2009

Performance analysis of multimodal biometric systems – An automated statistical approach

Gaurav Kumar
University of Windsor

Performance Analysis of Multimodal Biometric Systems – An Automated Statistical Approach

by

Gaurav Kumar

A Thesis

Submitted to the Faculty of Graduate Studies

through School of Computer Science

in Partial Fulfillment of the Requirements for

the Degree of Master of Science at the

University of Windsor

Windsor, Ontario, Canada

2009

Your file Votre référence
ISBN: 978-0-494-57560-4
Our file Notre référence
ISBN: 978-0-494-57560-4

Author's Declaration of Originality

I hereby certify that I am the sole author of this thesis and that no part of this thesis has been published or submitted for publication.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. Furthermore, to the extent that I have included copyrighted material that surpasses the bounds of fair dealing within the meaning of the Canada Copyright Act, I certify that I have obtained a written permission from the copyright owner(s) to include such material(s) in my thesis and have included copies of such copyright clearances to my appendix.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee and the Graduate Studies office, and that this thesis has not been submitted for a higher degree to any other University or Institution.

Abstract

This thesis proposes to study and extend the ability of the statistical methodologies that have been established to measure the performance of multimodal biometric systems. In particular, it takes into account the various noise factors that are inevitable in a real world scenario, which influence the performance of biometric systems. The work completed in the past uses the Design of Experiment framework to create a systematic approach to test the performance of biometric systems. Input parameters are varied including the data fusion methods and the normalization schemes (both controlled), and using discrete intervals based deviations in the matching scores (uncontrolled) of genuine and impostor users to represent noise. This work however, is limited provided the manual interface to the developed application. All parameters are fixed and operate over a comparatively small dataset. Further, the design of the existing application limits the extensibility of the same to incorporate additional data sources, increase or decrease the deviation values that contribute to the noise, and generate analytical graphs and reports.

It is the purpose of this thesis to establish a framework that is scalable to accommodate additional biometric databases for a larger subject pool. The developed application will also allow users to identify a larger set of deviation values for noise, automatically generate test cases for all possible biometric modalities defined within the system, etc. It is also the intent to provide, as results, the ability for the user to choose from a set of possible graphs and reports that are in tune with the common industry (commercial) standards as opposed to purely technical reports.

Dedication

"Knowing is not enough; we must apply!" - Goethe

This Master's thesis paper is dedicated to my parents as well as other members of my family who have consistently supported me throughout the course of my education and my life. It is through their guidance and teachings to be persistent and to strive for more knowledge that have enabled me to complete this thesis.

The thesis is also dedicated to the faculty and staff of the Computer Science department at the University of Windsor. Without the knowledge imparted by them and their constant support, I would have been unable to complete this paper.

Acknowledgements

The author wishes to express sincere appreciation and gratefulness to **Dr. Xiabou Yuan** for his assistance and guidance in the preparation and research of the thesis paper. Without his valuable support and patience, the research would not have materialized and completed. In addition, the author also extends his sincere thanks to **Dr. Ram Balachandran**, **Dr. Christie Eziefe** and **Dr. Subir Bandyopadhyay** for the input and support they provided during the preparation and evaluation of the thesis paper.

Table of Contents

List of Tables

List of Figures

Glossary of Terms

Modalities –	physiological or psychological biometric traits used in biometric systems to identify individuals. This can also be used to identify any algorithms employed in the identification process.
Unimodal –	biometric system utilizing only a single biometric trait or a type of algorithm for purposes of identification.
Multimodal –	biometric system utilizing multiple biometric traits or multiple flavors of algorithms to be used for the purposes of identification.
Matching scores –	numerical values identifying the similarity in the biometric data retrieved from the individual to be authenticated and the data stored in the biometric database.
DoE –	Design of Experiments refers to an experimental method used to study factors and their interactions statistically through methodically controlling their values within a system to be studied.
FAR –	an error measurable in a biometric system identifying the system's rate of accepting an impostor based on the biometric signals provided.
FRR –	an error measurable in a biometric system identifying the system's rate of rejecting a genuine user based on the biometric signals provided.

Chapter 1. Introduction

Authentication for the purpose of securing resources and accurately identifying individuals has evolved into the field of biometrics. Biometric systems are being deployed within government offices, high security facilities, major corporations, etc. to deny or allow access to resources. Further, as an identification tool, biometric systems allow enforcement agencies to identify suspects, for immigration authorities to authenticate travelers, etc. Within the field of biometrics, this has been made possible by using human physiological and psychological traits that can be measured through hardware including sensors and cameras.

Usually, a biometric system utilizes a single trait to identify individuals. Such systems suffer from performance issues and have paved the way for multimodal biometric systems. Multimodal biometric systems combine data from various unimodal biometric systems to achieve improved performance in its authentication abilities. Since the combining of data can occur at various levels and through different permutations, it is important to understand and evaluate the performance of such systems. A realistic factor that affects the performance of biometric systems is the influence of noise through various sources including faulty devices, change in traits, to name a few. This variability further enhances the need to study the performance of these systems.

Given biometrics is a young field and evaluation of such systems with any systematic approach younger still, some attempts have been made to analyze performance of multimodal biometric systems (Biometrics Testing and Statistics, 2006) (P. Jonathon Phillips, 2007). These evaluations, however, are done under controlled test environment for a particular set of biometric modalities or for specific applications. In (Gan, 2007), the author has provided a framework to analyze multimodal biometric systems to measure their performance using the DoE framework, but has had to carry manual experiments utilizing the MUBI tool (Samoska, 2006), which can be time consuming and cost ineffective.

Much of the performance evaluation is done using existing multimodal biometrics' databases that include matching scores for unique biometric traits. Evaluations are performed only through combinations of these modalities limited to the databases. The considered parameters or noise levels are also limited and may not be completely representative of the systems under study or may not apply

to individual modalities. For example, considering a 5% deviation across a multimodal biometric system as noise representing face modalities and finger modalities may not be a true representative. Noise is more likely to occur in hardware to detect fingerprints than face images due to its nature. Subjects directly interact with the fingerprint scanners while face images are taken through cameras without direct interaction with the subjects.

As evaluation is performed within the scientific community, measurements are usually reported through numbers. A better evaluation matrix is necessary to enable non-scientific community to analyze multimodal biometric systems in comparison with each other.

The intent of this thesis paper and the research performed within the premise allows for a study of the performance evaluation of multimodal biometric systems, especially under the influence of noise. Various existing applications, that enable users to measure the performance of biometric systems, have been researched and their functionality enhanced to allow for evaluation of a larger dataset with user defined modalities. Better reporting matrix have been included that allow users to perform a more direct comparison of multimodal biometric systems. An automation of existing applications has been performed to decrease the cost associated with the evaluation process.

The remainder of this paper has been organized into the following sections. Section 2 provides a more detailed understanding of biometric systems, unimodal and multimodal. It also presents the schemes of data combination to create multimodal biometric systems. Section 3 discusses the various performance measures that have been identified to evaluate a multimodal biometric system. In section 4, the theoretical framework identifying the method of analysis has been presented. Section 5 discusses the implemented system that supports, in theory, the proposed methodology for evaluation. Section 6 provides test experiment setups, results, and finishes with a discussion of these results. Section 7 presents the conclusion and scope of future work.

Chapter 2. Overview of Biometric System

In the present world scenario, the need for security ranging from simple applications such as protecting copyrighted material to sheltering a country has reached a new dimension. The shift from printed media to digital information, movement of people due to globalization and increasing crime are just some of the reasons that have fuelled the need for accurately identifying a person, or validating a person's identity. The response to such requirements has spawned the use of biometrics, an evolving field of science and resulting technology that enables identification (and verification of the identity) of individuals based on physiological and psychological traits. Essentially, biometrics emerged from its extensive use in the field of law enforcement but is increasingly being employed in other high security applications, including many civilian applications (A. K. Jain, 2004).

2.1 Biometric Systems

A biometric recognition system encompasses a shift from traditional identification and authorization mechanisms such as passwords, secret phrases, etc. to the use of features that humans inherently possess or can develop (J. Ortega-Garcia, 2004). A biometric system uses features in humans that can, to a degree of certainty, establish a person's identity. Consequently, a biometric system can be likened to a pattern recognition system. A biometric is an individual biological characteristic that can be a candidate for identifying a person pending the following requirements (K. Delac, 2004) (A. K. Jain, 2004) (Thieme, 2003):

- *Universality:* The physiological or psychological trait must be present as a common characteristic in all human population.
- *Distinctiveness:* The trait must differ (in the measured value) between people.
- *Permanence:* The trait (specifically the measured values of the trait) should remain unchanged over a period of time.
- *Collectability:* The trait must be measurable quantitatively.

Given in Figure 1 are some common biometric traits utilized in identifying individuals.

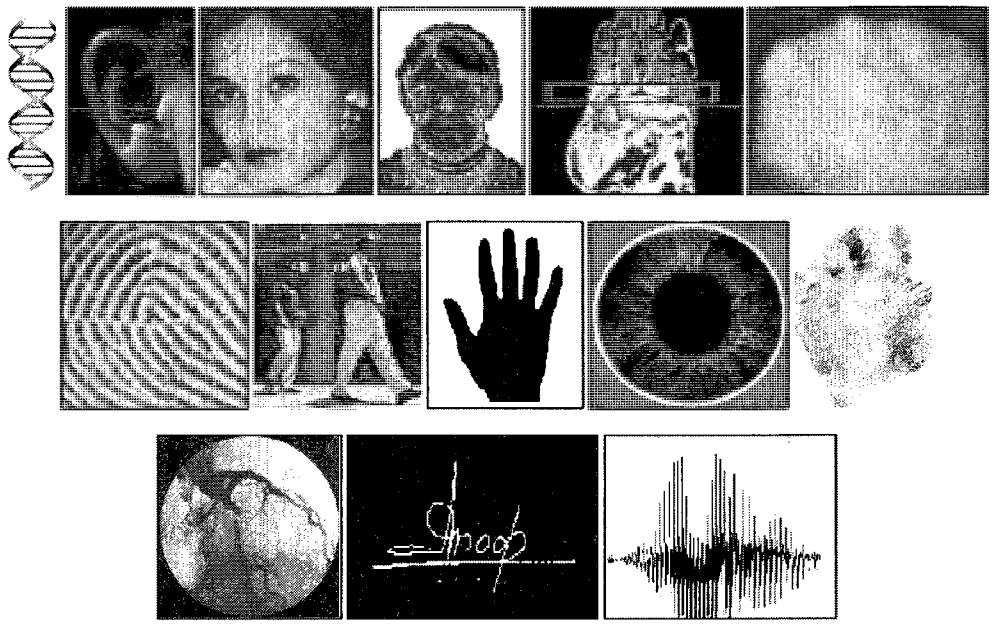


Figure 1: Common biometric traits (A. K. Jain, 2004)

Once the candidate traits for a biometric system have been identified, the system must still consider other issues in implementation including:

- *Performance:* This identifies the accuracy and speed of the system in achieving the desired functionality, the resources required to achieve the accuracy and speed in the identification process and the operational and environmental factors that affect the accuracy and speed of the system.
- *Acceptability:* All biometric systems interface with the human population, who are also the end users of the system. Therefore, the acceptability of a biometric system determines whether the biometric characteristics (or the system as a whole) are acceptable to the general public, and to what extent.
- *Circumvention:* This measures the ease of being able to bypass the system using fraudulent methods.

The author in (J. Ortega-Garcia, 2004) has identified and classified some of the commonly used biometric features (also called biometric modalities). One of the key criteria of classification established

in the paper distinguishes features as physiological or behavioral. Discussed below are the biometric features reported, but not limited to.

2.1.1 Physiological Features

Fingerprints

This is one of the most commonly used features that have been used to identify humans. Prior to the advent of biometric tools, fingerprints (captured on paper using ink marks) have been used extensively in forensics for the identification and verification of criminals. Provided the advent of new technologies, fingerprints are now captured using optical, capacitive or ultrasonic sensors, that measure the ridges, valleys and islands in a fingerprint.

Face

Humans are conditioned to recognize each other based on facial features. Consequently, facial features can be considered an "inherent" modality since it is widely used for recognition amongst humans. Captured usually as an image, facial features are normally used for identification or verification in a multimodal biometric system. Commonly used algorithms that support this process include measuring the distance between the facial features. Another approach employs scalar comparison between parts of the face using the sample image and the template set. Facial thermographs are also used as a facial trait.

Iris

This type of recognition identifies a subject utilizing the trabecular pattern which is formed based on the anatomy of the eyes' structure. It has been established that the iris in a human being retains its structure over time without being affected by the environment. Using the scanned images of the user's iris and those existing in the template database, the identity of the subject can be established through an image processing technique.

Palmprint Recognition

This modality includes matching features from a complete palm print. This is more accurate that using fingerprints provided the larger set of features available in the palm as opposed to those in a finger. The prints are captured using an optical CCD device and the measurements performed check for point

features identifying the deltas, ridges, islands and ridge ends, or line features including any wrinkles, or the texture of the skin.

Hand Geometry

Using hand geometry in biometrics involves measuring various parameters of a hand including the size of the fingers, the spacing between the fingers, and any other structural factors that can contribute to the uniqueness of a human hand. Comparison between images is employed to authenticate the user.

2.1.2 Behavioral Features

Voice

Speech recognition can be used in a biometric system and can establish the speaker's identity by processing the speech signal. The anatomical structure of the speaker can be identified using the amplitude spectrum of the speech patterns. The methodologies used in the process include dynamic time-warping, neural networks, and hidden Markov models.

Handwriting

Also generalized with the term "signature", handwriting is a trait that can, to a degree of confidence, identify a subject or verify the identity of a subject. A person's signature is legally accepted as a verification measure, although it is not scrutinized as per the true meaning of, and the implementation of biometrics. For true biometric systems, the verification of handwriting is performed by studying its time parameters such as velocity and acceleration, or its feature parameters. This is referred to as online signature verification in which case the sample is available for analysis while it is being written by the subject. Offline signature verification is performed with an existing sample. The measures include the shape of the letters, the pressure of the letters, their luminescence, etc.

Given on the next page, in Figure 2, is a list of common biometric traits and their performance based on the properties of universality, distinctiveness, permanence, collectability, performance, acceptability and circumvention (Jain, 2004).

Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention*
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

Figure 2: A comparison of various biometric traits for properties (Jain, 2004) (H=High, M=Medium, L=Low)

2.1.3 Biometric System Components

A biometric system, which can be used either under the verification mode or under identification mode, accepts as an input some biometric data from an individual and extracts a feature set that is then compared with the template set in the system database. A common biometric system consists of the following modules:

- *Sensor module:* This is the interface that captures the biometric data from an individual during enrolment (initial registration of a genuine user's biometric information) as well as the identification step. This module usually consists of the hardware that interfaces with the users such as cameras, voice recorders, fingerprint scanners, etc.
- *Feature extraction module:* This module processes the captured biometric data to extract the feature set (set of distinguishing features). The extracted "features" depend on the type of biometric modality being considered and the algorithm being used. For example, the feature extraction module may report the length and width of fingers, provided a hand is being used for comparison.

- *Matcher module:* This module compares the feature set against the template set stored in the system database to generate matching scores. The data in the template set is the information set captured during the enrolment process. This data is represented according to the chosen feature extraction algorithm. The biometric signal presented in the identification or verification process is extracted using similar feature extraction algorithms and compared by the matcher module. The matching scores generated indicate the probability that the user is either genuine, or impostor. Normally, a decision module is also available within the matcher module. The decision module makes the decision on the authentication of the subject based on the matching scores and a defined threshold value.
- *System database module:* This consists of the database containing the template sets of all enrolled individuals. The biometric information gathered during the enrolment process is verified to ensure quality expectations are met and then recorded in a usable digital form. For example, the scanned images of fingerprints, through feature extraction module, can be recorded as distance between ridges and valleys, the number of deltas, forks or ridge endings, etc. The matcher module uses the information in this database against which it verifies the identity of the subject.

Provided in Figure 3, are all biometric system components as used during the process of enrolment (initially recording user data that is used to authenticate the user later), during the process of verification and during the process of identification. The flow of information between the components is also indicated along with the matcher module's results.

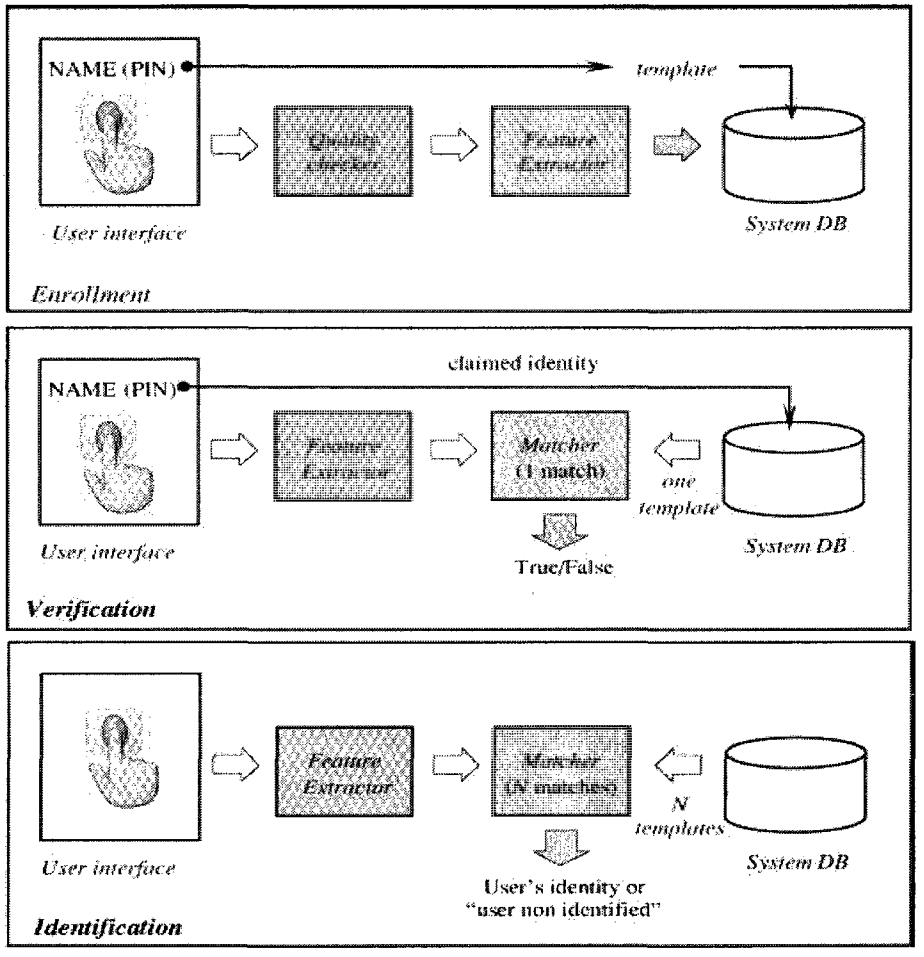


Figure 3: Diagrams identifying system modules within various application context modes (A. K. Jain, 2004)

2.1.4 Limitations of Unimodal Systems

Due to its infancy, and to a degree the limited acceptance of the technology, majority of the biometric systems in place are unimodal systems, i.e. they rely on a single biometric trait to identify (or verify the identity) of a person. Such systems have low performance in terms of their ability to identify a person with confidence measures necessary in security critical applications such as forensics and federal programs. Some of the issues with biometric systems commonly in use today have been identified in (A. Ross A. J., 2004) and discussed below.

- There might be noise present in the data due to factors including defective equipment used to collect the biometric signals, alteration in the biometric trait itself owing to physical injuries or due to health conditions. Noise due to the limitations in the physical environment may also be a factor. This type of noise includes lighting conditions, humidity, heat, etc.
- Intra-class variations are caused by changes in the subject's interaction with the system during enrolment and identification phases. For example, the user may improperly scan his/her fingerprint by placing the finger on the scanner inaccurately, or there might be a difference in the lighting conditions. Another reason for intra-class variations is the difference in the equipment itself. During enrolment, an optical state fingerprint sensor might be used and during the identification process a different solid state sensor might be used.
- Inter-class variations (or lack thereof) indicate the potential commonality in the measured features amongst the population. These similarities are usually magnified in case of biometric traits that are anatomically controlled by genetics. For example, facial features and voice are to a large extent similar in related individuals such as parents and children and amongst twins.
- Non-universality refers to the limitations in the presence of a biometric trait across all human population. It has been observed that not all (if any) biometric traits are universal. Even fingerprint, largely considered to be a uniquely identifying feature in humans, is not available in 2% of the population rendering it useless for those.
- Spoof attacks are performed by individuals unlawfully accessing sensitive resources by acting as masqueraders of authorized users. These attacks are usually carried out by replicating behavioral traits including voice and handwriting. Physical traits are also replicated, although not frequently.

2.2 Multimodal Biometric Systems

As the name suggests, multimodal biometric systems combine biometric information from multiple sources to establish the authenticity of a person. As identified in (A. Ross A. J., 2004), multimodal biometric systems resolve, to a degree, the issue posed by non-universality. This is done by taking into account multiple biometric traits that can better identify a person when used in conjunction as opposed to a single modality. Multimodal biometric systems also act as deterrent to spoof attacks by making it

more difficult to replicate the information since any illegitimate use will require the subject to imitate multiple features. More details have been provided in the following sub-section.

2.2.1 Necessity of Multimodal Biometric Systems

In section 2.1.4, some limitations of biometric systems relying on a single trait or modality have been identified. Multimodal biometric systems counter these limitations and present an improvement in the authentication performance. These improvements have been listed below.

- The noise present in the data due to factors such as defective equipment, alteration in the biometric trait or limitations in the physical environment have a lesser probability of affecting multiple hardware and multiple traits. Hence, a multimodal biometric system ensures improved performance.
- Intra-class variations are mitigated provided any degree of difference in user's interaction with a particular component of a multimodal system is distributed over the entire system during the authentication process, therefore, lessening its effects. The probability of change in hardware throughout the system is also less compared to a single modality biometric system.
- Inter-class variations are also mitigated provided the commonality in physical or psychological traits within individuals is of much lesser probability than a single trait.
- Non-universality is addressed in multimodal biometric systems due to the increased size of the biometric traits' set. The probability of finding a biometric signal to authenticate a user increases with an increase in the number of modalities.
- Spoof attacks are also limited in multimodal biometric systems, simply owing to the number of biometric signals that must be imitated to carry out such an attack.

Multimodal biometric systems, consequently, provide an improved performance over unimodal systems in their ability to authenticate a user in presence of various limiting factors discussed above. In addition, multimodal biometric systems also provide improved security within the systems themselves. Provided below, in Figure 4, is a sample chart comparing the performance of a multimodal biometric system and individual biometric systems. As can be observed, the black curve representing the combined multimodal system has a better acceptance rate for genuine users than both unimodal curves (individual

modalities) represented by the other two curves, for any given value of FAR. An understanding of the genuine acceptance rate (GAR) and the false acceptance rate (FAR) has been covered in a later section.

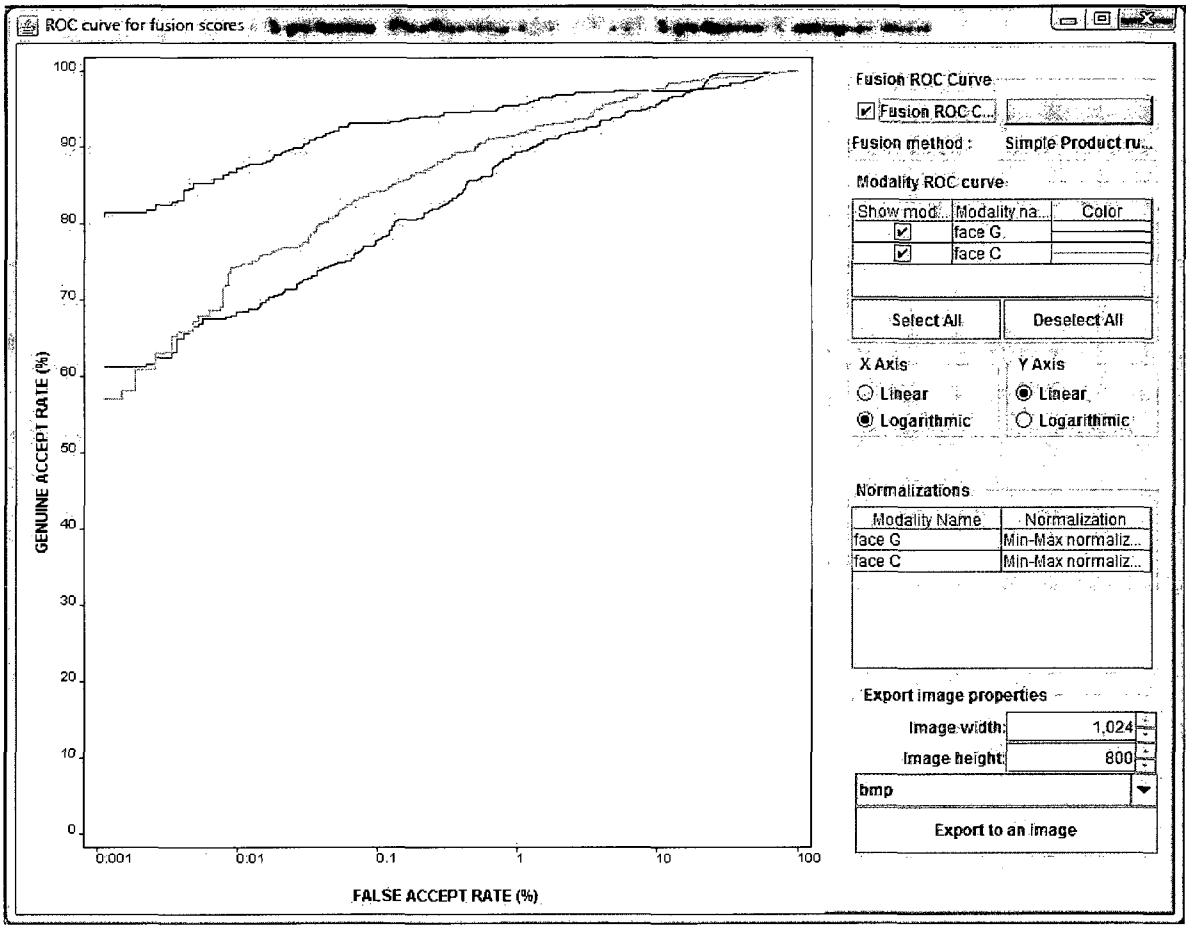


Figure 4: Comparison of multimodal biometrics system and unimodal systems in performance measured in GAR against FAR.

2.2.2 Multimodal Biometric Systems - Schemes

As described in previous sections, a multimodal biometric system is created by combining various unimodal systems. The information retrieved in these individual systems is combined to create a multimodal system. In such systems, the information can be combined through (Nandakumar, 2005):

- Multiple sources of a single biometric trait such as index fingers from the left and the right hands. In such case, the "index finger" provides the single biometric trait while the left and the right fingers, specifically, provide the biometric signal that is combined.
- Different equipment types to enroll a single biometric trait such as an optical state sensor and a solid state sensor. In such cases, a single biometric trait (and a single instance of that trait) such as an index finger is authenticated through multiple sensors. Information from each sensor is combined and provides an overall matching result.
- Multiple feature extraction or matching algorithms used on the same biometric data to provide separate results to be combined. Biometric signals from the same trait and same equipment are processed through more than one feature extraction module or matching module. Information from these is combined for an overall result.
- Multiple enrolment records for a single biometric trait such as various angles of the face.
- Information from different biometric traits such as face, fingerprints, retinas, etc. This, as a true multimodal biometric system, utilizes multiple biometric modalities (or traits) and combines information retrieved from these into a single decision level score to authenticate the user.

2.2.3 Combining Information in Multimodal Biometric Systems - 'Fusion'

Combining information within multimodal biometric systems is referred to as the process of fusing information. The information captured from various sources following the schemes mentioned in the previous section can be fused at any of the following levels (Faundez-Zanuy, 2005):

- *Sensor module level*: The information from a single biometric trait can be captured through multiple sensors. In this case, the information is usually in its native format. The combined information can improve accuracy, ensure completeness of data or add more information to the vector space. For example, images of a face taken at different angles can be used to indicate depth in the image.
- *Feature extraction module level*: At this level multiple features can be extracted from the same biometric trait (signal), or feature vectors from multiple biometric traits can be fused to provide a combined feature vector. For example, using a face image, the spatial data can be fused with the distance in feature points.

- *Opinion level*: This essentially combines information at the matcher module in terms of distance or similarity to result in a single combined confidence level of authenticity achieved through a chosen normalization technique. For example, matching scores from multiple biometric systems can be combined, through normalization at a similar scale, to create a single matching score indicating the authenticity of the subject. This type of fusion is also called matching level fusion.
- *Decision level*: Fusion at this level requires a combination of various decisions made through multiple unimodal biometric systems to achieve a final combined decision to establish the identity of the subject. Usually, the decision output from a biometric system is in the form of a probabilistic match between the provided biometric signal and the information stored in the template database. As an example, an aggregate function can be applied to individual decision probabilities to achieve a single unit authenticating a subject.

Chapter 3. Problem Statement

3.1 Performance Evaluation of Multimodal Biometric Systems

Performance in biometric systems, measured in terms of their accuracy, ease of use, speed, and other measurable is paramount given the increasing use of such systems in high security applications in government organizations, as well as in solving crimes through forensics. Given the access to information and the need to secure the same, biometric systems are on the rise in commercial applications as well, enhancing the requirement for such systems to perform well in varied circumstances. A comparison has been provided below in Figure 5. *(EER, FAR and FRR are measurable units for biometric systems explained in the following sections).*

Biometrics	EER	FAR	FRR	Subjects	Comment	Reference
Face	n.a.	1%	10%	37437	Varied lighting, indoor/outdoor	FRVT (2002)
Fingerprint	n.a.	1%	0.1%	25000	US Government operational data	FpVTE (2003)
Fingerprint	2%	2%	2%	100	Rotation and exaggerated skin distortion	FVC (2004)
Hand geometry	1%	2%	0.1%	129	With rings and improper placement	(2005)
Iris	< 1%	0.94%	0.99%	1224	Indoor environment	ITIRT (2005)
Iris	0.01%	0.0001%	0.2%	132	Best conditions	NIST (2005)
Keystrokes	1.8%	7%	0.1%	15	During 6 months period	(2005)
Voice	6%	2%	10%	310	Text independent, multilingual	NIST (2004)

Figure 5: Performance of various biometric systems using standard measurable (Biometrics, 2008)

Since multimodal biometric systems are more useful in comparison to unimodal systems, the thesis strives to provide a framework to evaluate such systems in an automated environment, however, under noise conditions that are unavoidable in commercial settings, following the findings in (Gan, 2007). The application proposed within this paper performs evaluation of biometric systems automatically to provide a scalable system that can then be used commercially or for further research.

According to (A. K. Jain, 2004), the two primary types of errors caused by a biometric verification system are the ***false match rate*** *(also called the false accept rate or* ***FAR****)* and the ***false nonmatch rate*** *(also called the false reject rate or* ***FRR****).* The false match rate is the degree of the system inaccurately accepting biometric inputs from two individuals to be the same person. The false nonmatch rate is due to the system rejecting inputs from the same person as being from two different individuals. Since a biometric system results in a matching score, a threshold is identified in context of its application for which a genuine subject would need a score higher than the threshold. The false match rate is inversely related, while the false nonmatch rate is directly related to the system threshold. Figure 6 (a) provides the probability distribution curves of the genuine and impostor matching scores. Against a chosen threshold, t, the FMR and FNMR have been displayed. Figure 6 (b) provides a curve for a function of FMR and FNMR. Provided is a generalization of application types as applied to the curve. As can be observed in the figure, forensic applications are tolerant to a higher FMR, which allows for a higher pool of suspects, while applications (or resources) that require a higher level of authentication allow a higher FNMR.

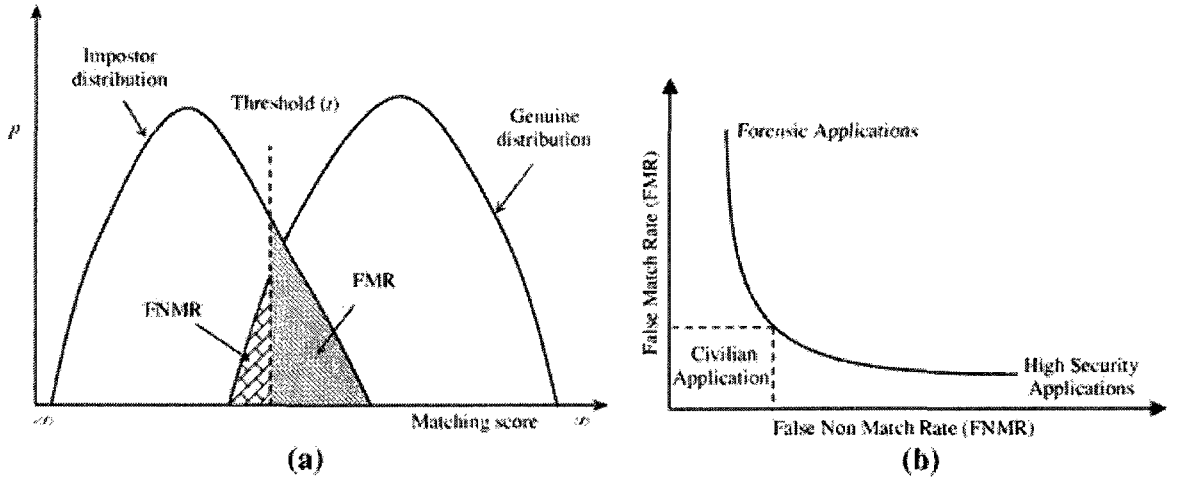


Figure 6: (a) Impostor and Genuine scores distributions for threshold t with corresponding FMR and FNMR. (b) Receiver Operating Characteristics (ROC) curve with varied operating points resulting in different FMR and FNMR. (A. K. Jain, 2004)

The FMR (referred to as FAR in this document from this point forth) and the FNMR (referred to as FRR in this document from this point forth) are discussed in more detail in the following sub-sections. Also discussed are additional biometric performance measures that are, however, used in limited scenarios.

3.1.1 FAR (False Accept Rate)

FAR represents the frequency with which a given biometric system identifies an impostor as a genuine subject. Mathematically, the FAR is the ratio of successful fraudulent attempts and the total number of fraudulent attempts. This is denoted by,

$$\text{FAR}(n) = \frac{successful\ fraudulent\ attempts\ made\ for\ identity\ n}{all\ fraudulent\ attempts\ made\ for\ identity\ n},$$

where, n is a unique identity.

The overall FAR of a biometric system can be calculated as an average through the formula,

$$\text{FAR}(N) = \frac{1}{N} \sum_{n=1}^{N} FAR(n),$$

where, N represents all identities being evaluated by the system.

The FAR represents a statistical value, and therefore is dependent on the size N of the identities against which the biometric system is tested as well as the number of fraudulent attempts made. In an effort to determine the FAR, a probability distribution curve is usually used that is an approximation of a histogram representing the frequency of similar matching scores for genuine and impostor users (Figure 6). Mathematically, the distribution curve is represented as,

$$\text{FAR}(t) = \int_{t}^{\infty} p(s|impostor)ds,$$

where, t is the threshold on the scale of the matching scores identifying genuine and impostor users. The FAR is the area under the impostor distribution curve with matching score values greater than the threshold.

3.1.2 FRR (False Reject Rate)

The FRR represents the frequency with which a biometric system rejects a genuine user, failing to correctly match the provided biometric signal with the stored template. Essentially, the FRR is the ratio

of the number of failed authentication attempts for genuine users and the total number of authentication attempts made for genuine users. The formula for the FRR is denoted by,

$$\text{FRR}(n) = \frac{rejected\ genuine\ attempts\ made\ for\ identity\ n}{all\ genuine\ attempts\ made\ for\ identity\ n},$$

where n is a unique identity in the system.

The overall FRR of a biometric system can be calculated using the average through the formula,

$$\text{FRR}(N) = \frac{1}{N} \sum_{n=1}^{N} FRR(n),$$

where N represents all identities within the biometric system.

Similar to the FAR, FRR represents a statistical value dependent on the size N of the identities against which the biometric system is tested as well as the number of authentication attempts made. In an effort to determine the FRR, a probability distribution curve is used that is an approximation of a histogram representing the frequency of similar matching scores for genuine and impostor users (Figure 6). Mathematically, the distribution curve is represented as,

$$\text{FRR}(t) = \int_{-\infty}^{t} p(s|genuine)ds,$$

where, t is the threshold on the scale of the matching scores identifying genuine and impostor users. The FAR is the area under the impostor distribution curve with matching score values greater than the threshold.

3.1.3 GAR (Genuine Accept Rate)

The GAR represents the frequency by which a biometric system accepts genuine users as authentic. The GAR is related to the FRR through the formula

GAR = 1 – FRR

Usually, to measure performance of a biometric system, the FAR is mapped against the GAR in an ROC curve.

3.1.4 EER (Equal Error Rate)

The FMR and the FNMR are both performance measures that rely on the chosen threshold values. The Equal Error Rate, EER, on the other hand is independent of the threshold. In general, the EER is the value on the ROC curve where the FMR and FNMR are equal. A low value of EER is considered to represent a biometric system with highly accurate performance. The EER has been claimed to be unreliable and limited provided any comparison performed between biometric systems using the EER is done within a small range of values, which may or may not provide a generalized result. Further, for the purpose of comparing multiple biometric systems, EER has limited usefulness given the curves denoting the biometric systems may overlap. Given below in Figure 7 is a representative ROC curve identifying the EER.

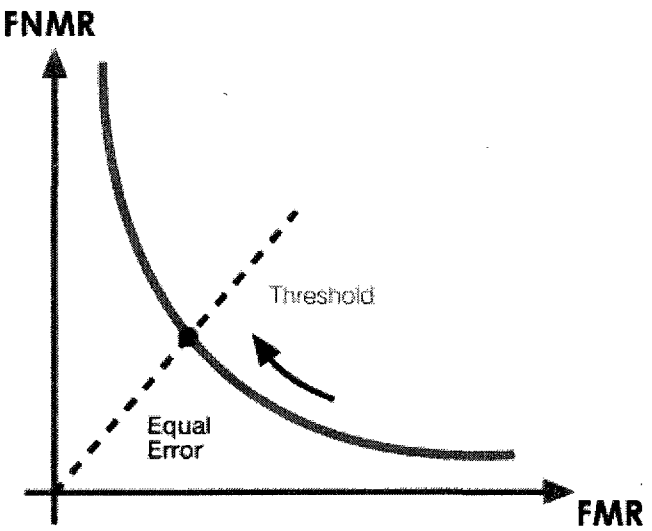


Figure 7: ROC curve indicating the Equal Error Rate (EER), where EER = FNMR = FMR

3.1.5 FTA (Failure to Acquire Rate)

The FTA (or FTC as Failure to Capture rate), identifies the frequency of a biometric system's inability to identify and correctly capture the biometric signal presented to it. The FTA can be considered as a measure of noise within the biometric system since it usually results in inaccurate biometric data. This type of error is usually caused due to the wear and tear in the biometric system's equipment.

3.1.6 FIR (False Identification Rate)

The FIR is the frequency of times a biometric system incorrectly identifies a genuine user and attributes the user with an identity not his/her.

FAR and FRR are the identified measurable that are utilized to establish the performance of biometric systems used by manufacturers. Further, the ROC curve (the FRR is replaced by the GAR and the biometric system(s) is plotted with GAR and FAR) is also commonly used to compare multiple biometric systems (Gan, 2007). (P.J. Phillips, 2000) has identified the following evaluation protocols.

- *Technology evaluation*: This involves testing the prototype algorithms and results in identifying technological progress and promising approaches in controlled laboratory conditions. The algorithms applied including those for acquiring biometric signals, retrieving feature sets from the provided signals and generating matching scores are tested to identify the performance of the biometric system.
- *Scenario evaluation*: Scenario evaluation revolves around measuring system performance of a biometric technology within a class of applications under conditions resembling real world deployment scenarios. As an example, the evaluation process might consider biometric systems as applied to providing access to high security buildings.
- *Operational evaluation*: This tests a particular biometric system within a particular application scenario. As an example, biometric systems might be tested to evaluate performance of fingerprint scans at the JFK airport in New York.

Both scenario and operational evaluations of biometric systems are specific to applications and situations. Consequently, the results from such evaluations cannot be generalized and do not promote an understanding of the performance of biometric systems as well as a comparison of such systems without the specificity of the environment under which these are studied. Technological evaluation of biometric systems (considering various technologies employed within such systems) provides means for a better analysis.

Within the context of technology evaluation, in (Gan, 2007), the author has established the limitations in traditional testing frameworks for performance analysis of multimodal biometric systems based on

varied biometric traits, databases, algorithms, normalization methodologies and fusion methods. The author has promoted factoring noise in performance evaluation since traditional tests provide situational outcomes that are inconsequential in a generalized context. Factoring noise in the performance evaluation allows users to conduct more realistic evaluations of biometric systems.

3.2 A Statistical Approach

With respect to evaluating performance of multimodal biometric systems, various assessment factors exist including technological performance, security performance, user acceptance, identification and verification performance, etc. Of paramount importance and of direct consequential value is a biometric system's performance in correctly evaluating the data presented to it to identify or verify a subject's authenticity. In (R. Snelick M. I., 2003), the authors have provided a framework to conduct performance evaluation of multimodal biometric systems. The authors have pointed the importance of fusion in any multimodal biometric system (essentially to achieve a multimodal biometric system, a level of fusion of data is necessary). They have also identified the benefits of performing fusion at the matching scores level including the ability to use existing matching score databases available in the public domain (or otherwise) and the ability to conduct tests without affecting existing biometric systems (since the experiments are conducted on data generated by these systems). The following framework has been suggested.

- Identify the target set and the query set consisting of signatures known to the biometric system and the signatures to be compared against the known signatures, respectively.
- Generate a matching score matrix (similarity matrix) for each pair of the target and query sets' signatures.
- Create gallery sets and probe sets from the target and the query set, respectively. Repeat the three steps for each biometric modality.
- Format the data from the different modalities into similar unit and ensure the size of the similarity matrices is the same. An assumption is that all modalities are statistically independent and can be combined to create virtual subjects (to indicate the information comes from the same subjects).
- Normalize the data from different modalities into a common range of values.

- Fuse the data from the various similarity matrices from each biometric modality to a single fused similarity matrix.
- Using the fused similarity matrix with (with fused genuine and impostor scores), achieve the performance measures including the FAR and the FRR. Create the ROC curve using the FAR and GAR to evaluate the multimodal biometric system being studied.

The above mentioned framework guidelines have been used by the author in (Gan, 2007) to validate performance of multimodal biometric systems under the influence of noise. The author indicates the difficulties in establishing a testing system taking into account every noise source due to the exponential growth of the noise factors. The use of robust parameter design has consequently been proposed to identify the values for system parameters to institute a high performance, functional and robust methodology. Design of Experiments (DoE) has been used within which a Parameter Diagram has been created outlining the various system parameters including the biometric signals, the noise factors and any control factors to generate the performance matrices. The author has further used the Gaussian Noise Model to generate noise factors through deviations based on interval values that are representative of the general continuous values.

It has been pointed out that using a full factorial experimentation method will be cumbersome due to the number of different combinations that can be achieved through the controllable and uncontrollable factors (and provided the lack of support to carry out such tests without an automated framework). The controllable and uncontrollable factors including the fusion methodologies, the normalization techniques, the number of modalities considered, the distribution of noise within each of those modalities considered, etc. result in an exponential growth in the number of possible test cases (considering also the various levels of operation in each of these parameters). In (R. Krishnan, 2007), the authors have discussed Orthogonal Array Based Testing Strategy (OATS) and displayed, with examples, the increased effectiveness and efficiency in using orthogonal arrays to generate test cases. In most practical implementations, OATS offers extensive coverage of the testing domain with minimal number of test cases through pair-wise combination of parameters affecting the tests. A library of multiple orthogonal arrays is available at the website http://www.research.att.com/~njas/oadir/index.html that includes arrays designed for various numbers of factors and levels. Even though orthogonal arrays provide an effective means of designing test cases, they can be considered limiting within the tests for

evaluating multimodal biometric systems given the benefits of even marginal improvements in the performance of such systems. A more flexible approach and selection of test cases (even though limited through OATS) is necessary for improved evaluations.

To evaluate the performance of the stated multimodal biometric systems considering a combination of face and fingerprint readings using the NIST BSSR1 database, the author in (Gan, 2007) has generated an evaluation matrix. The matrix consists of the control factors, discussed in the next paragraph, and possible combinations of the same. The noise added to considered modalities, valued at various deviation intervals, are the uncontrollable factors. Combinations of the values of these factors are achieved by using orthogonal arrays. For example, an L9 Taguchi orthogonal array has been used to specify the noise variations in the combination of the four modalities.

It has been observed that for performance analysis, partitioning the original dataset into training and testing datasets, referred to as cross validation within the statistical analysis field, yields more accurate results. To evaluate biometric systems, the partitioning of the BSSR1 dataset through one of the possible partitioning schemes such as re-substitution validation, holdout validation or leave one out validation results in a controlled factor to be considered in experimentation. Values for the normalization scheme and the fusion method are the other controlled factors.

3.3 Automated Analysis

Evaluating a biometric system to verify its performance based on a defined set of controlled and uncontrolled factors within the statistical analysis methodology can be time consuming. This complexity stems from the fact that the number of test cases that can be generated for each of the system parameters increases exponentially provided the noise factors, the fusion methodologies and the normalization schemes that are considered. The number of modalities considered is also an influence. Even though the test cases are reduced through the use of orthogonal arrays, previous use of manual applications to determine the performance of multimodal biometric systems has been shown to be cost ineffective. For example, in (Gan, 2007), the author has manually executed 126 experiments using various fusion methods and normalization schemes, with limited results. The solution proposed in the past employs tools that allow the user to perform some automated analysis, but still requires manual interaction with the system. This also poses as a limitation to the analysis capabilities.

Discussed in this section are the primary tools used to perform the experiments to analyze the performance of multimodal biometric systems based on the theoretical framework discussed in the previous section.

3.3.1 NIST BSSR1 Database

In (Gan, 2007), the author has chosen the NIST BSSR1 database as the database of choice for genuine and impostor matching scores. The BSSR1 database is a true (actual subjects) multimodal database and it provides the largest dataset available in the public domain. The BSSR1 contains matching scores in three variations; one set combining data from face and finger fusion, one set combining scores from two fingers fusion and one from combining two different algorithms. Further, each of these variations contains matching scores from 517, 6000 and 3000 subjects, respectively. The matching scores have been captured through cross comparison of all subjects in similarity files. Each file contains one genuine score and remaining impostor scores. As used in (Gan, 2007), only the data set combining the face and finger modalities have been considered to evaluate the resulting multimodal biometric system.

3.3.2 BSSR Processor

The BSSR Processor is a Java application that operates on the BSSR1 database. The author (Gan, 2007) has implemented the functionality to generate comma delimited files for genuine and impostor scores that are used as input to the MUBI tool. The files are generated, one each for the faces and fingers modalities. Noise is also added to the scores through the use of Gaussian noise generator module within the processor.

3.3.3 MUBI (Analysis Tool)

MUBI is a Java application developed at West Virginia University as an analysis tool for biometric systems by evaluating matching scores through a selection of fusion and normalization techniques. It allows the user to submit genuine and impostor scores in comma delimited files, one each for multiple biometric modalities. The user can then choose a normalization scheme and a fusion method to plot the density curves of genuine and impostor scores. As an output, MUBI also provides the ROC curves for the modalities of choice. This enables the user to understand the performance of the single multimodal biometric system.

3.4 Problem Definition

Even though earlier work has been done in measuring performance of multimodal biometric systems under the influence of noise factors (Gan, 2007) through experimentation, the existing tools such as the NIST BSSR1 database, the BSSR Processor and the analysis tool MUBI limit the test cases that can be generated due to the manual inputs. The experiments performed in the previous work have been conducted over a single dataset with provided modalities. To carry out meaningful performance comparisons for multimodal biometric systems over different biometric databases will require additional experiments with consideration to the levels of noise introduced in the system. From a usability point of view, it is also difficult to measure performance of various multimodal biometric systems against one another. Such a usage scenario will require the user to manually identify each multimodal biometric system individually and use the existing tools repeatedly to evaluate their performance separately. The results gathered will then have to be manually compared to generate a performance evaluation report. This process is tedious as well as time consuming. Further, use of the BSSR1 database limits the cases under study to a specific multimodal biometric system evaluation, provided it includes matching scores for face and fingers, fingers, and alternate algorithms only. The chosen intervals to introduce noise in the system also create system boundaries for the analysis performed.

Due to the shortcomings discussed above and the requirements of performance evaluation of biometric systems, the technical and commercial viability of the studied framework has its limitations. This thesis and the resulting application strive to automate the process of generating test cases and input to the analysis tool. It is the intent to allow users the ability to combine matching scores from various multimodal databases that are similar in structure to create a larger subject set. The user will be allowed to configure the noise intervals and the range of values for each. Depending on the dataset, the biometric systems will be generated automatically by considering individual modalities and by generating subsets of the modalities from the provided dataset. The proposed tool will scale the analytical capabilities of MUBI to generate reports and graphs using the ROC curve as a function of FMR and FNMR. The reports and graphs comparing the multimodal biometric systems will be created automatically based on user preferences. These can then be used in a generalized context to evaluate

competing multimodal biometric systems and identify the commercial viability of such systems under various conditions of noise.

Chapter 4. Method of Analysis

The purpose of this thesis is to extend and improve on the work that has been done in evaluating the performance of multimodal biometric systems from a statistical analysis point of view by automating the established framework. It is also the intent to develop an application that allows more freedom in the user's ability to control the test parameters including those for the noise factors, modalities, etc. It allows the system to operate over a larger dataset by combining multiple multimodal (or unimodal) biometric databases. This section identifies the observations made by authors in previous work (Gan, 2007) and consequently establishes the underlying theoretical and experimental framework as a solution to the discussed problem statement in extending the work completed so far.

In (Gan, 2007), the author has performed experiments to measure the performance of a multimodal biometric system consisting of facial images and fingerprint modalities. Using the framework discussed in section 3.2, the author has generated an evaluation matrix through the use of orthogonal arrays. The control parameters used include the data set partitioning method, the normalization schemes and the fusion methods. Given below, in Table 2, are the factors and the possible values. The table is followed by a summary of each factor including all partitioning methods, normalization methods and fusion methods, and indicates the underlying mathematical basis of each.

Factor Name	Possible Values
Dataset Partitioning Method	Re-substitution validation
	Holdout validation
	Leave one out validation
Normalization Method	Min-max normalization
	Decimal scaling normalization
	Z-score normalization
	Median and Median Absolute Deviation normalization
	Tanh-estimators normalization
Fusion Method	Simple sum rule based fusion
	Simple product rule based fusion
	Simple minimum rule based fusion

Factor Name	Possible Values
	Simple maximum rule based fusion
	Biometric Gain against Impostor based fusion

Table 1: Data set partitioning, data normalization and fusion methods used in previous work.

4.1 Dataset Partitioning Methods

As identified by the author in (Gan, 2007), dataset partitioning into training and testing sets is vital in conducting analysis of biometric systems' performance. It allows the evaluators to hypothesize various parameters to control the biometric systems' setup and measure performance using the training set to achieve optimum values. The performance of the system within these parameters is then validated through the testing set. Partitioning of datasets can be achieved through the following three methods, discussed in Table 3.

Partitioning Method	Description
Re-substitution Validation	Using this method, all values in the dataset are used for both initial testing as well as for the validation process. Essentially, both the training dataset and the testing dataset contain all values from within the original dataset. *Mathematical Representation* $O = T = V$, where $O = \{x \mid x \in$ genuine/impostor score$\}$, T is the training dataset and V is the testing dataset.
Holdout Validation	In this method, the user identifies a percentage of the original dataset for the testing data. The values are then chosen randomly from the original dataset up to the percentage value specified to form the testing dataset. The remaining values are used for the training (or validation) dataset.
Leave one out Validation	Using this method, each data point in the original dataset is used as a testing dataset and the remaining constitute the training dataset.

Partitioning Method	Description
	Consequently, for this method, the process is repeated for each unique data point resulting in a total of N samples, given N is the size of the original dataset.

Table 2: Summary of Dataset Partitioning Methods.

4.2 Normalization Methods

Usually, the matching scores of different modalities are provided on different numerical scales (also dependent on the matching algorithm used). To create and study the performance of a multimodal biometric system, these scores must be considered within the same scale. For the purpose, data normalization is used. The author (Gan, 2007) has identified the importance of the chosen normalization scheme to be robust to discount the presence of outliers and efficient to identify values as close to the values observed if the distribution of the data points was known. Various normalization methods used have been presented below in Table 4.

Normalization Scheme	Description
Min-Max Normalization	Within this scheme, each data value of the set is scaled within a provided range. The minimum value of the range is subtracted from each data point. The data points are then divided by the difference of the range. The values are then multiplied by the desired range and the minimum value of the desired range is then added to these. Generally this method is used to transform dataset to the range [0, 1]. *Mathematical Representation* $d'(i) = \left[\left(\frac{d(i) - min_{orig}}{max_{orig} - min_{orig}}\right) X\ (max_{new} - min_{new})\right] + min_{new}$ where, $d'(i)$ is the normalized data value for every point $d(i)$ in the dataset.

Normalization Scheme	Description
	As identified, the min-max scheme is not robust.
Decimal Scaling Normalization	In this normalization scheme, the normalized value is achieved by moving the decimal point of the original data value. The number of decimal places moved depends on the maximum absolute value of the dataset. *Mathematical Representation* $d'(i) = \frac{d(i)}{10^c}$ where, $d'(i)$ is the normalized value for the data point $d(i)$ and c is the smallest number such that $\max(\lvert d'(i) \rvert) \leq 1$ This method can be applied if the matching scores of the modalities considered follow a logarithmic scale. The method is not robust and is dependent on the matching scores being logarithmic.
Z-Score Normalization	This scheme is also called the zero-mean normalization scheme. The values are normalized by using the mean and standard deviation of the dataset. *Mathematical Representation* $d'(i) = \frac{d(i) - \mu_{orig}}{\sigma_{orig}}$ where, $d'(i)$ is the normalized value for data point $d(i)$, μ_{orig} is the mean of the original dataset and σ_{orig} is the standard deviation of the original dataset. This scheme works best if the nature of the dataset is already known in advance, thereby making the step of estimating the values of the mean and standard deviation unnecessary. The method is not robust since the

Normalization Scheme	Description
	mean and the standard deviation are both sensitive to outliers.
Median and Median Absolute Deviation Normalization	Under this scheme, the normalized value of each data point in a dataset is given by subtracting the median of the dataset from the data point and then dividing the value by the Median Absolute Deviation. The Median Absolute Deviation is the median of the absolute value of the median subtracted from the data point. *Mathematical Representation* $d'(i) = \frac{d(i) - median}{MAD}$ where, $d'(i)$ is the normalized value of the data point $d(i)$ and $MAD = median(|d(i) - median|)$ This method has low efficiency.
Tanh-Estimators Normalization	Discussed in (K. Nandakumar, 2008), the tanh-estimators were introduced by Hampel. This technique is both robust and efficient. *Mathematical Representation* $d'(i) = \frac{1}{2}\left[tanh\left\{0.01\left(\frac{d(i) - \mu_{GH}}{\sigma_{GH}}\right)\right\} + 1\right]$ where, $d'(i)$ is the normalized value of the data point $d(i)$, μ_{GH} is the mean of the genuine score distribution as per the Hampel estimators and σ_{GH} is the standard deviation of the genuine score distribution as per the Hampel estimators. Hampel estimators are based on the influence function given below. $\psi(u) = \begin{cases} u & 0 \le \lvert u\rvert < a, \\ a \times sign(u) & a \le \lvert u\rvert < b, \\ a \times sign(u) \times \left(\frac{c - \lvert u\rvert}{c - b}\right) & b \le \lvert u\rvert < c, \\ 0 & \lvert u\rvert \ge c \end{cases}$

Normalization Scheme	Description
	The influence function results in lesser influence of the points a, b and c at the tail of the distribution in estimating the location of the data points and the scaling parameters. In the paper, the authors have identified the use of only the genuine scores as having better results in recognition performance, which is why the mean and standard deviation of only the genuine scores are used.

Table 3: Summary of common Normalization Schemes.

4.3 Data Fusion Methods

In (Gan, 2007), the author has discussed some commonly used fusion methodologies to combine multiple modalities at the matching scores level. As identified, the fusion methods can be applied to the posteriori probability of subjects being genuine. Since the proposed performance evaluation is done at the matching score level (with the testing component being matching scores), these are combined directly to identify better recognition performance (A. K. Jain, 2004). Given below, in Table 5, is a summary of the fusion methods.

Fusion Method	Description
Simple Sum Rule	In this method, the scores are transformed linearly using weights and biases specified by the user. *Mathematical Representation* $s = (a_1 s_1 - b_1) + (a_2 s_2 - b_2) + \ldots + (a_n s_n - b_n)$ where, a and b are the weights and the biases, respectively. s_n represents the scores of individual modalities and s is the fused score. The subscript represents individual modalities.
Simple Product Rule	In this method, the scores are combined by simply calculating the product of individual scores.

Fusion Method	Description
	Mathematical Representation $s = s_1 \times s_2 \times \ldots \times s_n$ where, s_n represents the scores for the modalities considered and s is the fused score. The subscript identifies the individual modalities.
Simple Minimum Rule	In this method, the resulting fused score is simply the minimum score from the set of all scores for all modalities. *Mathematical Representation* $s = \min(s_1, s_2, \ldots, s_n)$ where, s_n represents the scores for the modalities considered and s is the final fused score.
Simple Maximum Rule	In this method, the resulting fused score is the maximum score from the set of all scores for all modalities. *Mathematical Representation* $s = \max(s_1, s_2, \ldots, s_n)$ where, s_n represents the scores for the modalities considered and s is the final fused score.
Biometric Gain against Impostor	BGI is defined as the ratio of the probability of a subject being an impostor based on biometric measurements and the probability of the subject being an impostor prior to making those biometric measurements. *Mathematical Representation* $BGI = \frac{probability\ of\ a\ subject\ being\ an\ impostor\ provided\ the\ biometric\ measurements}{probability\ of\ a\ subject\ being\ an\ impostor\ prior\ to\ the\ biometric\ measurements}$ For the purpose of utilizing the concept for data fusion, the BGI is modified as an approximation to the LRGI (Likelihood Ratio of Genuine to Impostor).

Fusion Method	Description
	This is represented as $BGI \approx LRGI = \frac{probability\ of\ a\ subject\ known\ to\ be\ an\ impostor}{probability\ of\ a\ subject\ known\ to\ be\ genuine}$ For each unimodal biometric system, the scores are transformed to achieve the BGI score for the modality. For a multimodal system, the individual BGI scores (modified) are then combined through a simple product rule to achieve the BGI scores of the multimodal system.

Table 4: Summary of Fusion Methods.

The uncontrolled factors for the experiments to evaluate the performance of multimodal biometric systems, in (Gan, 2007), include the modalities considered in the chosen NIST BSSR1 database. Although known, these act as uncontrolled parameters since the deviations based on the Gaussian noise model are applied directly to the matching scores within defined 1%, 5% and 10% intervals. The modalities include the Face C and G modalities as well as the right and left Index Finger modalities. The factors and their values have been listed below in Table 6.

Factor Name	Possible Values
Face C modality	Applied 1% deviation
	Applied 5% deviation
	Applied 10% deviation
Face G modality	Applied 1% deviation
	Applied 5% deviation
	Applied 10% deviation
Right Index Finger modality	Applied 1% deviation
	Applied 5% deviation

Factor Name	Possible Values
	Applied 10% deviation
	Applied 1% deviation
Left Index Finger modality	Applied 5% deviation
	Applied 10% deviation

Table 5: Noise rates applied to modality scores in previous work.

Considering the mentioned controlled and uncontrolled factors, the n matrix is generated for the NIST BSSR1 database limited to the multimodal biometric system defined by the modalities considered within the database. After generating the comma delimited genuine and impostor matching scores for each modality, the same are entered into MUBI. Given in the next few pages in Figures 8, 9, 10 and 11 are samples of the results observed in the experiments conducted in the paper (Gan, 2007).

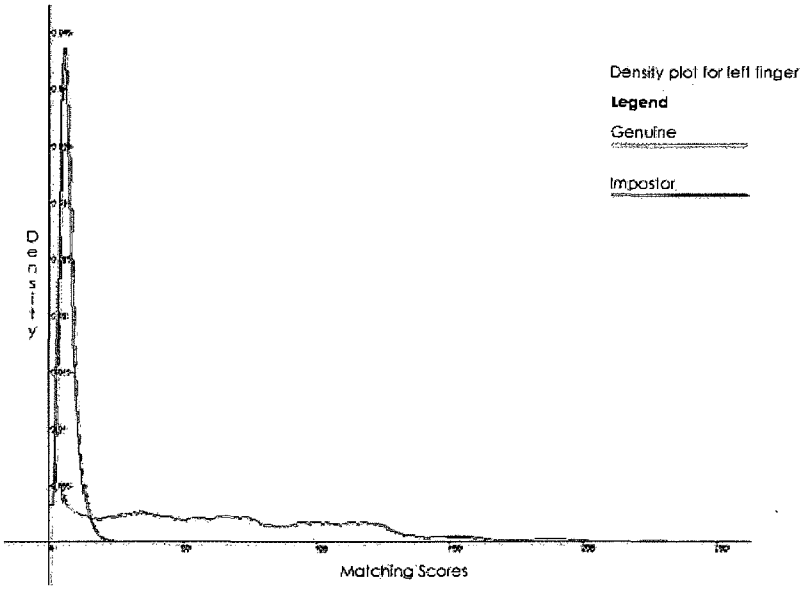


Figure 8: Density plot for left finger modality using original scores

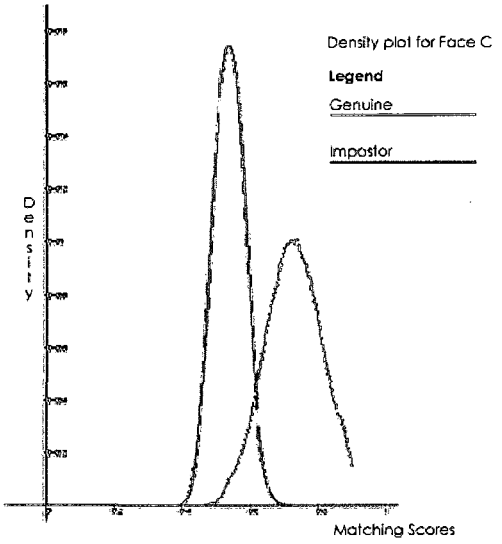


Figure 9: Density plot for Face C using original scores

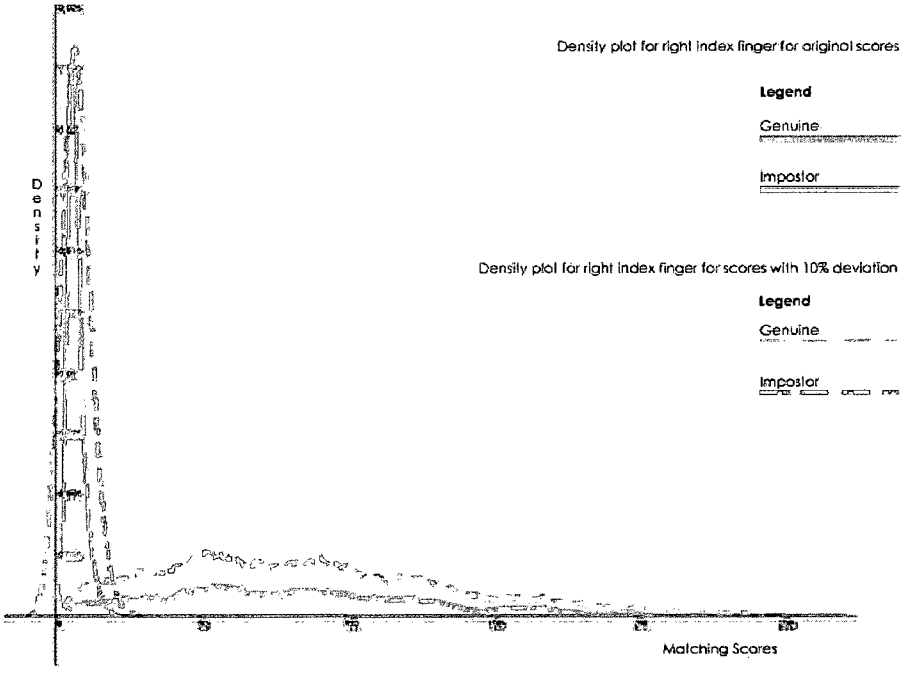


Figure 10: Probability density curves for right index finger with original scores and scores with 10% deviation added

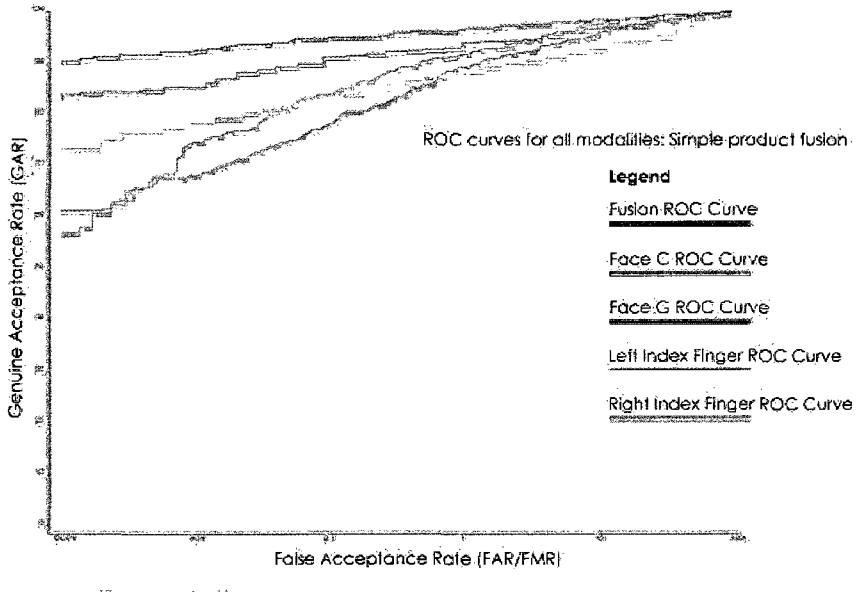


Figure 11: ROC curves for combined modalities with simple product fusion

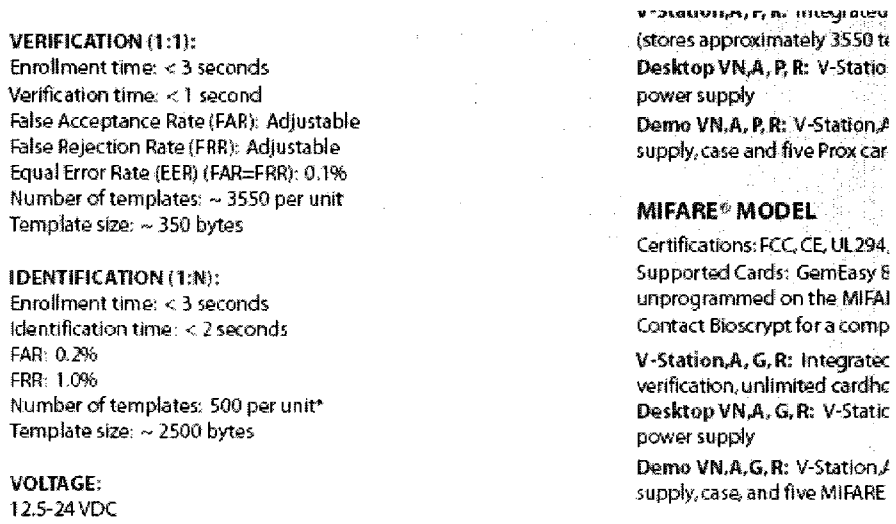
Based on the above graphs, the author has observed the overall performance of the multimodal biometric system consisting of the Face and Finger modalities. The experiments have been carried out as per an evaluation matrix and the results have indicated comparatively lesser impact of noise on certain combination of control factors while in other cases the noise deteriorates the performance of the system dramatically. The author has confirmed the need to perform more thorough experiments necessitating the increased size of test cases also discussed in (A.K. Jain A. R., 2006). The author also points out the dependence of the results on the chosen FAR values. This has a direct consequence on the type of applications the system under test is appropriate for.

One of the key aspects that limit the existing application in determining the performance of multimodal biometric systems is the dataset being considered. There are various multimodal databases available including the FRGC database from NIST, University of Surrey's XM2VTS, European BioSecure's MyIDea database, etc. (Flynn, 2008). These databases cover different modalities in different conditions and with different equipment. As indicated in (Gan, 2007), performing tests on a larger representative database allows for increased confidence in the accuracy, scalability and throughput of a biometric system. By

enabling the use of these databases through a common platform, the user is allowed to perform analysis over a much larger dataset and the inherent variance in these databases present a more real world scenario.

To study the effects of noise, the author in (Gan, 2007) has used values within interval levels as corresponding to the noise factors that are then added to the matching scores from the biometric databases. These intervals represent a continuous set of values that affect the system as noise. The size of the interval chosen, consequently, limits the ability of the system to analyze effectively the performance. Also, as per the experiments, the noise levels are applied to the overall biometric system implying that each modality considered is applied the same noise level. In a real world scenario, this is not true (A.K. Jain A. R., 2002). As an example, a fingerprint scanner will potentially suffer more wear and tear (due to direct interaction with the user) than a camera used to capture face images. Consequently, to simulate a multimodal biometric system with the two modalities, the noise level should be more for the fingerprint modality than the face modality. A larger set of values chosen using the Gaussian Noise Model within smaller intervals and applying noise levels independently (or to the overall system) can, therefore, be used to analyze the performance of biometric systems under noise more accurately. It is the purpose of this thesis to study the performance of multimodal biometric systems by allowing the user more freedom in specifying the deviations caused by noise factors over a much larger range of values.

It is also the purpose of this thesis to provide a commercially viable solution that can be adequately used to determine the performance of multimodal biometric systems considering the noise factors, and operating over a larger dataset. This paves the way for more accurate comparisons to be performed over various flavors of multimodal biometric systems and provide a direct comparison of such systems. As identified earlier, manufacturers usually provide a single value of FMR to identify the capabilities of their biometric systems (http://www.bioid.com/sdk/docs/About_EER.htm). As an example, given below in Figure 12 is an excerpt from the datasheet for a biometric system from Bioscrypt called the V-Station.



VERIFICATION (1:1):
Enrollment time: < 3 seconds
Verification time: < 1 second
False Acceptance Rate (FAR): Adjustable
False Rejection Rate (FRR): Adjustable
Equal Error Rate (EER) (FAR=FRR): 0.1%
Number of templates: ~ 3550 per unit
Template size: ~ 350 bytes

IDENTIFICATION (1:N):
Enrollment time: < 3 seconds
Identification time: < 2 seconds
FAR: 0.2%
FRR: 1.0%
Number of templates: 500 per unit*
Template size: ~ 2500 bytes

VOLTAGE:
12.5-24 VDC

(stores approximately 3550 t
Desktop VN,A, P, R: V-Statio
power supply
Demo VN,A, P, R: V-Station,
supply, case and five Prox car

MIFARE® MODEL

Certifications: FCC, CE, UL294,
Supported Cards: GemEasy 8
unprogrammed on the MIFAI
Contact Bioscrypt for a comp

V-Station,A, G, R: Integratec
verification, unlimited cardhc
Desktop VN,A, G, R: V-Static
power supply
Demo VN,A,G, R: V-Station,
supply, case, and five MIFARE

Figure 12: Datasheet excerpt from Bioscrypt's V-Station biometric system

Using just the FAR or the FRR is inadequate for a comprehensive comparison. Consequently, it is the intent of this thesis to identify multiple reporting criteria including the FAR, FRR, GAR and the ROC curves to promote automated comparison between systems and the applicability to different applications including high-security, forensics, civilian, etc. identified as per the required GAR values for a given value of FAR.

Discussed in the next section is the proposed application design that utilizes the theory covered in this section and previous sections to present the overall solution.

Chapter 5. Method of Approach

The material presented in earlier sections indicates to some of the shortcomings in the performance evaluation of multimodal biometric systems using existing methodologies and applications. Even though the underlying theory correctly forms the basis of the necessary analysis, the limitations arise due to the manual nature of existing applications. As has been mentioned earlier, the key limitations include:

- The limited dataset that can be used in performing the experiments manually.
- Since the dataset is limited, the multimodal biometric systems (by changing the test conditions) that can be considered are also limited.
- The noise factors are defined as deviations using a small number of discrete values (1%, 5% and 10%).
- The output observed using the existing tools is not sufficient to intuitively identify and compare different biometric systems.
- Since the process of generating the matching scores, using the MUBI tool to define a single multimodal biometric system as per controlled factors, and retrieving the results is manual, the solution is not cost effective and tedious.

This section focuses on providing an insight into the application modules that will be developed to support the thesis, and in the process, the use of existing applications to achieve the desired functionalities.

5.1 System Modules - Architecture

The implemented system includes developed modules in addition to existing components with enhanced capabilities, primarily in automation of the components. Where applicable, the design from existing modules has been implemented through new modules to ensure compatibility with the developed application. The suggested usage scenario includes existing databases released by government and independent agencies to generate test cases and consequently define the modalities in the biometric system. The BSSR1 database released by the NIST will be the candidate database. However, the system is scalable to retrieve genuine and impostor matching scores from other databases as well, provided the structure of the databases remains consistent. The BSSR Processor has been implemented considering existing design to automatically retrieve values from the test database for

selected modalities and add the Gaussian noise. The generated scores are then used to create modality objects for the MUBI analysis tool. A wrapper around the MUBI tool has been implemented to take, as input, the generated scores automatically. Further, the output from MUBI (in existing application, graphical charts) has been enhanced to capture information in a results database. Also added to the system is a module to execute over the results database to generate textual reports, graphical charts and various comparison matrices. Native graphs generated by MUBI are also displayed and can be captured as images for individual tests. The overall system architecture has been included below in Figure 13, followed by a discussion of the key individual modules in the next section.

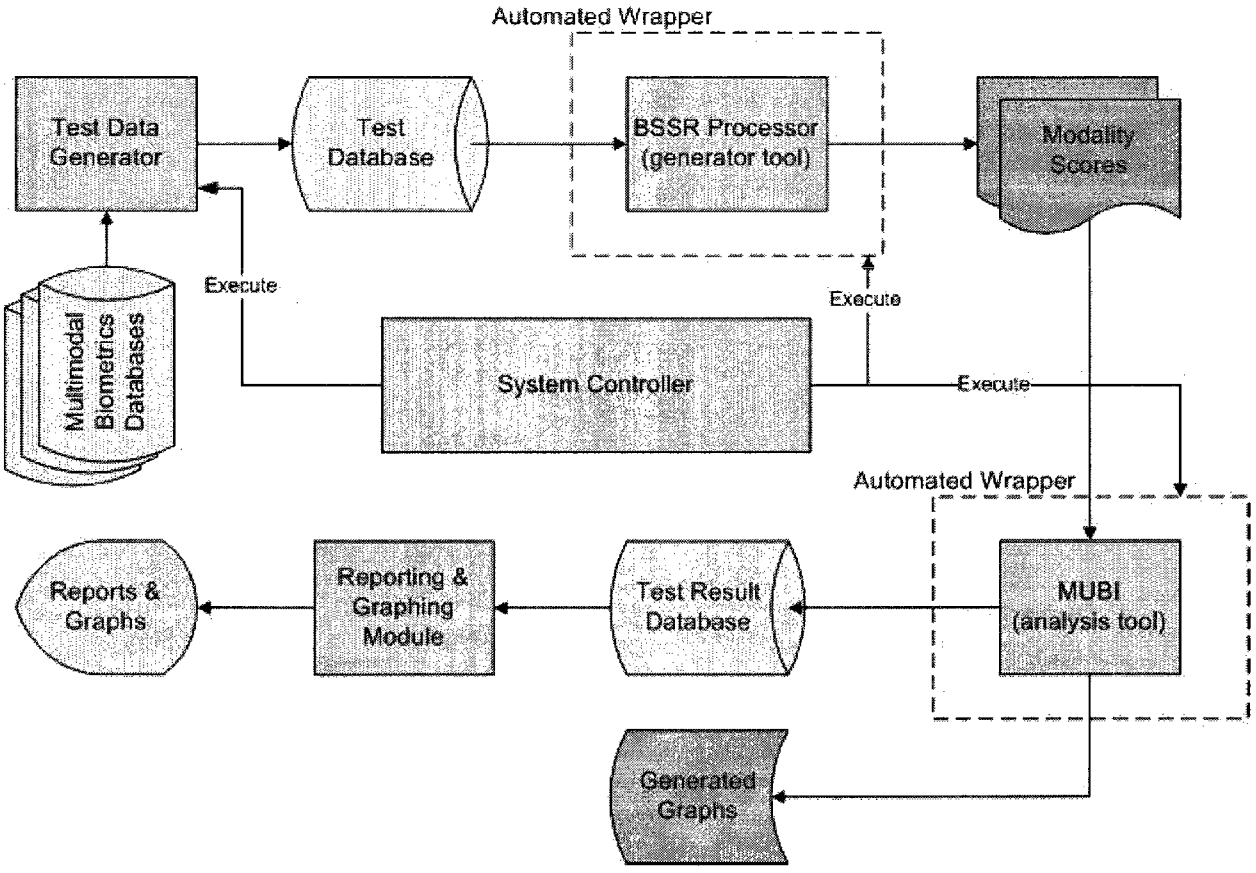


Figure 13: Automated System Modules

5.2 System Algorithm

Included in this section is an overall algorithm for the implemented application. The algorithm identifies the major inputs to the system as well as the outputs provided by the system. The major steps within the execution of the application have been included.

Algorithm BiometricPerformanceEvaluator

Input: matching scores from biometric databases
test setups configured in application database identifying
- modalities to be included in multimodal system
- partitioning scheme for data
- normalization scheme
- fusion scheme
- test FAR value

Output: ROC curves for individual modalities without fusion for test setup
ROC curves for individual modalities with fusion for test setup
comparison chart for all test setups

1.0 read biometric database matching scores for each modality, if biometric database supplied
2.0 insert each new modality found in the table BIOMETRIC_MODALITIES
2.1 insert each genuine score in the table MODALITY_GENUINE_SCORES
2.2 insert each impostor score in the table MODALITY_IMPOSTOR_SCORES
3.0 read TEST_SETUP_MASTER and create objects for each configured Test Setup
4.0 read MODALITIES_CONFIGURATION for each Test Setup element and create objects to be added to Test Setup objects
5.0 for each item in Test Setup objects, do
5.1 generate an analyzer Mubi system
5.2 set the system data partitioning scheme
5.3 for each modality in the current Test Setup object do
5.4 create an analyzer Mubi system modality
5.5 set all values of the Mubi system modality
5.6 add modality genuine and impostor scores
5.7 update modality scores to implement partitioning scheme
5.8 set modality normalization scheme and update scores
5.9 add modality to the current Mubi system
5.10 end for
5.11 generate and display ROC curve without fusion applied

5.12 apply fusion to the Mubi system
5.13 update all scores with the fusion methodology applied
5.14 generate and display ROC curve with fusion applied
5.15 end for
5.16 generate a comparison chart for all Test Setup objects
6.0 end execution

End Algorithm

5.3 Implemented Software Application Components

Included in this section is a discussion on the key modules that have been implemented to achieve the desired functionality of analyzing performances of multiple multimodal biometric systems. These have been identified with implemented Java components according to the overall system model given in the previous section. A list of all Java packages and classes has been included here.

Implemented Packages and Classes

Following are all the classes implemented within the system. These do not include existing modules that have been used in the analysis including the MUBI analysis tool. A discussion of the tool is outside of the scope of the thesis paper and has been covered comprehensively in (Samoska, 2006).

- com.biometrics.thesis.analyzer
    - AnalyzeTestConfiguration – The analyzer class that interacts with the MUBI system to analyze each test configuration individually. The class provides a comprehensive result on processing.
- com.biometrics.thesis.controller
    - SystemController – The system controller that performs each step in sequential order including adding a biometrics' database, creating test configurations, analyzing the configurations and reporting the results.
- com.biometrics.thesis.db
    - DBConnectionManager – Manages connection to the database for adding modalities to it as well as adding results.
- com.biometrics.thesis.elements

- GenuineScoreElement – A genuine score object added to the modality to be used within the system.
- ImpostorScoreElement – An impostor score object added to the modality to be used within the system.
- ModalityElement – An object representing a single modality within the system that is read from the database. This is then used to create modalities within the MUBI analysis tool. The object includes various properties relevant to the modality itself.
- TestConfiguration – An individual test configuration consisting of all parameters identifying the test and the modalities attached to the test.

- com.biometrics.thesis.generator
  - GenerateModalitiesScoreDatabase – Used to read from a user identified source database to create system modalities along with genuine and impostor scores in the test database.
  - GenerateTestModalities – Used to read the test configurations and generate a list of the same. The test configurations contain all relevant parameters for the test as well as individual modalities through TestConfiguration and ModalityElement objects, respectively.
- com.biometrics.thesis.testers
  - RunBiometricsTester – The test class to execute the system.
- com.biometrics.thesis.ui
  - GARResultChart – Creates a chart to compare the various test systems. The GAR values for configured FAR are used to compare the test systems.

5.4 Multimodal biometrics database

Although the system is scalable so that it can be used with various biometrics databases conforming to the NIST BSSR1 database's structure, the NIST's BSSR1 database has been used for the proof of concept. The NIST BSSR1 database contains 4 different modalities using a total of 517 subjects, along with their genuine and impostor matching scores. The modalities include matching scores for right index finger, left index finger, face using a matching algorithm C and face using a matching algorithm G. The properties of these modalities, as relevant to the system, have been included below in Table 2.

Modality	Score Scale	Minimum Value	Maximum Value	Score Range	Score Higher Better
Right Index Finger	250.0	0.0	257.0	1.0	True
Left Index Finger	250.0	0.0	246.0	1.0	True
Face Matching Algorithm C	1.0	-1.0	0.898	1.0	True
Face Matching Algorithm G	50.0	54.835	83.494	1.0	True

Table 6: NIST BSSR1 Modalities Parameters

5.5 Test Data Generator

The intent of this module is to utilize information provided in the multimodal biometrics databases to create a single dataset of matching scores (genuine and impostor). In implementation, the class GenerateModalitiesScoreDatabase included in the package com.biometrics.thesis.generator has been developed. This component of the system reads the biometrics database (in textual format), and ports the value to the test database. The user is able to identify the source database (NIST BSSR1, or otherwise) within a folder structure and the component reads through all scores' files for each modality included and stores the information in the database. The stored modalities, which are individually kept in the database from various source databases, can be combined together to produce more complex multimodal biometric systems. Consequently, the module addresses the limitations of a small dataset with a fairly small number of subjects considered. This also extends the capabilities of existing systems by allowing the user to conduct experiments over a larger dataset. Both the reasons mentioned here allow the user to conduct experiments using a more robust system design.

Component Process

The component assumes the structure of the source database as similar to the NIST BSSR1. For each modality within the database, the component reads the genuine and impostor scores and stores the information in the test database in two different tables. Modalities and their properties are stored in a separate table.

5.6 Test Database

The test database serves multiple purposes in context of the developed application. It captures, uniquely, data from multiple source biometrics databases to identify the genuine and impostor matching scores against the individual modalities. It also includes various other properties of the modalities relevant to be tested. Further, the database contains test configurations. Test configurations uniquely identify proposed multimodal biometric systems and include parameters pertaining to the test configurations. Included below are the structures of all tables and the purpose of each. Also included in Figure 14, is the database diagram indicating the tables and the relationships between the same.

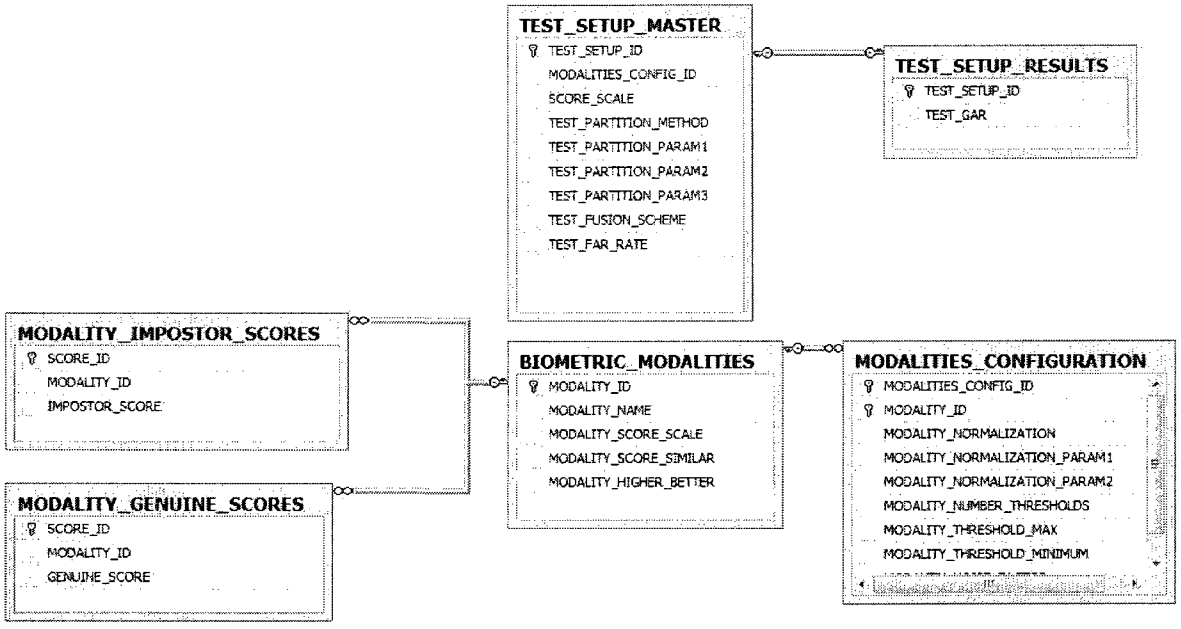


Figure 14: Test Database Tables and Relationships.

BIOMETRIC_MODALITIES

This table contains each modality that has been added to the system. Since the user can employ multiple biometrics databases, each modality in the databases is captured separately allowing the user to cross reference these modalities to generate multimodal biometric systems. The structure of the table is included below in Table 3 with a short description of each column.

Column Name	Column Purpose
MODALITY_ID	A unique identifier of the modality used for

Column Name	Column Purpose
	reference within the system.
MODALITY_NAME	Any string identifying the modality to the user.
MODALITY_SCORE_SCALE	The score scale for the modality.
MODALITY_SCORE_SIMILAR	Identifies whether the scores represent similarity or distance. These are used during the analysis process.
MODALITY_HIGHER_BETTER	Identifies if higher scores in the modality are better within the system. These are used during the analysis process.

Table 7: Table BIOMETRIC_MODALITIES structure.

MODALITIES_CONFIGURATION

This table contains additional properties that are relevant to a single modality to be analyzed using the system. The user, as part of configuring a test system, must add modalities here (linked with the test system identifier) and set up configurable parameters. A list of the parameters is included below, identified as columns in Table 4.

Column Name	Column Purpose
MODALITIES_CONFIG_ID	A unique identifier that denotes this particular configuration of the modality to be used in a test setup.
MODALITY_ID	The identifier of the modality being changed for this instance of the configuration.
MODALITY_NORMALIZATION	A string value identifying the normalization scheme to be applied to the modality in analysis. The values permitted are included in Table X.
MODALITY_NORMALIZATION_PARAM1	A decimal value as the first parameter of the normalization scheme (if required).
MODALITY_NORMALIZATION_PARAM2	A decimal value as the second parameter of the normalization scheme (if required).
MODALITY_NUMBER_THRESHOLDS	An integer number identifying the number of thresholds to be applied to the modality in the analysis process.
MODALITY_THRESHOLD_MAX	The maximum decimal value of a threshold for this modality.
MODALITY_THRESHOLD_MIN	The minimum decimal value of a threshold for this modality.

Column Name	Column Purpose
MODALITY_NOISE_FACTOR	A decimal value identifying the noise level to be applied to the scores of this modality.

Table 8: Table MODALITIES_CONFIGURATION structure.

MODALITY_GENUINE_SCORES

This table contains the genuine scores for all modalities, identified by the modality identifier. The columns have been included below in Table 5.

Column Name	Column Purpose
SCORE_ID	An auto-generated unique identifier for the score record.
MODALITY_ID	The modality identifier of the modality for which this record holds the genuine score.
GENUINE_SCORE	The decimal value of the genuine score.

Table 9: Table MODALITY_GENUINE_SCORES structure.

MODALITY_IMPOSTOR_SCORES

This table contains the impostor scores for all modalities, identified by the modality identifier. The columns have been included below in Table 6.

Column Name	Column Purpose
SCORE_ID	An auto-generated unique identifier for the score record.
MODALITY_ID	The modality identifier of the modality for which this record holds the impostor score.
IMPOSTOR_SCORE	The decimal value of the impostor score.

Table 10: Table MODALITY_IMPOSTOR_SCORES structure.

TEST_SETUP_MASTER

The table contains the various test setups devised by the user that are to be analyzed and compared. Various parameters that are relevant to generating the performance analysis of the test setups have also been included. The following Table 7 provides a list of all columns and identifies their purpose within the system.

Column Name	Column Purpose
TEST_SETUP_ID	An auto-generated unique identifier for the test configuration record.
MODALITIES_CONFIG_ID	The modalities configuration from table MODALITIES_CONFIGURATION that is used in this test as a multimodal biometric system.
SCORE_SCALE	The decimal value of the overall test score scale to be used.
TEST_PARTITION_METHOD	A string identifying the partitioning method used for the test. The permissible partitioning methods include the ones provided in Table.
TEST_PARTITION_PARAM1	A decimal value identifying the first parameter to be used for the partitioning method. This may or may not have a value depending on the partition method chosen.
TEST_PARTITION_PARAM2	A decimal value identifying the second parameter to be used for the partitioning method. This may or may not have a value depending on the partition method chosen.
TEST_PARTITION_PARAM3	A decimal value identifying the third parameter to be used for the partitioning method. This may or may not have a value depending on the partition method chosen.
TEST_FUSION_SCHEME	A string representing the fusion method chosen for this test setup. The permissible values include the ones provided in Table.
TEST_FAR_RATE	A decimal value identifying the FAR rate to be used for the test setup. At this value, the GAR of the test system is calculated (approximation) and provides a comparison factor between various test setups representing the multimodal biometric systems.

Table 11: Table TEST_SETUP_MASTER structure.

TEST_SETUP_RESULTS

This table contains the results for each test configuration in terms of the GAR value against the configured FAR. In Table 8, the columns and their purpose have been outlined.

Column Name	Column Purpose
TEST_SETUP_ID	The unique identifier of the test configuration for which this record indicates the GAR value.

Column Name	Column Purpose
TEST_GAR	The decimal value of the GAR for the test configuration against the defined FAR.

Table 12: Table TEST_SETUP_RESULTS structure.

5.7 BSSR Processor

The BSSR Processor was an existing module that adds noise based on Gaussian distribution to the matching scores. The component processes the biometric database directly and generates comma delimited files that provide the input to the MUBI analysis tool. Currently a manual process, this module has been automated in a new implementation to generate genuine and impostor matching scores for different biometric modalities based on the Test Database. In the existing tool, the noise added to the scores is one of 1%, 5% or 10% deviation. A feature of automation added to this module will be a user configured element to determine the amount of noise added. The user, for each individual test setup is able to add arbitrary values of noise to the modalities. This allows the user to study the effects of noise using higher degree orthogonal arrays enabling a more realistic simulation as well as promotes the study of application based analysis of the biometric systems.

Component Process

Within the process, the class GenerateTestModalities reads information from the database to generate individual test configurations (represented in the system through the element TestConfiguration). Each test configuration contains multiple modality elements represented by the Modality class. The list of TestConfiguration objects are then passed for analysis within the system. The existing BSSR Processor has not been modified for the purpose. Instead, the design has been implemented to conform with the created application. This forms a part of the analyzing class AnalyzeTestConfiguration within which the MUBI system modality elements are created with genuine and impostor scores after applying the defined noise rate.

5.8 Modality Scores

For each test system being studied, the application creates a separate MUBI analysis system and measures the performance of the same. For this purpose, the modality scores provided to MUBI are

retrieved from the test database and after having been applied the necessary noise through the BSSR Processor component, added directly to the MUBI system. Therefore, the scores are kept in memory as GenuineScore and ImpostorScore elements linked to the various modalities.

5.9 MUBI Analysis Tool

This existing application uses a combination of biometric modalities, normalization techniques and fusion methods to generate ROC curves corresponding to genuine and impostor test scores. The application can also generate the probability density curves for genuine and impostor distribution for each modality. In its present state, the application requires the user to manually create a simulated multimodal biometric system by adding modalities. Matching scores for each must be provided through text files along with configuring the normalization scheme and the fusion method to generate results for the specific case.

In the process of automating this component, it has been used as a Java repository to make use of the exposed functions. The class AnalyzeTestConfiguration acts as an automated wrapper that creates multiple objects of the MUBI system based on the number of test configurations to be analyzed and compared. The normalization schemes, partitioning methods and fusion methods are then applied directly to the system (and modalities within it). The data collected from this is then stored in the database (to be used in further analysis, as needed) as well as displayed to the user through graphs, textual reports and a comparison charts.

Component Process

As part of the process, the AnalyzeTestConfiguration creates MUBI system objects for each test configuration based on the TestConfiguration objects. For each test configuration, linked modalities are added and normalized as per the parameters defined in the database. The system is then partitioned and scores are fused. Graphs for each system are then displayed to the user and textual data reported. A comparison chart is then provided comparing the performance of each test configuration for a given FAR value. The performance is measured in terms of the GAR.

5.10 Reporting and Graphing module

The module is responsible in providing the users a textual report on the performance of the various configured multimodal biometric systems (through different test configurations). It also provides the

user a comparison chart reporting the performance of the various multimodal biometric systems being tested against each other. The comparing value used is the GAR. A bar chart is created by the system outlining, in percentage, the success in accepting users based on a FAR value. The class GARResultChart performs the stated tasks.

5.11 System Controller

This module acts as an authority to delegate the tasks defined, as per process, to other modules. Provided the complete solution involves various modules that have either been developed or have been extended for automated functionality, these modules must operate within a defined process cycle. The System Controller module identifies, through rules, the necessary user configuration elements and the process with which it controls the generation of the test database, the addition of noise factors, the analysis by MUBI and finally the generation of reports.

Chapter 6. Sample Experiments & Results

Discussed in this section are some sample test experiment setups and the observed results. In the first sub-section, a random test experiment setup is explained along with the values of all parameters considered and the relevance of each. The test results are then briefly discussed. In the following sub-section, test setup to compare the previous experiments performed manually in (Gan, 2007) has been constructed for the automated approach. The results of the experiments have been compared and an analysis presented outlining the benefits of the new approach.

6.1 Experiments Setup – Random Test Values

Setting up the test system requires adding values to the tables listed in the section 5.5. Given below are excerpts of all tables with the sample data added to them.

BIOMETRIC_MODALITIES

This table has been designed to accommodate any modality for which genuine and impostor scores can be provided. For the purpose of the test, this table contains the modalities from the NIST BSSR1 biometric database. For each modality, the score scale, similarity boolean value and score higher better value has been added. Given below in Figure 15 is a sample excerpt from the table.

Table - dbo.BIOMETRIC_MODALITIES Summary

MODALITY_ID	MODALITY_NAME	MODALITY_SCORE_SCALE	MODALITY_SCORE_SIMILAR	MODALITY_HIGHER_BETTER
[illegible]	face C	1.00000000	True	True
b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	right finger	250.00000000	True	True
5d2572ea-0601-401b-a2f3-d5f7efa59516	left finger	250.00000000	True	True
d13e9793-7ba9-4872-8fff-d781e81d1aa0	face G	50.00000000	True	True

Figure 15: BIOMETRIC_MODALITIES table with initial test setup data from NIST BSSR1 biometric database.

MODALITY_GENUINE_SCORES

This table contains the genuine scores, in their original form, for all modalities listed in the table BIOMETRIC_MODALITIES. The scores are recognized based on the MODALITY_ID. Given below is the table containing actual data from the NIST BSSR1 database. A total of 2068 records are available in the present environment (provided the NIST BSSR1 database contains 517 genuine scores for each modality, resulting in 517 X 4 = 2068 genuine scores). Figure 16 contains a sample.

Table - dbo.MO..._GENUINE_SCORES Summary

SCORE_ID	MODALITY_ID	GENUINE_SCORE
25e2d425-e4bd-4b90-8868-0027f6b56651	d13e9793-7ba9-4872-8fff-d781e81d1aa0	80.14683000
9db138fc-59ae-4fe0-8257-003db290eab8	1ccd8755-3566-4e11-8a70-9e6794687781	0.60790000
ef502fad-2109-4d8e-82f1-006059924edc	5d2572ea-0601-401b-a2f3-d5f7efa59516	84.00000000
2a051435-1a59-4151-9dc3-00a3f7c5e670	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	57.00000000
5be2a403-d3ed-4d3d-9ad4-00e40591c735	5d2572ea-0601-401b-a2f3-d5f7efa59516	50.00000000
833d864f-83bc-4825-a72f-00fbf958f368	5d2572ea-0601-401b-a2f3-d5f7efa59516	11.00000000
931d6458-b270-495d-b11c-0101b48dbe69	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	11.00000000
c6d2fa01-cd02-4289-a36f-011509a269ea	d13e9793-7ba9-4872-8fff-d781e81d1aa0	82.11810000
d67325da-9e35-49b7-b9b8-011aa03fcb37	5d2572ea-0601-401b-a2f3-d5f7efa59516	64.00000000
85f7d595-1986-4d29-b653-01803a5824a1	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	61.00000000
f745d64f-3f6a-48ca-8f83-018ecdde068d	5d2572ea-0601-401b-a2f3-d5f7efa59516	19.00000000
b8e48030-b376-4d2e-bf58-01a73f535fe5	1ccd8755-3566-4e11-8a70-9e6794687781	0.78832000
4ff75e6f-902f-40b1-80a5-01aba198dcb4	5d2572ea-0601-401b-a2f3-d5f7efa59516	107.00000000
bf663a74-2b1a-4d0d-8425-01b3e0c1c16f	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	7.00000000
ce7c83ea-a8d3-4f70-bb98-01bdf1ff3e1b	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	38.00000000
0e8aa8f2-8310-4292-ad68-01d53039ff21	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	39.00000000
219d8fc9-3c87-499a-8fd9-01f4f68efc15	5d2572ea-0601-401b-a2f3-d5f7efa59516	77.00000000
24a2fccb-3bc3-43fc-b329-023f0481e827	d13e9793-7ba9-4872-8fff-d781e81d1aa0	76.90302000
3af91829-13f1-4836-b3c7-024b033d88d8	1ccd8755-3566-4e11-8a70-9e6794687781	0.52017000
3d7bfe7b-9fb2-417e-b1aa-025988d3a711	5d2572ea-0601-401b-a2f3-d5f7efa59516	87.00000000
9d6a9d15-efd1-49d0-ad51-027010f7c0f0	5d2572ea-0601-401b-a2f3-d5f7efa59516	11.00000000
c5f37f22-e06e-45f9-81b4-0285a3029f78	5d2572ea-0601-401b-a2f3-d5f7efa59516	73.00000000

Figure 16: MODALITY_GENUINE_SCORES table with initial test setup data from NIST BSSR1 biometric database.

MODALITY_IMPOSTOR_SCORES

This table contains the impostor scores, in their original form, for all modalities listed in the table BIOMETRIC_MODALITIES. The scores are recognized based on the MODALITY_ID. Given below is the table containing actual data from the NIST BSSR1 database. A total of 1067088 records are available in the present environment (provided the NIST BSSR1 database contains 516 impostor scores for each subject and for each modality, resulting in 517 X 516 X 4 = 1067088 impostor scores). Figure 17 contains a sample.

Table - dbo.MOD...IMPOSTOR_SCORES | Summary

SCORE_ID	MODALITY_ID	IMPOSTOR_SCORE
[illegible]	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	8.00000000
a1da6545-e5aa-480b-a92a-00003d31eda0	5d2572ea-0601-401b-a2f3-d5f7efa59516	10.00000000
2c252f79-5d86-4591-9546-00004e0dfc6a	d13e9793-7ba9-4872-8fff-d781e81d1aa0	59.63693000
d4ac0a6e-2af8-4ba8-a4d3-000055f0b13c	d13e9793-7ba9-4872-8fff-d781e81d1aa0	63.94175000
1990e64f-2c89-4754-89b3-0000ce2d5836	5d2572ea-0601-401b-a2f3-d5f7efa59516	7.00000000
7416e7c1-2e37-49f3-9bb5-0000e0154cab	d13e9793-7ba9-4872-8fff-d781e81d1aa0	64.89241000
bcfe4386-5598-458f-a5ff-0000e53b59c9	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	6.00000000
b45393fd-2d61-4d93-91af-0000e6e99cd2	d13e9793-7ba9-4872-8fff-d781e81d1aa0	67.02085000
7e3ab0e0-5a36-4a4d-a11d-0000e8d634ad	d13e9793-7ba9-4872-8fff-d781e81d1aa0	65.99216000
b29e06a3-f23e-4d41-9c97-0000fa0144e9	d13e9793-7ba9-4872-8fff-d781e81d1aa0	72.33743000
99ba1ed3-7f7f-4242-a185-000127662a6e	d13e9793-7ba9-4872-8fff-d781e81d1aa0	65.59457000
aa1d035c-cd2e-4db0-9178-000142416d95	1ccd8755-3566-4e11-8a70-9e6794687781	0.49131000
bf72a235-85b9-4c27-a412-000158a89b47	5d2572ea-0601-401b-a2f3-d5f7efa59516	5.00000000
b0d9ebd7-ed2e-42b6-ab02-0001863fff8c	1ccd8755-3566-4e11-8a70-9e6794687781	0.47528000
25f91997-87c6-47fe-b703-00018be6d8a8	1ccd8755-3566-4e11-8a70-9e6794687781	0.50819000
7b1451c2-1ba3-469a-83fd-00019079e0e8	5d2572ea-0601-401b-a2f3-d5f7efa59516	8.00000000
fbdfbc11-5a08-4b8f-ab49-00019ce2e8da	d13e9793-7ba9-4872-8fff-d781e81d1aa0	66.48464000
76b8db42-70f7-4fa2-a491-0001a3b1c7f7	d13e9793-7ba9-4872-8fff-d781e81d1aa0	66.17708000
7b79a28d-857a-4efb-a825-0001afbf7063	5d2572ea-0601-401b-a2f3-d5f7efa59516	7.00000000
ddea2cd9-f5bf-4192-a798-0001b7312593	5d2572ea-0601-401b-a2f3-d5f7efa59516	5.00000000
5ad5b0fd-6b8c-4661-8bf4-0001c32fc658	d13e9793-7ba9-4872-8fff-d781e81d1aa0	66.01602000
14fab38f-ebed-42aa-9284-0001ec26183f	d13e9793-7ba9-4872-8fff-d781e81d1aa0	72.52839000
9fd7fdb0-7d86-4abe-9c31-000200882798	5d2572ea-0601-401b-a2f3-d5f7efa59516	6.00000000
82ccc348-494f-4d3d-b4c2-0002037fb9c6	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	6.00000000
5cc1e3d1-24a8-4b8e-a26c-0002065aab28	b7241f2b-eef2-4ead-86ef-af4faf9bf4a8	11.00000000
[illegible]	[illegible]	[illegible]

Figure 17: MODALITY_GENUINE_SCORES table with initial test setup data from NIST BSSR1 biometric database.

MODALITIES_CONFIGURATION

This table includes the specific configurations for the modalities to be considered within a multimodal biometric system. For each MODALITIES_CONFIGURATION_ID, multiple modalities exist through the MODALITY_ID. This indicates for a particular multimodal biometric system with MODALITIES_CONFIGURATION_ID, the related modalities exist with the configured properties. In this sample provided below, a test system with MODALITIES_CONFIGURATION_ID *[e442f6fa-d689-4cef-bc6f-*

a8654e944016] includes two modalities with MODALITY_IDs *[1ccd8755-3566-4e11-8a70-9e6794687781]* and *[b7241f2b-eef2-4ead-86ef-af4faf9bf4a8]*. For both the modalities, parameters including the normalization scheme, normalization parameters, number of thresholds, minimum and maximum values for the threshold and the noise to be applied to the modalities are configured. Figure 18 contains a sample.

Table - dbo.MOD...S_CONFIGURATION Summary

MODALITIES_C...	MODALITY_ID	MODALITY_NO...	MODALITY_NO...	MODALITY_NO...	MODALITY_NU...	MODALITY_TH...	MODALITY_THR...	MODALITY_NOISE...
[illegible]	1ccd8755-3566-4e...	Min-Max Normali...	-1.000	0.898	10	0.898	-1.000	1.500
882b483e-2378-...	d13e9793-7ba9-48...	Min-Max Normali...	54.835	83.494	10	83.494	54.835	2.000
e442f6fa-d689-...	1ccd8755-3566-4e...	Min-Max Normali...	-1.000	0.898	10	0.898	-1.000	1.500
e442f6fa-d689-...	b7241f2b-eef2-4ea...	Min-Max Normali...	0.000	257.000	10	257.000	0.000	3.250
d985bd57-fa06-...	b7241f2b-eef2-4ea...	Min-Max Normali...	0.000	257.000	10	257.000	0.000	3.250
d985bd57-fa06-...	5d2572ea-0601-40...	Min-Max Normali...	0.000	246.000	10	246.000	0.000	4.000

Figure 18: MODALITIES_CONFIGURATION table as configured for the sample test environment consisting of three multimodal biometric systems, each with two modalities.

TEST_SETUP_MASTER

This table contains the configuration of individual test systems. The configuration elements are those that are applied to all modalities combined. These include partitioning schemes, fusion scheme, etc. The value of the FAR is used to compare the various test systems. Given below is the test setup for the three tests for which configuration has been provided in the previous section detailing MODALITIES_CONFIGURATION. Figure 19 contains the test setups.

Table - dbo.TEST_SETUP_MASTER Summary

TEST_SETUP_ID	MODALITIES_C...	SCORE_SCALE	TEST_PARTITI...	TEST_PARTITI...	TEST_PARTITI...	TEST_PARTITI...	TEST_FUSION_...	TEST_FAR_RATE
[illegible]	e442f6fa-d689-...	0.000	Leave One Out	NULL	NULL	NULL	Simple Product R...	0.100
bad95161-abcd-...	d985bd57-fa06-...	0.000	Leave One Out	NULL	NULL	NULL	Simple Product R...	0.100
51ba6a89-9de0-...	882b483e-2378-...	0.000	Leave One Out	NULL	NULL	NULL	Simple Product R...	0.100

Figure 19: TEST_SETUP_MASTER table outlining the configuration for test multimodal biometric systems with partitioning and fusion schemes.

Provided in the next section are the observed results from executing the implemented tool with the test environment discussed in the configuration tables.

6.1.1 Experiment Results

As outlined in section 5, the various components of the system were executed sequentially as per the defined process. The genuine and impostor values for each test configuration are retrieved from the database and after applying noise levels, passed to the MUBI analysis tool to generate the resulting graphs. The system performances are also captured in the database to present the user an overall comparison of the various configured multimodal systems. Included below, in screen shots, are the observed results.

ROC Curves without Fusion

Included in this section are the ROC curves for the genuine and impostor scores for the three test setups without fusion applied. The curves indicate the independent modalities with noise levels applied.

Given below in Figure 20, for the multimodal system [7f060644-f3e0-47f8-bf25-18f99844da8f], the right finger modality performs much better than the face C modality with a higher GAR value against the FAR value range. In this case, the noise factor applied to the right finger modality is 3.250% while a noise factor of 1.5% is applied to the face C modality. Despite of a smaller noise factor, the facial modality performs worse than the right finger modality as provided through the matching scores in the NIST BSSR1 database.

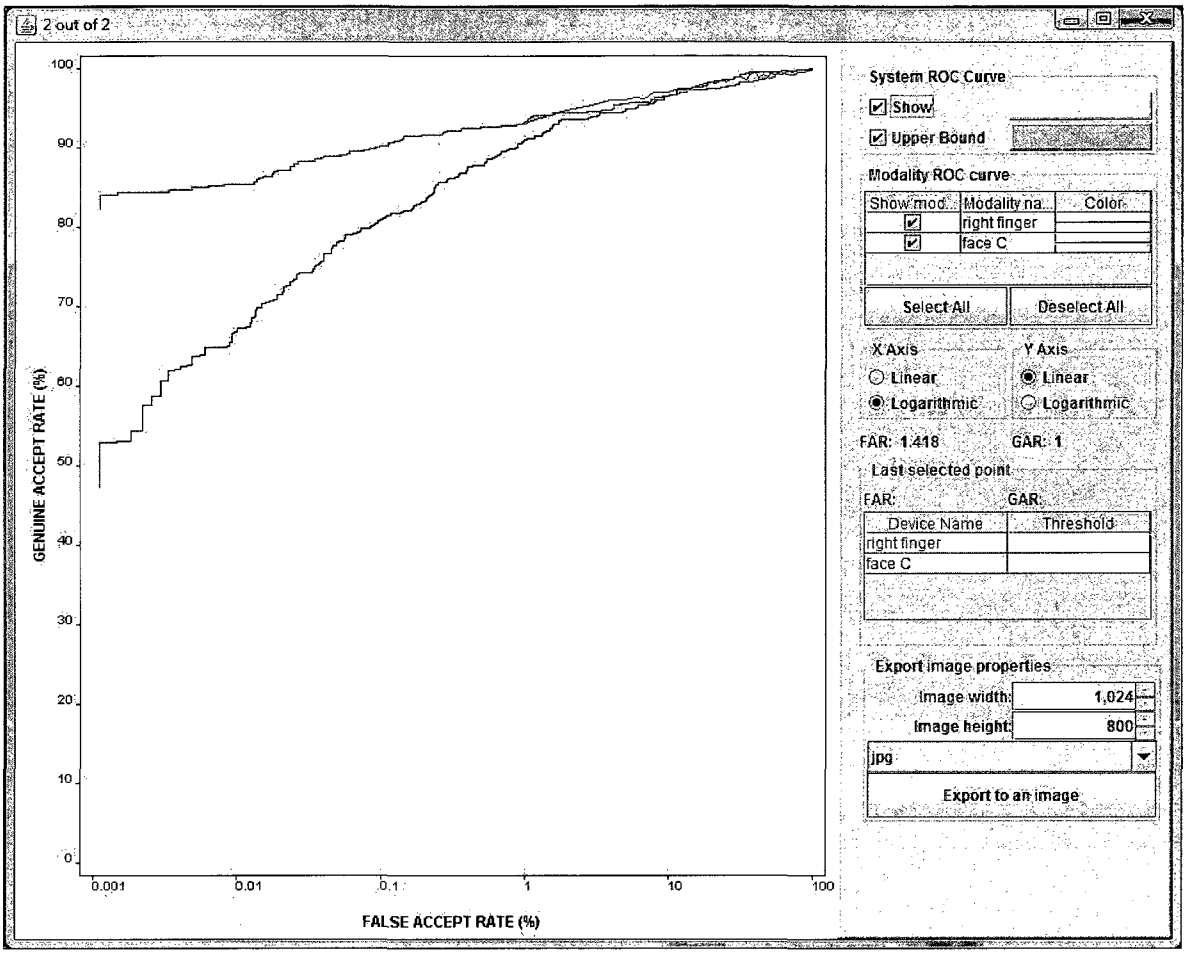


Figure 20: ROC curves, without fusion, for multimodal system ID [7f060644-f3e0-47f8-bf25-18f99844da8f]

In Figure 21, the multimodal system [bad95161-abcd-4859-a02c-c12e0a98e374] is considered with modalities left finger and right finger. The right finger modality is shown to perform better with a higher GAR value than the left finger. The noise factors applied to the genuine and impostor scores for the modalities left and right finger modalities are 4.0% and 3.25% respectively.

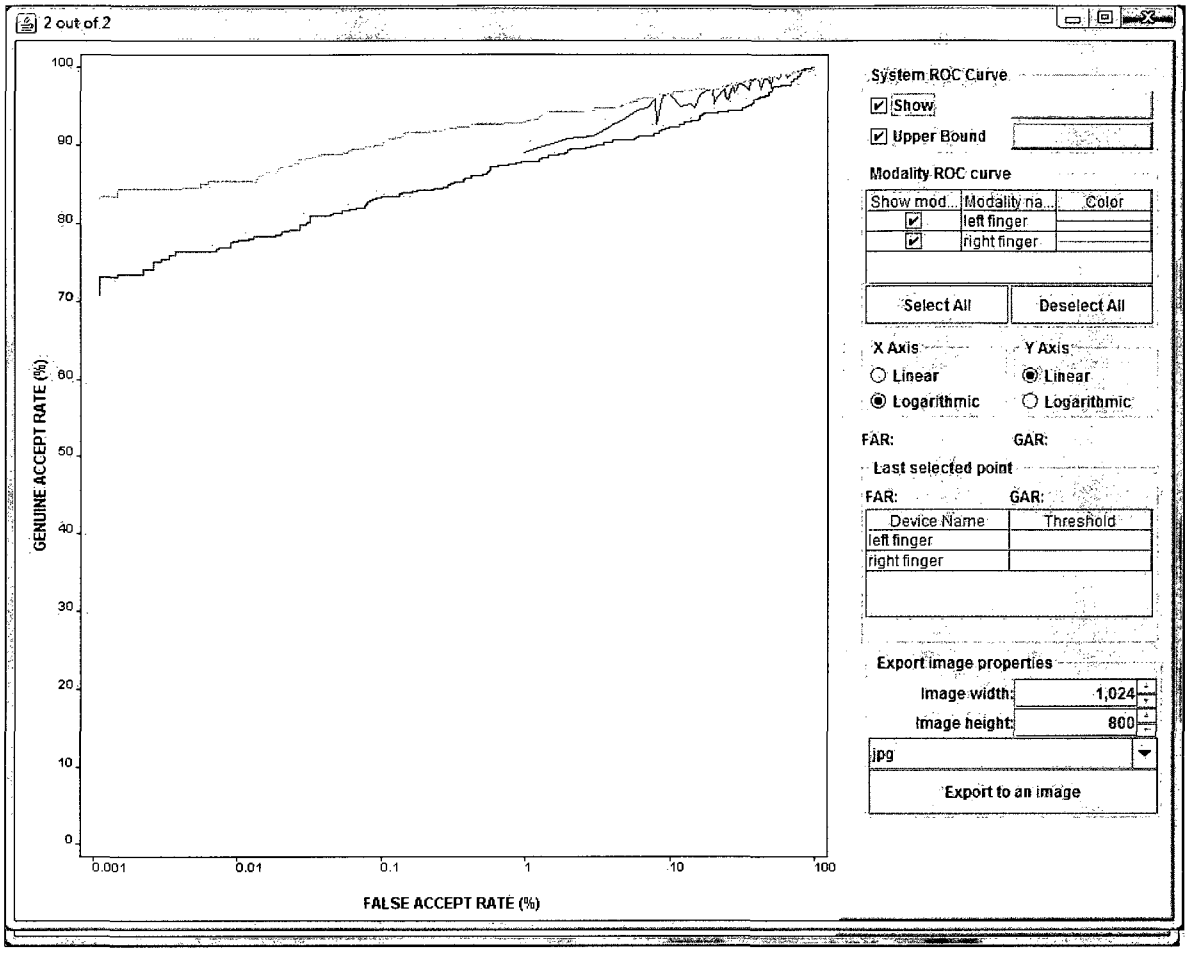


Figure 21: ROC curves, without fusion, for multimodal system ID [bad95161-abcd-4859-a02c-c12e0a98e374]

Provided in Figure 22, are the ROC curves for the modalities considered in multimodal system [51ba6a89-9de0-4e13-afa3-c2d593ae0639]. The modalities include face G and face C unimodal biometric systems. A noise factor level of 1.5% and 2.0% is applied to the two modalities face G and face C respectively. As can be observed, for higher values of the FAR, the face C modality performs better, but the curves intersect at around FAR value of 0.5%, after which face G performs better.

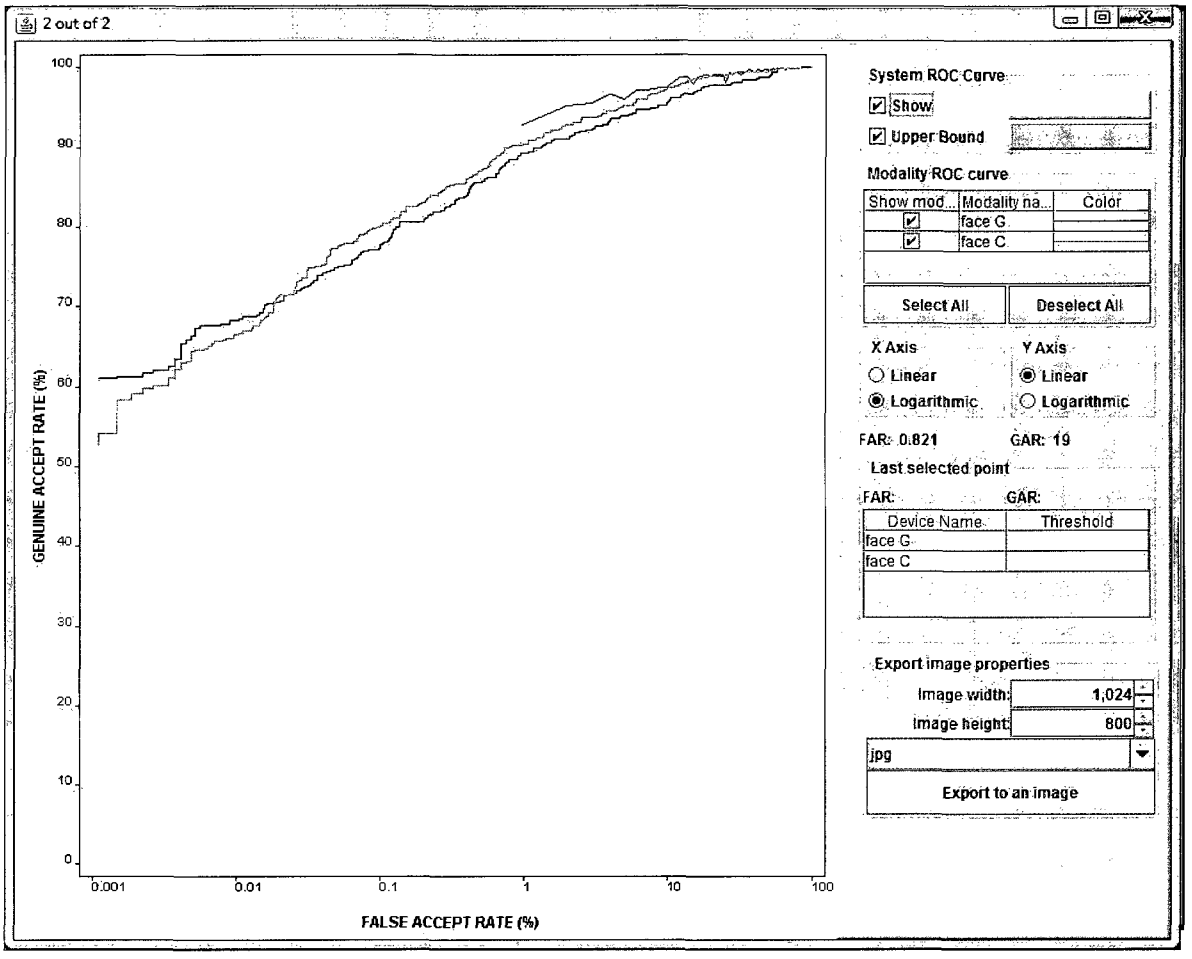


Figure 22: ROC curves, without fusion, for multimodal system ID [51ba6a89-9de0-4e13-afa3-c2d593ae0639]

ROC Curves with Fusion

In this section, the ROC curves of the different test systems have been included along with the curve reporting the fused performance as a multimodal system. As observed, the overall performance of the multimodal systems is better than the individual unimodal system. More details have been provided below.

Provided in Figure 23, are the ROC curves for the multimodal system [7f060644-f3e0-47f8-bf25-18f99844da8f]. The right finger and face C modalities included are first normalized using the Min-Max normalization at a scale of 1.0. The data is partitioned using the Leave One Out scheme. Simple product

rule fusion is applied. The fused result, indicated by the black curve is consistently better (in values of GAR against FAR) than the individual modality performances.

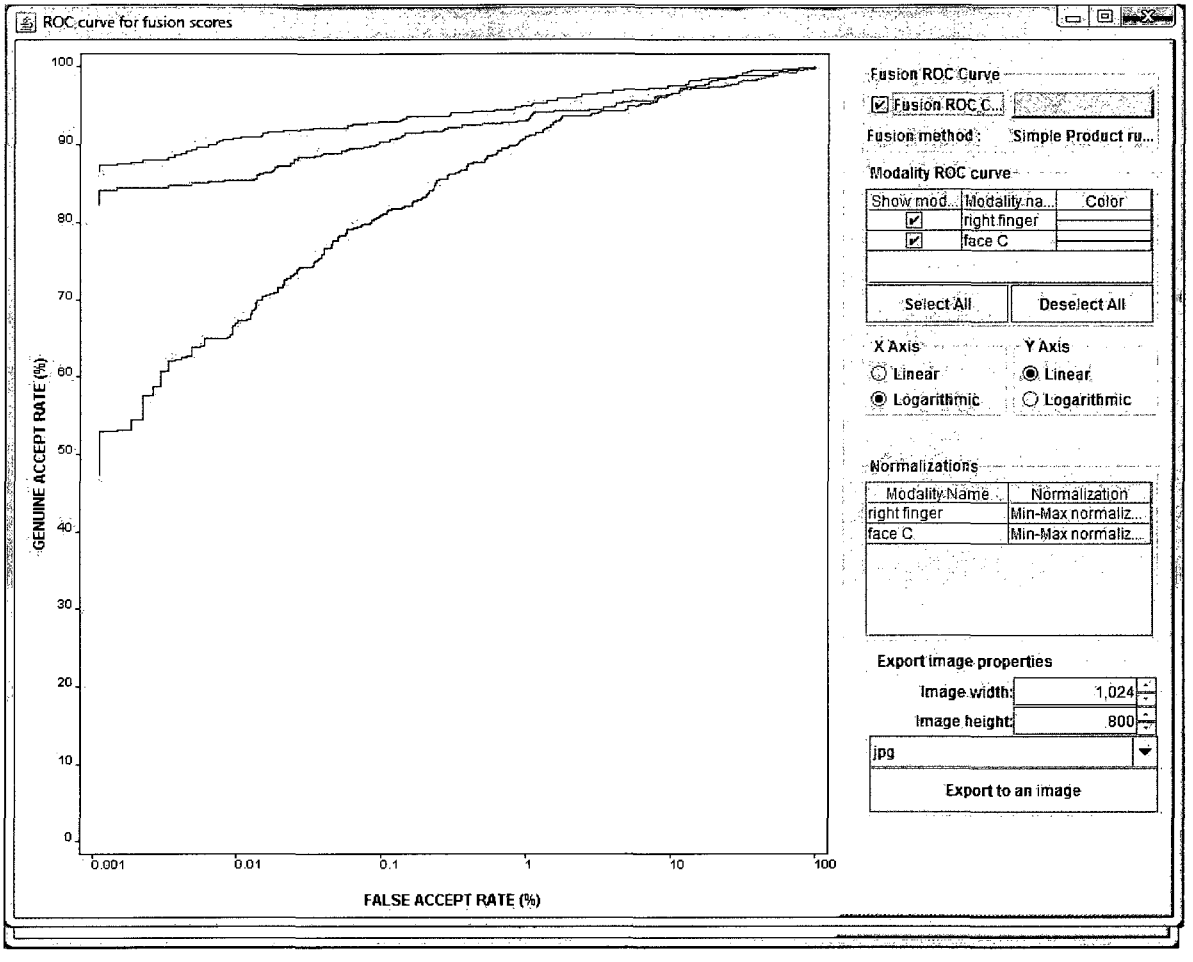


Figure 23: ROC curves, with fusion, for multimodal system ID [7f060644-f3e0-47f8-bf25-18f99844da8f]

In Figure 24, the performance results for the multimodal biometric system [bad95161-abcd-4859-a02c-c12e0a98e374] are captured which entails the modalities left and right fingers. The modalities are normalized using the Min-Max Normalization scheme with the score scale of 1.0. Leave One Out partitioning scheme has been employed along with the Simple Product rule based fusion methodology. Once again, the black curve representing the multimodal system performs better than the individual modalities.

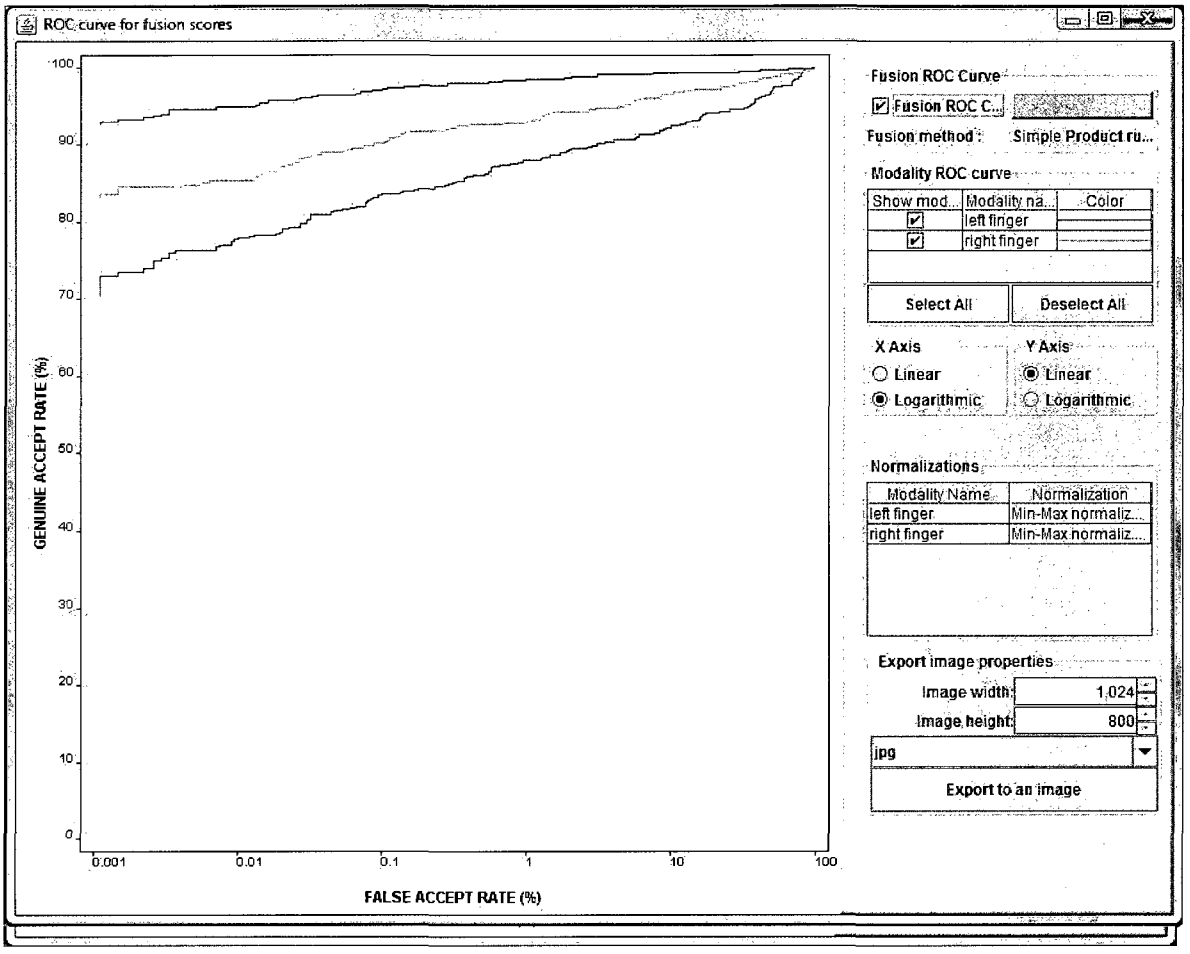


Figure 24: ROC curves, with fusion, for multimodal system ID [bad95161-abcd-4859-a02c-c12e0a98e374]

Figure 25 provides the ROC curves for the multimodal system [51ba6a89-9de0-4e13-afa3-c2d593ae0639] consisting of the individual modalities face G and face C. The reported noise factors have been applied along with Min-Max Normalization scheme at a scale of 1.0. The system then utilizes Leave One Out partitioning methodology and Simple Product Rule based fusion. The curve representing the multimodal system (black curve) is observed to perform consistently better than the unimodal systems.

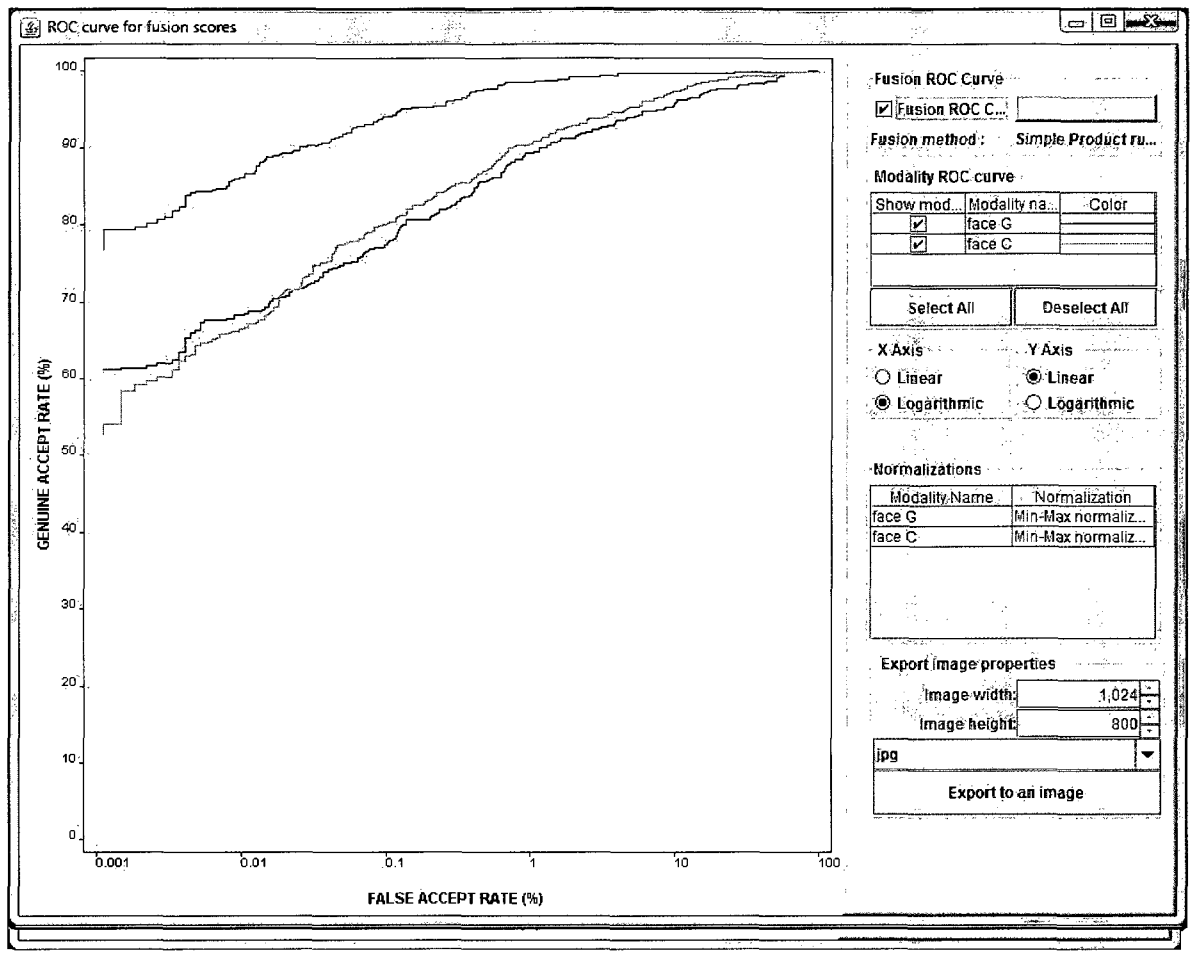


Figure 25: ROC curves, with fusion, for multimodal system ID [51ba6a89-9de0-4e13-afa3-c2d593ae0639]

Multimodal System Comparison

The implemented system captures all data relevant to the modalities and the test configurations after the matching scores from the database are processed through partitioning, normalization and fusion schemes. This allows the user to generate a graph identifying the performance of the various configured multimodal systems. The performance is captured as the GAR value against a configured FAR value. For the purpose of the reported experiments, all test configurations included a FAR value of 0.1%. The performance of the systems is reported at the closest approximate of the GAR value at the configured FAR value. Given in Figure 26, is a chart reporting the performance of the three test systems [7f060644-f3e0-47f8-bf25-18f99844da8f], [bad95161-abcd-4859-a02c-c12e0a98e374] and [51ba6a89-9de0-4e13-

afa3-c2d593ae0639]. As can be observed, the test system [bad95161-abcd-4859-a02c-c12e0a98e374] consisting of the right and left finger modalities performs better than the other two. The reported GAR value for this system is 96.905% at 0.1% FAR. The other two systems report a marginally lower value of GAR.

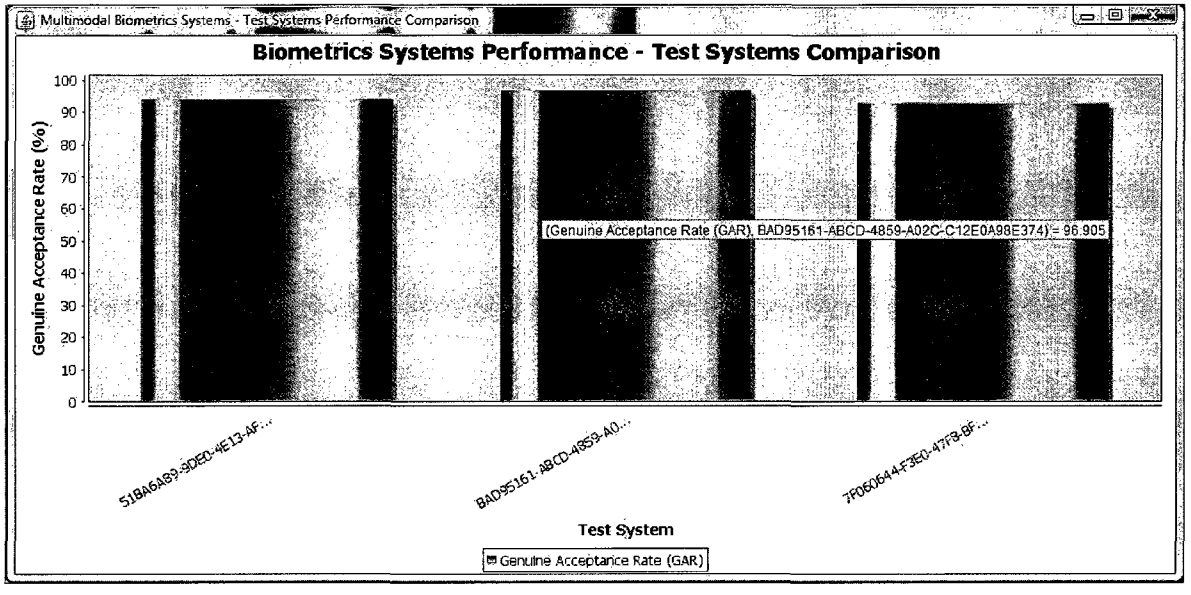


Figure 26: Comparison of test multimodal systems using the GAR value against the FAR value of 0.1%.

6.2 Experiments Setup – Comparative Analysis

In this section, a test setup to mimic some multimodal biometric systems has been designed. The experiments conducted in (Gan, 2007) have been given on the next page in Table 14. The multimodal systems corresponding to the provided values (highlighted in green) have been used to create the test cases. As per the evaluation matrix, the values for each test configuration are:

Test system 1

Biometric modalities with noise levels: face C (10%), face G (5%), left finger (1%), and right finger (10%)

Partitioning method: Re-substitution partitioning

Normalization method: Min-Max normalization scheme

Fusion method: Simple sum fusion

				1	2	3	4	5	6	7	8	9	No.	S/N Ratio
				1	1	1	2	2	2	3	3	3	a	
				1	2	3	1	2	3	1	2	3	b	
				1	2	3	2	3	1	3	1	2	c	
No.	A	B	C	1	2	3	3	1	2	2	3	1	d/Mean	
1	1	1	1	**99.424**	**99.135**	**99.28**	**99.247**	**99.28**	**99.247**	**99.28**	**99.548**	**99.28**	**99.302**	**39.939**
2	1	2	2	95.101	94.236	92.807	93.524	92.939	94.428	93.516	94.277	93.948	93.864	39.449
3	1	3	3	84.15	84.582	82.709	84.036	84.006	84.639	84.15	82.229	83.573	83.786	38.462
4	1	4	4	97.983	99.28	99.135	98.795	96.974	96.235	98.847	97.44	95.101	97.754	39.800
5	2	1	2	97.152	97.152	97.152	97.152	98.101	98.101	98.101	92.247	97.152	96.923	39.724
6	2	2	3	88.449	89.399	91.297	84.494	87.5	90.348	86.551	81.646	85.443	87.236	38.799
7	2	3	4	99.051	99.051	99.051	95.253	98.101	99.051	99.051	95.253	99.051	98.101	39.830
8	2	5	1	99.842	98.101	99.051	98.101	98.101	99.842	97.152	98.101	99.051	98.594	39.876
9	3	1	3	86.167	85.443	84.652	84.652	86.551	84.968	86.709	83.386	86.551	85.453	38.633
10	3	2	4	78.481	76.741	71.994	78.165	77.215	71.519	79.114	76.108	71.044	75.598	37.549
11	3	4	1	99.367	99.525	98.892	98.576	99.367	99.367	99.367	99.367	98.892	99.191	39.929
12	3	5	2	99.051	98.559	98.271	98.271	98.559	98.703	98.559	98.559	97.983	98.502	39.869
13	1	*	5	98.559	99.135	98.559	98.795	98.271	98.795	98.559	98.494	99.28	98.716	39.888
14	2	*	5	98.101	99.841	98.101	99.051	99.842	99.051	99.842	98.101	97.152	98.787	39.893

Table 13: Test setups in (Gan, 2007). The configurations marked have been used for experiments in this paper.

Test system 2

Biometric modalities with noise levels: face C (1%), face G (10%), left finger (10%), and right finger (10%)

Partitioning method: Hold-out partitioning

Normalization method: Min-Max normalization scheme

Fusion method: Simple product fusion

Test system 3

Biometric modalities with noise levels: face C (1%), face G (5%), left finger (5%), and right finger (5%)

Partitioning method: Leave one out partitioning

Normalization method: Min-Max normalization scheme

Fusion method: Simple minimum fusion

Test system 4

Biometric modalities with noise levels: face C (5%), face G (10%), left finger (1%), and right finger (5%)

Partitioning method: Leave one out partitioning

Normalization method: Decimal scaling normalization scheme

Fusion method: Simple maximum fusion

The four test system configurations presented above have been randomly selected across the range of the GAR values achieved in experiments conducted in (Gan, 2007). Similar to the application database configurations presented in section 6.1, the test systems were configured as independent multimodal biometric systems. Given in the following section are the results for each of the configured multimodal systems along with a comparison with earlier experiments carried out in (Gan, 2007).

6.2.1 Experiment Results

The results for performance evaluation of the multimodal biometric systems created in the implemented application based on the test setups discussed in the previous section have been reported here. Included is a review of the ROC curves generated for each multimodal system without applying

fusion to them, followed by ROC curves generated for each multimodal system with the application of fusion algorithms.

ROC Curves without Fusion

Provided in this section are the results of utilizing the developed system prior to applying the configured fusion methods. Figures 27, 28, 29 and 30 provide the results of evaluating the test setups 1, 2, 3 and 4, respectively. For all noise variations, in general, the finger modalities outperform the face modalities. The results are consistent with previous work in (Gan, 2007), however, the values of the measurable units GAR and FAR are observed to be slightly different.

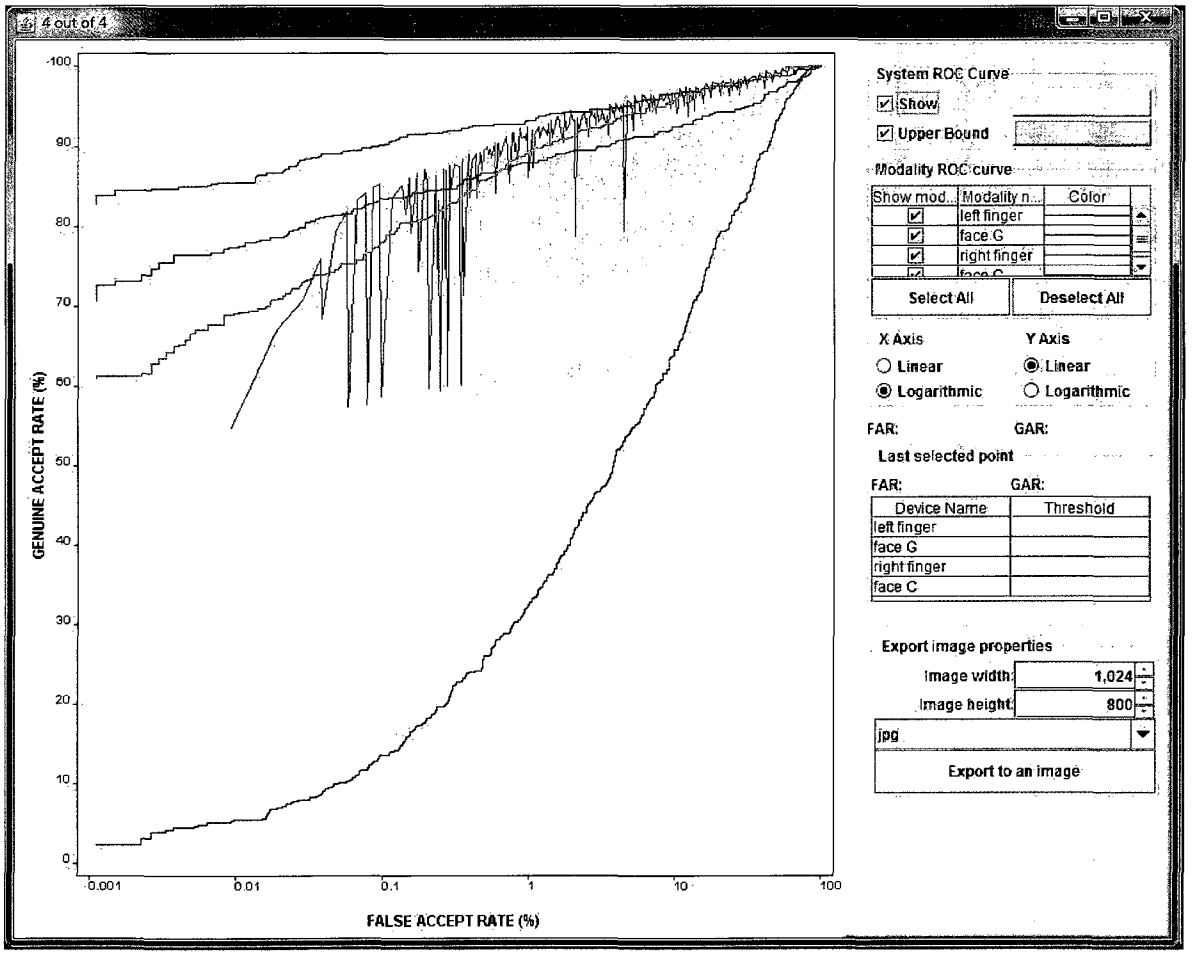


Figure 27: ROC curve, without fusion, for Test setup 1.

The above graph provides the ROC curve for Test setup 1 consisting of all modalities provided in the NIST BSSR 1 database. The setup includes the applied noise levels, partitioning scheme and normalization scheme.

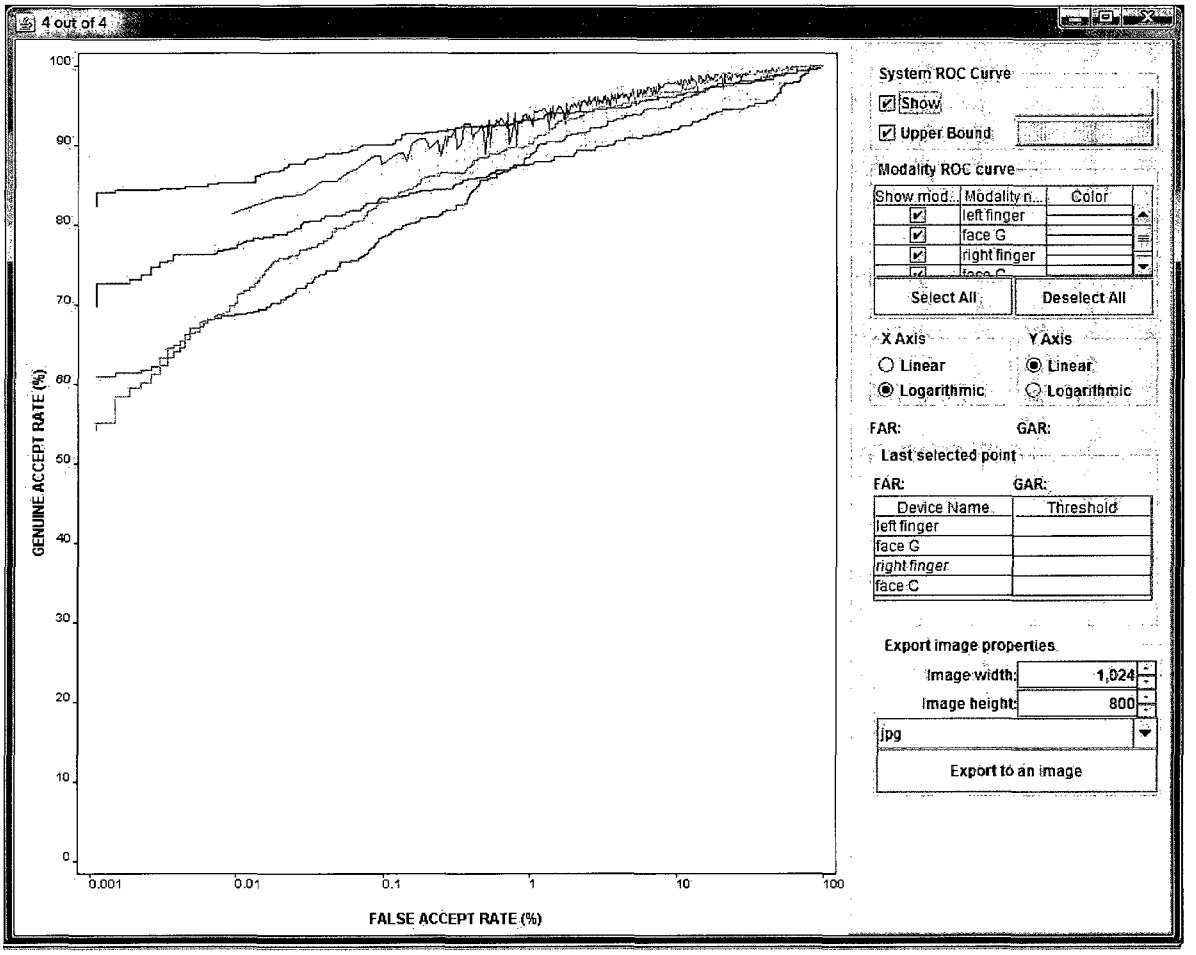


Figure 28: ROC curve, without fusion, for Test setup 2.

The above graph provides the ROC curve for all NIST BSSR1 modalities with noise deviations, partitioning scheme and normalization schemes applied. The matching scores in the above graph have not been fused for this result.

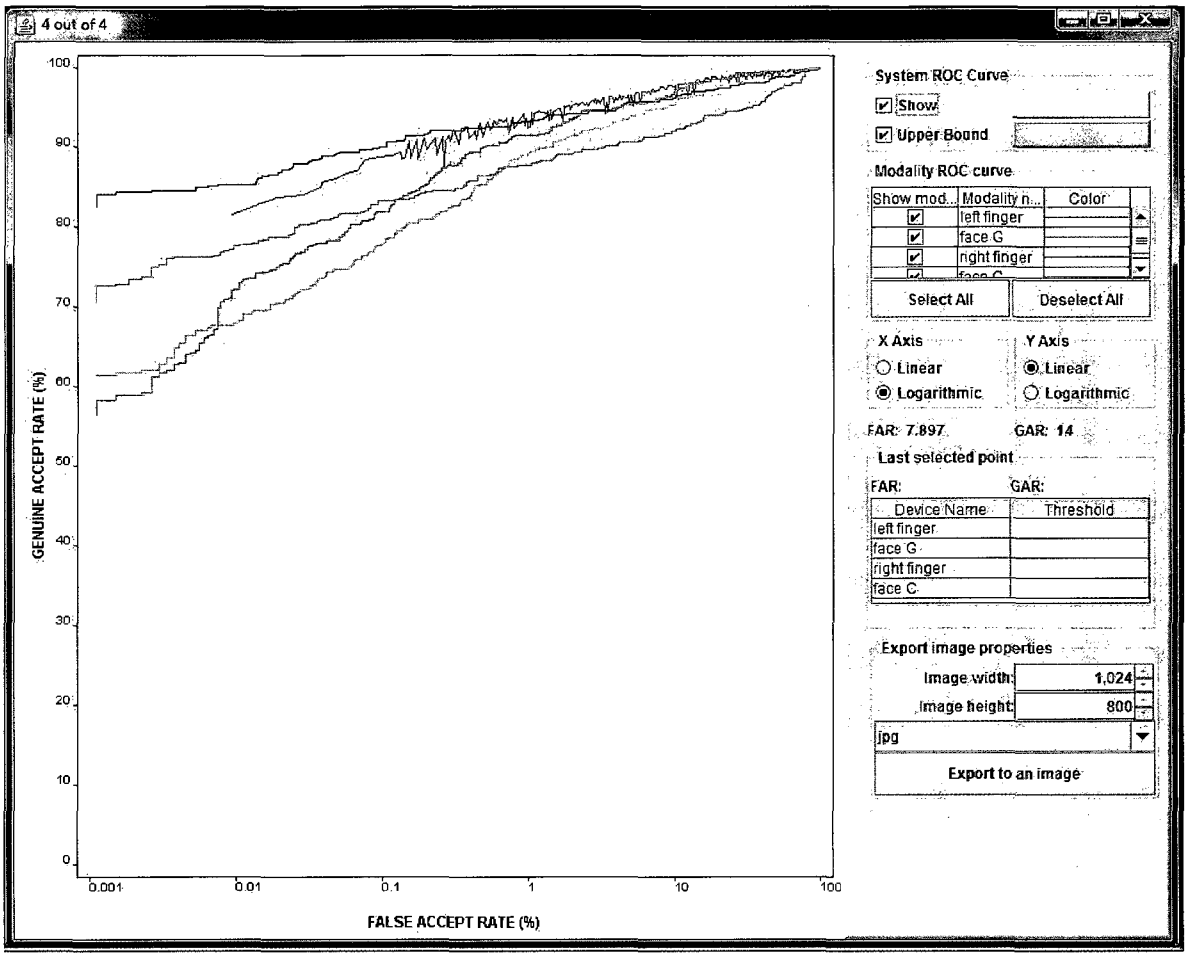


Figure 29: ROC curve, without fusion, for Test setup 3.

The above graph identifies the results in the ROC curve for Test setup 3. The normalization scheme, partitioning scheme and noise deviation levels have been applied for the results. No fusion method has been utilized for these results.

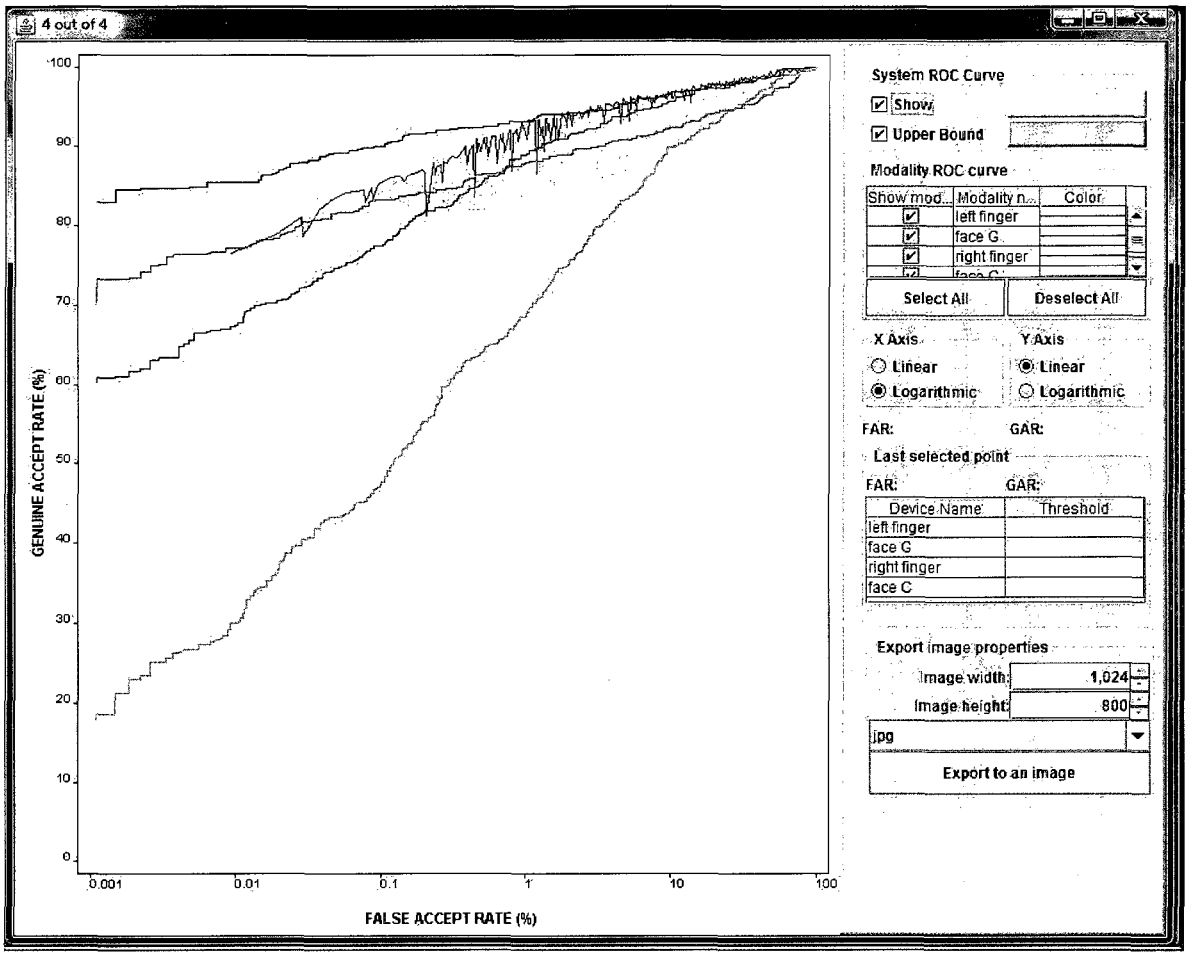


Figure 30: ROC curve, without fusion, for Test setup 4.

The above graph identifies the results for Test setup 4 without the application of a fusion method. All modalities of the NIST BSSR1 database have been used along with the configured noise deviation levels, partitioning scheme and normalization scheme.

ROC Curves with Fusion

The results provided in this section include graphs retrieved from the implemented application identifying the performance of the configured multimodal biometric test systems after having applied the fusion methods. The black curve identifies the fused performance of the systems combining

performance of all individual modalities. The following Figures 31, 32, 33 and 34 provide the ROC curves for the biometric systems after the application of the fusion method.

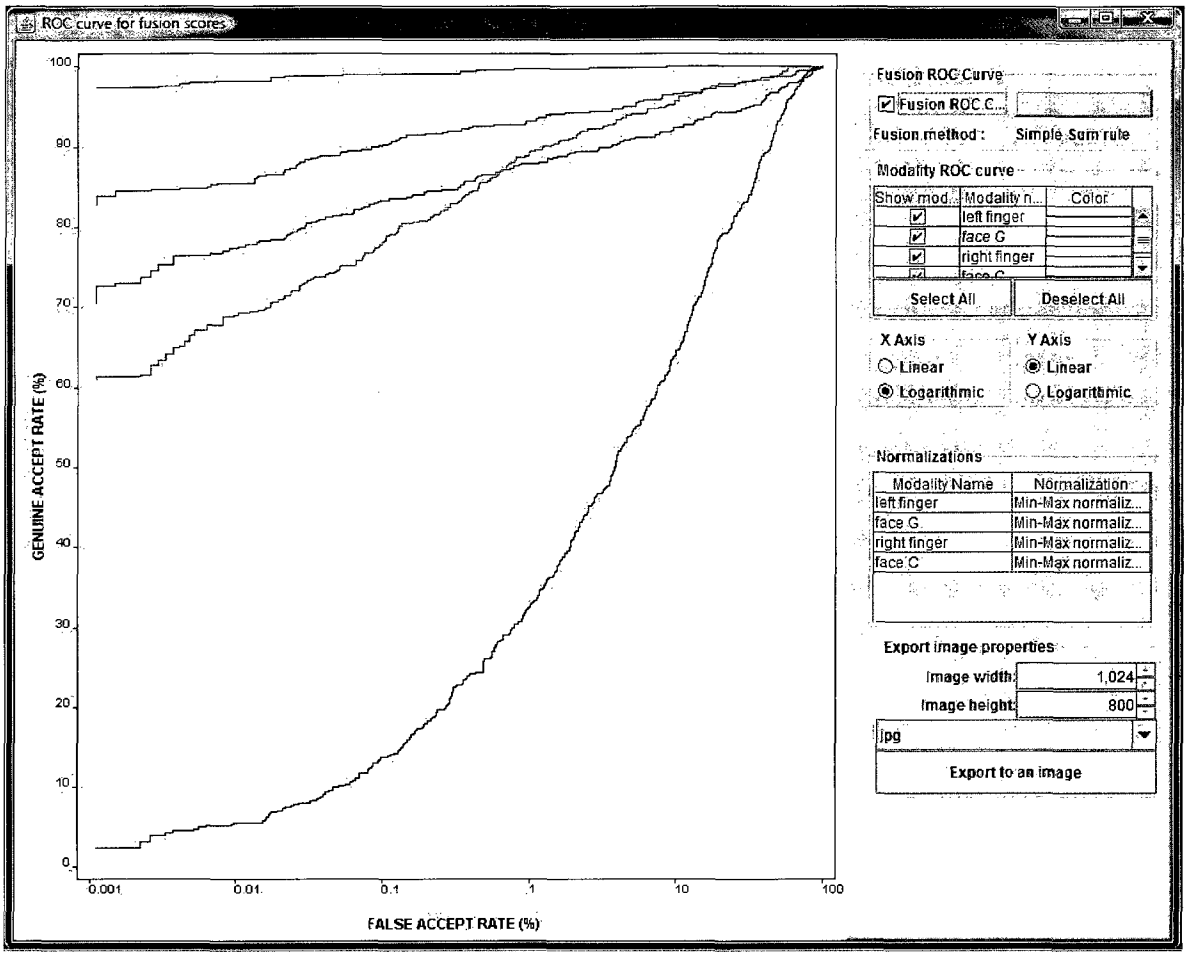


Figure 31: ROC curve, with fusion, for Test setup 1. Utilizes Simple Sum rule based fusion.

The above graph indicates through the black curve, the performance of the multimodal system configured through Test setup 1. The multimodal system performs better consistently for all values of the FAR in comparison with the individual modalities. The GAR value for FAR = 0.1% is observed to be slightly lower in comparison with the experiments carried out in (Gan, 2007). This can be attributed to the precision in the matching scores. The implemented solution retrieves true values from the NIST BSSR1 database while previous work allowed for capturing lower precision values.

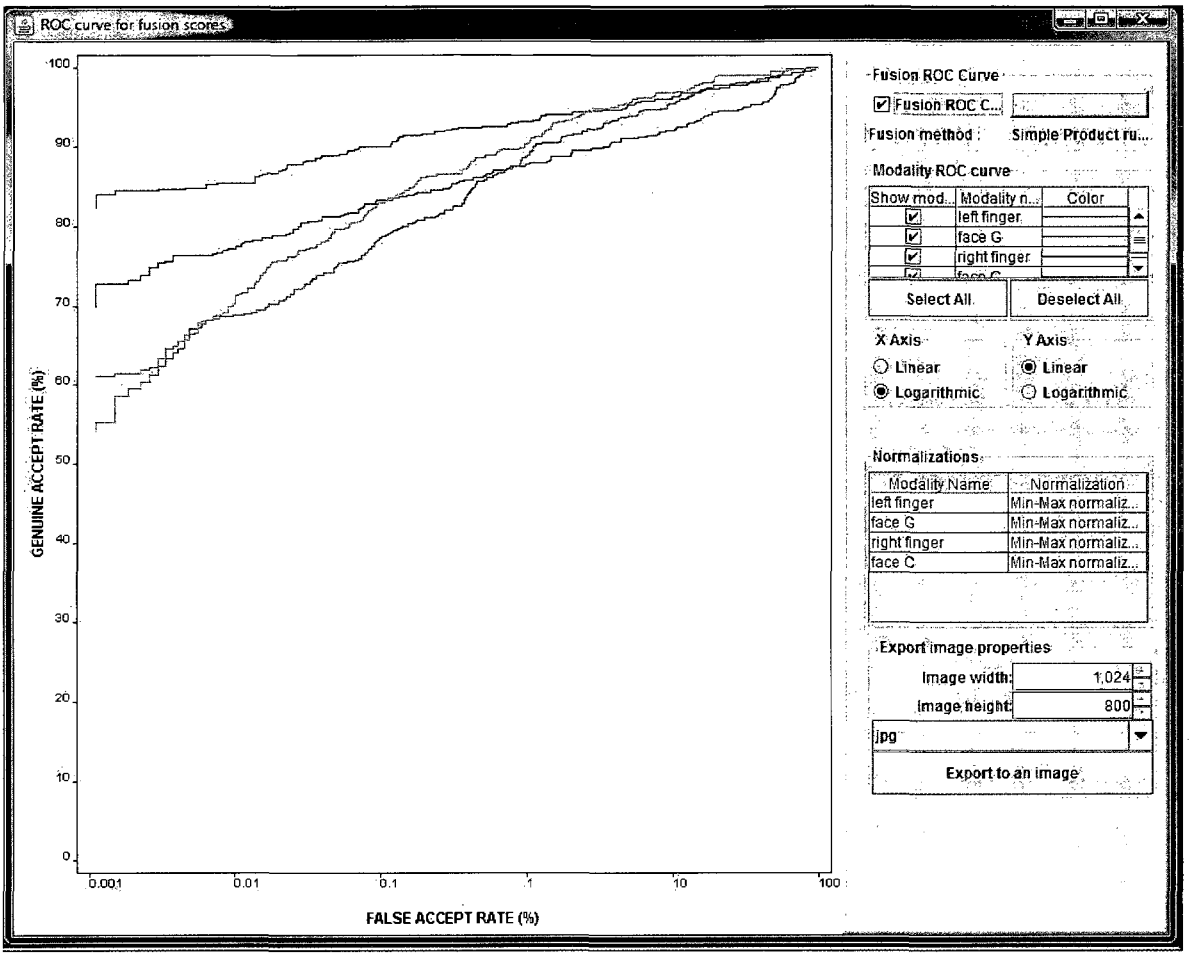


Figure 32: ROC curve, with fusion, for Test setup 2. Utilizes Simple Product rule based fusion.

The above graph provides the ROC curve for Test setup 2. Again, similar to Test setup 1, the multimodal system performs better than individual modalities.

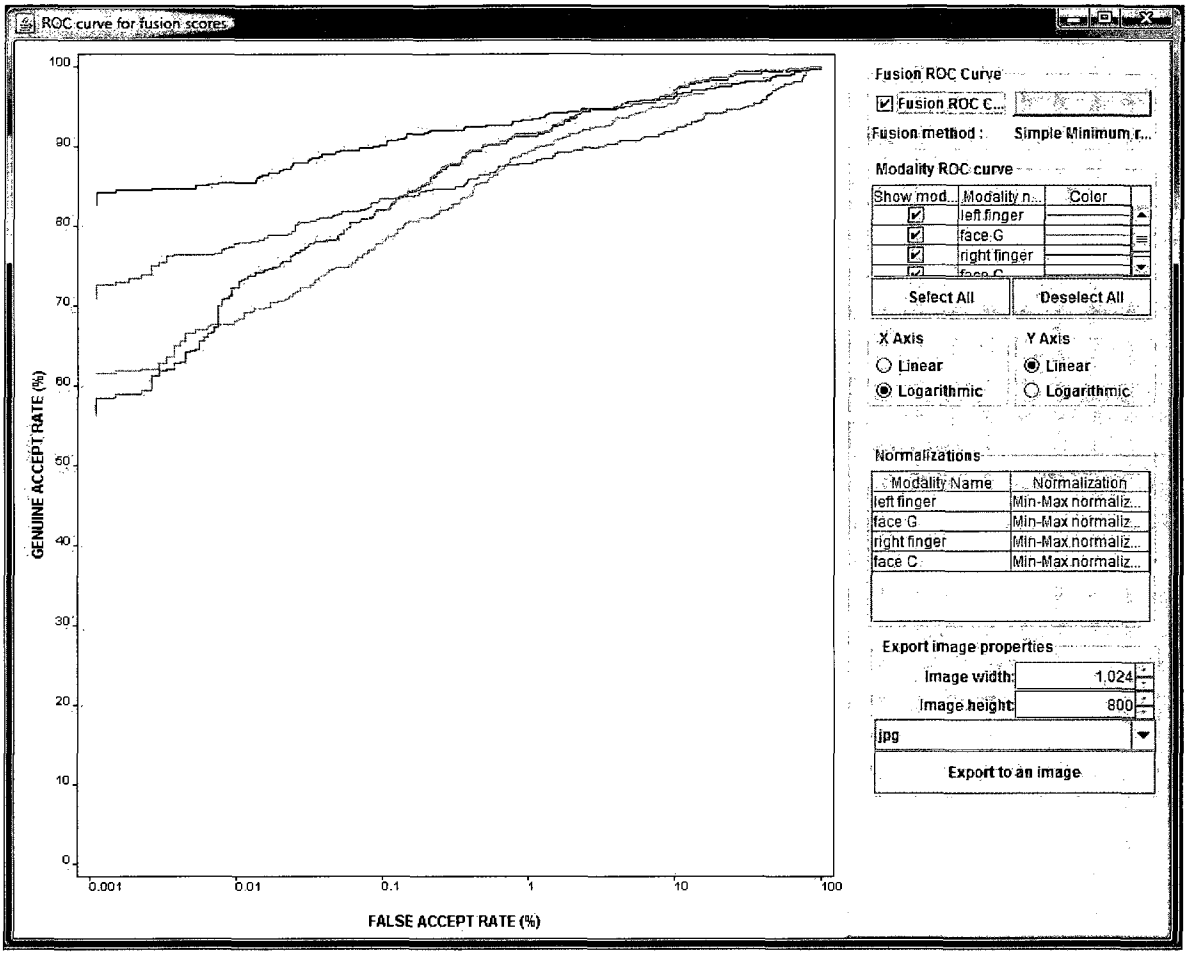


Figure 33: ROC curve, with fusion, for Test setup 3. Utilizes Simple Minimum rule based fusion.

The above graph identifies the ROC curve for the four modalities from NIST BSSR1 database and the combined multimodal system (black curve). The multimodal system performs better than individual modalities over the range of FAR values. This system, however, does not perform as well as the previous two tested systems.

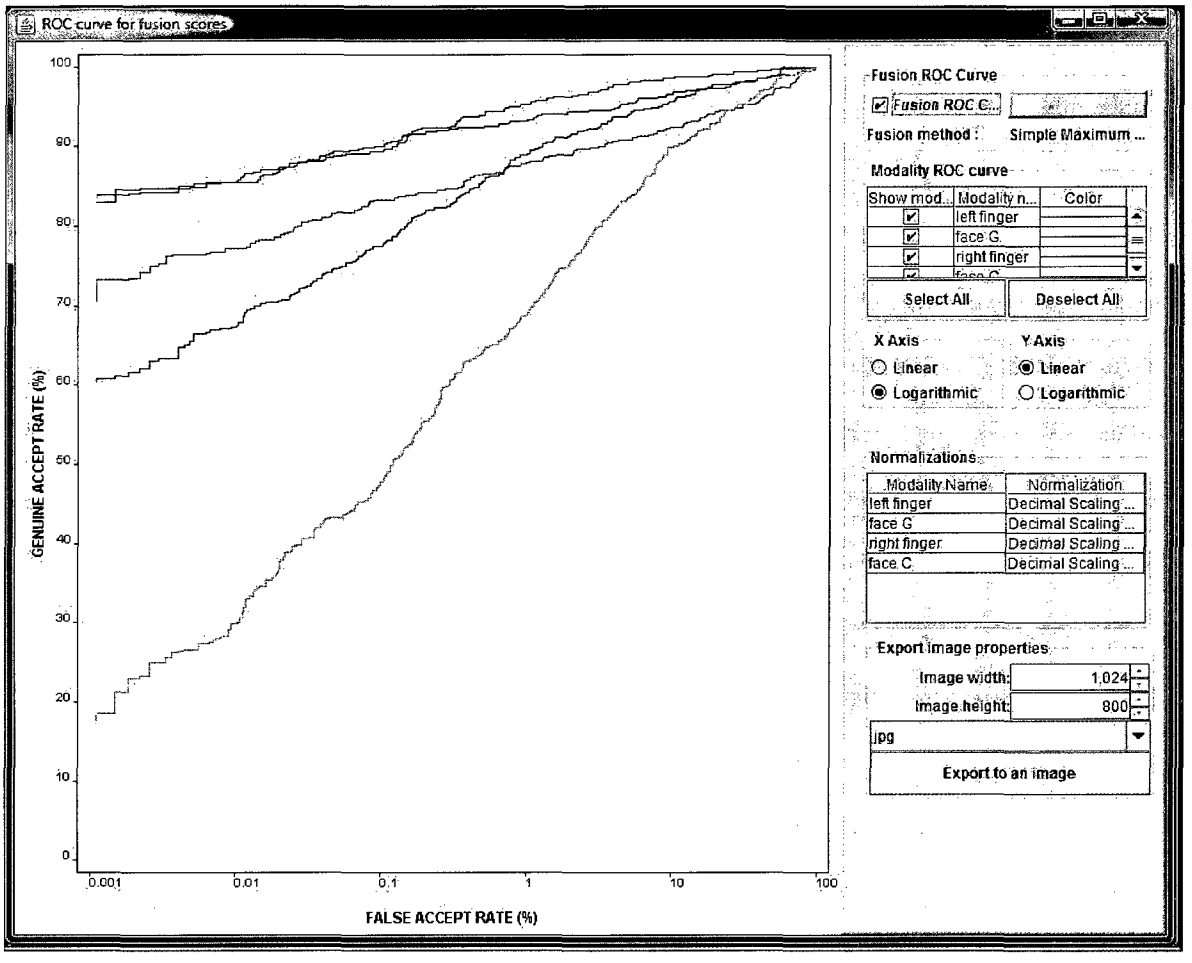


Figure 34: ROC curve, with fusion, for Test setup 4. Simple Maximum rule based fusion used.

The above graph indicates the performance of the multimodal system configured through Test setup 4. The graph identifies that the overall multimodal system utilizing Decimal Scaling normalization, Leave one out partitioning scheme and the Simple Maximum rule based fusion method does not perform as well as the other Test system setups. It can also be derived from the graph that over intervals of FAR values, the multimodal system performs worse than the right finger modality for the applied noise deviations.

Multimodal Systems' Comparison

Given below in Figure 35 is the chart comparing the performance of the four Test system setups configured in section 6.2. The Test setup 1 performs better than the rest with a GAR value of 99.033% for the configured FAR value of 0.1%. The performance of the remaining systems (between 79% and 88%) deteriorates consistently, with Test system 4 performing worse than an individual modality. The values observed for each test system are slightly different than those observed for the same setup in (Gan, 2007). This is potentially due to the difference in precision of decimal values in the system. This can also be attributed to the various parameters for normalization schemes, partitioning methods and fusion methods that the author of this paper did not have access to.

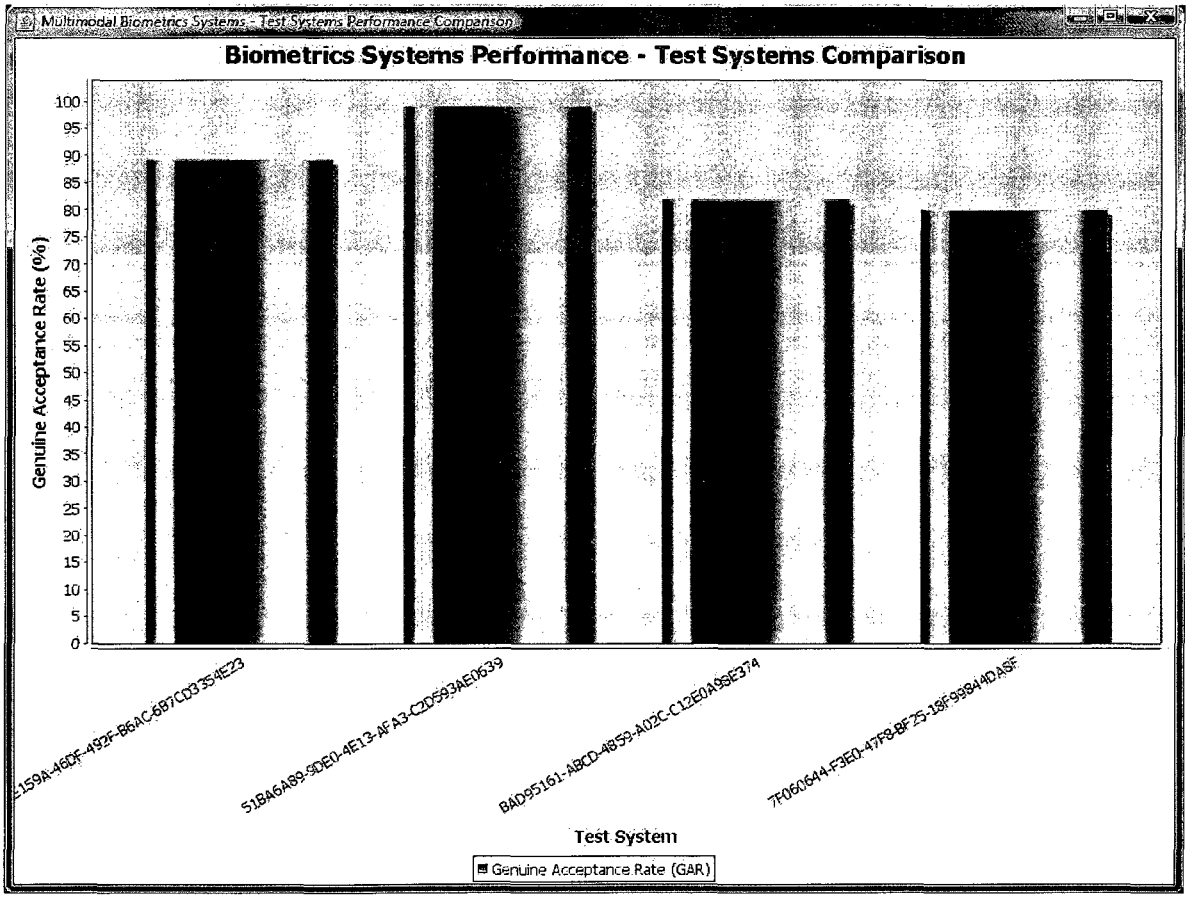


Figure 35: Comparison of the performance of multimodal systems configured in Test setups 1, 2, 3 and 4.

Further analysis of the results and the conclusions drawn from the same has been covered in the next section. The next section also discusses directions for future work based on the limitations of the implemented approach and the potential for improvements in the same.

Chapter 7. Conclusion

The underlying research and the developed application enhance our ability to systematically evaluate the performance of multimodal biometric systems. The thesis has identified some of the shortcomings in existing methods in their efficiency, effectiveness and the ease of use. The resulting application that has been developed by combining the theoretical framework provided in previous research and existing applications demonstrates a viable solution to conduct more evolved experiments. Given in the next sub section are the contributions of this research followed by a section identifying potential enhancements for the future.

7.1 Contributions

As indicated in the problem statement covered in section 3.4, existing work in the field of performance evaluation of multimodal biometric systems suffers from the inability of a researcher to combine multiple biometric databases, retrieve results that are user friendly, or conduct a large number of experiments. The configurable system developed as part of this thesis provides enhancements and allows the users to create multimodal biometric systems by combining matching scores provided through various multimodal databases. It also allows the users to generate results in the forms of graphs and charts to easily analyze performance of the configured biometric systems. Other factors to be considered in evaluating performance including the partitioning scheme, the normalization scheme, the fusion methods and noise levels, are also configurable to allow users to conduct a larger number of experiments with more educated parameter values. As per design, the developed application is scalable to retrieve any multimodal databases added to it, for users to arbitrarily combine modalities and enhances the user's ability to generate and consider various multimodal biometric systems. As identified in (Gan, 2007) for future work, the system alleviates the shortcomings of limited factors that can be considered (within previous work). An internal database is utilized that enables users to combine multiple biometric databases (unimodal or multimodal), thus providing a larger dataset. This enhances previously conducted research. Enhanced reusability is also provided by capturing test system configurations and results in increased efficiency.

7.2 Future Work

Even though this thesis enhances the researchers' and commercial users' ability to evaluate biometric systems for their performance, it allows for future work to further enhance various aspects of the implementation. These have been listed below.

1. **Technical hurdles in using the application** – The application has been designed to be portable across all platforms. However, it is a single implementation based system. This requires for a high end system with sufficient memory to maintain millions of data records in memory and generate graphical results. A distributed system provided through services can allow this application to be used without physical access to the machine where it resides. It also can ensure more effective use of computing resources.
2. **Reporting abilities** – The application provides reports that are displayed to the users using the system locally. The graphs generated can be viewed on the host machine which may not be accessible by others. A web based interface that allows users to access the application and view results remotely will be an effective enhancement.
3. **Services based system** – The application is modular in nature but tightly coupled to execute on a single machine. This also makes it difficult for a more collaborative effort in evaluating performance of multimodal biometric systems. The same application implemented using a Service Oriented Architecture will allow researchers and other users from any physical location to submit biometric databases for consideration, configure modalities and test multimodal biometric systems.

Bibliography

A. Adler, R. Y. (2006). Towards A Measure of Biometric Information. *Proceedings of The Canadian Conference on Electrical and Computer Engineering*, (pp. 210 – 213).

A. K. Jain, A. R. (2004, January). An Introduction to Biometric Recognition. *IEEE Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1* , pp. 4 - 20.

A. Ross, A. J. (2001). Information Fusion in Biometrics. *Proceedings of the 3rd International conference on Audio- and Video-Based Biometric Person Authentication*, (pp. 354 - 359).

A. Ross, A. J. (2006). Levels Of Fusion in Biometrics. In A. J. A. Ross, *Handbook of Multibiometrics* (pp. 59 – 90).

A. Ross, A. J. (2004). Multimodal Biometrics: An Overview. *Proceedings of 12th European Signal Processing Conference*, (pp. 1221 – 1224).

A.K. Jain, A. R. (2006). Biometrics: A Tool for Information Security. *IEEE Transactions on Information Forensics and Security* , 125 – 143.

A.K. Jain, A. R. (2002). Learning User-Specific Parameters In A Multibiometric System. *Proceedings of The International Conference on Image Processing.*

A.K. Jain, P. F. (2007). Introduction to Biometrics. In P. F. A.K. Jain, *Handbook of Biometrics* (pp. 1 – 22).

Anil K. Jain, A. R. (2004). Multibiometric Systems. *Communications of the ACM, Vol. 47, No. 1* .

Bernadette Dorizzi, S. G.-S. (2006). Multimodality in Biosecure: Evaluation on Real vs. Virtual Subjects. *Proceedings of The ICASSP 2006*, (pp. 1089 - 1092).

Biometrics. (2008, 04 12). Retrieved 04 12, 2008, from Wikipedia Website: http://en.wikipedia.org/wiki/Biometrics

Biometrics FAQ. (2008, 04 10). Retrieved 04 10, 2008, from Bromba Biometrics: http://www.bromba.com/faq/biofaqe.htm

(2006). *Biometrics Testing and Statistics*. National Science and Technology Council.

Brad Ulery, A. H. (2006). *Studies of Biometric Fusion.* National Iinstitute Of Standards And Technology.

Chang Shu, X. D. (2006). Multi-Biometrics Fusion for Identity Verification. *Proceedings of The 18th International Conference on Pattern Recognition (ICPR'06).*

Faundez-Zanuy, M. (2005). Data Fusion in Biometrics. *IEEE Aerospace and Electronic Systems Magazine* , pp. 34 – 38.

Flynn, P. (2008). Biometrics databases. In A. K. Jain, *Handbook of Biometrics* (pp. 529 – 548).

Gan, W. (2007). A Statistical Approach towards Performance Analysis of Multimodal Biometrics Systems. *Master's Thesis, University of Windsor.*

J. Ortega-Garcia, J. B.-R. (2004). Authentication Gets Personal with Biometrics. *IEEE Signal Processing Magazine* , pp. 50 - 62.

Jain, A. (2004). Biometric Recognition: How Do I Know Who You Are? *Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference, 2004*, (pp. 3 - 5).

K. Delac, M. G. (2004). A Survey of Biometric Recognition Methods. *Electronics in Marine, 2004, Proceedings Elmar 2004. 46th International Symposium*, (pp. 184 – 193).

K. Nandakumar, A. J. (2008). *Score Normalization in Multimodal Biometric Systems.* Michigan State University and West Virginia University, http://biometrics.cse.mse.edu.

K. Toh, W. Y. (2004). Fusion of Auxiliary Information for Multi-modal Biometrics Authentication. *Lecture Notes in Computer Science, Biometric Authentication, Vol. 3072/2004* , pp. 678 – 685.

Ko, T. (2005). Multimodal Biometric Identification for Larger User Population Using Fingerprint, Face and Iris Recognition. *Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop.*

Lin Hong, A. J. (1999). Can Multibiometrics Improve Performance? *Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies.*

M. Gamassi, M. L. (2005). Quality Assessment of Biometric Systems: A Comprehensive Perspective Based on Accuracy and Performance Measurement. *IEEE Transactions on Instrumentation and Measurement, Vol. 54, No. 4* , pp. 1489 – 1496.

M. Indovina, U. U. (2003). Multimodal Biometric Authentication Methods: A COTS Approach. *Proceedings of Multimodal User Authentication Workshop*, (pp. 99 - 106).

Multimodal Biometrics - Is Two Better Than One? (2008, 04 10). Retrieved 04 10, 2008, from Biometrics Resource - findBiometrics.com: http://www.findbiometrics.com/Pages/multimodality.htm

Nandakumar, K. (2005). Integration of Multiple Cues in Biometric Systems. *Master's Thesis, Michigan State University.*

P. Jonathon Phillips, W. T. (2007). *FRVT 2006 and ICE 2006 Large-Scale Results.* National Institute of Standards and Technology.

P.J. Phillips, A. M. (2000). An Introduction to Evaluating Biometric Systems. *IEEE Computer, Vol. 33* , pp. 56 - 63.

Phillips, P. J. (2004). Multi-biometrics, Deja-Vu? *Proceedings of The Biometric Consortium Conference.*

R. Krishnan, S. K. (2007). Combinatorial Testing: Learnings from our Experience. *ACM SIGSOFT Software Engineering Notes, Vol. 32, No. 3* , pp. 1 – 8.

R. Snelick, M. I. (2003). Multimodal Biometrics: Issues in Design and Testing. *Proceedings of the 5th International Conference on Multimodal Interfaces*, (pp. 68 - 72).

R. Snelick, U. U. (2005). Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems. *IEEE Transactions on Pattern Analysis and Machine Inteliigence, Vol. 27, No. 3* .

R. Zewail, A. E. (2004). Soft and Hard Biometrics Fusion for Improved Identity Verification. *Proceedings of The 47th IEEE International Midwest Symposium on Circuits and Systems, Vol. 1*, (pp. 225 – 228).

Ruud M. Bolle, S. P. (2000). Evaluation Techniques for Biometrics-based Authentication Systems (FRR). *Proceedings of 15th International Conference on Pattern Recognition (ICPR).*

S. Ribaric, I. F. (2006). Experimental Evaluation of Matching-Score Normalization Techniques on Different Multimodal Biometric Systems. *Proceedings of The IEEE Mediterranean Electrotechnical Conference*, (pp. 498 – 501).

S.C. Dass, Y. Z. (2006). Validating a Biometric Authentication System: Sample Size Requirements. *IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 28, No. 12* , pp. 1902 – 1913.

S.K. Dahel, Q. X. (2003). Accuracy Performance Analysis of Multimodal Biometrics. *Proceedings of the 2003 IEEE Workshop on Man and Cybernetics Society Information Assurance*, (pp. 170 - 173).

Samoska, N. (2006). Evaluation and Performance Prediction of Multimodal Biometric Systems. *Master's Thesis, West Virginia University.*

Sedgwick, N. (2003). *The Need for Standardisation of Multi-Modal Biometric Combination.* Cambridge Algorithmica Limited.

Sinjini Mitra, M. S. (2007). Statistical Performance Evaluation of Biometric Authentication Systems using Random Effects Models. *IEEE Transactions on Pattern Analysis and Machine Intelligence, Volume 29 , Issue 4* , pp. 517 - 530.

The Biometric Consortium. (2008, 02 04). Retrieved 02 04, 2008, from The Biometric Consortium: http://www.biometrics.org/

Thieme, M. (2003). Multimodal Biometric Systems: Applications and Usage Scenarios. *Proceedings of The Biometric Consortium Conference.*

Wayman, J. (2006). A Path Forward for Multi-biometrics. *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Vol. 5*, (pp. 1069 – 1072).

Vita Auctoris

Gaurav Kumar was born in Haridwar, India, October 9th, 1981. He completed high school at Suraj Bhan D.A.V. Public School in New Delhi, India in 1999. After high school he completed the Bachelor of Computer Science (Honors) degree from the University of Windsor, Ontario with a minor in Business Administration in Winter 2004. He is currently a candidate for Master's degree in Computer Science at the University of Windsor, Ontario and hopes to graduate in Winter 2009 with focus in Software Engineering.