NOTE TO USERS

This reproduction is the best copy available.

UMI®

**MULTIMODE BIOMETRIC VERIFICATION SYSTEM USING
FINGERPRINT AND VOICE INFORMATION**

by

Karine Pellerin

A thesis submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of
Master of Engineering in Telecommunications Technology Management

Department of Systems and Computer Engineering

Carleton University

Ottawa, Canada, K1S 5B6

September 18, 2003

© Copyright 2003 Karine Pellerin

National Library
of Canada

Bibliothèque nationale
du Canada

Acquisitions and
Bibliographic Services

Acquisitions et
services bibliographiques

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file   Votre référence

ISBN: 0-612-88979-3

Our file   Notre référence

ISBN: 0-612-88979-3

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this dissertation.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de ce manuscrit.

While these forms may be included in the document page count, their removal does not represent any loss of content from the dissertation.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

ABSTRACT

The proliferation of computers has considerably increased the need for proper authentication. Widely used authentication methods provide proof of possession and not proof of identity. Biometrics offers to provide proof of identity. Researchers suggest that multimode biometric systems can improve the authentication performance of mono-mode systems. This thesis reports on the results of an experiment that compares the performance of a multimode biometric system that combines fingerprint and voice attributes with the performances of its fingerprint and voice subsystems. It is the first study known to report on the performance of a multimode system that combines fingerprint and voice attributes from large databases. Results of the experiment suggest that: i. multimode biometric systems do not always perform better than their mono-mode subsystems do, and ii. the performance of a multimode system is highly dependent on the initial performances of its mono-mode subsystems and the fusion strategy used.

ACKNOWLEDGEMENTS

The author thanks Dr. Tony Bailetti from Carleton University for his unfailing guidance, editing and encouragement. Profound thanks to Dr. Qinghan Xiao from Defence Research and Development Canada for his expertise and valuable suggestions. Special recognition must also go to Maj. Pierre Godon for providing the necessary contacts to perform the experiment described in this thesis. Many others have contributed in various ways and their support is greatly appreciated.

Table of contents

ABSTRACT	iii
ACKNOWLEDGEMENTS	iv
Table of contents	v
List of Tables.....	viii
List of Illustrations	ix
List of Appendices	xi
 Chapter 1 – Introduction	 1
1.1 Introduction	1
1.2 Thesis objectives	3
1.3 Motivation	4
1.4 Why expect the multimode system to perform better than its two subsystems?	5
1.4.1 Research results	5
1.4.2 Examples	7
1.5 Thesis structure	11
 Chapter 2 - Literature review.....	 12
2.1 Main processes in biometrics	12
2.2 Multimode biometrics	13
2.3 Biometric accuracy performance	15
2.4 Multimode biometric research	17
2.4.1 Integration strategies	17
2.4.2 Voice and facial.....	17
2.4.3 Fingerprint and facial	20
2.4.4 Fingerprint, facial and hand	21

Chapter 3 - Experimental setup	23
3.1 Objectives of the experiment.....	23
3.2 Evaluation protocol	23
3.3 Evaluation type.....	24
3.4 Influencing factors.....	24
3.5 Cost of errors.....	25
3.6 Fingerprint subsystem	26
3.6.1 The FVC 2000 (DB3 Set A) database.....	27
3.6.2 VeriFinger version 4.1 software.....	29
3.7 Voice subsystem.....	30
3.7.1 The XM2VTS database.....	31
3.7.2 The VoiceSafeEvaluator software.....	33
3.8 Multimode system.....	33
Chapter 4 - Conducting the experiment	35
4.1 Fingerprint subsystem	35
4.1.1 Enrolment process.....	36
4.1.2 Verification process.....	36
4.2 Voice subsystem experiment.....	38
4.2.1 Enrolment process.....	38
4.2.2 Verification process.....	39
4.3 Multimode system experiment.....	40
Chapter 5 - Results.....	42
5.1 Fingerprint subsystem results.....	42
5.1.1 Quality of impressions	42
5.1.2 Results of genuine attempt trials	44
5.1.3 Results of impostor attempt trials	45
5.1.4 ROC and DET curves.....	47
5.2 Voice subsystem results	48
5.2.1 Results of genuine attempt trials	48
5.2.2 Results of impostor attempt trials	49
5.2.3 ROC and DET curves.....	51
5.3 Multimode system results.....	52
5.3.1 Strategy 1 DET curves	52
5.3.2 Strategy 2 DET curves	53

Chapter 6 - Discussion of results	55
6.1 Multimode system vs. subsystems	55
6.1.1 Strategy 1.....	56
6.1.2 Strategy 2.....	57
6.2 Effectiveness of different weight combinations.....	62
6.3 Summary of results.....	63
Chapter 7 – Conclusion	65
7.1 Thesis objectives	65
7.2 Conclusions	66
7.3 Contributions.....	68
7.4 Future research	70
References	72

List of Tables

Table 4.1. Different weights assigned to each subsystem (Strategy 2).....	41
Table A.1: Biometric errors	99
Table A.2: Different levels of fusion and fusion strategies.....	104

List of Illustrations

Figure 1.1. Results Reported by A. Ross, A.K. Jain and J. Qian in 2001	6
Figure 1.2. Results Reported by Sanderson in 2002	7
Figure 2.1. Different levels of biometric fusion.....	14
Figure 3.1. Fingerprint subsystem.....	26
Figure 3.2. Age distribution of DB3 Set A used in Fingerprint Verification Competition of 2000 (FVC 2000)	27
Figure 3.3. Voice subsystem	31
Figure 3.4. Multimode system	34
Figure 5.1. Number of low and good quality enrolment impressions.....	42
Figure 5.2. Number of low quality enrolment impressions per finger.....	43
Figure 5.3. Number of low and good quality verification impressions.....	43
Figure 5.4. Number of low quality verification impressions per finger.....	44
Figure 5.5. Scores obtained from genuine attempt trials.....	45
Figure 5.6. Scores obtained from impostor attempt trials.....	46
Figure 5.7. Fingerprint subsystem ROC curve.....	47
Figure 5.8. Fingerprint subsystem DET curve	47
Figure 5.9. Scores obtained from genuine attempt trials.....	49
Figure 5.10. Scores obtained from impostor attempt trials	50
Figure 5.11. Voice subsystem ROC curve	51
Figure 5.12. Voice subsystem DET curve.....	51
Figure 5.13. Strategy 1 DET curve	52
Figure 5.14. DET curves of all combination under Strategy 2	54
Figure 6.1. DET curves of Strategy 1 and the two subsystems.....	56
Figure 6.2. DET curve of the multimode system using Strategy 2 combination 1 (fingerprint subsystem = 0.1) and the DET curves of the fingerprint and voice subsystems.....	57
Figure 6.3. DET curve of the multimode system using Strategy 2 combination 2 (fingerprint subsystem = 0.2) and the DET curves of the fingerprint and voice subsystems.....	58
Figure 6.4. DET curve of the multimode system using Strategy 2 combination 3 (fingerprint subsystem = 0.3) and the DET curves of the fingerprint and voice subsystems.....	58
Figure 6.5. DET curve of the multimode system using Strategy 2 combination 4 (fingerprint subsystem = 0.4) and the DET curves of the fingerprint and voice subsystems.....	59
Figure 6.6. DET curve of the multimode system using Strategy 2 combination 5 (fingerprint subsystem = 0.6) and the DET curves of the fingerprint and voice subsystems.....	59
Figure 6.7. DET curve of the multimode system using Strategy 2 combination 6 (fingerprint subsystem = 0.7) and the DET curves of the fingerprint and voice subsystems.....	60

Figure 6.8. DET curve of the multimode system using Strategy 2 combination 7 (fingerprint subsystem = 0.8) and the DET curves of the fingerprint and voice subsystems.....	60
Figure 6.9. DET curve of the multimode system using Strategy 2 combination 8 (fingerprint subsystem = 0.9) and the DET curves of the fingerprint and voice subsystems.....	61
Figure 6.10. DET curves of the multimode systems using all combinations of weights..	62
Figure A.1. General methodology in using a biometric system.....	87
Figure A.2. A Performance Curve with an EER at approximately 85	97
Figure A.3. An example of ROC curves	98
Figure A.4. An example of DET curves.....	98
Figure A.5: Different levels of fusion	103

List of Appendices

Appendix A – Overview of Biometrics and Multimodal Biometrics	76

1 Chapter 1 – Introduction

1.1 Introduction

The proliferation of computers has considerably increased the need for proper authentication. The security service that ensures legitimate identification of an individual prior to their access to computer resources is called authentication.

Cyber crime is the number one fraud fear of the future [SHA 02]. The cost of fraud to US organizations is estimated at \$400 billion annually. Widely used authentication methods do not provide proof of identity. Passwords, personal identification numbers (PINs), smart cards and tokens can be shared, stolen and forged. There is an urgent need for authentication techniques that provide proof of identity.

Biometrics offers to provide proof of identity. A survey of Gartner analysts selected the 10 high-impact technologies for 2002 to 2007 [FEN 01]. Biometric authentication and speech recognition were among the 10 technologies selected. The most significant obstacle to the wide adoption of biometric-based personal identification systems is their poor performance. Thus, improving the performance of biometrics systems is a significant research challenge [HON 99].

Multimode biometric systems combine two or more biometric identifiers to obtain a more accurate decision about a user's identity. Results of recent research [BEN 99B][HON 99][JAI 02][POH 01][ROS 01] suggest that multimode biometric systems can improve the performance of mono-mode biometric systems. The improvement in performance can be achieved when the multimode system uses the strengths of one mode to compensate for the weaknesses of another. Multimode systems are more difficult to spoof. This is because multiple biometric characteristics need to be forged in order to defeat the system.

To date, researchers have examined two types of multimode biometric systems: those that combine voice and facial attributes and those that combine fingerprints and facial attributes. Voice-facial systems require template updates because voice and face attributes change over time. In addition, voice and face attributes are dependent on environmental conditions such as light and noise. Fingerprint-facial systems cannot address voice authentication over telephone networks.

This thesis reports on the results of an experiment that compares the performance of a multimode biometric system that combines fingerprint and voice attributes with the performance of its fingerprint subsystem and the performance of its voice subsystem. It is the first study known to combine fingerprint and voice attributes from large databases.

1.2 Thesis objectives

The objectives of this thesis are to:

1. Test whether or not a voice-fingerprint biometric system can perform better than its voice subsystem and its fingerprint subsystem.
2. Identify the weights which are most effective at combining the opinions of the voice and fingerprint subsystems into an accurate authentication decision

To compare the performance of the voice-fingerprint system with the performance of the voice subsystem and the performance of the fingerprint subsystem, the Detection Trade-off (DET) curve is used. The DET curve plots false non-match rates (FNMR) against false match rates (FMR) using logarithmic axes. The system that has its DET curve closest to the horizontal axis is the system that performs best.

To identify which combination of weights is the most effective, the DET curves of all weight combinations are plotted on the same graph. The DET curve closer to the horizontal axis will establish which combination was the most effective at combining the two subsystems' opinions into an accurate decision.

1.3 Motivation

Two reasons motivated me to undertake this research. First, two research papers had recently reported results of experiments showing that multimode biometric systems performed better than their subsystems. The authors of [ROS 01] conducted an experiment focused on system performance using fingerprint and hand geometry. They concluded that the fingerprint-hand geometry system performed better than both of its subsystems when the sum rule was used and equal weights were assigned to each subsystem. The author of [SAN 02] conducted an experiment using speech and facial attributes. The author also concluded that the multimode system he tested performed better than both of its subsystems.

The second motivation for undertaking this research is that I wanted to experiment with a combination of biometric identifiers that had not been researched previously. There is a need in real applications to use voice attributes. The use of voice biometrics would be quite suitable for wireless communications. Fingerprint verification is also very popular because it blends nicely in an office environment and can be very accurate. This is why I selected the voice and fingerprint subsystems for my research.

1.4 Why expect the multimode system to perform better than its two subsystems?

Two reasons led me to expect that the performance of the multimode biometric system used in this experiment, a voice-fingerprint system, could be better than the performance of its two individual subsystems:

- results in recently published research studies
- four examples of real situations

1.4.1 Research results

Results of the experiments reported in [ROS 01] and [SAN 02] show that multimode biometric systems can perform better than their individual subsystems.

Figure 1.1 shows the Receiver Operating Characteristics (ROC) curves provided by [ROS 01]. The ROC plots impostor attempts accepted against genuine attempts accepted. In this case, the ROC curve farthest away from the horizontal axis identifies the better performing system.

Figure1.1. Results Reported by A. Ross, A.K. Jain and J. Qian in 2001

Source: A. Ross, A.K. Jain and J. Qian, "Information fusion in biometrics," in Proceedings of the Audio and Video-based Person Authentication (AVBPA'01), pp. 354-359, Halmstad, Sweden 2001.

Figure 1.2 shows the Total Error (TE) at different signal to noise ratios (SNR). The TE is the sum of false acceptance and false rejection rates. In the experiment, the researchers corrupted speech information by adding white Gaussian noise. Figure 1.2 shows that the signal to noise ratio varied from 28 to -8 dB in the experiment.

Figure 1.2. Results Reported by Sanderson in 2002

Source: C. Sanderson, "Information fusion and person verification using speech & face information,"

Research paper IDIAP-RR 02-33, IDIAP, Martigny, Switzerland, September 2002

1.4.2 Examples

The following four examples support the expectation that a multimode biometric system can perform better than its subsystems. The examples use a weight summation approach where equal weights are assigned to each of the two subsystems ($W_1 = W_2 = 0.5$). The

first two examples illustrate that a multimode system can perform better than one of its two subsystems. The last two examples illustrate that it is possible for a multimode system to perform better than both of its subsystems.

Example 1

This example is for a genuine user who attempts authentication. This user belongs to the five percent of the total population that has poor or not quantifiable fingerprints. When trying to authenticate using the fingerprint subsystem, the genuine user obtained a score of 0.93. The threshold of the fingerprint software is set at 0.94 (t_1). The genuine user is rejected because his score of 0.93 is lower than the threshold of 0.94. This attempt results in a false non-match error. When trying to authenticate with the voice subsystem, the user obtained a score of 0.91. The threshold of the voice software is set at 0.86 (t_2). The genuine user is accepted because his score of 0.91 is higher than the threshold of 0.86. This attempt does not result in an error. When attempting authentication with the multimode system, the user obtained a score of 0.92 ($0.5 \times 0.93 + 0.5 \times 0.91$). The threshold of the multimode system is set at 0.90 ($0.5 \times t_1 + 0.5 \times t_2$). The genuine user is accepted because his score of 0.92 is higher than the threshold of 0.90. This attempt does not result in an error. In this example, a genuine user has been rejected by the fingerprint subsystem. Using a combination of both his voice and fingerprint information the user was able to obtain a score above the multimode threshold and was accepted in the multimode system. Therefore, the performance of the multimode system was better than the performance of the fingerprint subsystem.

Example 2

This example is for an impostor who attempts authentication. When trying to authenticate with the fingerprint subsystem, the impostor obtained a score of 0.91. The threshold of the fingerprint software is set at 0.94 (t_1). The impostor is rejected because his score of 0.91 is lower than the threshold of 0.94. This attempt does not result in an error. When trying to authenticate with the voice subsystem, the impostor obtained a score of 0.87. The threshold of the voice software is set at 0.86 (t_2). The impostor is accepted because his score of 0.87 is higher than the threshold of 0.86. This attempt results in a false match error. When attempting authentication with the multimode system, the user obtained a score of 0.89 ($0.5 \times 0.91 + 0.5 \times 0.87$). The threshold of the multimode system is set at 0.90 ($0.5 \times t_1 + 0.5 \times t_2$). The impostor is rejected because his score of 0.89 is lower than the threshold of 0.90. This attempt does not result in an error. In this example, an impostor has been accepted by the voice subsystem. Using a combination of both his voice and fingerprint information the impostor was not able to obtain a score above the multimode threshold and was rejected in the multimode system. Therefore, the performance of the multimode system was better than the performance of the voice subsystem.

Example 3

This example is for a genuine user who attempts authentication. This user belongs to the five percent of the total population that has poor or not quantifiable fingerprints and has a

cold. When trying to authenticate with the fingerprint subsystem, the user obtained a score of 0.93. The threshold of the fingerprint software is set at 0.94 (t_1). The genuine user is rejected because his score of 0.93 is lower than the threshold of 0.94. This attempt results in a false non-match error. When trying to authenticate with the voice subsystem, while having a cold, the user obtained a score of 0.85. The threshold of the voice software is set at 0.86 (t_2). The genuine user is again rejected because his score of 0.85 is lower than the threshold of 0.86. This attempt results in a false non-match error. When attempting authentication with the multimode system, the user obtained a score of 0.89 ($0.5 \times 0.93 + 0.5 \times 0.85$). The threshold of the multimode system is set at 0.86 ($\min(t_1, t_2)$). The genuine user is accepted because his score of 0.89 is higher than the threshold of 0.86. This attempt does not result in an error. In this example, a genuine user has been rejected by both subsystems. Using a combination of both his voice and fingerprint information the user was able to obtain a score above the multimode threshold and was accepted in the multimode system. Therefore, the performance of the multimode system was better than the performance of both subsystems.

Example 4

This example is for an impostor who attempts authentication. When trying to authenticate using the fingerprint subsystem, the user obtained a score of 0.95. The threshold of the fingerprint software is set at 0.94 (t_1). The impostor is accepted because his score of 0.95 is higher than the threshold of 0.94. This attempt results in a false match error. When trying to authenticate using the voice subsystem, the impostor obtained a

score of 0.87. The threshold of the voice software is set at 0.86 (t_2). The impostor is accepted because his score of 0.87 is higher than the threshold of 0.86. This attempt results in a false match error. When attempting authentication to the multimode system, the impostor obtained a score of 0.91 ($0.5 \times 0.95 + 0.5 \times 0.87$). The threshold of the multimode system is set at 0.94 ($\max(t_1, t_2)$). The impostor is rejected because his score of 0.91 is lower than the threshold of 0.94. This attempt does not result in an error. In this example, an impostor has been accepted by both subsystems. Using a combination of both his voice and fingerprint information the impostor was not able to obtain a score above the multimode threshold and was rejected in the multimode system. Therefore, the performance of the multimode system was better than both of its subsystems.

1.5 Thesis structure

The thesis is organized into seven chapters. Chapter 1 is the introduction. Chapter 2 explains the key concepts in assessing the accuracy performance of biometric systems and presents a summary of previous work on multimode biometrics. Chapter 3 describes the experimental set-up and introduces the multimode system and subsystems that are part of the experiment. Chapter 4 explains the accuracy performance tests conducted on the multimode system and the two subsystems. Chapter 5 presents the experimental results of the accuracy performance tests. Chapter 6 discusses and analyzes the results obtained from the experiment. Finally, chapter 7 draws conclusions, describes the contributions made by the research, and suggests future areas of research.

2 Chapter 2 - Literature review

This chapter starts by explaining key concepts in biometrics. An extensive overview of biometrics and multimode biometrics is provided in Appendix A. The remainder of this chapter will review the literature on multimode biometrics—the use of multiple identifiers to arrive at a more accurate and reliable authentication decision. It is organized by the different combination of identifiers that have been researched. The section on integration strategies has been added due to its importance to the field.

2.1 Main processes in biometrics

There are three main processes involved in biometric systems: the enrolment process, the storage of templates, and the verification process.

The enrolment process consists of an individual providing a series of samples (usually three) of the specific biometrics. A digital representation is created to generate a biometric template using an averaging process. This template is then used in all subsequent authentications. A unique identifier is associated with the template for future recall. The identifier can be a PIN or a card number.

The second process is the storage of the templates collected in the enrolment process so they can be referenced later. Templates can be stored within the biometric device itself, in a central repository, or on a portable token carried by individuals.

The verification process requires the individual to claim an identity by providing either a PIN or by presenting a token. The template is called from the database and brought into memory for comparison. The individual needs to provide a live sample. The biometric system compares the live sample with the template in memory and evaluates if the sample and the template match within the predefined threshold and returns a binary true or false message.

2.2 Multimode biometrics

Multimode biometric systems combine two or more biometric identifiers to obtain a more accurate decision on a user's identity. In a multimode biometric system, each subsystem will provide an opinion on the user's identity claim. A supervisor module will combine the different opinions delivered by the subsystems and make a final decision (accept/reject). The supervisor module can use different fusion strategies to combine each subsystem opinions in order to reach the final decision. Fusion can be performed at different levels: sensor level and feature level are called pre-mapping fusion techniques while confidence level and abstract level are called post-mapping fusion techniques

[SAN 02]. Figure 2.1 illustrates the different levels of fusion for a multimode system using a fingerprint and a voice subsystem.

Figure 2.1. Different levels of biometric fusion

Sensor level occurs when the raw data of the sensors are combined. Fusion at the feature level is performed at the sensor level where the features extracted from the different sensors are concatenated to create a joint feature vector. Fusion at the confidence level occurs when the matching scores of each subsystem are combined using techniques such as weighted summation, weighted product and the Bayesian Rule. Fusion at the abstract

level takes place when the decisions of the subsystem are combined using the AND rule, the OR rule, Majority Voting and Ranked List Combination.

2.3 Biometric accuracy performance

In password-based authentication systems, a user who provides the correct password will always be granted access. In a biometric authentication system, the limitations of the feature extractor and matcher, the biometric sensor's noise as well as the environment's noise can prevent access to a legitimate user.

Traditionally, biometric performance is stated in terms of decision error rates [MAN 02]. Decision error rates include the false rejection rate (FRR) and the false acceptance rate (FAR). The false rejection rate is expressed as a percentage and refers to the likelihood that an authorized user was denied access by the system. The false acceptance rate is also a percentage and refers to the likelihood that an impostor was wrongly accepted in the system.

Decision errors are due to matching errors or acquisition errors [MAN 02]. Matching errors are accuracy performance measures resulting from a single comparison or attempt and are expressed as false match rate (FMR) and false non-match rate (FNMR). FMR is described as the expected probability that a sample will be falsely declared to match a single randomly selected "non self" template [MAN 02]. FNMR is the expected

probability that a sample will be falsely declared not to match a template of the same measure from the same user supplying the sample [MAN 02]. Image acquisition errors occur when users are not able to provide the required biometric trait, have insufficient distinctive biometric characteristics, are unable to subsequently verify their enrolment template to confirm enrolment, or have enrolled successfully but are constantly rejected at verification.

The performance of a biometric system is summarized using the Receiver Operating Characteristics (ROC) curves or the Detection Error Trade-off (DET) curves. The ROC curve is threshold independent. It is used to effectively and objectively compare different imperfect diagnostic and pattern matching systems under comparable conditions. The ROC plots imposter attempts accepted (FMR) against genuine attempts accepted (1-FNMR). The DET curve is a modified version of the ROC curve. In [MAR 97] the authors assert that the DET curve is preferred in the case of biometrics. The DET curve provides a much clearer view of well performing systems as it plots FNMR against FMR directly using logarithmic axes.

2.4 Multimode biometric research

2.4.1 Integration strategies

In 1997, the authors of [KIT 97] recognized that the work done developing multimode systems was using different integration strategies. They suggested a common theoretical framework for combining evidence and demonstrated that existing schemes could be considered as a special case of compound classification where a decision is reached with the participation of all modalities. The authors simplified the Bayesian decision rule that leads to the product and sum rules to perform efficient integration strategies. They also theoretically demonstrated that the sum rule was less affected by estimation errors. They conducted experiments to demonstrate that integrating multiple face recognition frames using the sum, product and majority rules to derive a decision would yield better performance than making a decision on a single frame. They confirmed that all integration strategies dramatically improved the imposter acceptance rate and that the best performance was offered by the sum rule.

2.4.2 Voice and facial

In 1995 the authors of [BRU 95] combined acoustic and visual cues to identify people. The output of two classifiers (static and dynamic) from acoustic features and three classifiers (eyes, nose, mouth) from visual features were normalized and integrated using

a weighted product approach to render a decision. The recognition performance of static and dynamic acoustic features was 77% and 71% respectively. When combining static and dynamic classifiers together a recognition performance of 88% was achieved. The recognition performance of the eyes, nose and mouth visual features were 80%, 77% and 83% respectively. When combining the three classifiers a recognition performance of 91% was achieved. By combining all five classifiers, the recognition performance increased to 98%. Their experiment clearly demonstrated that the integrated system performed better than the subsystems. This confirmed that the use of multiple cues is an effective way to improve performance.

In 1996, a multimode person verification tool using speech and images was proposed [ACH 96]. The final decision was rendered by applying a Furui threshold to the methods of subsystems and then combining the individual results with a majority law. It demonstrated that the combination of voice and speech achieves an increased performance and that future research should estimate the performance achievable using large multi-modal databases.

In 1997, the authors in [BIG 97] used Bayes' theory to estimate the biases of individual subsystem opinions. Those biases were then used to integrate the different subsystems' opinions into one opinion. From experiments using real and simulated images and speech, they were able to verify that their confidence level fusion model improved decision-making in both the simulated and real databases.

In April of 1999, the authors of [VER 99] conducted experiments based on speech and face modalities using three subsystems: voice, frontal face and profile images. They used soft decision fusion techniques. These techniques use fusion at the confidence level. They evaluated 9 different methods for solving decision fusion problems. The following classifiers were experimented on a database of 37 subjects: Gaussian, Logistic regression, Linear, Quadratic, MLP, Majority vote, k-NN, k-NN +VQ and Binary Decision Tree. It was confirmed that the Total Error Rate (TER) of the integrated system outperformed even the best mono-mode system regardless of the classifier used. They argue that the fusion method that will perform best depends on the application; in their case it was Logistic regression that provided the best results.

In 1999, the authors of [WAR 99] investigated the use of lip information as a secondary source of information for a robust speaker verification system in noisy conditions. Their experiment showed that fusion of lip and speech outperforms the performance of either one of the two subsystems.

In June 2001, the authors of [POH 01] presented an authentication system using face and text-dependent voice biometrics. The chosen classifiers for each of the biometric data are Multi-Layered Perceptions with a logical decision-merging scheme. Their prototype was tested and evaluated on real-life databases and results demonstrated that a multimode approach was better than any single modality and that the extractor performance played an important role.

In November 2002, the author of [XIA 02] proposed a new approach on adaptive multimode biometric fusion. Current adaptive methods pre-assign different weights to each biometric trait. The proposed approach, however, adjusts dynamically. For an accept decision, a weighted summation is used but when a reject occurs, the weight is adjusted dynamically based on feedback received from the reject reason, the working conditions, and the estimated noise level.

2.4.3 Fingerprint and facial

In 1998, Michigan State University published a report [HON 98] on a prototype that integrated faces and fingerprints for personal identification. The decision fusion module used fusion at the confidence level, i.e. based on the integration of the confidence values provided by each module. The authors computed an impostor distribution for the face and fingerprints and estimated the FAR (confidence level) of each subsystem. By combining face and fingerprint in an identification system, they were able to overcome the limited reliability of face recognition and the ineffectiveness of fingerprint technology in identification mode. They were able to meet response time and accuracy requirements. At a fixed FAR of 0.01%, the FRR of the integrated prototype was 6.6%. While this value was better than the face subsystem (61.2%), it was only slightly better than the performance of the fingerprint subsystem (10.6%). Following those results, the authors published the article “Can Multibiometrics Improve Performance?” [HON 99]. The authors clearly stated the assumptions of multiple biometric integration and proved that

integration schemes, like confidence level fusion, can indeed result in an improvement of performance.

2.4.4 Fingerprint, facial and hand

In 2001, Jain et al. conducted an experiment with fusion at the confidence level using face, fingerprint and hand geometry information [ROS 01]. The genuine and impostor scores were plotted and the two distributions were reasonably well separated. For this reason, the authors decided to use sum rule, decision tree, and linear discriminant classifiers for fusion. Empirical results demonstrated that the sum rule performed better than the decision tree and the linear discriminant. They were unable to fix the FRR and then calculate the FAR in the cases of the decision tree and linear discriminant classifiers. They also conducted fusion experiments at the feature level and obtained better results than fusion at the confidence level. They concluded on the note that it would be instructive to study other datasets involving large number of users and additional biometric indicators.

In 2002, the same authors published an article on an innovative idea and successfully improved the performance they had obtained with the sum rule in their previous experiments [13]. While other studies [BEN 99A][BRU 95][HON 98][KIT 97][ROS 01] used a common threshold to determine if it was a genuine user or an impostor, they suggested that learning user-specific parameters could further improve performance.

They computed matching threshold for each user using cumulative histograms of impostors' scores for each biometric trait. Using the Receiver Operating Curve (ROC), they observed an increase in performance when using a user-specific threshold versus a common threshold. They also experimented on weighting individual biometric traits. By learning user-specific weights for each of their traits, a low weight could be assign to a less reliable trait and a higher rate to a more reliable one. It was demonstrated that the error rates were reduced for that particular individual. This paper clearly demonstrates the benefits of using user-specific parameters as opposed to common parameters.

3 Chapter 3 - Experimental setup

This chapter first describes the objectives of the experiment, the protocol used, the type of evaluation, the factors that influence accuracy performance and the cost of decision errors. It then introduces the fingerprint and voice subsystems and the multimode system.

3.1 Objectives of the experiment

The experiment has two objectives:

1. Test whether or not a voice-fingerprint biometric system can perform better than its voice subsystem and its fingerprint subsystem.
2. Identify the weights that are most effective at combining the opinions of the voice and fingerprint subsystems into an accurate authentication decision.

3.2 Evaluation protocol

The experiment follows the guidelines in the recently published Best Practices in Testing and Reporting Performance of Biometric Devices [MAN 02]. Reference [MAN 02] provides a framework for developing and fully describing test protocols. It helps testers avoid systematic bias due to incorrect data collection or analytic procedures in evaluations. This thesis adopts the terminology used in [MAN 02].

3.3 Evaluation type

The evaluation types listed in [MAN 02] are: technology evaluation, scenario evaluation and operational evaluation. Technology evaluations compare competing algorithms for a single technology. Scenario evaluations determine the overall performance of a prototype or a simulated application. Operational evaluations determine the performance of a complete biometric system in a specific application environment and with the targeted population. The type of evaluation performed in this research does not correspond exactly to any of the evaluation types listed in [MAN 02] but it is a modified version of a technology evaluation. It is related to technology evaluation in the sense that different algorithms are compared to one another but they are not from a single technology.

3.4 Influencing factors

Performance can be affected by the application, the environment, and the people used in the experiment. The performance results of the fingerprint subsystem are dependent on the quality of the samples in the fingerprint database and the fingerprint software. The performance results of the voice subsystem are dependent on the voice samples in the audio database and the voice software. The performance results of the multimode system are dependent on both databases and both software systems. For the purpose of testing a technology, the authors of [MAN 02] state that a generic population is an accepted

practice when the generic population follows the “Three Bears” rule¹. Both databases used in the experiment have been created from the generic population. The fingerprint software accepts the image resolution of the samples in the fingerprint database and the voice software accepts the sound quality of the samples in the voice database.

3.5 Cost of errors

A biometric system can make two types of errors: a false match where an impostor is accepted in the system and a false non-match where a genuine user is denied access. Most biometric devices in the market today have a threshold adjustment that allows tightening or relaxing of the criteria associated with matching live samples with the stored templates. This becomes a trade-off between relaxing the requirements to provide a user-friendly system (increasing the number of false acceptance) or tightening the requirements for security purposes (higher level of false rejection).

The cost of errors varies depending on the situation. In a high security application, the cost associated with an impostor accessing the system (false match) is much higher than the cost associated to a false non-match. On the other hand, in an application where availability is paramount and the sensitivity of the information is low, the cost associated with a valid user being denied access (false non-match) is higher than the cost associated with an impostor getting access. This research makes the assumption that the cost of both errors is equal.

---

¹ “The Three Bears” rule is named after the traditional English children’s story [SOU 37] in which Goldilocks enters the vacant cottage of the three bears. Inside, she samples everything she finds. The Great Huge Bear’s porridge/chair/bed is too hot/hard/high, the Middle Bear’s too cold/soft/low, but the Little Small Wee Bear’s things are “Just Right!”

3.6 Fingerprint subsystem

To evaluate the performance of the fingerprint subsystem illustrated in Figure 3.1, matching errors need to be collected. Matching errors will occur when a sample is falsely declared to match a genetically different template (FMR) or when a sample is falsely declared not to match a genetically identical template (FNMR). To collect matching errors, one needs:

- enrolled fingerprints (fingerprint templates)
- fingerprint impressions to compare to enrolled fingerprints
- a fingerprint system which includes the feature extraction module, the matching module and the decision module

Figure 3.1. Fingerprint subsystem

The remainder of this section will describe the database of fingerprint impressions and the fingerprint software used to conduct the fingerprint experiment.

3.6.1 The FVC 2000 (DB3 Set A) database

Fingerprint templates and fingerprint impressions must come from a test sample. The larger the sample, the greater the accuracy of error rate measurements. The cost of collecting a large test sample is extremely high. A cost effective and accepted option is to use existing databases of fingerprint information to conduct research and testing. The fingerprint database known as DB3 Set A was used in this research. It was created for the Fingerprint Verification Competition of 2000 [MAI 02]. The sensor used to collect the fingerprint images stored in the database is named Identicator Technology Optical Sensor “DF-90”.

The following data collection information was provided in [MAI 02]. The fingerprints are from 19 volunteers between ages 5 to 73 where 55% are male. Figure 3.2 describes the age distribution of DB3 Set A.

Figure 3.2. Age distribution of DB3 Set A used in Fingerprint Verification Competition of 2000 (FVC 2000)

Each of the 19 volunteers was seen at four sessions, with no more than two sessions on any single day. The time between the first and the last sessions was at least 3 days and as long as 43 months, depending upon the volunteer. The sensor platen was systematically cleaned between acquisition of each image and at one session each volunteers had their fingers cleaned with rubbing alcohol and dried.

Two images of six fingers (thumb, fore and middle on left and right hands) were taken for each volunteer without interleave from each volunteer at each session. Some part of the core was apparent in each image, but care was taken to avoid complete overlap between consecutive images taken during a single session. All acquired fingerprints were analyzed manually to ensure that the maximum rotation was within the prescribed range of $[-15^\circ, 15^\circ]$. Each pair of impressions of the same finger has a non-null overlapping area. This data collection effort resulted in 114 different fingers with 8 impressions per finger.

DB3 set A has been created using this data collection effort. It has 100 fingers with 8 impressions per finger for a total of 800 fingerprints. For the purpose of this experiment, 80 fingers with seven impressions each will be used for a total of 560 fingerprints. Each fingerprint has been saved as a .tif file of size 448 X 478 at a resolution of 500 dpi. The fingerprints are labeled using the finger number followed by the impression number. For example, the seven impressions of finger 1 are labeled as follow:

- 1_1.tif;
- 1_2.tif;
- 1_3.tif;
- 1_4.tif;
- 1_5.tif;
- 1_6.tif;
- 1_7.tif.

The “Biometric Testing Best Practices” requires researchers to collect a number of samples per volunteers to ensure that the total number of attempts satisfies the “Rule of 30” [MAN 02]. The rule states that to be 90% confident that the true error rate is within $\pm 30\%$ of the observed error rate, there must be at least 30 errors. This requirement was not met using the data set available. The cost of collecting additional data precluded using this option for the purpose of this research.

3.6.2 VeriFinger version 4.1 software

The software used for the fingerprint verification experiment is the identification engine VeriFinger version 4.1 released on December 3rd, 2002 by Neurotechnologija Ltd [NEU 03]. The engine is intended for biometric system developers and integrators. The software Development kit (SDK) has been used by the author to customize the application and provide the required information for this experiment.

The fingerprint recognition algorithm follows the discontinuities and irregularities of fingerprint ridges and valleys called minutiae. In addition to this scheme it utilizes an

adaptive image filtration algorithm which eliminates or reduces noises such as ridge ruptures and stuck ridges. The VeriFinger recognition engine is highly reliable and has earned the 6th position overall in the Fingerprint Verification Competition in 2002 where 31 algorithms were tested. Using the ROC curve provided for Neurotechnologija in the Fingerprint Verification Competition, an FMR of 0.001% has been evaluated for a FNMR of 2.07% [MAI 02]. The algorithm matching speed is among the highest. It has received one silver and two bronze medals against the standard databases. The software can be used in 1:1 matching (verification) mode as well as 1: N matching (verification) mode.

3.7 Voice subsystem

To evaluate the accuracy performance of the voice subsystem illustrated in Figure 3.3, matching errors and matching scores need to be collected. To collect matching errors, one needs:

- enrolled sentences (speech templates)
- sentence repetitions to compare to enrolled sentences
- a voice system which includes the feature extraction module, the matching module and the decision module

Figure 3.3. Voice subsystem

The remainder of this section will introduce and describe the database of voice samples and the voice software used to conduct the voice experiment.

3.7.1 The XM2VTS database

Voice templates and sentence repetitions must come from a test sample. The database in [MES 99] used for this research has been created by the University of Surrey and is referred to as the Extended M2VTS database or XM2VTSDB. The database contains head rotation information and audio information. It was acquired using a Sony VX1000E digital camcorder and DHR1000UX digital VCR. A high quality clip-on microphone was used to record the voice information.

A total of 295 subjects of both sexes and different ages were asked to utter predefined sentences twice at four different sessions. Sessions took place over a period of five months. Each subject read each sentence 8 times. For the purpose of this experiment,

only 80 subjects out of the 295 subjects and only one sentence will be used. The sentence used in the experiment read: “zero one two three four five six seven eight nine”. Each sentence repetition has been recorded as mono, 16 bit, 32 KHz, PCM wave file.

The sentences are labeled using the subject number followed by the session number and the repetition number (only repetitions 1 and 4 were utilized). For example, the 8 voice samples for subject 1 are labeled as follow:

- 001_1_1.wav;
- 001_1_4.wav;
- 001_2_1.wav;
- 001_2_4.wav;
- 001_3_1.wav;
- 001_3_4.wav
- 001_4_1.wav;
- 001_4_4.wav.

The XM2VTS database is currently the largest database available for voice information.

The “Biometric Testing Best Practices” requires researchers to collect a number of samples per volunteer to ensure that the total amount of attempts satisfies the “Rule of 30” [MAN 02].

3.7.2 The VoiceSafeEvaluator software

The software used for the voice verification experiment is the VoiceSafe™ speaker verification software from Patni Computer Systems Inc. The voice recognition algorithm is based on voice biometrics technology that analyzes the physiological characteristics of the vocal tract to create and compare the voiceprints of a speaker. The algorithm is a text dependent, language independent library developed in C [PAT 03]. The author of this thesis has customized the VoiceSafeEvaluator command-line utility tool to provide the required information for the experiment. Using VoiceSafe™, the users must use the same utterance for enrolment and verification. The user has the flexibility to choose a passphrase of any length. The software performs well in noisy environments as the voice spectrum used in the system is modified for robustness using various techniques based on adaptive and non-adaptive algorithms.

3.8 Multimode system

The multimode system used in this experiment is shown in Figure 3.4. To evaluate the performance of the multimode system illustrated in Figure 3.4, matching errors and matching scores need to be collected. To collect matching errors, one needs:

- enrolled fingerprints and enrolled sentences
- fingerprint impressions and sentence repetitions to compare to enrolled fingerprints and sentences

- a multimode system that maps each opinion in a $[0,1]$ interval and performs weighted summations with different weight combinations

Figure 3.4. Multimode system

The enrolled fingerprints are from the FVC 2000 (DB3 Set A) database described in section 3.5.1. The enrolled sentences are from the XM2VTS Database described in section 3.6.1. Microsoft Excel 2002 SP-2 for Windows XP was used to map each score into the $[0, 1]$ interval and perform the appropriate weighted summations.

4 Chapter 4 - Conducting the experiment

The experiment consists of evaluating the performance of the fingerprint subsystem, the voice subsystem, and the multimode system. This chapter is divided into three main sections. Each section explains the accuracy performance tests conducted on the fingerprint subsystem, the voice subsystem, and the multimode system.

4.1 Fingerprint subsystem

To collect matching errors, fingerprints need to be enrolled and verification attempts against the enrolled fingerprints must be performed. For the purpose of the experiment, fingerprint impressions have been divided in two distinct categories: enrolment impressions and verification impressions. The first three impressions of each finger have been used for enrolment impressions while the other four impressions have been used for verification impressions. For each finger, impressions 1, 2 and 3 are used for enrolment purposes (a total of 240 enrolment impressions) and impressions 4, 5, 6 and 7 are used for verification purposes (a total of 320 verification impressions). Enrolment impressions were never used for verification attempts. The remainder of this section will discuss the enrolment process as well as the verification process against the enrolled templates.

4.1.1 Enrolment process

The enrolments of fingerprint impressions were performed using the features generalization mode available in VeriFinger. VeriFinger performed the conjunction of several features coming from impression 1, 2 and 3 of each finger to create a high quality template, validating each feature and removing noisy features.

4.1.2 Verification process

Impressions 4, 5, 6 and 7 were used for verification purposes for a total of 320 verification impressions. The verification impressions are used for verification attempts. Verification attempts can be divided into two categories:

1. genuine attempt trials - a fingerprint impression genetically identical to the claimed fingerprint template is attempting authentication
2. impostor attempt trials - a fingerprint impression genetically different to the claimed fingerprint template is attempting authentication

Genuine attempt trials consisted of impressions 4, 5, 6 and 7 attempting to verify against the template created by the first three impressions of the same finger. Therefore for each of the 80 fingers, 4 genuine attempt trials were performed for a total of 320 genuine

attempt trials. All the impostor attempt trials were conducted using full cross-comparison. Cross-comparison is achieved when each template is compared with every genetically different enrollment template. For each of the 80 fingers in the database, the 4 verification impressions were compared to the 79 non-self fingerprint templates. Using this method, 25 280 impostor attempt trials ($80 \times 4 \times 79$) were generated. All impostor attempts are qualified as zero-effort attempts. Zero-effort attempts are described in [MAN 02] as an impostor submitting their own biometric features as if they were attempting successful verification against their own template.

For each genuine and impostor attempts the matching score which is the opinion of the fingerprint subsystem was recorded into a database. Assuming that impostor and true claims follow Gaussian distributions, each original opinion ($o_{f,orig}$) from the fingerprint subsystem was mapped to a $[0, 1]$ interval using a sigmoid described in [SAN 02]:

$$o_f = \frac{1}{1 + \exp[-\tau_f(o_{f,orig})]}$$

where

$$\tau_f(o_{f,orig}) = \frac{o_{f,orig} - (\mu_f - 2\sigma_f)}{2\sigma_f}$$

and μ_f and σ_f are the mean and the standard deviation of original opinions of the fingerprint subsystem for true claims.

4.2 Voice subsystem experiment

To collect matching errors and matching scores, voice samples need to be enrolled and verification attempts against the enrolled sentences must be performed. For the purpose of the experiment, voice repetitions will also be divided in two distinct categories: training utterances and verification repetitions. The 4 voice repetitions recorded in session one and two will be used as the 4 training utterances required to create the voice template for each subject. The 4 voice repetitions recorded in session three and four will be used for verification repetitions. Therefore, voice samples 1_1, 1_4, 2_1 and 2_4 of each subject will be use for enrolment purpose for a total of 320 training utterances and voice samples 3_1, 3_4, 4_1 and 4_4 of each subject will be use for verification purpose for a total of 320 verification repetitions. Training utterances will never be used for verification attempts.

4.2.1 Enrolment process

The enrolments of sentences consisted of the preprocessing of the four recorded training utterances where the voice signals were enhanced while the background noise was reduced by the VoiceSafe^{TM} software [PAT 03]. The features of the four training utterances were extracted and then clustered together to create the voice templates that were enrolled in the database.

4.2.2 Verification process

Genuine attempt trials consisted of voice samples 3_1, 3_4, 4_1 and 4_4 of each subject attempting to verify against the enrolled voice template created with the first four voice samples of the same subject. For each of the 80 enrolled voice templates in the database, the 4 genuine attempt trials were performed for a total of 320 genuine attempt trials. All the impostor attempt trials were conducted using full cross-comparison. For each of the 80 voice templates in the database, the 4 verification repetitions were compared to the 79 genetically different voice templates. Using this method, 25 280 impostor attempt trials (80X4X79) were generated. All impostor attempts are, once again, qualified as zero-effort attempts.

For each genuine and impostor attempt the matching score was recorded into a database. The matching score is the opinion provided by the voice subsystem. Assuming that impostor and true claims follow Gaussian distributions, each original opinion ($o_{v,orig}$) from the voice subsystem was mapped to a [0, 1] interval using a sigmoid described in [SAN 02]:

$$o_v = \frac{1}{1 + \exp[-\tau_v(o_{v,orig})]}$$

where

$$\tau_v(o_{v,orig}) = \frac{o_{v,orig} - (\mu_v - 2\sigma_v)}{2\sigma_v}$$

and μ_v and σ_v are the mean and the standard deviation of original opinions of the voice subsystem for true claims.

4.3 Multimode system experiment

To evaluate the accuracy performance of the multimode verification system, matching errors and matching scores need to be collected. For each subsystem, a total of 320 genuine attempt trials and 25,280 impostor attempt trials were conducted. For each subsystem, genuine attempt trials were labeled 1 to 320 and impostor attempt trials 1 to 25,280. A matching score was recorded for each of the genuine and impostor attempt trials as part of the subsystem experiments. The accuracy performance results of the multimode verification system will be established using a confidence level fusion strategy. The opinions of each subsystem will be combined using a weighted summation approach with different weights assigned to each subsystem.

The first strategy is to assign equal weights to the fingerprint and the voice subsystems. Because the sum of the weights of both subsystems must equal 1, this means that each subsystem will have a weight of 0.5. The second strategy will vary the weight of each subsystem. Table 4.1 shows the weights assigned to each subsystem in eight different combinations.

Table 4.1. Different weights assigned to each subsystem (Strategy 2)

	Fingerprint Subsystem	Voice Subsystem
Combination 1	0.1	0.9
Combination 2	0.2	0.8
Combination 3	0.3	0.7
Combination 4	0.4	0.6
Combination 5	0.6	0.4
Combination 6	0.7	0.3
Combination 7	0.8	0.2
Combination 8	0.9	0.1

5 Chapter 5 - Results

This chapter is divided into three main sections. Section 5.1 presents the results of the fingerprint subsystem; Section 5.2 the results of the voice subsystem; and section 5.3 the results of the multimode system.

5.1 Fingerprint subsystem results

5.1.1 Quality of impressions

Impressions 1, 2 and 3 were used for enrolment purposes for a total of 240 enrolment impressions. The following figures describe the quality assessment of the 240 enrolment impressions provided by the software. Figure 5.1 depicts the number of low and good quality enrolment impressions while figure 5.2 shows the number of low quality enrolment impressions per finger.

Figure 5.1. Number of low and good quality enrolment impressions

Figure 5.2. Number of low quality enrolment impressions per finger

Impressions 4, 5, 6 and 7 were used for verification purposes for a total of 320 verification impressions. The following figures describe the quality of the 320 verification impressions. Figure 5.3 depicts the number of low and good quality verification impressions while figure 5.4 shows the number of low quality verification impressions per finger.

Figure 5.3. Number of low and good quality verification impressions

Figure 5.4. Number of low quality verification impressions per finger

5.1.2 Results of genuine attempt trials

In a genuine attempt trial, a matching/decision error occurs when a sample is incorrectly declared not to match a genetically identical template. This is reported using FNMR.

Given 320 comparisons, the matching module provided 320 matching scores. A total of 27 of those matching scores were below the threshold of 47 selected by the software. Of the 320 samples provided, a total of 27 samples were declared not to match their own template. This resulted in 27 matching errors.

$$FNMR = \frac{27 \text{ Legitimate User Rejections}}{320 \text{ Legitimate Claims}} \times 100\% = 8.43\%$$

Figure 5.5 depicts the 320 original matching scores obtained from the genuine attempt trials. The highest matching score obtained was 797 and the lowest matching score was 0. A total of 6 scores of 0 were obtained.

Figure 5.5. Scores obtained from genuine attempt trials

For each genuine attempt the matching score and the decision was recorded into a database. The report of all genuine attempts is available on request.

5.1.3 Results of impostor attempt trials

In an impostor attempt trial, a matching error occurs when a sample is falsely declared to match a genetically different template. This is reported using FMR. Given 25 280 comparisons, the matching module provided 25 280 matching scores. There was no

impostor score that were equal or above the threshold selected by the software of 47. Of the 25 280 samples provided, not a single one was declared to match a genetically different template. This resulted in 0 matching error.

$$FMR = \frac{0 \text{ Impostor Acceptances}}{25\,280 \text{ Impostor Claims}} \times 100\% = 0.00\%$$

Figure 5.6 depicts the 25 280 matching scores obtained from the impostor attempt trials. The highest original matching score obtained was 22 and the lowest matching score was 0. A total of 13 957 scores of 0 were obtained. It is worth noting that 98% of all scores were equal or below 10. For each impostor attempt the matching score and the decision was recorded into a database and a report of all impostor verification attempts was created. The report of all impostor attempts is available upon request.

Figure 5.6. Scores obtained from impostor attempt trials

5.1.4 ROC and DET curves

Figure 5.7 and figure 5.8 show the ROC and DET curves of the fingerprint subsystem.

Figure 5.7. Fingerprint subsystem ROC curve

Figure 5.8. Fingerprint subsystem DET curve

5.2 Voice subsystem results

5.2.1 Results of genuine attempt trials

In a genuine attempt trial, a matching/decision error occurs when a sample is falsely declared not to match a genetically identical template. This is reported using FNMR. Given 320 comparisons, the matching module provided 320 matching scores. A total of 93 scores were below the optimal threshold selected by the application. Of the 320 samples provided, a total of 93 samples were declared not to match their own template resulting in 93 matching errors.

$$FNMR = \frac{93 \text{ Legitimate User Rejections}}{320 \text{ Legitimate Claims}} \times 100\% = 29.06\%$$

Figure 5.9 shows the original 320 matching scores obtained from the genuine attempt trials. To improve the clarity of figure 5.9, a total of 14 scores of -2000000 are not shown. The highest matching score obtained was 1064 and the lowest matching score besides the scores of -2000000 was -18450. A total of 45 scores of 0 were obtained. From the scores and decisions obtained, it can be determined that the optimal threshold selected by the application is in the range 524 to 566 depending on the training utterances. For each genuine attempt, the matching score and the decision was recorded into a database. The report of all genuine verification attempts is available on request.

Figure 5.9. Scores obtained from genuine attempt trials

5.2.2 Results of impostor attempt trials

In an impostor attempt trial, a matching error occurs when a sample is falsely declared to match a genetically different template. This is reported using FMR. Given 25 280 comparisons, the matching module provided 25 280 matching scores. A total of 3992 scores were at or above the optimal threshold of 0. Of the 25 280 samples provided, a total of 3992 samples were declared to match a genetically different template resulting in 3992 matching error.

$$FMR = \frac{3992 \text{ Impostor Acceptances}}{25\,280 \text{ Impostor Claims}} \times 100\% = 15.79\%$$

Figure 5.10 shows the ordered 25 280 matching scores obtained from the impostor attempt trials. Once again to increase the clarity of the figure, a total of 2502 scores of -2000000 are not shown. The highest matching score obtained was 1104 and the lowest matching score besides the scores of -2000000 was -23 940. A total of 3664 scores of 0 were obtained. For each impostor attempt, the matching score and the decision were recorded into a database and a report of all impostor verification attempts was created. The report of all impostor verification attempts is available on request.

Figure 5.10. Scores obtained from impostor attempt trials

5.2.3 ROC and DET curves

Figure 5.11 and figure 5.12 show the ROC and DET curves of the voice subsystem.

Figure 5.11. Voice subsystem ROC curve

Figure 5.12. Voice subsystem DET curve

5.3 Multimode system results

5.3.1 Strategy 1 DET curves

Using the pre-recorded matching score mapped to a $[0, 1]$ interval from the fingerprint subsystem (opinion 1) and from the voice subsystem (opinion 2) the supervisor module performed a weighted summation with equal weights assigned to each subsystem.

Figure 5.13 shows the DET curves for the multimode verification system using Strategy 1.

Figure 5.13. Strategy 1 DET curve

5.3.2 Strategy 2 DET curves

Using the pre-recorded matching score mapped to a [0, 1] interval from the fingerprint subsystem (opinion 1) and from the voice subsystem (opinion 2) the supervisor module performed a weighted summation with the eight different combinations of weights shown below:

	Fingerprint Subsystem	Voice Subsystem
Combination 1	0.1	0.9
Combination 2	0.2	0.8
Combination 3	0.3	0.7
Combination 4	0.4	0.6
Combination 5	0.6	0.4
Combination 6	0.7	0.3
Combination 7	0.8	0.2
Combination 8	0.9	0.1

Figure 5.14 shows the DET curves for the multimode system using Strategy 2 for all combinations.

Figure 5.14. DET curves of all combination under Strategy 2

6 Chapter 6 - Discussion of results

This chapter discusses the results obtained from the fingerprint subsystem, the voice subsystem, and the multimode fingerprint-voice system. This chapter is divided into three sections. The first section addresses the first objective of the thesis. It compares the performance of the multimode system to the performances of the fingerprint subsystem and the voice subsystem. The second section addresses the second objective of the thesis. It compares the two strategies and all the combinations of weights to one another. The last section summarizes the performance results.

6.1 Multimode system vs. subsystems

The DET curves are used to compare different biometric systems. The closer the curve is to the horizontal axis, the better the performance of the biometric system. To evaluate if the performance of the fingerprint-voice multimode system has surpassed the performance of the fingerprint system and the performance of the voice system, their DET curves are plotted on the same graph.

6.1.1 Strategy 1

Figure 6.1 shows the DET curves of the multimode system using Strategy 1 as well as the DET curves of the fingerprint and voice subsystems.

Figure 6.1. DET curves of Strategy 1 and the two subsystems

Figure 6.1 shows that the DET curve of the multimode system using Strategy 1 falls between the DET curves of the fingerprint and voice subsystems. It can be concluded that the DET curve of the multimode system using Strategy 1 is better than the voice subsystem but worse than the fingerprint subsystem. Therefore, the multimode system using confidence level fusion and equal weights assigned to each subsystem has outperformed the voice subsystem but not the fingerprint subsystem.

6.1.2 Strategy 2

Figures 6.2 to 6.9 show the DET curves of the fingerprint-voice system, the fingerprint subsystem and the voice subsystem using Strategy 2 and the combination shown in Table 4.1

Figure 6.2. DET curve of the multimode system using Strategy 2 combination 1 (fingerprint subsystem = 0.1) and the DET curves of the fingerprint and voice subsystems

Figure 6.3. DET curve of the multimode system using Strategy 2 combination 2 (fingerprint subsystem = 0.2) and the DET curves of the fingerprint and voice subsystems

Figure 6.4. DET curve of the multimode system using Strategy 2 combination 3 (fingerprint subsystem = 0.3) and the DET curves of the fingerprint and voice subsystems

Figure 6.5. DET curve of the multimode system using Strategy 2 combination 4 (fingerprint subsystem = 0.4) and the DET curves of the fingerprint and voice subsystems

Figure 6.6. DET curve of the multimode system using Strategy 2 combination 5 (fingerprint subsystem = 0.6) and the DET curves of the fingerprint and voice subsystems

Figure 6.7. DET curve of the multimode system using Strategy 2 combination 6 (fingerprint subsystem = 0.7) and the DET curves of the fingerprint and voice subsystems

Figure 6.8. DET curve of the multimode system using Strategy 2 combination 7 (fingerprint subsystem = 0.8) and the DET curves of the fingerprint and voice subsystems

Figure 6.9. DET curve of the multimode system using Strategy 2 combination 8 (fingerprint subsystem = 0.9) and the DET curves of the fingerprint and voice subsystems

Figures 6.2 to 6.9 show that for all combinations under Strategy 2, the DET curve of the multimode system falls above the DET curve of the fingerprint subsystem and below the DET curve of the voice subsystem. We conclude from these results that the multimode system performed better than the voice subsystem, but worse than the fingerprint subsystem.

6.2 Effectiveness of different weight combinations

One needs to select which combination of weights is the most effective at combining the two subsystems' opinions about a user's claim into an accurate authentication decision. In order to achieve this, the DET curves of the multimode system using all combinations of weights have to be plotted on the same graph. Figure 6.10 shows the DET curves of the proposed multimode system using Strategy 1 and Strategy 2 with all weight combinations.

Figure 6.10. DET curves of the multimode systems using all combinations of weights

The DET curve that is closest to the horizontal axis is the DET curve of Strategy 2 combination 8. It can be concluded that the DET curve of the multimode system using Strategy 2 combination 8 is the most effective at combining the two subsystems opinions about a user's claim into an accurate authentication decision. .

6.3 Summary of results

The experiment had two objectives:

1. Test whether or not a voice-fingerprint biometric system can perform better than its voice subsystem and its fingerprint subsystem.
2. Identify the weights which are most effective at combining the opinions of the voice and fingerprint subsystems into an accurate authentication decision

Based on the DET curves shown in sections 6.1.1 and 6.1.2, I conclude that:

- The fingerprint-voice system performs better than the voice subsystem. This result supports the findings that conclude that multimode systems perform better than single mode systems reported in [BEN 99B][HON 99][13][POH 01][ROS 01].
- The fingerprint-voice system did not outperform the fingerprint subsystem. This result contradicts the view widely held in the biometrics community that the

integration of biometrics always results in significant performance improvements [HON 99].²

- Strategy 2 combination 8 is the most effective at combining the opinions of the fingerprint and voice subsystems into an accurate authentication decision.

Strategy 2 combination 8 is the combination assigning the highest weight to the fingerprint subsystem, 0.9. The accuracy performance of the fingerprint subsystem however surpasses the combination 8 of Strategy 2.

The results of my experiment, lead me to conclude that multimode biometric systems do not always perform better than their two subsystems as it is assumed. I surmise that if the accuracy performance of two subsystems is significantly different, the accuracy performance of the multimode system using a confidence level biometric fusion can be higher than the less reliable subsystem and lower than the performance of the more reliable subsystem. Therefore, the consistent and significant performance improvement when integrating multiple biometrics discussed in [HON 99] is highly dependent on the initial accuracy performance of the biometrics to be integrated and the integration method used.

---

² In [HON 99] the performance analysis was based on the accuracy performance and it was assumed that cost and speed did not play a significant role in the performance assessment.

7 Chapter 7 – Conclusion

This thesis reports the results of an experiment conducted to compare the performance of a fingerprint-voice multimode system with the performance of its fingerprint and voice subsystems.

7.1 Thesis objectives

Is the performance of a fingerprint-voice biometric system using a weighted summation approach superior to the performances of its fingerprint and speech subsystems? The answer is: no. The performance of the multimode system is not superior to its fingerprint and voice subsystems when a weighted summation approach is used. In the experiment, the accuracy performance of the multimode system is only superior to the accuracy performance of the voice subsystem.

This thesis had two objectives

1. Test whether or not a voice-fingerprint biometric system can perform better than its voice subsystem and its fingerprint subsystem.
2. Identify the weights which are most effective at combining the opinions of the voice and fingerprint subsystems into an accurate authentication decision.

Based on the results of the experiment I conclude that:

- the performance of the multimode system is better than the performance of the voice subsystem but lower than the performance of the fingerprint subsystem
- the most effective combination of subsystem opinions was the one that assigned a weight of 0.9 to the fingerprint subsystem and a weight of 0.1 to the voice subsystem.

7.2 Conclusions

Four conclusions can be drawn from the results of the experiment undertaken in this thesis.

1. The performance of the fingerprint-voice system is lower than the performance of the fingerprint subsystem regardless of the weight assigned to each subsystem. Thus, the integration of multiple biometrics does not always result in a significant performance improvement.
2. The performance improvement of a multimode system in comparison to its subsystems is dependent on the initial accuracy performance of its subsystems and the fusion strategy used.

3. The rule of 30 described in [MAN 02] is not realistic. The rule states that to be 90% confident that the true error rate is within $\pm 30\%$ of the observed error rate, there must be at least 30 errors. For the fingerprint subsystem, no false match error was collected after 25280 attempts. With the cost associated with data collection and the limited number of standardized databases the rule of 30 is not possible to achieve.
4. The accuracy performance of the multimode system is higher than the accuracy performance of the voice subsystem regardless of the weight combination assigned to each subsystem.

7.3 Contributions

The experiment is the first experiment combining fingerprint and voice information. The results contribute to research in the emerging area of biometrics. The most significant contributions this thesis makes to biometric research are two:

- finding that the integration of multiple biometrics does not result in a consistent and significant performance improvement as originally believed.
- realization that the improvement in performance of a multimode system is a function of the initial performance of the subsystems to be integrated and the integration method used.

The matching scores obtained from the experiment can further increase the contribution to biometric research. Finding the most efficient way to combine subsystem opinion in a valid decision is a major research challenge. The experiment recorded in a database the 320 genuine-matching scores as well as 25 280 impostor-matching scores for both subsystems. These scores can be used to attempt different fusion techniques and the results can be compared to the confidence level fusion (weighted summation) that was performed as part of this experiment.

The experiment used two major databases: the FVC 2000 (DB3 Set A) database and the XM2VTS database. The software used in the experiment provided insights on the quality of the fingerprint and voice samples available from those databases. This information can be useful in assessing currently available databases and in creating new standardized databases.

The experiment follows the terminology and the best practices in testing and reporting performance of biometric devices suggested in [MAN 02]. In an emerging field like biometric testing where conflicting definitions are implicit in literature, conducting experiment that follows an accepted framework is valuable.

An understanding of the critical need for more accurate authentication methods and the different fusion techniques used in multimode biometrics is essential for engineering management practitioners. A better comprehension of biometric and multimode biometric technology facilitates the challenging task of managing emerging technologies in a rapidly changing world.

7.4 Future research

More research is needed to clearly understand how the use of multiple biometric identifiers affects system performance. The relationship between the initial accuracy performances of the subsystems and the final accuracy performance of the multimode system is not clear.

Finding the most effective way to fuse independent subsystem opinions into a more accurate decision and improving system performance is a significant research challenge. Further research needs to be done using other integration methods like the weighted product or the Bayesian rule. As accuracy performance are also dependent on the environment, the people and the application used, it would be informative to have more research done with other large databases and different applications.

The accuracy performance in the experiment was based on a non-adaptive approach (i.e., the weight of each subsystem is fixed a priori). Moreover research is needed in the use of an adaptive approach. An adaptive approach would learn user-specific parameters and adjust the weight of each subsystem depending on the user's identity claim as suggested in [JAI 02]. It would be informative to study the effect of varying the weight assigned to the voice subsystem according to the consistency of a specific user at uttering his pass phrase. Similarly, the weight of the fingerprint subsystem could vary according to the quality of the specific user's fingerprint and to the consistency at presenting his

fingerprint to the fingerprint sensor. Another adaptive approach could vary the weight of each subsystem depending on the environment conditions like signal to noise ratio. Furthermore, as proposed in [XIA 02], a dynamically adjusted weighted summation can be used based on the rejection reason.

The impostor attempts conducted in this experiment were based on zero-effort attempts. Cross-comparison is achieved when each template is compared with every genetically different enrollment template. While this is an accepted practice, it does not provide a clear view on false match rate. More research is needed in how to measure active impostor attempts.

The impostor attempts in the experiment were generated using full cross-comparison where each sample is compared to each non-self template. From looking at the voice results obtained from the impostor attempts, it can be seen that when one sample was wrongly accepted, often the other utterances of the same voice samples were also accepted. This suggests that those results may be dependent and may not reflect accurately the false match rate. More research is needed to validate the use of cross-comparisons when calculating FMR.

References

- [ACH 96] M.P. Acheroy, C. Beumier, J. Bigüm, G. Chollet, B. Duc, S. Fischer, D. Genoud, P. Lockwood, G. Maitre, S. Pigeon, I. Pitas, K. Sobottka and L. Vandendorpe, "Multi-modal person verification tools using speech and images," in Proceedings of the European Conference on Multimedia Applications, Services and Techniques (ECMAST '96), pp. 747-761, May 1996.
- [ASH 00] J. Ashbourn, Biometrics: Advanced Identity Verification, The Complete Guide. Springer, London, 2000.
- [BEN 99A] S. Ben-Yacoub, Y. Abdeljaoued and E. Mayoraz, "Fusion of face and speech data for person identity verification," IEEE Trans. Neural Networks, vol. 10, pp. 1065-1074, 1999.
- [BEN 99B] S. Ben-Yacoub and J. Luetttin, "Robust person verification based on speech and facial images," in Proceedings of the European Conference on Speech Communication and Technology, volume 2, pp. 991-994, September 1999.
- [BIG 97] E.S. Bigun, J. Bigun, B. Duc and S. Fischer, "*Expert conciliation for multimode person authentication systems by bayesian statistics*," in Proceedings of the Audio and Video based Person Authentication (AVBPA'97), Crans-Montana, Switzerland, pp. 311-318, 1997.
- [BOM 03] M. Bomba, "BioIdentification frequently asked questions," Retrieved 3/24/03 World Wide Web, <http://home.t-online.de/home/manfred.bomba/biofaq.htm>
- [BRU 95] R. Brunelli and D. Falavigna, "Person identification using multiple cues," IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 17, pp. 955-966, October 1995.
- [DOD 00] G.R. Doddington, M.A Przybocki, A.F.Martin and D.A. Reynolds, "The NIST speaker recognition evaluation: Overview methodology, systems, results, perspective," *Speech Communication*, pp. 225-254, 2000.
- [FEN 01] J. Fenn, "Ten technologies for 2002-2007", Gartner Research Note T-150205, December 2001.

- [FRI 00] R.W. Frischholz and U. Dieckmann, "BioID: A multimode biometric identification system," *IEEE trans. Computer*, vol. 33, pp. 64-68, February 2000.
- [HON 98] L. Hong and A.K. Jain, "Integrating faces and fingerprints for personal identification," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 20, pp. 1295-1307, December. 1998.
- [HON 99] L. Hong, A.K. Jain and S. Pankanati, "Can multibiometrics improve performance?" in *Proceedings AutoID'99*, NJ, pp. 59-64, October 1999.
- [JAI 02] A.K. Jain and A. Ross, "Learning user-specific parameters in a multibiometric system (2002)," *Proc. International Conference on Image Processing (ICIP)*, Rochester, New York, September 2002.
- [KIT 97] J. Kittler, Y.P. Li, J. Matas and M.U. Ramos Sánchez, "Combining evidence in multimode personal identity recognition systems," in *Proceedings of the Audio and Video based Personal Authentication (AVBPA '97)*, Crans-Montana, Switzerland, pp. 327-334, 1997.
- [MAI 02] D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman and A.K. Jain, "FVC2000: Fingerprint verification competition", *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 24, pp.402-412, 2002.
- [MAN 02] A.J. Mansfield and J.L. Wayman, "Best practices in testing and reporting performance of biometric devices," *National Physical Laboratory*, Middlesex, Aug. 2002.
- [MAR 97] A. Martin, G.R.Doddington, T. Kamm, M. Ordowski and M.A. Przybocki, "The DET curve in assessment of detection task performance," in *Proceedings of Eurospeech*, Rhodes, Greece, pp. 1895-1898, 1997.
- [MAT 02] T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," in *Proceedings of SPIE*, vol. 4677, *Optical Security and Counterfeit Deterrence Techniques IV*, 2002.
- [MES 00] K. Messer, "The XM2VTS database: CDS003 audio dataset," *Centre for Vision, Speech and Signal Processing*, University of Surrey, Feb. 2000.
- [MES 99] K. Messer, J. Matas, J. Kittler, J. Luetten and B. Maitre, "Xm2vtsdb: The extended m2vts database," in *Proceedings of the Second International Conference on Audio and Video-based Biometric Person Authentication*, pp. 72-77, 1999.

- [NAN 02] S. Nanavati, M. Thieme and R. Nanavati, Biometrics: Identity Verification in a Network World. A Wiley Tech Brief, Wiley Computer Publishing, 2002.
- [NEU 03] Neurotechnologija Ltd, "VeriFinger: Fingerprint identification system," Retrieved 3/24/03 World Wide Web, <http://www.neurotechnologija.com/verifinger.html>
- [ONW 01] On World, "Fingerprint recognition technology," Published by On World, Nov. 2001.
- [PAT 03] Patni Computer Systems Limited, "Voice technology white paper", Retrieved 3/24/03 World Wide Web, <http://www.mobilizesite.com/Brochure/VoiceTech.pdf>
- [POH 01] N. Poh and J. Korczak, "Hybrid biometric person authentication using face and voice features," in Proceedings of the Audio and Video-based Person Authentication (AVBPA '01), pp. 348-353, Halmstad, Sweden, 2001.
- [POH 02] N. Poh, S. Bengio and J. Korczak, "A multi-sample multi-source model for biometric authentication," Research paper IDIAP-RR-02-14, IDIAP, Martigny, Switzerland, April 2002.
- [ROS 01] A. Ross, A.K. Jain and J. Qian, "Information fusion in biometrics," in Proceedings of the Audio and Video-based Person Authentication (AVBPA'01), pp. 354-359, Halmstad, Sweden 2001.
- [SAN 02] C. Sanderson, "Information fusion and person verification using speech & face information," Research paper IDIAP-RR 02-33, IDIAP, Martigny, Switzerland, September 2002.
- [SHA 02] C. Shaw, "Who is expected to fight fraud," PricewaterhouseCoopers, Management Magazine, June 2002.
- [SOU 37] R. Southey, The story of the three bears. The doctor: Volume iv, Longman, 1837.
- [THA 03] L.Thalheim, J. Krissler and P.M. Ziegler, "Body check: Biometric access protection devices and their programs put to the test", Retrieved 3/24/03 World Wide Web, <http://www.heise.de/ct/english/02/11/114>

- [VER 99] P. Verlinde, G. Chollet and M. Acheroy, "About multi-modal identity verification in interactive dialogue systems," in Proceedings of the ESCA/IDS99, Kloster Irsee, Germany, April 1999.
- [WAR 99] T. Wark, S. Sridharan and V. Chandran, "Robust speaker verification via fusion of speech and lip modalities", in Proceedings of the International Conference of Acoustics, Speech and Signal Processing, volume 6, pp.3061-3064, Phoenix, Arizona, 1999.
- [XIA 02] Q. Xiao, "An approach on adaptive multimode biometric fusion", Defence R&D Canada, working paper, November 2002.

Appendix A – Overview of biometrics and multimode biometrics

This appendix provides an overview of traditional authentication methods and their limitations. It also describes the different biometric techniques, their general operating methodology and the different accuracy performance metrics for biometric systems. Multimode biometric is introduced and the different fusion strategies are explained.

Traditional authentication methods

There are several methods in use for checking personal identity today. The traditional authentication methods are related to something that the individual has (possession based) or something that the individual knows (knowledge based). Possession is often related to an identity card, a smart card or a token. Knowledge is frequently associated with a password, a personal identification number (PINs) or a piece of information (e.g. mother's maiden name).

The possession based authentication methods are limited in the sense that cards and tokens can be shared, stolen and forged. The knowledge based authentication methods are problematic for the following three reasons. First, individuals frequently choose inappropriate PINs in order to remember them easily. Second, PINs can be easily guessed

by knowing minimum information on the individual e.g. birthday and address or can be quite obvious e.g. 1234. Third, people write their PINs in obvious places e.g. diaries.

Combining cards and PINs increases slightly the level of confidence. However, when this is done the card and the PIN are authenticated but not the individual who is presenting them. While several solutions have been proposed and tested to improve the situation (i.e. randomly generated PINs, scrambled key pads), the fact remains that only the card and the PIN are authenticated instead of the individual who provides them.

Traditional authentication methods are inadequate for personal identity. They have several limitations and only offer a proof of possession or knowledge. Without a proof of identity, resources protected by traditional authentication methods are at risk.

Biometrics

Biometrics measures the unique physical and behavioural characteristics of individuals in order to verify their identity. Biometrics increases convenience because the information cannot be forgotten and also ensures greater accountability by including auditing and reporting capabilities. Biometric samples have to be provided in person and cannot be borrowed or poorly chosen.

Biometric authentication systems can be divided into two categories: biometric verification and identification systems. Verification systems use a one to one matching process where the live sample of an individual is compared to a previously stored biometric template associated with the claimed identity. The individual needs to make an explicit claim of identity. In order to be verified, the live sample and the template need to match according to the system's matching criteria. Identification is quite different in the sense that it is a one to many matching process where the live biometric provided by the individual is not compared with the implicit claimed identity biometric template but with a database of possible users according to multiple matching criteria. The system needs to evaluate the suitability of the live biometric received and then search the entire database for a possible match.

Biometric techniques

This subsection introduces briefly the most common physiological and behavioural biometric techniques. Physiological and behavioural techniques are interrelated. On one hand, a physiological biometric trait is influenced, for example, by stress, user behaviour and presentation. On the other hand, behavioural biometric are subjected to physiological characteristics like palate, teeth and dexterity.

Fingerprint authentication

Fingerprint authentication is the most familiar technique in biometrics. People understand identification using fingerprints as it is commonly used in forensic laboratories. It has been the way of identifying criminals among law enforcement agencies for nearly a century. A fingerprint is the patterns found on an individual's fingertip. Each individual has a set of unique characteristics associated with their fingerprints such as arch, loop and whorl. The characteristics that are the most unique are the minutiae, the forks, the endings in the ridges and their relative positions. The most common approach to fingerprint authentication copies the traditional method used by the police to compare minutiae while others use straight pattern-matching devices.

The quality of the template and the fingerprint scan are extremely important in order to obtain good quality prints. There factors that affect the quality of the template include: position and attitude of fingertip, temperature, humidity, degree of dryness of the skin, damage to fingerprints, the cleanliness of the scanning area, calibration of the scanning function.

Fingerprint authentication has many advantages. Fingerprints are accurate and do not change over time. The devices used for scanning fingerprints are relatively small, unobtrusive, affordable and their integration relatively simple. The fingerprint

authentication technique is seen by many as the best choice for workstation access applications.

A disadvantage to fingerprint technology is its vulnerability to spoof attack. A new study from Yokohama National University in Japan shows that phony fingers concocted from gelatin, called “gummy dummies” easily trick fingerprint systems [MAT 02]. Therefore the environment where the devices are installed needs to be controlled. There is also a privacy concern with fingerprints as they are associated with criminals.

Five percent of the total population has poor or not quantifiable fingerprints [ONW 01]. Fingerprint verification or recognition is quite difficult for these individuals. A person with finger injury/surgery or swollen fingers may have trouble being verified by the system. Hairdressers or people that work with harsh chemicals may also have problems with fingerprint systems.

Hand geometry

Hand geometry is a biometric technique based on the three dimensional measurement of the physical characteristics of the individual's hand and fingers. Hand geometry was the first biometric technique to be proven practical. It is easy to use and performs really well for physical access control and time monitoring applications.

There are many advantages to hand geometry. The small size of the template allows for multiple storage options and short processing time. The technique is also easy to use. The consequences associated with variation of the hand on the scanner are less than fingerprints variations because of its size. Also individuals are quite open to this biometric technique compared to the others. Some disadvantages of this biometric technique are that the readers are bulky and the platen surface requires regular cleaning. People with advanced arthritis, swollen fingers, Parkinson disease, or paralysis may experience authentication problems. The same applies to young children. The creation of an artifact in three dimensions that would represent a valid hand could defeat some hand authentication devices.

Retinal scanning

Retinal scanning involves the analysis of the blood vessels at the back of the eye. This technique is known for its high accuracy but also for being invasive because the individual is required to look into a binocular or monocular receptacle and focus on a central point.

Retinal scanning has several advantages, the most important one being its accuracy even with identical twins. It is not subject to change with age therefore does not require periodical updates. It is well suited for high security applications as the threshold for false accept can be set extremely low.

While this technique has evolved and does not require physical contact anymore, it is still not warmly accepted. Most individuals find looking into a receptacle intrusive and will need to remove their glasses before using the device. The authentication process is slightly longer than other biometric techniques.

Iris scanning

The iris is defined as the flat circular coloured membrane behind the cornea of the eye, with a circular opening (pupil) in the centre. Iris scanning is therefore the analysis of the colored ring around the pupil and is one of the most interesting biometrics. The most attractive fact about iris scanning is that it is not only unique to individual both the left and the right irises are different, but also unique even among identical twins. Scanning iris is complex in the sense that the iris surface is mobile when the pupil contracts or expands. It is sometime difficult with individual with dark eyes to determine where the iris stops and the pupil starts. The portion of the iris that is visible is not constant and varies according to ethnic origin and genetic inheritance.

The major advantage of iris scanning is the high accuracy and is not subject to change with age. Duplicate artificial eyes are not an issue as they do not respond to light and the constant movement of the pupil is used as evidence of live sample. Just like retina scanning it is well suited for high security applications as the threshold for false accept can be set extremely low. It does not require the individual to look into a receptacle and

individuals can keep their glasses or contact lenses. Some disadvantages is that people that are blind or have damaged eyes from diabetes will not be able to use this technique. It is considered less intrusive than retina scanning but still faces some acceptability problem among the general population.

Facial recognition

Facial recognition is an interesting biometric technique as it is quite natural to be identified by facial characteristics. This technique identifies individuals by their facial characteristics like the shape of their nose, eyes, chin, eyebrows and mouth etc.

The challenges in face recognition in verification and identification mode differ substantially. In a verification scenario, the environment is somewhat controlled i.e. the scene does not vary much, the distance of the individual to the camera will likely be somehow constant, the lighting conditions similar and that the individual will be facing the camera at a comparable angle most of the time. On the other hand, in identification mode, the individual could be at various degrees of axis from the straight head position and at various distances.

While the advantages of facial recognition are significant from a point of intrusiveness and ease of use, one needs to be realistic about the possibility to use it for identification. This technique may have some problems verifying and identifying individuals that

modify their physical characteristics (grow beard). Facial expression is another issue.

Another disadvantage to this technique is that facial skeleton and facial characteristics tend to change with age requiring the template to be updated with time. The most significant disadvantage of facial recognition is that facial technologies could undermine or threaten personal or informational privacy as it has the possibility to collect biometric information without consent.

Voice verification

This technique is attractive when looking at the number of business transactions taking place every day using voice communication. Voice can be captured using audio devices including telephones, cellular phones and PC microphones. The author of [ASH 00] explains that the principle behind voice authentication is that the physical construction of an individual's vocal chords, vocal tract, palate, teeth, sinuses and tissue within the mouth will affect the dynamics of speech.

Voice verification systems can be either text dependent or text independent. In a text dependent recognition system, the same passphrase must be used for every authentication while in a text independent system, different passphrases can be used. To enroll in a text dependent system, the user will be required to select and repeat a passphrase three to five times. Some processing are then required removing gaps at the beginning and end of the recording so only the passphrase is used for template creation. The authors in [NAN 02]

explain that the generation of the voice template usually relies on a statistics-based pattern matching system, most commonly Hidden Markov Models. The voiceprint is then stored in a template that will be used in later comparisons.

Voice verification has tremendous potential for many applications (e.g. automated call center) and is publicly acceptable. It is not as accurate as biometric techniques based on physical characteristics and voice templates are often large in comparison with other biometric templates. Other disadvantages are that several factors (i.e. fatigue, stress, sore throat, dental anesthesia) can prevent legitimate individuals to be verified. Templates will need to be updated as voice changes over years.

Signature authentication

The biometric method is based on the fact that individual signature are quite personal and distinctive. It has characteristics like rhythms, velocity, acceleration, how hard the surface writing has been pressed down, time to perform the signature, how the letter T is crossed, etc.

One advantage is that most people perceived providing a signature for authentication as natural and will mostly be comfortable to present a signature as part of a biometric system. Signatures are used for cheques, credit cards, access control, medical

prescriptions in several other occasions. It presents great potential for many applications where signature and is an acceptable identifier. Disadvantages are that people with Parkinson's disease or people that are illiterate may have trouble being verified by the system. Also people that provide considerably different signature each time or that are under the influence of alcohol may have difficulties.

Keystroke patterns

This technique is based on a person's distinctive typing patterns. It measures variables like the length of each key is hold down and the time between different keystrokes. The advantages of this technique are that it is accessible to anyone able to type on a keyboard and therefore well suited for computer security. It is widely accepted and does not disturb the regular work flow. Being a pure software solution, it leverages existing hardware. It is quite difficult to observe and therefore cannot be easily spoofed. Disadvantages are that it is not as accurate as physiological biometrics and sometime individual's patterns are not consistent. Major progress has been made recently allowing keystroke patterns to compete with other biometric technologies.

General operating methodology

Each biometric technology has its own operating methodology but there are several processes that are quite similar among all biometric techniques. Figure A.1 provides a simple diagram explaining the processes that are involved when using a biometric system for user authentication. The rest of this subsection will briefly describes the three main processes involved in biometric systems which are the enrolment process, the storage of templates and the verification/identification process.

Figure A.1. General methodology in using a biometric system

Enrolment process

The first step when using a biometric system is the enrolment process. The individual will be required to provide a series of sample (usually three) of the specific biometrics. A digital representation will be created by using an averaging process to generate a

biometric template. This template will be used in all subsequent authentications. The quality of the template captured in the enrolment process is crucial in order to minimize the number of subsequent false rejects and the need for re-enrolment which cause great frustration for users. A unique identifier will be associated with the template for future recall. The identifier could be a personal identification number (PIN) or a card number.

It is crucial to understand the relevance of the enrolment process. The key is to ensure that credentials are verified to certify the identity of the enrolees registering their biometric samples. If the enrolment is performed by the administrators the level of confidence in the enrolment process is much higher than if the enrolment takes place over the Internet. If the enrolment process is done over a network like the Internet many privacy issues prevent the administrators to cross check the reference of the enrolee with other databases. Identity theft is also an issue with the enrolment process. If the credentials are not thoroughly verified by the administrators, an impersonator could register biometric samples for an identity profile that is not his.

Template storage

The second component is the storage of the templates collected in the enrolment process so it can be referenced later. The size of each template and the number of templates required (in the case of multimode systems) is of prime importance. The author of [ASH 00] states that the leading hand geometry device boasts a raw template of only 9 bytes.

Typical fingerprint device may create a template of several hundred bytes or more and some biometric devices create raw template exceeding 1k bytes in size. The amount of storage required and the processing capabilities need to be assessed. The location where the template is stored is of great interest. Typically there are three ways to store biometric templates. The first one is to store the template within the biometric device itself. The second is to store the template in a central repository and the third one is to store the template on a portable token carried by individuals. These options offer different advantages and disadvantages.

The first option is to store the template within the biometric device itself. It has the advantage of offering good transaction speed assuming that the device contains the number of templates required for good efficiency. Also, you are not relying on a network that could induce delays or be unavailable. In some architecture where devices are connected together it is possible to share the templates across the different devices. But in that case, you are relying on the network connections between the devices. The possible disadvantage with this option is that if the device becomes unavailable or malfunctions, you may have to either re-install all the templates or even worse need to re-enrol the affected users.

The second option is to store the templates in a central repository. User acceptance is an important aspect of the success of a biometric system and unless your system can provide sufficient speed for template retrieval, you may have to deal with user's frustrations. The

traffic created by several devices working concurrently attempting to retrieve templates that can vary in size needs to be carefully assess. One should also keep in mind that if the network fails, there is no way to retrieve templates and be able to perform authentication if there is no proper redundancy or backup strategy. Local storage can be used with some devices but one must be careful when having multiple copies of templates or databases. If the system is to be used where the network and communication protocols are vulnerable the security of the templates may be compromise. Data encryption and transmission error checking are desirable.

The third option is to store the template on a portable token which is an attractive option as no central storage is required and users carry their own templates with them. This option has greater user acceptance as the user has control and ownership of his template. The disadvantage is that if the token is lost or damaged, the user will need to re-enrol. One could combine option 2 and 3 using a portable token with a central repository of templates for backup purposes. Using this combination, users must be aware that a copy of their template is also stored in a central database. If the option to store the templates on a selected token is chosen, the template needs to be small enough to fit on the token. Several characteristics of the selected token like the current maximum capacity of storage, the processing power/capabilities, the compatibility with the hardware involved need to be considered. Users will also need assurance that their template is secure on the selected token.

Verification/Identification process

The verification process will require the individual to claim an identity by providing either a PIN number or by presenting his token. If a PIN is used, the template will be called from the database and brought into memory for comparison. If a token is used the biometric template would be stored directly on it. The individual claiming an identity will then provide a live sample for comparison with the template in memory. The system will evaluate if the live sample and the previously stored template match within the predefined threshold and return a binary true or false. Some systems will most likely provide the individual with a second chance at verification. While you want to ensure that legitimate users are not denied, you do not want to provide the individuals trying to defeat the system too many chances.

In identification mode, the individual will not claim an identity therefore no specific template will be called up. The user simply provides a live biometric sample and the task of the system is to recognize the individual as an authorized user. When a good quality biometric sample is captured, the system will compare the sample with all the templates stored in the database to find a possible match.

Accuracy performance

In password-based authentication systems, a user providing the correct password will always be granted access. In a biometric authentication system, the limitations of the feature extractor and matcher, the biometric sensor's noise as well as the environment noise can prevent access to a legitimate user.

The performance of a biometric system is usually provided in terms of matching errors, image acquisition errors and decision error rates. Matching errors consist of false match rate (FMR) and false non-match rate (FNMR). Image acquisition errors comprise of failure-to-enrol (FTE, also FER) and failure-to-acquire (FTA) while decision error rates include false rejection rate (FRR) and false acceptance rate (FAR). The summarized performance of a biometric system is sometime depicted using the Receiver Operating Characteristics (ROC) curves or the Detection error trade-off (DET) curves. Equal Error Rates (EER) and the Ability to Verify (ATV) are sometime also used. The rest of this subsection will explain each error in detail and provide a table summarizing the different biometric errors and performance metrics.

Matching errors (FMR and FNMR)

Matching errors are accuracy performance measures resulting from a single comparison or attempt. Therefore if the decision policy allows for more than one attempt, matching errors will not result in an acceptance or rejection of a claim. FMR is also referred as False Positive Rate (FPR) and describe as the expected (expectations are those for a user selected randomly from the target population) probability that a sample will be falsely declared to match a single randomly-selected “non self” template [MAN 02]. Non self refers to genetically different. The FMR is calculated over the number of comparisons. FNMR is also referred as False Negative Rate (FNR) and described as the expected (expectations are those for a user selected randomly from the target population) probability that a sample will be falsely declared not to match a template of the same measure from the same user supplying the sample [MAN 02]. The FNMR is also calculated over the number of comparisons.

Image acquisition errors (FER and FTA)

Image acquisition errors are divided into two types: FER and FTA. FER is the proportion of users who are unsuccessful at enrolling. It occurs when users are not able to provide the required biometric trait, have insufficient distinctive biometric characteristics or are unable to subsequently verify their enrolment template to confirm enrolment. No biometric identifier is truly universal therefore, users that possess biometric identifiers

that are not easily quantifiable will have trouble enrolling and subsequently verifying in a biometric authentication system. Considering that [ONW 01] states that approximately 5% of the population have poor fingerprints this becomes an important issue. Therefore, a company with 5000 employees deploying a finger-scan biometric authentication system may end up with 250 employees that will not be able to use the system. By providing those employees with traditional authentication methods, the company will revert back to their vulnerable situation since 250 high risk accounts could provide access to their corporate resources.

Using [BOM 03], the probability than an enrolment will be unsuccessful is:

$$FER(i) = \frac{\text{Number of unsuccessful enrolment attempts for a person (or feature) } i}{\text{Number of all enrolment attempts for a person (or feature) } i} \quad (1)$$

The overall FER for N participants is defined as the average of FER (i):

$$FER = \frac{1}{N} \sum_{i=1}^N FER(i) \quad (2)$$

Users that have enrolled successfully but are constantly rejected at verification or identification are accounted for in the Failure-to-acquire (FTA) rate. It occurs when a user is unable to meet that quality threshold. For example, when a user has been injured, he may not have measurable features for a period of time.

Decision error rates (FRR and FAR)

A decision error results from a combination of matching and image acquisition errors depending on the number of attempts allowed and the type of identity claim (positive, negative, implicit, explicit). The false acceptance rate is a percentage, which refers to the likelihood that an impersonator was wrongly accepted in the system. It is therefore the possibility that an imposter's template will be misjudged to match a genuine user's template. This occurs when two people have similar biometric traits and results in an authorized access to some resources. FAR is also referred as Type II error and using [BEN 99A] can be expressed as follow:

$$FAR = \frac{\text{Number of Impostor Acceptances}}{\text{Number of Impostor Claims}} \times 100\% \quad (3)$$

Depending on the decision policy, a transaction may consist of one or more unsuccessful attempts therefore include FTA and FNMR. In a positive authentication system where three attempts at verifying are allowed, a false acceptance will occur if any of the three attempts is successful.

The false rejection rate is a percentage referring to the likelihood that an authorized user was denied access by the system. It is therefore the possibility that a genuine user's template will be misjudged not to match his enrolment template. This occurs when live template provided by the user does not sufficiently correlate its enrolment template. It could be caused by temporal changes in the biometric traits, improper presentation or modification to the environment. FRR results in frustrated users, a lost of productivity and may lead to a re-enrolment. FRR is also referred as Type I error and can be expressed as follow:

$$FRR = \frac{\text{Number of Legitimate User Rejections}}{\text{Number of Legitimate Claims}} \times 100\% \quad (4)$$

Again, depending on the decision policy, a transaction may consist of one or more unsuccessful attempts therefore including FTA and FNMR.

Summarizing performance (EER, ROC, DET, ATV and TE)

There are currently several methods for summarizing performance. Most biometric devices in the market today have a threshold adjustment that allows tightening or relaxing of the criteria associated with matching live samples with the stored templates. This becomes a trade-off between relaxing the requirements to provide a user-friendly system (increasing the number of false acceptance) or tightening the requirements for security purposes (higher level of false rejection), the two parameters being mutually exclusive.

The accuracy level at which the probability of a false acceptance is equal to the probability of a false rejection is called the equal error rate (EER) or the Crossover Rate. Figure A.2 shows a performance curve dependant on the selected threshold with an EER at approximately 85.

Figure A.2. A Performance Curve with an EER at approximately 85

Another method for summarizing performance is the ROC curves which is threshold independent and used to effectively and objectively compare different imperfect diagnostic and pattern matching systems under comparable conditions. The ROC plots imposter attempts accepted (FMR) against genuine attempts accepted (1-FNMR). It is independent of threshold scaling because FMR values are plotted directly against 1-FNMR values. The ROC curve is a plot of genuine acceptance rate against false acceptance rate for all matching score thresholds and measures the overall performance of the system. An example taken from [MAN 02] is given at Figure A.3.

Figure A.3. An example of ROC curves

In [MAR 97] the authors assert that the Detection error trade-off curve (DET curve) which is a modified version of the ROC curve is preferred in the case of biometrics. It provides a much clearer view of well performing systems as it plots FNMR against FMR directly using logarithmic axes. The authors of [MAN 02] explain that the DET curve is obtained by ordering the genuine and impostor scores. As the score varies over all possible values, each point on the DET curve represents the false match and false non-match rate using that score as the decision threshold. The DET curve in Figure A.4 has been derived with the same data used in the ROC curves in Figure A.3.

Figure A.4. An example of DET curves

The ability to verify rate represents a combination of failure-to-enroll and the false rejection rate. It indicates the overall percentage of users capable of authenticating. The total error (TE) combines false acceptance and false rejection rates into one number.

$$ATV = (1-FER) (1-FRR) \quad (5)$$

$$TE = FAR + FRR \quad (6)$$

Table A.1 provides a summary of the different biometric errors and the performance metrics that have been introduced in this section.

Table A.1: Biometric errors

	Sometimes referred as	Refers to
1) Matching Errors		
False Match Rate (FMR)	False Positive Rate (FPR)	An impostor's sample matches a legitimate user's template
False Non-match Rate (FNMR)	False Negative Rate (FNR)	A legitimate user's sample does not match his/her own template
2) Image Acquisition Errors		
Failure-to-enrol (FTE)	Failure to Enrol Rate (FER)	A user that is unable to successfully enroll in a biometric system
Failure-to-acquire (FTA)		A user that is unable to provide a good quality biometric trait at authentication
3) Decision Errors		
False Rejection Rate (FRR)	Type I errors	Likelihood that a legitimate user is denied access to the system
False Acceptance Rate (FAR)	Type II errors	Likelihood that an impostor is wrongly accepted in the system
4) Summarizing Performance		
Error Equal Rate (ERR)	Crossover Rate	The level at which the probability of a false acceptance = probability of a false rejection
ROC Curve		A threshold independent curve used to effectively and objectively compare different system.
Detection Error Trade-off Curve (DET Curve)		Modified version of the ROC curve which is more adapted for biometric systems.
Ability-to-verify Rate (ATV)		Indicates the overall percentage of users capable of authenticating.
Total Error (TE)		Combines FRR and FAR.

Spoofing

Spoofing is the biggest threat to authentication systems. Biometric systems are vulnerable to spoofing. Spoofing occurs when an unauthorized user is able to masquerade as an authorized user.

The authors of [THA 03] evaluated eleven biometric protection applications including capacitive, optical and thermal fingerprint technologies, iris-scan technology and face recognition. Using different attacks, they were able to outwit all the systems tested with simple means. The potential threats caused by fake or artificial fingers were evaluated in [MAT 02]. The experiment demonstrated that artificial fingers cloned with plastic molds could enrol in the 11 tested fingerprint systems and were accepted in the verification procedures with the probability of 68-100% depending on the system. Artificial fingers cloned from residual fingerprints could also enrol in all the systems and were accepted in the verification procedure with a probability higher than 67%. The “gummy” fingers were created with cheap and readily available gelatine.

In summary, biometric systems are the most convenient and secure way of providing personal identity. It increases security and solve the inadequacy of the traditional authentication methods. Unfortunately they also have problems. The limitations of the feature extractor and matcher, the biometric sensor’s noise as well as the environment noise can prevent access to legitimate users. Those limitations correspond to FNMR,

FER, FTA and FRR. The vulnerability to spoofing of biometric systems can result in the authentication of an impostor to protected resources. This problem is represented by FMR and FAR. The best way to summarize the accuracy performance of biometric systems is to use the DET curve.

Multimode biometrics

Multimode systems combine biometric identifiers to obtain a more accurate decision on a user's claim based on multiple evidences. This improvement in performance is achievable because multimode systems use modalities possessing different strengths and weaknesses. By using the strengths of one modality to compensate for the weaknesses of the other, a substantial improvement in performance can be achieved. In contrast, the system performance of monomodal authentication systems varies depending on the performance of the modality selected i.e. the performance of a fingerprint authentication system is associated with the discrimination capability, complexity and robustness of the fingerprint technology. Multimode systems are also more difficult to spoof for two major reasons: first, multiple biometric characteristics need to be forged in order to defeat the system; second, a multimode system that uses an changeable biometric trait like voice verification and keystroke recognition can participate in a challenge-response protocol diminishing the risk of replay attacks.

Multimode biometrics techniques

Multimode systems alleviate the performance and spoofing problems related to monomodal systems. A subsystem, using data captured by its sensor, will provide an opinion on a user's claim. The supervisor module will combine the different opinions delivered by the subsystems and make a final decision (accept/reject). The author of [XIA 02] explains the following approaches for multimode verification system:

- Capture multiple samples of the same biometrics by the same sensor;
- Capture multiple samples of the same biometrics by different sensors;
- Capture multiple samples of different biometrics by different sensors.

Recent research [BEN 99B][HON 99][JAI 02][POH 01][ROS 01] has demonstrated that a more accurate decision can be made if multiple biometric identifiers (modalities) are provided. Multimode systems combine biometric identifiers to obtain more accurate decisions based on multiple evidences. Using multiple modalities alleviate the problem related to the non universality of biometric identifiers. It is also harder to spoof as multiple biometric characteristics need to be forged in order to defeat the system. A multimode system using modalities with different strengths and weaknesses can achieve substantial improvement by using the strengths of one modality to improve the weaknesses of the other.

Biometric fusion

In a multimode biometric system, each subsystem will provide an opinion on the user's claim. A supervisor module will combine the different opinions delivered by the subsystems and make a final decision (accept/reject). The supervisor module can use different fusion strategies to combine each subsystem opinions in order to reach the final decision. Fusion can be performed at different levels: sensor level and feature level are pre-mapping fusion techniques while confidence level and abstract level are post-mapping fusion techniques [SAN 02]. Figure A.5 illustrates the different levels of fusion for a multimode system using a fingerprint and a voice subsystem.

Figure A.5: Different levels of fusion

Sensor level occurs when the raw data of the sensors are combined. Fusion at the feature level (also referred as representation level fusion) is performed at the sensor level where the features extracted from the different sensors are concatenated to create a joint feature vector. Fusion at the confidence level (also referred as score level integration, measurement level integration, opinion fusion and soft decision fusion) occurs when the matching scores of each subsystem are combined using techniques such weighted summation, weighted product and the Bayesian Rule. Fusion at the abstract level (also referred as decision fusion) take place when the decision of the subsystem are combined using the AND rule, the OR rule, Majority Voting and Ranked List Combination. Table A.2 provides a summary of the different levels of fusion and fusion strategies.

Table A.2: Different levels of fusion and fusion strategies

	Sometimes referred as	Refers to
Pre-mapping fusion Techniques		
Sensor Level		Raw data of the sensors are combined
Feature level	Representation Level	Features extracted from the different sensors are concatenated to create a joint feature vector
Post-mapping fusion Techniques		
Confidence Level	Score Level Integration Measurement Level Integration Opinion Fusion Soft Decision Fusion	Matching scores of each subsystem are combined using techniques such as: • Weighted Summation • Weighted Product • Bayesian Rule
Abstract Level	Decision Fusion	Decisions from each subsystem are combined using techniques such as: • AND Rule • OR Rule • Majority Voting (odd number of subsystems) • Ranked List Combination

Multimode systems can achieve a substantial increase in performance by combining modalities with different strengths and weaknesses and are harder to spoof than monomodal biometric systems. While achieving better performance is the main goal, other factors like convenience, robustness, privacy and total solution are critical.

Finding the most effective strategy to fuse independent subsystem opinions into a more accurate decision is a great area of research.