image by an automated algorithm. Such measures should be quantifiable to allow the system for further processing.

We proposed a few quality measures from a single fingerprint block, thus mapping of the quality measures to a single quality score is needed. The mapping is established using a carefully chosen classifier. The target vector to the classifier is approached through subjectively assigned quality score as well as matcher-based quality score. The mapped quality score is then added to the matching process for match/non-match decision. The ROC curve of the system is reported.

6.2 Quality Measures

Uniformity, Orientation Certainty Level, Signal-to-Noise Ratio and Curvature are the four new Quality Measures that were proposed in this Thesis. From Experiment III, the Quality Measures were extracted from the fingerprint image and mapped to quality score (low level classification). The quality score is then added to the original matching score by the fingerprint matcher for second level classification and the final matching result is shown to have improved. The Quality Measures defined in our context is able to reflect the quality features from the fingerprint images and contribute to the effective improvements in the subsequent analysis.

6.3 Subjective Quality Evaluation

No significant overall system improvement was observed through introduction of the subjective quality evaluation. The ROC performance of the fingerprint identification with the inclusion of subjective quality evaluation was seen to be improved for the mid-range of FAR setting. For lower and higher settings of FAR, however, the performance of the new system was observed to be sometimes poorer than the original system.

These results indicate that subjective assignment of fingerprint quality may not be suitable for used as a target value in fingerprint matching. Better quality visibly does not necessary imply that fingerprint image segmentation, ridge tracing as well minutiae detection can be more easily performed.

6.4 Matcher-based Quality Evaluation

In contrast to Subjective Quality Evaluation, our experiments showed that matching score can be effectively used as target value in the training phase. When presented with a new dataset for testing, a carefully tuned fingerprint identification system with quality evaluation was able to perform better than the original non-quality system for all FAR settings.

Common fingerprint identification system uses fingerprint minutiae, ridge frequency, spectral signal and so on as the criteria for matching. In general, addition of a new feature can effectively reduce the False Acceptance Rate but False Rejection Rate may suffer at the same time. However, Fingerprint Quality as a new feature in this work was shown to reduce False Acceptance Rate (New curve to the left of the original curve) and at the same time, lower False Rejection Rate (New curve above the original curve). The implemented Matcher-based Quality Score (MBQ) is thus shown to provide a good estimation of the quality of the fingerprint image with respect to the matcher, and hence it improves the performance of the matcher.

6.5 Some Concluding Remarks

Our results show that views from machine and from human appeared different in the quality context. To achieve good matching performance of a fingerprint system, a machine which includes the historical matching results in its learning process would perform better than one which does not. This also holds when the additional information (subjective quality training data) included in learning does not conform to the ultimate

performance goal. In other words, the quality evaluation which is targeted to estimate the matching performance is fingerprint matcher dependent, which is why we suggest the term “matcher-base” quality evaluation in the later proposed scheme.

6.6 Recommendation for Future Work

Quality is not only important in the final fingerprint matching process but it might also contribute to other phases for examples image segmentation and minutiae detection stages in fingerprint identification. For image segmentation, quality information is important to determine which image area contains reliable information that should be segmented as foreground for processing. In minutiae detection, however, we can make use of quality information to identify which are the spurious minutiae that should not be included in the matching process.

The effect of including quality at different phases of the fingerprint identification process should be studied and further enhancement in the overall matching accuracy is possible. On the other hand, quality analysis can also be extended to other biometrics for example face, hand geometry and so on, by choosing different quality features for each of the different biometrics.

Bibliography

- [1] A. K. Jain, R. Bolle and S. Pankanti. *Biometrics : personal identification in networked society*. Kluwer, Boston, c1999.
- [2] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846-- 859, 2000.
- [2] D. Maltoni, Dario Maio, A. K. Jain and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer, 2003.
- [3] J. Zhang, Y. Yan, and M. Lades. "Face Recognition: Eigenfaces, Elastic Matching, and Neural Nets, in *Proceedings of the IEEE*, 85(9):pp. 1423–1435, 1997.
- [4] P. Jonathon Phillips et al, *An Introduction to Evaluating Biometric Systems*, Computer (2000), <http://www.dodcounterdrug.com/facialrecognition/DLs/Feret7.pdf>.
- [5] Sickler N. C. and Elliott S. J., "An Evaluation of Fingerprint Quality across an Elderly Population vis-à-vis 18-25 Year Olds", *4th Annual CERIAS Research Symposium*, Purdue Memorial Union & Stewart Center, West Lafayette Campus, April 2003
- [6] The BioAPI Consortium, "Version 1.1 of the BioAPI Specification", [http://bioapi.org/New%20Downloads%20\(Add%20to%20Site\)/BioAPI%201.1.doc](http://bioapi.org/New%20Downloads%20(Add%20to%20Site)/BioAPI%201.1.doc)
- [7] R. A. Hicklin, "Comparative Fingerprint Quality and Performance: Rolls, Slaps, and Flats", *Biometric Consortium Conference BC2002*, Crystal City, Arlington, VA USA, September 2003.
- [8] Mansfield A. J. and Wayman J. L., "Best Practices in Testing and Reporting Performance of Biometric Devices Version 2.01", *NPL Report*, August 2002.

- [9] U. Halici, L.C. Jain and A. Erol "Introduction to Fingerprint Recognition" in Intelligent Biometric Techniques in Fingerprint and Face Recognition, L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, Editors, CRC Press, Boca Raton, 1999.
- [10] Wei Liu, Pu-liu Yan, De-ling Xia, Cong Zhou. "An Approach to Dynamic Fingerprint Image Enhancement," *Third International Conference on Image and Graphics*, vol. 00, no. , pp. 294-297, Third 2004.
- [11] Jianwei Yang, Lifeng Liu, Tianzi Jiang, Yong Fan, "A modified Gabor filter design method for fingerprint image enhancement", *Pattern Recognition Letters* 24 (2003) 1805–1817
- [12] Takahiro Nakamura, Miwako Hirooka, Hideto Fujiwara, Kazuhiko Sumi. "Fingerprint Image Enhancement using a Parallel Ridge Filter," *icpr*, vol. 01, no. 1, pp. 536-539, Pattern 2004.
- [13] Sang-Keun Oh, Joon-Jae Lee, Chul-Hyun Park, Bum-Soo Kim, and Kil-Houm Park, "New Fingerprint Image Enhancement Using Directional Filter Bank," *Journal of WSCG*, vol. 11, no. 1, WSCG 2003, February 3-7, 2003, Plzen, Czech Republic
- [14] Park, C.H., Lee, J.J., Smith, M.J.T., Park, S.I., Park, K.H., Directional Filter Bank-Based Fingerprint Feature Extraction and Matching, *CirSysVideo*(14), No. 1, January 2004, pp. 74-85.
- [15] Park, S.I., Smith, M.J.T., Fingerprint Enhancement Based on the Directional Filter Bank, *ICIP00*(Vol III: 793-796).
- [16] Mohammad A.U. Khan, M. Khalid Khan and M. Aurangzeb Khan, "Fingerprint Image Enhancement Using Decimation-free Directional Filter Bank", *Information Technology Journal* 4 (1): 16-20, 2005

- [17] Hung, D.C.D., Enhancement and Feature Purification of Fingerprint Images, PR(26), No. 11, November 1993, pp. 1661-1671.
- [18] Sherlock, B.G., Monro, D.M., and Millard, K., Fingerprint Enhancement by Directional Fourier Filtering, VISP(141), No. 2, April 1994, pp. 87-94.
- [19] Almansa, A., Lindeberg, T., "Fingerprint Enhancement by Shape Adaptation of Scale-Space Operators with Automatic Scale Selection", IP(9), No. 12, December 2000, pp. 2027-2042.
- [20] Greenberg, S.[Shlomo], Aladjem, M.[Mayer], Kogan, D.[Daniel], "Fingerprint Image Enhancement using Filtering Techniques", RealTimeImg(8), No. 3, June 2002, pp. 227-236.
- [21] Bazen, A.M.[Asker M.], Gerez, S.H.[Sabih H.], Systematic Methods for the Computation of the Directional Fields and Singular Points of Fingerprints, PAMI(24), No. 7, July 2002, pp. 905-919.
- [22] Tahmasebi, A.M., Kasaei, S., "A novel adaptive approach to fingerprint enhancement filter design", SP:IC(17), No. 10, November 2002, pp. 849-855.
- [23] Tico, M.[Marius], Onnia, V.[Vesa], Kuosmanen, P.[Pauli], Fingerprint Image Enhancement Based on Second Directional Derivative of the Digital Image, JASP(2002), No. 10, October 2002, pp. 1135-1144.
- [24] Hsieh, C.T.[Ching-Tang], Lai, E.[Eugene], Wang, Y.C.[You-Chuang], "An effective algorithm for fingerprint image enhancement based on wavelet transform", PR(36), No. 2, February 2003, pp. 303-312.

- [25] A.R. Roddy and J.D. Stosz, "Fingerprint Feature Processing Techniques and Poroscopy" in *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, Editors, CRC Press, Boca Raton, 1999.
- [26] X. Jiang, W. Y. Yau and W. Ser., "Detecting the fingerprint minutiae by adaptive tracing the gray-level ridge", *Pattern Recognition*, 34(5): pp. 999–1013, 2001.
- [27] D. Maio, D. Maltoni, "Direct Gray-Scale Minutiae Detection in Fingerprints", *IEEE PAMI*, v. 19, no. 1, 1997.
- [28] G. Bebis, T. Deaconu and M. Georgiopoulos, "Fingerprint Identification Using Delaunay Triangulation", *IEEE International Conference on Intelligence, Information and Systems (ICIIS'99)*, pp. 452- 459, Maryland, 1999.
- [29] N.K. Ratha, R.M. Bolle, V.D. Pandit and V. Vaish, "Robust Fingerprint Authentication Using Local Structural Similarity", *Fifth IEEE Workshop on Applications of Computer Vision*, pp. 29-34, 2000.
- [30] X. Jiang and W. Y. Yau, "Fingerprint Minutiae Matching Based on the Local and Global Structures", *Proceedings of International Conference on Pattern Recognition*, pp. 1038–1041, 2000.
- [31] C.D. Kuglin and D.C. Hines, "The phase correlation image alignment method," *Proc. Int. Conf on Cybernetics and Society*, pp. 163-165 1975.
- [32] H. Nakajima, K. Kobayashi, M. Kawamata, T. Aoki, and T. Higuchi, "Pattern collation apparatus based on spatial frequency characteristics (USP 5915034)", *US Patent*, May 1995.

- [33] T. Aoki, T. Kenji, T. Higuchi, and K. Koji, "Phase-based image matching and its application to intelligent vision systems," Proc. Int. Symp. New Paradigm VLSI Computing, pp.95-100, Dec. 2002.
- [34] K. Ito, H. Nakajima, K. Koji, T. Aoki and T. Higuchi, "A Fingerprint Matching Algorithm Using Phase-Only Correlation", IEICE Transaction Fundamentals, vol. E87-A No.3 March 2004.
- [35] Q. Chen, M. Defrise, and F. Deconinck, "Symmetric phase-only matched filtering of fourier-Mellin transforms for image registration and recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol.16, no. 12, pp. 1156-1168, Dec. 1994.
- [36] T. Kenji, T. Aoki, Y. Sasaki, T. Higuchi, and K. Kobayashi, "High accuracy subpixel image registration based on phase-only correlation," IEICE Trans. Fundamentals. Vol.E86-A, no.8, pp.1925-1934, Aug. 2003.
- [37] M.A. Muquit, T. Kenji, T. Aoki, and T. Higuchi, "High-accuracy passive 3D measurement using multi-camera system based on phase-only correlation", Proc. IEEE Int. Symp. Intelligent Signal Processing and Communication Systems, pp.91-95, Nov. 2002.
- [38] R. Bahuguna, "Fingerprint Verification Using Hologram Matched Filterings," in Proc. Biometric Consortium Eighth Meeting, San Jose, CA, June 1996.
- [39] Access Control Applications Using Optical Computing. (1997). [Online]. Available: <http://www.mytec.com/>.
- [40] S. Gold and A. Rangarajan, "A graduated assignment algorithm for graph matching," IEEE Trans. Pattern Anal. Machine Intell., vol. 18, no. 4, pp. 377-388, 1996.

- [41] D.K. Isenor and S. G. Zaky, "Fingerprint identification using graph matching," Pattern Recognition, vol. 19, no. 2, 1986. Federal Bureau
- [42] Identix, "Minutia vs. Pattern Based Fingerprint Templates", White Paper, http://www.ibia.org/membersadmin/whitepapers/pdf/9/M_vs_P_White%20Paper_v2.pdf.
- [43] Bolle et al, "System and method for determining the quality of fingerprint images", United State Patent number, US596356, 1999.
- [44] L.L.Shen, A. Kot and W.M Koo, "Quality Measures of Fingerprint Images", 3rd International Conference AVBPA 2001, p182-271, June 2001.
- [45] Kang H., Lee B, Kim H., Shin D. and Kim J., "A Study on Performance Evaluation of Fingerprint Sensors", 4th International Conference on Audio- and Video-based Biometric Person Authentication, University of Surrey, Guildford, UK, June 2003.
- [46] L.Hong, Y.Wan and A.K.Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol.20, no.8, Aug 1998.
- [47] Nalini K. Ratha and Ruud M. Bolle, "Fingerprint Image Quality Estimation", IBM Computer Science Research Report RC 21622, 1999.
- [48] T. Kohonen, "Self-organized formation of topologically correct feature maps," Biol. Cybern., vol. 43, pp. 59-69, 1982.
- [49] K. Frank, "Naïve Bayes Classifiers", Department of Computational Linguistics and Phonetics, Saarland University, <http://www.coli.uni-sb.de/~crocker/courses/learning/lecture10.pdf>
- [50] Androutsopoulos I, Koutsias J, Chandrinos K. V. and Spyropoulos C. D. "An experimental comparison of Naïve Bayesian and keyword-based anti-spam filtering with

personal e-mail messages”, Proc. 23rd ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 2000), pages 160-167, Athens, Greece.

[51] Sahami M., Dumais S., Heckerman D. and Horvitz E, “A bayesian approach to filtering junk e-mail”, Learning for Text Categorization, AAAI Workshop, pages 55-62, Madison Wisconsin. AAAI Press. Technical Report WS-98-05, 1998.

[52] McCallum A. and Nigam K, “A comparison of event models for Naïve Bayes text classification”, Proc. AAAI-98 Workshop on Learning for Text Categorization, pages 41-48 AAAI Press.

[53] N. Otsu, “A threshold selection method from gray-level histograms,”IEEE Trans. Syst., Man, Cybern., vol. 9, no. 1, pp.62-66,1979.

[54] Shigeru Ando, “Image Field Categorization and Edge/Corner Detection from Gradient Covariance” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 22, no. 2, pp. 179--190, 2000.

[55] M.J.Donahue and S.I.Rokhlin, “On the Use of Level Curves in Image Analysis”, Image Understanding, vol 57, no. 2, pp.185-203, 1993.

[56] K.-A. Toh, W.-Y. Yau and X. Jiang, “A Reduced Multivariate Polynomial Model For Multimodal Biometrics And Classifiers Fusion”, *IEEE Trans. on Circuits and Systems for Video Technology* (Special Issue on Image- and Video-Based Biometrics), vol.14, no.2, pp.224-233, 2004.

[57] V. N. Vapnik, *Statistical Learning Theory*. New York: John Wiley and sons, 1998.

[58] Bernhard Scholkopf and Alex Smola. *Learning with Kernels*. MIT Press, Cambridge, MA, 2002.

[59] U. Kressel, “Pairwise classification and support vector machines”. *Advances in*

- Kernel Methods - Support Vector Learning* (L. C. Jain and et. al., eds.), ch. 5, (Eds) B. Scholkopf, C. Burges, and A. J. Smola, MIT Press, Cambridge, 1999.
- [60] J. Ma, Y. Zhao, and S. Ahalt, OSU SVM classifier Matlab Toolbox (ver 3.00) in <http://www.eleceng.ohio-state.edu/~maj/osu-svm/>. Ohio State University, Dept. of Electrical and Computer Engineering.
- [61] K. Hornik, M. Stinchcombe, and H. White, "Multi-layer feedforward networks are universal approximators". *Neural Networks*, 2(5): pp. 359–366, 1989.
- [62] Jurgen Schurmann. *Pattern Classification: A Unified View of Statistical and Neural Approaches*. John Wiley & Sons, Inc, New York, 1996.
- [63] K.-A. Toh, Q.-L. Tran, and D. Srinivasan. "Benchmarking a Reduced Multivariate Polynomial Pattern Classifier". *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 26(6): pp. 740–755, 2004.
- [64] K. A. Toh, "Fingerprint and speaker verification decisions fusion," in *Int. Conf. on Image Analysis and Processing, Mantova, Italy, (ICIAP'03)*, pp. 626–631, 2003.
- [65] <http://www.bioapi.org/>, BioAPI Consortium Website,