



A Framework for Improving Accuracy of Multimodal Biometrics Security Based on Bayesian Network

By

Emmanuel Eric Morwaagole

Reg. No: 14100377

Bachelor of Sciences Honors (Computer Security) (Staffordshire University, UK)

College of Science,
Department of Computer Science and Information Systems,
Botswana International University of Science and Technology
emmanuel.morwaagole@studentmail.biust.ac.bw

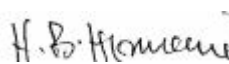
Phone No: (+267)72503925

A Thesis Submitted to the College of Science in Partial Fulfillment of the Requirements for the
Award of the Degree of Master of Science in Computer Science
of BIUST

Supervisor(s) Hlomani Hlomani, PhD
Department of Computer Science and
Information Systems
College Of Science, BIUST

Dimane Mpoeleng, PhD
Department of Computer Science and
Information Systems
College Of Science, BIUST

hlomanihb@biust.ac.bw
Tel: +267 4931107

Signature: 
Date: 04/10/2018

mpoelengd@biust.ac.bw
Tel: +267 4931112

Signature: 
Date: 04/10/2018

September 2018

Declaration and Copyright

I **Emmanuel Eric Morwaagole**, hereby declare that this is my original work and it has never been published or submitted elsewhere for the requirement of a master's degree program.

A handwritten signature in dark ink, appearing to read 'Emmanuel Eric Morwaagole', is written on a light gray rectangular background.

Emmanuel Eric Morwaagole

Date: 26/09/2018

This thesis is copyright material protected under the Berne Convention, the Copyright Act of 1999 and other international and national enactments, in that behalf, on intellectual property. It must not be reproduced by any means, in full or in part, except for short extracts in fair dealing; for researcher private study, critical scholarly review or discourse with an acknowledgement, without the written permission of the office of the Provost, on behalf of both the author and the Botswana International University of Science and Technology.

Certification

The undersigned certifies that he has read and hereby recommends for acceptance by the College of Science a thesis titled: **A Framework for Improving Accuracy of Multimodal Biometrics Security Based on Bayesian Network**, in fulfillment of the requirements for the degree of Master of Science (Computer Science) of the Botswana international University of Science and Technology.



.....
Hlomani Hlomani, PhD
(Supervisor)
Date..04/10/2018.....



.....
Dimane Mpoeleng, PhD
(Co-Supervisor)
Date..04/10/2018.....

Abstract

This thesis addresses the problem of biometrics security and accuracy through the fusion of fingerprint and face images. The Biometrics community in recent years came up with different approaches to improve the accuracy and security of systems. Multimodal authentication has attracted a lot of attention because of its advantage over single biometrics matchers. Even though efforts were made to improve these systems, they are, however, still vulnerable to security threats such as spoofing where a forged biometric copy and/or artificially recreated biometric data (which maybe legitimate) may be used to spoof the system. Multimodal biometric systems overcome various limitations of uni-modal biometric systems, such as non-universality, lower false acceptance, and higher genuine acceptance rates. We thus propose a framework, based on Bayesian Network, which is tailored to deal with the fusion of fingerprint and face. In our proposed framework, face and fingerprint data are fused at Feature level, using probabilistic inference to map posterior probability distributions of unobserved variable to make a basic decision of authentication. We present our proposed framework for fusing bimodal biometrics systems by combining face and fingerprint images to better the performance of biometrics security system. In this research we wanted to exploit prior knowledge as much as possible hence our use of the Bayesian Network to provide reasoning to our framework. Although Bayesian Networks have been used before, our focus in this study is to fully exploit the graphical structure of Bayesian Networks and explicitly model their statistical dependencies between relevant variables per sample measurement. The evaluation of the proposed framework used multimodal chimerical databases formed from publicly available databases. The evaluation of our framework shows an improved performance of 0.03 Error Equal Rate over the performance of the face or finger biometric modalities when each is implemented. The Error Equal Rate for Face and Finger biometric modalities were 0.31 and 0.28, respectively. **Key words:** Bayesian Networks, Inference, Multimodal Biometrics, Principal Component Analysis, Linear Discriminant Analysis, Pre-processing, Probabilistic Inference, feature extraction.

Acknowledgements

The completion of this thesis would not have been possible without the support and encouragement of so many personalities.

First and foremost, I thank the almighty God, for the completion of my thesis. If it was not for his blessings I would have not finished my Masters' thesis.

I am forever indebted to my supervisors Dr. Hlomani Hlomani and Dr. Dimane Mpoeleng for their unwavering support, encouragement and patience throughout the process. I could never be able to pay you back for all the help you have provided, the experience you have helped me to gain and the precious time you spent making sure my thesis was always on the right track. I thank you very much and I hope you find some satisfaction in this modest thesis.

Dedication

I dedicate this thesis to my beloved late nephew, Mpho Phatsima-Morwaagole who has meant and continue to mean so much to me. Although you are no longer in this world boy, your memories continue to regulate my life. Your life was cut short at the tender age of 19. I will always love you and remember you. May you find peace and happiness in Paradise!

Table of Contents

List of Tables.....	ix
List of Figures	x
List of Acronyms.....	xi
CHAPTER ONE.....	1
Introduction.....	1
1.1 Overview of Biometrics Systems.....	2
1.1.1 Verification versus Identification	4
1.1.2 Single/Uni-modal biometrics system	5
1.1.3 MULTIMODAL/ BIMODAL BIOMETRIC SYSTEMS.....	6
1. 2 General Background	7
1.3 Problem Statement.....	8
1.4 General and Specific Objectives	8
1.4.1 General Objectives.....	8
1.4.2 Specific Objective	8
1.5 Research Questions.....	9
1.6 Expected Outcomes	9
1.7 Justification of Study	9
1.8 Thesis Structure.....	9
CHAPTER TWO	10
Related Works	10
2.1 Overview of existing authentication methods.....	10
2. 2 Face Recognition.....	12
2.3 State of Art.....	14
2.3.1 Appearance-Based algorithms.....	15
2.3.2 Feature-Based Algorithms	16
2.4 Fingerprint Recognition.....	19

2.4.1 Formation and Individuality	19
2.4.2 Fingerprint Features.....	19
2.4.3 Fingerprint Classification Algorithms.....	21
2.5 Bayesian Networks.....	27
2.5.1 Inference.....	29
2.6 Bimodal Biometrics Fusion.....	29
2.7 Multimodal Biometrics Security	31
2.8 Related Work Conclusion.....	33
CHAPTER THREE.....	34
Methods Description and Proposed Approach	34
3.1 Proposed Approach.....	34
3.1.1 Pre-processing.....	35
3.1.2 Face Feature extraction.	38
3.1.3 Finger Feature Extraction.....	39
3.2 Fusion of Features using Bayesian Networks.....	39
3.2.1 The Chain Rule (Probability)	41
3.2.2 Independence in Probability	42
3.2.3 Conditional Independence Probability.	42
3. 3 Performance Evaluation Metrics Approach	43
3.3.1 False Accept Rate (FAR)	43
3.3.2 False Rejection Rate (FRR).....	44
3.3.3 Genuine Accept Rate (GAR)	45
3.3.4 Equal Error Rate (EER).....	45
CHAPTER FOUR.....	47
Presentation and Discussion of Results	47
4.1 Performance Analysis	47
4.2 Experiment Setup.....	47
4.3 Face Analysis.....	48
4.4 Fingerprint Analysis.....	49

4.5 Face Fused with Fingerprint	50
4.6 Implications of fusion.....	51
CHAPTER FIVE	55
Conclusion.....	55
5.1 Conclusion	55
REFERENCES	57
List of Appendices.....	64

List of Tables

Table	Pages
2.1 Fingerprint classifications.....	23

List of Figures

Figure	Pages
1.....	2
2.....	2
3.....	5
4.....	17
5.....	20
6.....	21
7.....	21
8.....	28
9.....	46
10.....	36
11.....	48
12.....	49
13.....	50
14.....	51
15.....	53
16.....	54

List of Acronyms

FAR	FALSE ACCEPT RATE
GAR	GENUINE ACCEPT RATE
FMR	FALSE MATCH RATE
FU	FUSION
FNMR	FALSE NON MATCH RATE
BN	BAYESIAN NETWORK
EER	ERROR EQUAL RATE
FRR	FALSE REJECTION RATE
FTE	FAILURE TO ENROLL
MM	MATCHING MODULE
GA	GENETIC ALGORITHM
CRC	CYCLIC REDUNDANCY CHECK
PCA	PRINCIPAL COMPONENT ANALYSIS
LDA	LINEAR DISCRIMINANT ANALYSIS
SVM	SUPPORT VECTOR MACHINE
EBGM	ELASTIC BUNCH GRAPH MATCHING
LBP	LOCAL BINARY PATTERN
RNN	RECURSIVE NEURAL NETWORKS
ANN	ARTIFICIAL NEURAL NETWORKS
FNN	FUZZY NEURAL NETWORKS
K-NN	K-NEAREST NEIGHBOUR
ROC	RECEIVER OPERATING CURVE
CDF	CUMMULATIVE DISTRIBUTION FUNCTION
PDF	PROBABILITY DISTRIBUTION FUNCTION

CHAPTER ONE

Introduction

Biometrics affirmation, or essentially biometrics, alludes to the automatic recognition of people in view of their physiological as well as behavioral attributes. A physiological characteristic is a moderately stable physical trademark, for example, unique mark, iris design, facial element and hand topography. This sort of estimation is perpetual and unalterable without noteworthy pressure. A behavioral characteristic is progressively an impression of a person's psychological makeup like signature, speech, or how one type at keyboard [1].

Biometric systems have various advantages over tradition confirmation techniques, for example, 1) biometric data can't be gotten by coordinate undercover perception, 2) It is hard to share and repeat, 3) It enhances client effortlessness by diminishing the need to retain long and arbitrary passwords, 4) It shields against disavowal by the client. Various biometric qualities are being utilized today, which includes unique finger impression, DNA, iris design, retina, ear, thermo gram, confront, walk, hand geometry, palm-vein design, smell, keystroke elements, mark, and voice [2].

Figure 1 depicts the Biometrics system types and also summarizes the difference between physiological characteristics and behavioral characteristics.

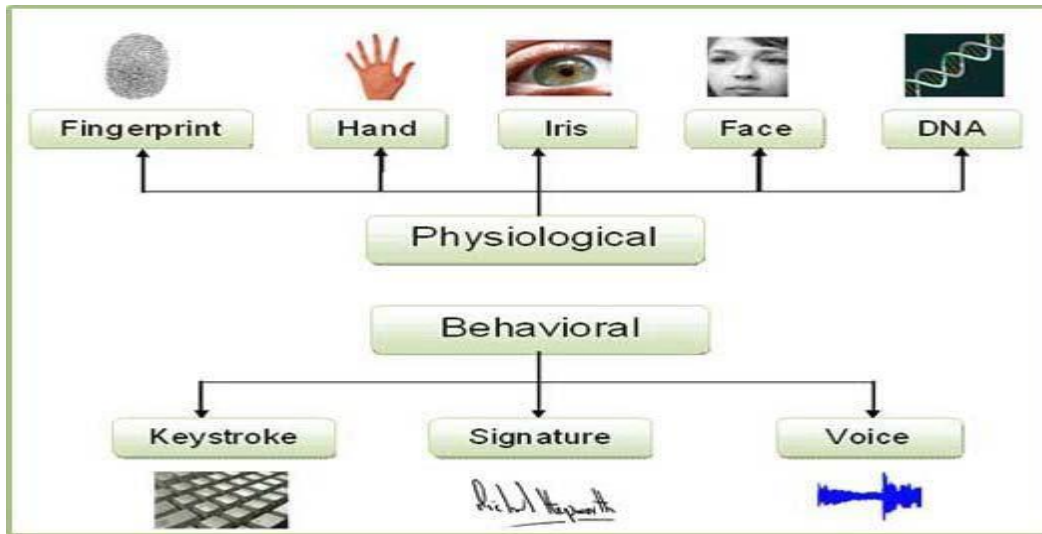


Figure 1: Biometric system type [5].

Our general public has turned out to be electronically connected to form one major worldwide digital network. It has been vital to perform uniqueness of an individual recognition either remotely or and by an automatic process. It has turned out to be important to regularly do solid individual recognition remotely or by automation. Unique character representation such as unique identification number (common automated security door) and ecards (predominant for managing an account, which supports government systems) are failing to excel well because of cybercrime. Furthermore unique identification numbers and ecards are shareable and hence cannot give non renouncement all things considered; Biometrics frameworks have been observed to be more predominant with regards to non-repudiation [3].

1.1 Overview of Biometrics Systems

A biometrics system is fundamentally an pattern classification process which operates by obtaining a biometric data from a person, extract features of the provided data sets and comparing its matching capabilities with the feature set stored [4]. The system is depicted in Figure 2 below consisting of four main modules.

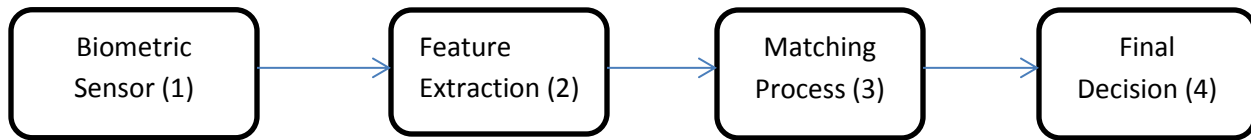


Figure 2: Biometrics main modules [5].

The classification results for each biometric channel are combined by mechanism called biometric fusion. Bimodal biometrics fusion is the combination of measurements from different biometric traits to enhance strength [6]. A multimodal biometric system has four important fusion modules as depicted in Figure 2 and described below [7]:

1. The sensor module which catches the attribute as a crude biometric information
2. The module for extraction of features, are for the removal of a list of capabilities, which are, reduces the representation quality. This set may contain biometric trait that can be either asked for/accumulated or not, contingent on the biometric quality.
3. The module for matching performances classification in order to contrast the extricated attributes set with the templates contained in the data storage to make coordinating scores. Separation function was used for, example, the hamming distance, variable distinction and Euclidean distance which are depicted using a segment metric space.
4. The decision module that utilizes the coordinating scores to either decide a character or approve a guaranteed personality.

The other extra module is a system database module. It is utilized by biometrics system to store templates of enrolled clients. The enrolment module stored enrolled

templates from different individuals into the biometric database system. During the enrollment process, the biometric characteristics of an individual are first scanned by fingerprint scanner or face peruser to create an advanced portrayal of the characteristics. A human relying upon the application might separate this captured information also called templates, amid enlistment process. The feature extractor is used to generate compact but expressive representation called template to further process a digital representation. This is done to properly facilitate matching.

1.1.1 Verification Versus Identification

Biometrics recognition systems are generally made of three different modules including: enrollment, identification and verification [8] as depicted in Figure 3.

(1) Enrollment mode, here only two processes are taking place. The first is the acquisition of the user biometric data; this is where biometric traits of an individual are first captured by biometric reader to produce a raw digital representation of individual characteristics. The raw images are processed further by feature extraction method to create a conservative portrayal containing a format. Then on this second process, this biometrics data for each individual are stored in the database for reference.

(2) Identification: In this mode, the system perceives a man by means of matching their templates of the significant number of users stored in a database for recognition. Furthermore, the structure drives a one-to-various relationship that develop an individual's personality (probably crashes and burns if the images isn't enrolled in the system's data storage) and this gives the subject no guarantee of claiming the character (e.g., "Whose biometrics data belongs to?"). ID is a fundamental part in adverse affirmation applications in which a system determines if the person is who she/he (unquestionably or explicitly) rejected to be in the system. The reasons for negative recognition is meant prevent a user to gain various identities [9]. Identification proof may in like manner be used as a piece of positive affirmation for convenience (the user isn't required to state a character). Since traditional strategies for individual's affirmation, for instance, passwords, Personal Identification number,

keys, and tokens used for affirmation, wrong acknowledgement have to go through biometric process.

(3) **Verification mode**, it is where the system authenticate and validate a person's identity by matching biometric characteristics of individual templates, which check against the database. It allows an individual to prove his or her Identity. This mode is typically used for positive recognition, where the aim is to prevent different people from using the same identity.

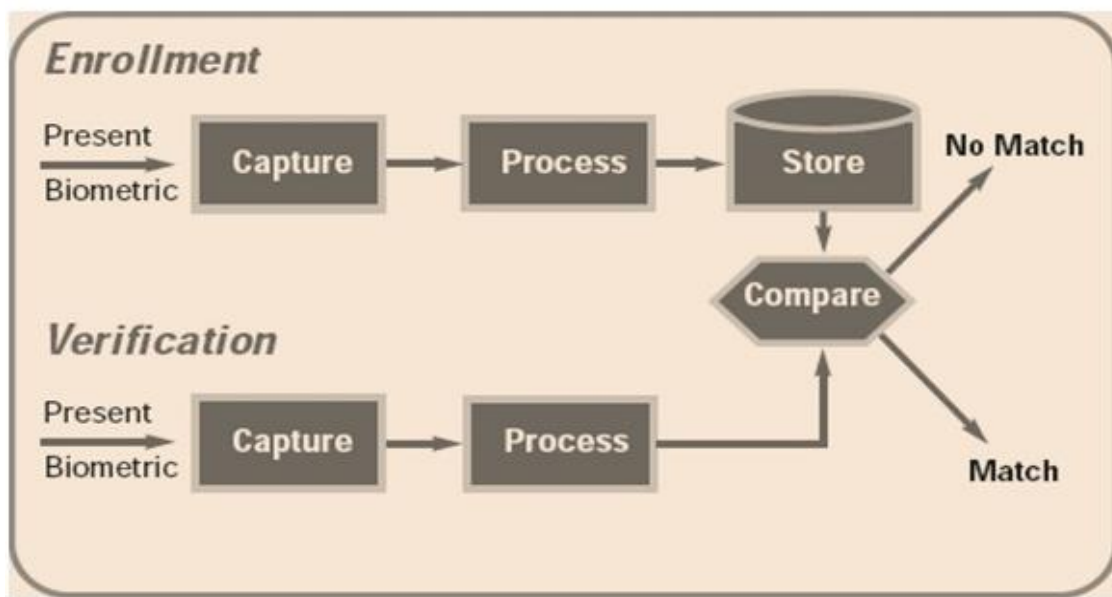


Figure 3: Block diagram of the basic process in biometric system consists of Enrolment mode, verification mode and identification mode [10]

1.1.2 Single/Uni-modal biometrics system

Single or uni-modal biometrics framework utilizes one physiological or behavioral characteristics for acknowledgment, confirmation or compassion [11]. Uni-modal biometric systems have a number of limitations such as spoof attacks, non-universality and noise sensitivity. The problem associated with uni-biometrics systems can be solved by multi-biometric systems which combines or fuses multiple biometric modalities because they usually compensate for the inherent limitations of others [12]. The current automatic systems of biometric have had successful

applications. Nevertheless they differ in each module level where there is room for improvement.

Uni-modal biometric frameworks, which perform individual acknowledgment in light of single source of biometric data, are influenced by the following issues [13].

Noisy sensor data: Noise can be available in obtained biometric information principally because of damaged or malfunctioning sensors. The acknowledgment precision of a biometric system is exceedingly sensitive to the nature of the biometric input and boisterous information can bring about a critical reduction in the accuracy of the biometric system.

Non-universality: When each client's biometrics characteristics are required to be procured, it is actually feasible that clients have no specific biometrics in its little subset. In this manner, there is an inability to select/failure to enroll (FTE) rate related with utilizing a single biometric attribute.

Spoof attacks: Behavioral traits, for example, voice and signature are defenseless against parody assaults by an impostor endeavoring to impersonate the characteristics corresponding to really selected subjects.

1.1.3 MULTIMODAL/ BIMODAL BIOMETRITCS SYSTEMS

Multimodal biometric is the combination of more than one biometric modality e.g. fingerprints and faces recognition. The study carried out by [11] shows that combining two biometrics improves accuracy and it recovers positive reception rate. The idea of the proposed multimodal biometrics fusion framework is to lessen the following:

- False Acceptancy Rate: the number of chances that the system erroneously coordinates the info to non-coordinating templates with the enrolled ones. It

calculates the rate at which the invalid sources of info that were mistakenly acknowledged.

- False Rejects Rate (FRR): the number of chance that the system neglects to distinguish a correlation between the information design and a coordinating templates with the enrolled ones. It calculates the rate at which legitimate sources of info were mistakenly dismissed.

1. 2 General Background

There has been some research in the field of biometrics security where different approaches were followed including frameworks, process models and algorithms. The variation in these results can be attributed to different goals and some specific problems that these works were designed to address.

The global industry has taken a huge interest on the Biometrics filed with the necessary goal of protecting and safeguarding information. Biometrics is used to identify authorized person based on specific physiological or behavioral features [14]. Abdolahi et al.[15], proposed a multimodal biometrics system fusion using fingerprint and Iris with fuzzy logic. The multimodal biometric system improves the recognition accuracy more than of uni-modal methods. The decision level for fusion and each biometrics results are highlighted for participation in final decision.

One of the notable researches by Jagadeesan et al. [16] presented a secure cryptographic key generation from bimodal biometrics in which they fused fingerprints and Iris. It was based on feature level extraction. The system is addressing only limited modules such as feature extraction, generating multimodal templates and generating cryptographic key.

In addition, there are different studies that applaud multimodal biometrics over single or un-bimodal biometrics systems. These include some frameworks of multimodal biometrics, which only addresses the problem of fusion even though they have had some success. Anis et al. [6] came up with a framework for person authentication that consists of sensing different biometrics systems using multiple

sensors, multiple algorithms, multiple classifiers and multiple fusion levels. The framework also proved to be giving good results in fusing multimodal biometrics.

1.3 Problem Statement

The problem this study addresses is in the areas of security and privacy concerns of single biometric systems with respect to their accuracy. We contend that there is a lack of improved feature fusion schemes to generate a compact multi-biometrics template that retains most of the information content in the individual templates. This also translates to the lack of methods to progress the security analysis by modeling the biometric feature distributions. Even though some efforts have been made to secure biometrics templates, there still exist security vulnerabilities in biometrics where templates can be compromised by an attacker. These sentiments have been shared by [17], [18] and [19] and hence the following general and specific objectives.

1.4 General and Specific Objectives

The general and specific objectives of this research are as follows;

1.4.1 General Objectives

This study aims to develop a framework for multimodal biometrics to improve the accuracy and security of fused biometrics templates.

1.4.2 Specific Objective

The specific research objectives are:

1. To identify the limitations of the existing face and fingerprint recognition fusion frameworks.
2. To perform pre-processing of image data by discarding redundant data and noise reduction set for classification.
3. To develop a framework that fuses face and fingerprint recognition systems.
4. To evaluate the developed framework using Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (ERR).
5. To validate the developed framework through a proof of concept.

1.5 Research Questions

- What are the current approaches to enhance security of multimodal biometrics?
- How can the implementation of multimodal biometrics framework strengthen the security and accuracy of bimodal biometrics when using Bayesian Network?
- What are the likely challenges that might affect the implementation and evaluation of results?

1.6 Expected Outcomes

The expected outcome of this research is the production of a framework that will provide a better accuracy performance and security to bimodal biometrics systems. The proposed framework is based on Bayesian Network, which is tailored to deal with the fusion of fingerprint and face.

1.7 Justification of Study

The extensive literature review has shown that there are gaps in the security and accuracy of bimodal biometrics. It also proves that uni-modal biometrics poses security threats. The research on bimodal biometrics has been carried out but there are still security concerns which will be address by this study. Sireesha et al [20], presented an innovative technology for multimodal biometric authentication and the evaluation for precision proves an improved performance based on FAR and FRR. It is very vital to carry out this research to solve the following problems faced by un-modal biometrics:

- i. Accuracy
- ii. Spoof attacks

1.8 Thesis Structure

The reminder of this thesis will be organized as follows: in chapter 2 it will be a review of related research work for multimodal biometrics systems and fusion of face and finger print systems. Chapter 3 highlights the proposed method of research. Chapter 4 discusses the experimental results and its analysis. Chapter 5 summarizes the conclusion of results and outlines the future recommendations for the improvements of the study.

CHAPTER TWO

Related Works

The use of biometrics for access controls is commonly used in different areas and applications such as login to machines, on distributed machines like ATM and boarder gates for security reinforcement. The use of this technology saw different implementations throughout generations. Despite its use for many years and the growth of expertise in this technology there still exist security and privacy loopholes which this study is trying to address.

2.1 Overview of existing authentication methods.

A wide assortment of systems requires solid individual recognition plans to either affirm or decide the character of an individual asking for their services [21]. Yan [22]described authentication as to prevent unapproved people from accessing resources and guaranteeing that approved people can get to the resources they require with a specific end goal to achieve the three essential security objectives which confidentiality, integrity and availability. The most important element is to recognize that different mechanisms provide authentication services pertaining to their degrees of certainty. It is therefore vital to choose a proper authentication method basing on the location of the entities being authenticated and the degree of trust placed in particular facets of network or any assigned storage mechanism.

Abdolahi et al, [15] proposed a multimodal biometric system fusion using fingerprint and iris with fuzzy logic. The system was introduced to solve the limitations faced by single biometric system and it showed improved results as for accuracy using False Acceptancy Rate (FAR) and Error Equal Rate (EER) metrics. This system was however focused on the decision level for fusion to obtain results in final decision module which later fuzzy logic was used for the effort of each biometrics results.

Another paper proposed by Meva et al, [23] in 2013, which focused on a comparative study of different fusion techniques in multimodal biometric authentication. In this paper the focus was to find the best possible fusion

technique, it was how however very important to explore at which fusion level the results obtained. From different techniques it has proven that fusion gives better accurate results as compared to a single biometric system.

In 2015, system proposed by Shayam et al, [24] continued to explore fusion by identifying individuals using multimodal face recognition techniques. The discussion in this paper was mostly centered on joining the comparability scores of the unimodal modalities, for example, appearance based and surface based methods of face recognition, which provides the outcomes at the level of matching score. The focus in this paper is to utilize the combination of unimodal systems to devise the multimodal models in four conceivable mixes, for example, Eigenface and Local Binary Pattern (E-LBP), Fisherface and LBP, Organics' and expanded nearby paired example and A-LBP. The experimental results continued to prove a significant improvement in the performance of recognition accuracy.

Rajagopal et al, [25] further proposed a system in 2015 for performance evaluation multimodal multifeature authentication system using K-nearest neighbor (K-NN) classification. The focus in their proposed system was to improve recognition accuracy using feature level fusion with the emphasis on K- NN classifier. Principal Component Analysis (PCA) was utilized to solve the issue of revile in dimensionality of feature set as there are high dimensional.

Further studies were presented by Patnaik et al, [26] and they were adamant unimodal biometric systems are powerless to assortment of issues, for example, noise, intra-class varieties and spoofing attacks among others.

They proposed a system which provides an effective scheme that combines the presented information by multiplying domain experts which were based on the rank level fusion integration method. The integration thus increases the efficiency of the system which is a limitation in unimodal biometric system. In their system they explored the uniqueness of Principal Component Analysis (PCA) and Fisher Linear Discriminate method for individuals' matchers' authentication.

Another research effort was introduced by Madane et al, [27] in 2016. Their framework provides a method to extricate features in spatial space from Iris and palm print. Accuracy was improved by a GAR in multimodal biometric system by matching Iris and Palm print at the score level. In this paper they explored different matching score proportions of Iris: palm print and the result showed a better performance through combination as it was indicated by a higher GAR values than all other matching scores.

Garg et al, [28] in 2017 came up with a survey on different levels of fusion in multimodal biometrics. In their paper they have compiled a survey which was specifically based on the comparison of various techniques which were mostly used by multimodal biometrics system. The objective of the survey was to explore different techniques used in various levels of fusion in which they have shown a significant improved accuracy rates and a robust improvement at each level of fusion. In their paper they accomplished the idea of fusing two different biometric traits with high performance and the survey also proves that Bayesian Networks was overlooked and it is of importance to be explored in our study with anticipation of improving results.

2. 2 Face Recognition.

It is more into nonexclusive of biometric attestation, which contains in recuperating the personality of individuals in light of the normal physical characteristics. It has a particular great favourable advantages than a built up recognizable proof techniques, hence they do not need any data that people normally keep, for instance, travel papers, identity cards or PIN codes for instance. In fact, those strategies for recognizable identity could be easily ignored, stolen or even being fabricated. Or maybe, subject biometric acknowledgment relies upon the person's own attribute, for instance, finger impression uniqueness, iris, stride, and obviously, face recognition.

At the point when matched with other biometric techniques, it has a standpoint of not being intrusive to the client; likewise it could work at a separation without unequivocal client collaboration

However, the recognition of face are still a testing issue hence it needs to manage an extensive variety of difficulties, such as stance and illumination which is described by Zhao et al, [29]. There is also an issue of instability in such biometric sample. Face appearance may enormously differ after some time because of external antiquities (glasses, facial hair) and aging for instance. At any rate and interestingly with various modalities, the face as a biometric ascribe has all the earmarks of being a conventional decent trade-off of its convenience, user requirements and participation and accuracy requirements.

Face recognition development could be connected in a huge scope of utilization: The most imperative thing is irrefutably security: fringe controls, criminal examinations, premises access control are situation where biometric security systems are installed. It is however vital indicating different applications that could profit by this advancement, for instance, human-PC cooperation, customized photograph or video requesting or picture recovery to name few.

Fundamentally, face recognition of any framework involves in looking at the already known sample of face images of the other given face images samples. Be that as it may, before acknowledgment undertaking itself, variety imperative steps advances that ought to be kept an eye on: it starts with the face recognition, of which goal is to recognize the availability of face images or to check from the system input for the given images. After the detection of face, the enrolment take place (that is remarkable face features being availed) and this is more frequently geometrically standardized. The recognition procedure now takes place, and may likewise be isolated into three specific assignments: the discretionary pre-processing of the enrolled images, the component extraction step, furthermore, classification of features depending on the already extracted features.

This can be done through various three excellent modules: watch list, verification and identification. Regardless of the way the algorithms are being connected, they have different specific particular arrangements; moreover, exceptional care ought to be made when organizing a specific system. The essential refinement is whether the applications deal with implied shut set or open-set situations.

Identification: Identification is a one-to-numerous process that compares the biometric data introduced by an individual with all the biometric data enrolled in a database, and chooses regardless of whether a match can be declared [30] .

Authentication: Face authentication is having a tendency to going with situation; for example, an individual claims a character by giving their face images. After matching process it can be determined whether the system rejects or recognize the individual claim Verification has thusly to supervise impostors, individuals' identity trying to trap the framework. It is therefore most certainly as an open-set situation hence imposters are not available.

Watch-list: The watch-list issue includes in performing recognizable proof of evidence of an open-set situation: a person to be recognized could be now known to the system. For this circumstance, phenomenal care must be settled on choice: the best match between the show and the test does less relate to the correct character.

2.3 State of Art

For over 40 years, face recognition has been a common and active research area and different systems are presently prepared to do accurately recognizing individuals' faces under controlled environment. There is an immense measure of face recognition algorithms, and it is subdivided into two different approaches which are appearance based method and feature based method. The extraordinary distinction between these systems is that all encompassing methodologies uses the whole part of the face area as an input to a classifier, the face is considered as an arrangement of perceptions, which will be utilized on analyzing observations. The following

subsections will be for discussing the face recognition algorithms, their drawbacks and advantages.

2.3.1 Appearance-Based algorithms

The accentuation on this area will center on the two primary specific algorithms: Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA).

Principal Component Analysis: PCA is the most effective dimensional decrease device which is ordinarily utilized in image processing particularly face acknowledgment [31]. The Principal Component Analysis is found to be a useful statistical technique that has found applications in fields such as recognition, image processing and classification with different classifying algorithms. It is a common technique used in feature extraction from data of high dimensional space. The face image is thusly portrayed by a vector of weights, which represents the straight blend of the indicated Eigen faces. Considering the all-encompassing representation of face as a vector signified as m , linearly it is anticipated in obtaining the element n vector:

$$n = W_{pca}^T m \quad (2.1)$$

Where $n = W_{pca}^T$ is a grid containing the fundamental eigenvectors of the planning information covariance matrix. At that point classification is carried out specifically in this subspace and simple matrix such as Euclidean distance will be applied and even more sophisticated techniques such as Support Vector Machine (SVM) and Multi-Layer Perceptron (MLP) for example.

Linear Discriminant Analysis: according to Balakrshnama et al, [32], Linear Discriminant Analysis effectively handles the situation where the within-class frequencies are unequal and their performance has been examined on randomly created test data. LDA is considered to be one the most successful algorithm in face recognition [33]. This algorithm relies upon Fisher's direct discriminant equation to find the perfect discriminative subspace where data will be anticipated. There are two methods defined in Linear Discriminant Analysis. Between-Class scatter matrix (S_B) represents the scatter of features around the overall mean for all faces class and

Within-Class scatter (S_W) represents the scatter of features around the mean of each class.

$$S_B = \sum_{j=1}^c N_j (\mu_j - \mu) (\mu_j - \mu)^T \quad (2.2)$$

Where N_j , is the number of training examples in $class_j$, c is the number of distinct classes, μ_j is the mean vector of samples of $class_j$.

$$S_B = \sum_{i=1}^c \sum_{j=1}^{N_i} (x_j^i - \mu_i) (x_j^i - \mu_i)^T \quad (2.3)$$

Where x_j^i is the j^{th} sample of $class_i$, μ_i is the mean of $class_i$, C is the number of classes and N_i is the number of samples in $class_i$.

2.3.2 Feature-Based Algorithms

Unlike appearance-based methods, they normally consider a local features rather than the entire image. Here, we describe the prominent approaches which belong to this group. The algorithm which will be discussed primarily they handle faces. Infact, early face acknowledgment algorithms were thoroughly feature based, since they endeavored to see people in light of geometrical properties of the face [34].

There are considerable researches which were proposed for feature-based algorithm in face recognition. One notable system was developed by Kanade et al, [24] to handle this task. The system automatically localizes features, for example, corners of the eyes, nostrils, mouth, nose and so forth. At that point an arrangement of sixteen facial parameters relating to the features is computed. A basic Euclidian distance measure is used to compute the similarity between a test face and stored face. The emphasis on this subsection will be on feature-based algorithm which will be discussed below.

Elastic Bunch Graph Matching (EBGM): Wiskott et al, [35] defines EBGM as the eminent nearby element based face recognition algorithm. The algorithm presents

face images by a course of wavelets coefficients, named jets, and sorted out in a graph, whose nodes compares to fiducial focuses. In the midst of the acknowledgement procedure, the grid is permitted to be deformable with a specific end goal to boost the connection between comparing wavelet coefficients of the display and of the sample picture.

Local Binary Patterns (LBP): Another feature-based algorithm was proposed by Ahonen et al, [36], With LBP it is conceivable to depict the surface and state of digital image. This is done by dividing images into a few little regions from which the features are. Depicted below is Figure 4 showing LBP operator.

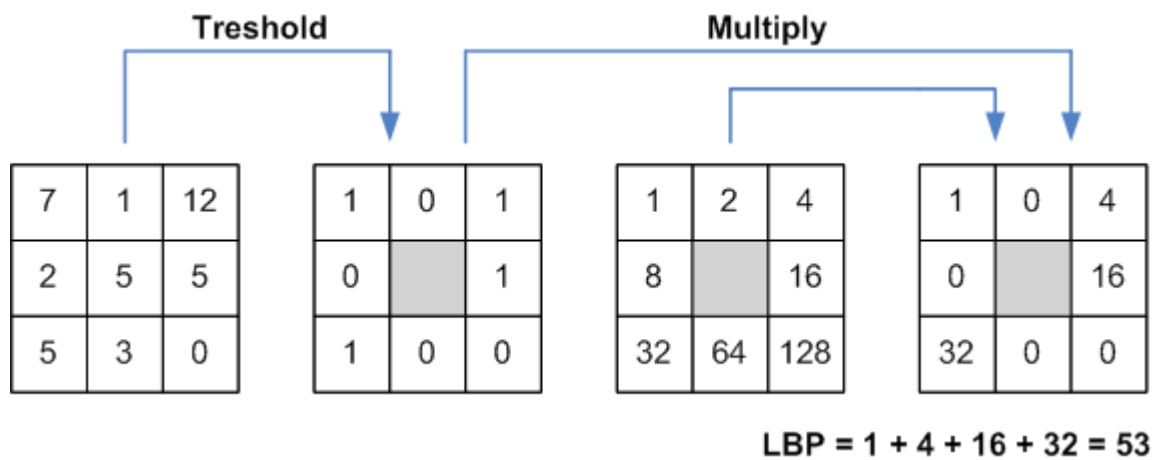


Figure 4: Local Binary Pattern Operator [37]

Statistical Models: Statistical Models are prestigious as another prevalent way to deal with local feature based face recognition [38]. The point of such frameworks is to demonstrate the distribution of a list of capabilities extricated from the image of face traits. The following section will clarify more subtle elements based on the model discussed.

2.4 Fingerprint Recognition

In recent years, Fingerprint applications, which are authentication based, are popular across government security agencies and business enterprises. It has been also adopted by the general purpose devices such as laptops, mobile phone, and memory stick. Fingerprint word is also expressed as individuality, however its unique characteristics are not fairly settled, and its templates are essentially run as experimental perception over other multiple obtained ones. This section focus on presenting fingerprint recognition problems, we discuss fingerprint recognition common algorithms and then we move forward to structural analysis of fingerprint to describe the most common database and why they are used.

2.4.1 Formation and Individuality

Fingerprints are fully developed at around seven months of embryo. They then remain unchanged through the individual's existence (diligence property). On the off chance that shallow harm occurs, the skin will develop back in the plain same course way amid childbirth. All this makes fingerprints a reliable method for identification in all phases of human life. Fingerprints features are the last to decompose after death. The embryologic development epidermal ridges were described by Barbler et al, [39] and scientific clarification for the improvement of epidermal edges of fingers can be found in [40]. As indicated by the presumption of uniqueness, variations of people have various striking features: In a situation of sharing more than one feature, a specialist presumes those features have a place with a similar individual.

2.4.2 Fingerprint Features

The issue of portrayal of a one of a kind unique finger impression is a deciding factor for an acknowledgment framework and there is a need to find viable strategies to pick astounding features. After the detecting stage with a fingerprint device, we have an image based representation, constituted by pixel constrain data, or, in other words to twists, splendour variations, and affine changes and requires a lot of capacity. Finger ridges and valleys are depicted in figure 5 below.

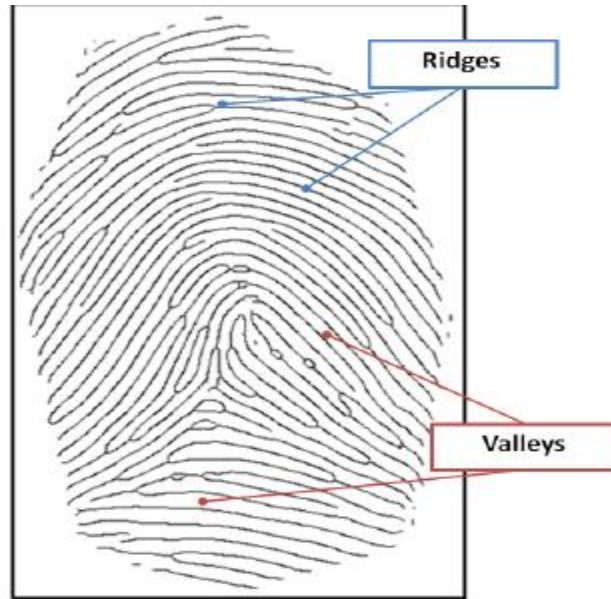


Figure 5: Finger image Ridges and Valleys [29]

There are distinctive accessible unique finger impression features, which are composed and can be contingent upon especially on the securing goals. As it is depicted in Figure 6 below, it shows that the most evident structural characteristics of a fingerprint is a “pattern” of interleaved ridges and valleys. Fingerprint also has a smoothed structure with the exception of in at least one region that contains classifiable qualities called singularities, which are depicted below on Figure 6.

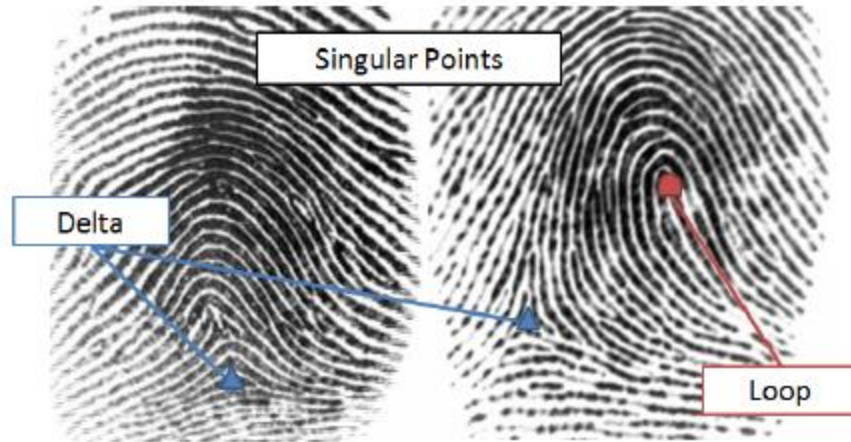


Figure 6: Singular Points in Fingerprint [41]

Rajanna et al, [42] discussed the Henry classification classes which are organized in the main five categories or classes. Their organization system is meant to possibly accelerate the inquiry particularly in the event that where available databases are too large. The Henry fingerprint classifications are depicted in Figure 7 below.

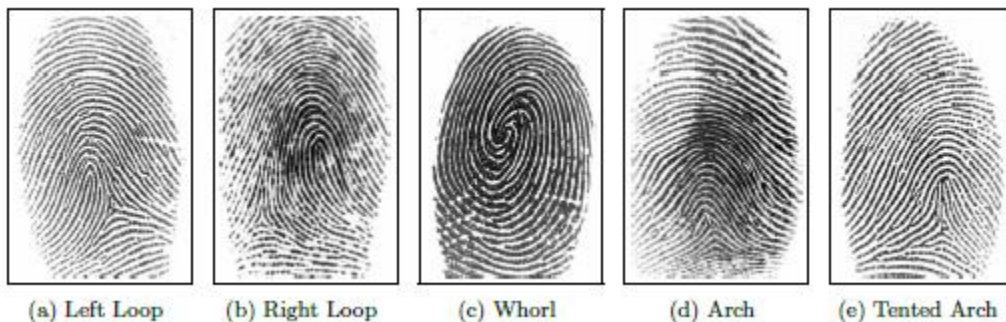


Figure 7: Henry Fingerprint classes [43]

2.4.3 Fingerprint Classification Algorithms

Fingerprint classification has been playing important role in classifying big data large scale fingerprint systems. Classification permits an information unique mark that is matched with a part of database, which is basic for accelerating fingerprint identifiers. The essential goal of a unique finger classification is that it should be invariant to revolution, understanding and versatile twisting of the frictional skin. Unique mark arrangement algorithms are used to make unique finger impression record that can

be utilized to decrease the time many-sided quality while performing coordination with vast databases.

There are lot of fingerprint classification algorithms and they come in different ways, therefore in this subsection will be focusing on reviewing some of the algorithms which then will be summarized in Table 2.1. The classification approach is based on Artificial Neural Networks, which uses a neural system where arrangement for unique finger impression images is produced, that can order a complex unique finger impression features. They utilizes a double advance learning approaches for a preparation of neural system which four layers with sub-organized for a class,

Initially an algorithm was proposed by Yao et al, [44]. For classification they used Recursive Neural Networks (RNNs) and Support Vector Machines (SVM). The RNNs are prepared on a basic introduction of the unique finger image and were also used to remove an arrangement of distributed features which are incorporated to the SVMs. SVMs are joined with error remedying coding plan, which exploits information held in vague unique finger images. Another classification approach was proposed by Bhuyan et al, [45] which were based on ANN, where neural network for fingerprint image classification is constructed, which have the ability to classify complex finger-images. They utilizes a double advance learning approaches for a preparation of neural system which four layers with sub-organized for a class. Principal Component Analysis is used as unit of values of second concealed layers. Further researches on fingerprint classification are represented by the internal network. Therefore, the method confirms that the unique finger impression designs are for the most part grouped into every classification covered for a suitable learning process.

Mohamed et al, [46], also presented a fingerprint classification method using Fuzzy Neural Networks (FNN). In this system, fingerprint features are gotten from a binarised image. This classification method produced good results of classification when using FNN. Another classification algorithm based on directional fields was proposed by Wang et al, [47].

In this classification method, there were two classifiers used which were K-means and K-nearest neighbour (K-NN). They were responsible for classifying features into different types, namely, Arch, Left Loop, Right Loop or Whorl. There is however an approach presented by Shah et al, [48]. This approach unlike the one proposed by [46], it arranges unique mark images into five different classes: left Loop, Right Loop, Whorl and rose Arch. It is discovered helpful over a low-dimensional component vector created from the yield of a criticism based locator. Feature extraction procedure of this method depends on classifying the conveyance of introductions around the fingerprint. Three classifiers used are namely K-NN, Support Vector Machines (SVM) and Neural Network classifier. Table 2.1 below summarizes fingerprint classification algorithms.

Table 2.1: Fingerprint classifications

Author	Features	Technique used	Classes	Dataset Used	Areas to be improved
Kamijo (1993)	PCA, ridge lines, singular points	Neural Network Classifier	5Cb	-	Performance degradation with large databases
and Jain (1996)	 Cores and Delta	Rule-based Classifier	5Cb and unknown type	-	Unknown fingerprint type can be eliminated
Ballan (1998)	Singular Points from directional histograms	Rule-based Classifier	Lasso and Wirbel	-	Time Complexity increases with image size.
Cho <i>et al.</i> (2000)	Features related to core points	Rule based Classification	4C	Own database	Hard to dispose of false particular point(s) which are utilized amid class choice. Require refined techniques to take out those false center focuses towards a commotion tolerant classification Framework
Yao <i>et al.</i>	Finger code features and structural	SVM and RNN	5Ca	NIST	Utilization of two machine learning algorithms

(2001)	representation				expanded the time unpredictability
Wang <i>et al.</i> (2002)	Directional Fields, delta points and Singular Points	K-Means and 3-Nearest Neighbour	5Ca	NIST14 database	Performs ineffectively with optical sensor fingerprints (where delta focuses are most certainly not accessible)
Mohamed and Nyongesa (2002)	Singular points, positions and direction of core and delta	Fuzzy Neural Network	5Cb	NIST-4 database	High event of misclassification among fingerprints with comparable features
Tan <i>et al.</i> (2003)	Image composite operations and features	Genetic Programming and Bayesian Classifier	5Ca	NIST-4	Handling of low quality fingerprint
Shah and Shastri (2004)		SVM, Nearest neighbour and neural network	5Ca	NIST	The line detector algorithm can be enhanced to work with boisterous images
Afsar <i>et al.</i> , (2004)	Singular points	Rule based Classifier	5Ca	FVC 2000 database	Time complexity and High False Rejection Rate
Park and	Fast Fourier				

Park (2005)	transform coefficient and directional features	SVM, MLP, KNN, RNN	5Ca	NIST	-
Zhou <i>et al.</i> , (2007)	Grid Features (Mean, variance, contrast, coherence and energy)	SVM	L & W	Own database, FVC2000 and NIST Special Database	Correct estimation of size is required and strategies to proficiently asses this size can be tested
Ji and Yi (2007)	Directional block Features of a class	RNN and SVM	5Cb	FVC2004	-

2.5 Bayesian Networks

Bayesian networks (BNs) also known as Beliefs Networks are graphical models for reasoning under uncertainty, where the nodes represent variables (discrete or continuous) and arcs represent direct connections between them [49]. It can be viewed as a connection between probability hypothesis and chart graph theory. Bayesian Networks give a natural strategy to represent the joint likelihood scattering over an arrangement of factors: irregular factors are represented to as hubs in a coordinated non-cyclic chart, and connections express causality connections between these variables.

To be exact, the nodes in a Bayesian Network makes an uneven variable Y, (and parent of variable Y is represented by variable X) and subsequently forms a restrictive probability P (Y|X). Y is said to be caused through the Bayes rule, knowing the estimation of Y gives information on X [49].

More generally, let us define Pa (Xi) as the set of parents of the variable Xi in the directed acyclic graph. The joint probability encoded by a Bayesian Network over the set of variables X = (X1, ...,Xn)is then given by the following chain rule:

$$P(x) = \prod_{i=1}^n P(x_i|Pa(x_i)) \quad (2.1)$$

In this rule thus a Bayesian Network is completely characterized by the graphical structure and by its parameters, which comprises in the restrictive probability conveyances of every single variable given their parents. Depending on a scenario, it might however a variable x_i does not have a parent, for this situation its probability dissemination is just given by prior P (x_i). For better understanding of casual relationships and conditional independence, Figure 8 below provides an example of a Bayesian Network. This example was adopted from Asia Network.

Breath shortness (dyspnea, hub D) maybe of TB (Hub T), cancer (lungs) (hub B) or all negative, and maybe just one of them affirmative. An ongoing trip to Asia (hub A) built the best shot of TB, whereas smoking (Hub S) said to be hazard for both lungs and bronchitis diseases. The consequence of a solitary chest X beam (Hub X) neither

does not segregate in between the lung growth and TB (whether the lungs diseases or TB, Hub E) nor does the closeness' or nonappearance of dyspnoea [50].

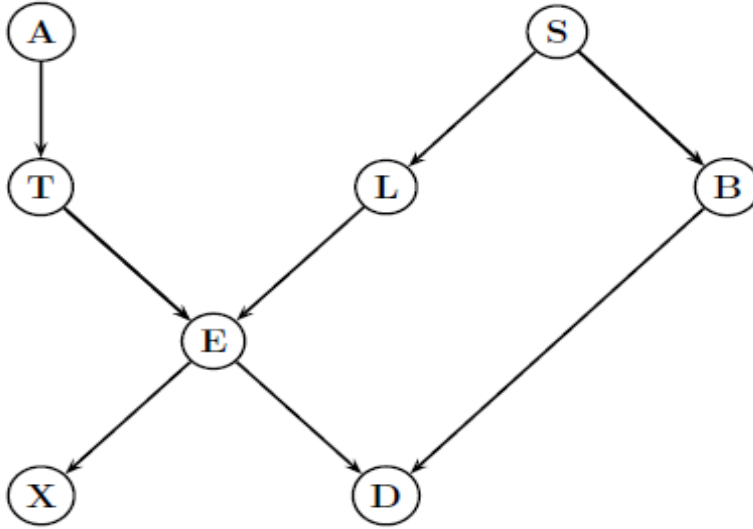


Figure 8: The Asia Nets [51]

As it is demonstrated in Figure 8, network encodes dependencies between different variables, let's look closer for instance at the dyspnoea, it correlates to both TB and smoking activities. There is also conditional independencies assumption which can be noticed on the depicted diagram above: for instance there is no relationship for the smoking activity to Asia. This cause conditional distributions and as it is notable, smoking builds the shot of creating lung disease. Hence thus give [52];

$$P(L = 1|S = 1) > P(L = 1|S = 0) \quad (2.2)$$

These networks can lead into beliefs on variables being updated and some of variables being observed. To compute these probabilities in Bayesian Network is known as *inference* which is discussed in the next sub-section.

2.5.1 Inference

Inference is an aspect or a construct in Bayesian Network. It is an important task which utilized for registering likelihood of intrigue, once the confirmation has been gone into a system. Giving confirmation contains either in settling the state of a discrete variable to one of its conceivable esteem or to assign a motivator investigating the issue of a predictable variable.

This process is also called reasoning or Bayesian updating or belief updating [53]. They are two ways to approach inference which is either by exact or approximate. An exact technique clearly gives a correct outcome, while an approximate strategy tries to approach the correct outcome as close as possible. Inference algorithms are hence captivated by finding the impact this confirmation has on the dissemination of the other in secret (or disguised) variables.

2.6 Bimodal Biometrics Fusion

It has been described by I. O' Gorman [54] that there is a plethora of ways in which a perpetrator may attack a biometric system in the aspect of security of which he mentioned two very serious issues of criticism against biometric technology: (1) biometrics are not secrets (2) biometrics patterns are not revocable. The first scenario implies that the attacker already has a good knowledge leading to intrusion of information of legitimate biometric identifier and therefore, could fraudulently inject it into the biometric system to gain access. On the second scenario where biometrics patterns are not revocable it implies that when biometric identifiers have been compromised, the legitimate user has no recourse to revoking the identifiers to switch to another set of uncompromised identifiers.

In addition, El-Abed et al, [55] supported that biometric systems have powerful potential to provide security for variety of applications. While biometrics may improve security in different environments, like many other systems they are susceptible to vulnerabilities and threats.

To address those vulnerabilities, a safe biometric framework that will acknowledge just genuine introduction of biometrics identities without being compromised or any malevolent measures being infused into the framework. Advancement of such a framework would forestall the requirement for repudiating the "traded off" identifiers. The outlines of such frameworks are a challenge.

Another paper proposed by An et al., [56] proposed an algorithm based on Bayes theory in order to fuse individual expert's opinions. They considered two modalities to be used in their system which are face and speech for every person involved. After conducting experiments, the results showed that fusing two biometrics modalities improves accuracy over uni-biometrics systems which scored success rate of 83.5%. The system did not clearly show at which level results are conducted and only focused in improving accuracy but not paying attention to security of templates in the database. However, an algorithm proposed by Poh et al. [57] about fusion based on score level was discussed. This combiner algorithm was based on ensemble classifier for facilitating multi-modal authentication. The two discussed algorithms are giving credit to either fusion level by providing high accuracy of biometrics templates as compare to single or uni-modal biometrics systems.

The research presented by Nandakumar [58] in his thesis proposed a fusion methodology base on the Neyman- Pearson theorem for combination of matching scores provided by multiple biometric matchers. It shows that the likelihood ratio (LR) test used in this theorem directly maximizes the genuine acceptance rate (GAR) at any false acceptance rate (FAR). The LR was also extended based on fusion scheme to integrate the quality of samples. This theorem proved that the likelihood ratio framework can be implemented in designing sequential bimodal biometric systems through the construction of a binary decision tree basing on the marginal likelihood ratios of the individual matchers. This theorem however did not receive more attention as the matching was taking more to be interpreted as binary decision tree which made it complicated for performance assessment.

Sasidhar et al. [17] however, established a framework based on improving accuracy and performance with assessing the performance of bimodal biometrics systems. In

this study they examined relatively large face and fingerprint data sets over a spectrum of normalization and fusion techniques. It is evident from the results of conducted experiments that multimodal biometric systems better perform than unimodal biometric systems in terms of accuracy and performance. After studying different fusion level approaches, it shows that the method chosen for fusion has a significant impact on the results and performance.

2.7 Multimodal Biometrics Security

The security management in discipline observes three main security management goals commonly known as CIA (confidentiality, integrity and availability). Biometric as access control has been an upcoming area which many researchers targeted with many devices requiring a very unique security system. Many studies have been conducted to come out with the outstanding security measures to secure biometric templates with different algorithmic combinations being proposed.

Erlangug et al. [59] proposed biometric cryptosystem based on authentication, encryption and signature for biometrics identities. They came out with cryptographic conventions for biometric in the system of a practical and solid security demonstration and furthermore assure a less security difficulties. Muncaster et al. [60] evaluated the primary biometric confirmation systems that surveys biometrics as an open information and it was assessed in lesser score of security. This study elaborated that biometric remote authentication; simultaneous attack against biometric systems can only be presented by multi-factor solutions.

Jagadeesan et al. [38] also came with yet another suggestion for generating encryption key of multimodal biometrics. Securing information system becomes a more challenging task because of increased number of spoof attacks [33] The concern that was raise was that even though biometric seen as a better alternative for access control over passwords and token, if it is stolen one time it can be used by attackers to access system until it exists. It is a very humorless issue because if one's biometrics templates are stolen it will be live at all times unlike passwords.

The conclusion made from their survey suggested the use of bimodal biometrics systems as it is very difficult for the attackers to break fused biometric traits.

Encryption is the way toward encoding a message with the goal that its significance isn't self-evident. A framework for encryption and unscrambling is called cryptosystem [61]. Another terminology which will be discussed in this section is encryption algorithms, which are a set of rules for encryption and decryption and often use a device called a Key, denoted by K.

A paper proposed by Arunachalam et al. [62] discussed about AES using cryptographic level fusion with fingerprint and finger knuckle print. This research paper shows that authentication and confidentiality are established through secret ID by the help of Cyclic Redundancy Check (CRC) function. They used K-means algorithm to generate Key for both fingerprint and Finger Knuckle Print. Here, the secret ID is encoded twofold times by AES calculation with two diverse keys created from unique mark and FKP to deliver the secret ID 1 and 2 by bundle show cryptographic combination [62]. The system can effectively secure data because of double encryption capabilities of AES but on the other hand it can still be bypassed by crypt analysts where they can study the encryption Key. A further security of hiding encrypted imaged can be used to increase security strength.

Much like the above proposal, Fu et al. [63] proposed the study of bimodal biometrics crypto systems with different levels of cryptography fusion strategies.. In the study, they proposed a situation of coordinating the biometrics of unique finger impression and Finger Knuckle Print fused with AES to shape a multimodal biometric crypto framework by analysing the framework utilizing decision level fusion. They also discussed about two bimodal crypto system phases: encryption phase and decryption phase.

2.8 Related Work Conclusion

Different approaches are used in order to secure biometrics templates and to improve accuracy by implementing bimodal biometrics systems. We can deduce that security is very crucial in sensitive data of an individual biometrics as it poses a privacy threat. There are some notable limitations in the existing algorithms; the combination approach to score level fusion has received considerable attention. We therefore deduce that from the literature there is no standard technique either for converting the scores into probability or for normalizing the scores obtained from multiple matching algorithms. It further shows that a systematic evaluation of different normalization techniques and probabilistic inference are not available.

Attempts were made to try maximizing security of biometrics templates but with the growth of technology, new methods of security are vital to keep up to date with the growing technology. In many reviewed papers it can be concluded that more effort was made to improve accuracy of biometrics. It is also important to note that fusion using other methods such as Bayesian Networks was not given much emphasis hence our study will explore more into that area to close the gaps left and with Bayesian Networks it can improve fusion accuracy with less Genuine Acceptance Rate (GAR).

CHAPTER THREE

Methods Description and Proposed Approach

This chapter presents the methods followed to develop the framework for improving the accuracy and security of multimodal biometrics templates. It starts by introducing the performance evaluation of biometrics systems. This framework addresses the limitations of uni-modal biometric systems by improving the accuracy and security using bimodal biometric system. It will then make a model which integrate security and accuracy of bimodal biometrics at a feature level fusion.

3.1 Proposed Approach

In this section we present our proposed framework for fusing bimodal biometrics systems. This framework hinges on the combination of face and fingerprint images to better the performance of biometrics security system in terms of accuracy. There are many factors and constructs that build up to this framework which primarily start with training images for both fingerprint and face. The main contribution of our framework is fusing of the two modalities based on Bayesian networks. This is done within the identification process. Hence our framework uses probabilistic inference. The fusion of finger and face is expected to produce a better performance as compared to just fingerprint alone or just face alone.

There are various approaches and factors which contribute to the improved performance of bimodal biometric system using fusion techniques but Bayesian networks are not overused; thus, giving us more chance to explore it. Our proposed Framework for multimodal biometrics security based on Bayesian Network is depicted in Figure 3.1 below.

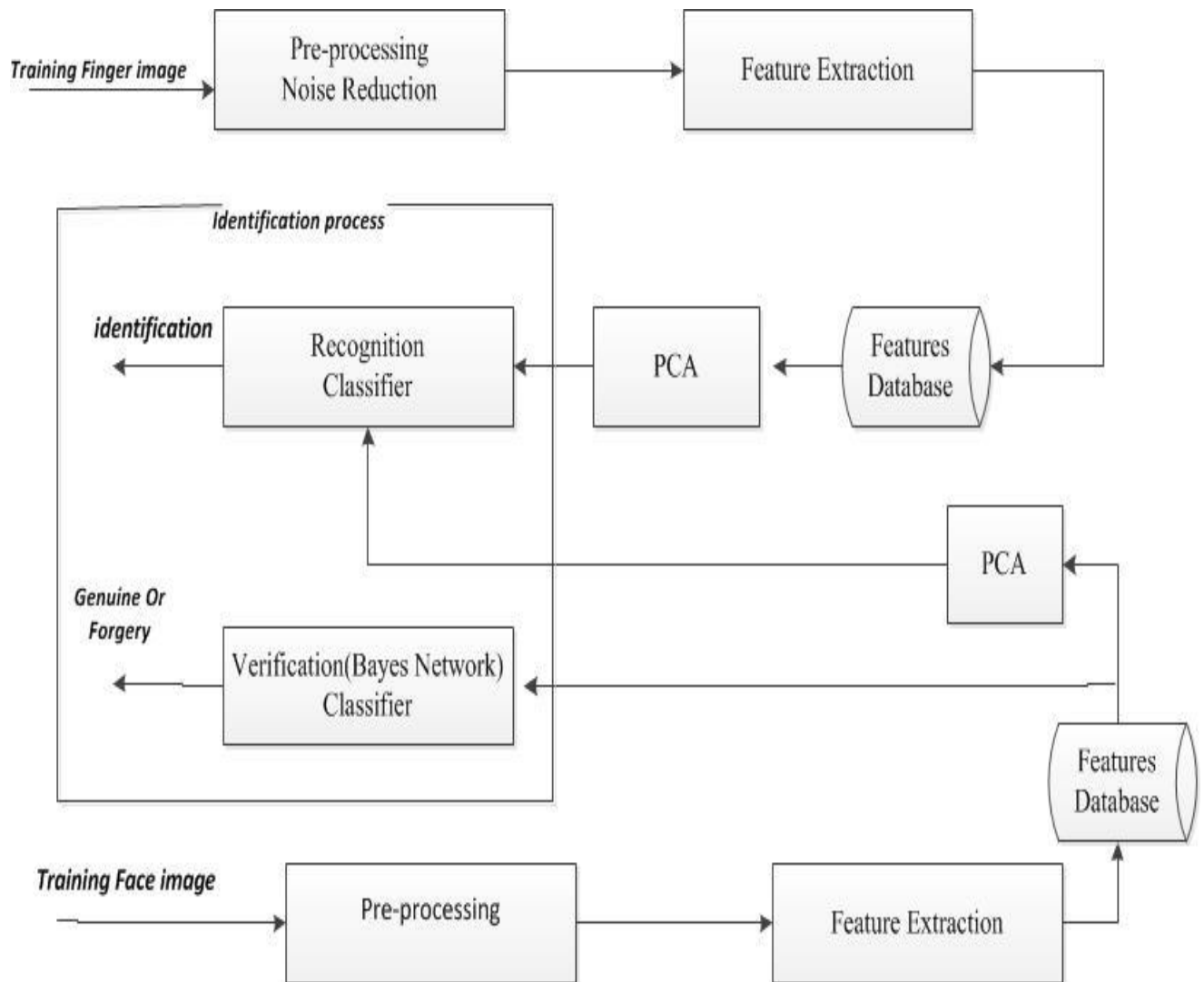


Figure 3.1 Proposed Framework: Multimodal Biometrics Security Based on Bayesian Networks

3.1.1 Pre-processing

Pre-processing of images is an important step for fingerprint recognition. It gives the quality and produces an image in which minutae can be detected correctly. This step involves refining of the thin images, detecting the minutae points and extracting features from images. Noise is also reduced in this step to give a quality images.

There are different pre-processing methods and techniques as depicted in Figure 10.

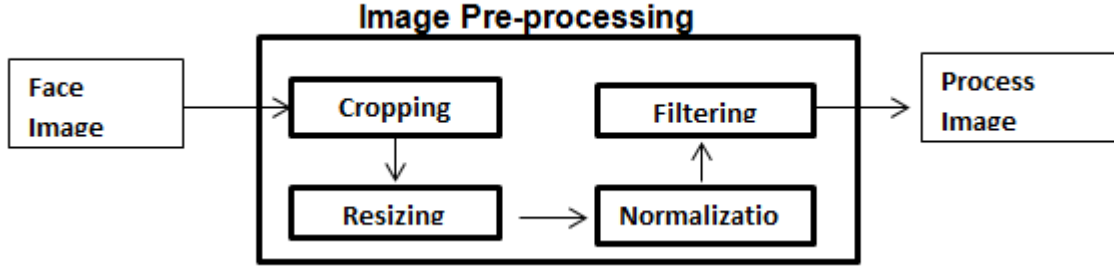


Figure 10: Pre-processing Approach [64]

Image Cropping: face cropping is one of the first important task which lead to achieving high recognition rate. The cropping was carried out with face detection technniques which are skin color model and geometric model,they invlove detecting face images using eigenfaces techniques to detect more different face features such as lips, nise and eyes.

Image Resizing: face images were resized using the nearest neighbor interpolation method. Cropping is the removal of the outer face image to improve framing, change aspects ration or accutuate subject matter.This process is determined by the specific size needed.

Image Normalization: images then go through normalization. It is the process that changes the range of pixel intensity values. This process is also called contrast stretching. Usually images with uncontrolled lighting conditions contain non-uniform contrast. Thus normalization would give a distribution of intensity or gray leves not to be alike. Therefore these levels are being made equal by using a histogram equalization techniques by using Cummulative Distribution function (CDF). Given M x N image, Cumulative Distribution Function (CDF) at each Pixel Value (PV) is used to find pixels equalization value (h) over L gray levels . Mathematically is given as [65],

$$h = \left(\frac{CDF(V) - CDFmin}{MXN - CDFmin} \right) (L - 1), \quad (3.1)$$

The cumulative distribution function can also be demonstrated by two different transformations: Continuous case and Discrete case. The histogram equalization can be by having a transformation function $T(r)$, which can be given by CDF of a given Probability Density Function of dim levels in a given image [66].

- i. Continuous Case: for intensive levels that continuous quantities normalised to the range of [0, 1].

Let $Pr(r)$ be the probability density function (PDF) of intensity level. Therefore work out the accompanying change on the information levels to obtain levels, s :

$$S = T(r) = \int_0^r P_{r(y)} dy \quad (3.2)$$

y –dummy variable of integration.

The probability density functions produces a uniform output levels[67]:

$$P_{s(s)} = \begin{cases} 1 & 0 \leq s \leq 1 \\ 0 & \text{otherwise} \end{cases}$$

Image, of which they produce equally intensity levels, and does cover the given range of [0,1]. By this transformation, it brings intensity levels equalization process which basically is just the total cumulative density function (CDF) [65].

- ii. Discrete Case (Quantities): Here the equalization transformations becomes:

$$S_k = T(r_k) = \sum_{j=1}^k P_r(r_j) = \sum_{j=1}^k \frac{n_j}{n}, \text{ for } k = 1, 2, \dots, L, \quad (3.3)$$

S_k -Intensity value of the output image corresponding to value r_k in the input image.

Image Filtering: images by default often have gaussian noise due to illumination variations and therefore it is necessary to de-noise basing on filtering techniques. Our dataset images used Low Pass Filter (LPF) to reduce high frequency information and to only retain low frequency.

Recognition Classifier

3.1.2 Face Feature extraction.

Principal Component Analysis (PCA) was utilized for face image vector extraction. PCA is the most intense dimensional diminishment tool which is ordinarily utilized in image processing especially particularly biometric recognition [68]. Principal Component Analysis is found to be a useful statistical technique that has found applications in fields such as recognition, image processing and classification with different classifying algorithms. It is a common technique used in feature extraction from data of high dimensional space. We used this technique to classify our face features using K-Nearest Neighbor (K-NN). We found PCA as an interesting tool for our study because of its high quality. it was also used for initial learning of images (training sets). The images were stored as the feature vectors in database which are projecting every trained image to the set of Eigen faces obtained. Principal Component Analysis is applied on the Eigen face approach to reduce the dimensionality of a larger data set.

Given a training set of images,

$T = \{T_x\}_{x=1}^C$ where $T_x = \{t_{xy}\}_{y=1}^{c_x}$, C is the number of classes, and $S = \sum_{x=1}^C C_x$ denotes the total number of images in the training set.

The covariance of the dataset can be computed as

$$S_{cov} = \sum_{y=1}^C \sum_{x=1}^{C_1} (txy - \bar{t}) - (txy - \bar{t}),^P \quad (3.4)$$

where $\bar{t} = \frac{1}{S} \sum_{x=1}^C \sum_{y=1}^{C_x} txy$ is the mean of set T . In the event that we introduce the chose eigenvectors utilizing network Φ , at that point each vector image Z_{xy} extracted from test data storage can be exchanged by linear mapping [69].

3.1.3 Finger Feature Extraction

Finger mark is the example of edges and valleys over the fingertip [70]. We introduced a basic version of the algorithm for finger classifying. Fingerprint images are stored in databases and we used its data sets. The fingerprint images were first pre-processed and we used Principal Component Analysis technique for image spacing to create a space of reduced images [63]. We used PCA as the fingerprint classification algorithm together with the K-NN. PCA improves the performance of the system and speed up the convergence of model training. Our proposed approach is in view of the utilization of fixed length unique fingerprint vector which will be fused with face feature vector using bayes networks.

3.2 Fusion of Features using Bayesian Networks

We used probabilistic inference to combine our biometric features. We specifically used Bayesen Netoworks to accomplish our method. Probabilistic inference was use in favour of bayesian networks. Probabilistic inference is a task of deriving the probability of one or more random variables taking specific values or set of values [45]. From probabilistic inference, we decided to be more specific and use Bayesian Networks. It is a belief network which belongs to probabilistic graphical models.

In our proposed model we have a list of assumptions based on fingerprint and face recognition. Face has more features hence we assume that eyes, mouth, nose and eyebrows provides enough discriminative information between the individuals. A lot of work has been put on place to insure that the discriminative information given is accurate as per many algorithms such as support vector machines (SVM), K-NN and EBG by Kim et al, [71]

Facial features are correlated. The Gaussian blend modules demonstrate covering pieces of face images are thought to be autonomous, consequently the probability of set of feature vectors is given as $\alpha = \{\alpha_1, \alpha_2, \dots, \alpha_T\}$

From the block is represented by [72]:

$$\int(\alpha|\Phi) = \prod_{t=1}^T P(\alpha_t|\Phi), \quad (3.5)$$

This is not always true because for example the block containing the right eye is related to the block containing the left eye.

To create an even more powerful model than the Gaussian mixture model, the horizontal mixture model can be applied. One dimensional horizontal mixture model (HMM) will consist of face images as sequence of horizontal strips which are extracted from the Gaussian mixture model that's why observation $\alpha = \{\alpha_1, \alpha_2, \dots, \alpha_T\}$ is unchanged. The likelihood will be given by the following equation for the ID-HMM [73].

$$\int(\alpha|\Phi) = \prod_{t=1}^T P(\alpha_t|\alpha_1, \Phi), \quad (3.6)$$

With the assistance of Bayesian Networks we planned a model equipped for encoding relationships between various features extricated images. Through perceptions we can consider that specific features are produced by some shrouded reason. The conclusion that can be drawn is that they are not completely independent. In this way the thought is that all the data is extricated from a similar face is created by a similar identity.

Hidden nodes make up discrete valued-nodes whereas observed nodes are multivariate Gaussians. Therefore the probability distribution of the nodes in the second level will be given by the likelihood table and the likelihood appropriation of perceptions will be given by the Gaussian distributors as follows [72]:

$$P(\beta = r | Pa(r) = i) = \frac{1}{(2\pi)^{\frac{n}{2}} |\Sigma_i|^{\frac{1}{2}}} \exp\left(-\frac{1}{2} (r - \mu_i)^T \Sigma_i^{-1} (r - \mu_i)\right) \quad (3.7)$$

Where $\beta = r$ stands for the characteristics of the observations and $Pa(r) = i$ for a is the possible configuration of the parent to the observation node and n is the dimension representing the value of the parent node. μ_i Represents the mean and the covariance matrix. Σ_i Represents the Gaussian distribution parameter which depends on the value the parent node. The parameter of the Bayesian networks to

be learned are represented by Φ and consists of entries of probability tables as well as μ_i , covariance matrix Σ_i of conditional Gaussian distribution.

To fit the model into an observed portrayal is done by figuring likelihood of the perceptions given the model. The variable observations discussed earlier would be:

$\alpha = (\text{Oreb}, \text{Oleb}, \text{Ore}, \text{On}, \text{Om})$. The probability of the distribution will be registered by first inducing the conveyance of shrouded factors utilizing the junction tree. The subsequent stage is enter the proof and in the inference algorithm, the joint likelihood dispersion over all variables.

3.2.1 The Chain Rule (Probability)

The chain rule also called the general product rule presents the estimation of any individual from a joint conveyance of an arrangement of arbitrary variables utilizing just conditional probabilities [72]. The Chain rule was applied in our study as it is useful to Bayesian networks (BN), which describe a probability distribution in terms of conditional probabilities.

Lets consider a listed arrangement of set $A, \dots, A_n$. To find the rule of this member of joint distribution, we can apply the definition of conditional product to obtain:

$$P(A_n, \dots, A_1) = P(A_n | A_{n-1}, \dots, A_1) \cdot P(A_{n-1}, \dots, A_1)$$

Repeating this process with each final term creates the product:

$$P(\cap_{k=1}^n A_k) = \prod_{k=1}^n P(A_k | \cap_{j=1}^{k-1} A_j) \quad (3.8)$$

With three variables, the chain rule produces this product of conditional probabilities:

$$P(A_3, A_2, A_1) = P(A_3 | A_2, A_1) \cdot P(A_2 | A_1) \cdot P(A_1)$$

We suppose this rule is used to compute our false acceptance rate (FAR), false reject rate (FRR) and error equal rate (EER) using the following scenario. In our

case we randomly selected three classes only from twenty classes used in our study from the images. Three classes are from both face and finger images. Suppose we randomly pick face class (A) and pick from finger class (B) and then select either true positive or false negative from either of the classes. Let event A be choosing first image $P(A) = P(\sim A) = 0.5$. Let the event B be the chance to choose the other class. The chance of choosing class A, given class B that we've chosen is $P(A|B)$. Event A would be the intersection which will determine our EER in our case. The probability can be found by the chain rule for probability:

$$P(A,B) = P(B|A)P(A)$$

As it was previously discussed in this chapter, the error equal rate determines the performance of biometrics systems against others and the lower the EER the better. It meets between FAR and FRR. For our finger given face, we calculate the EER to determine how it performs against single face values or single finger values.

3.2.2 Independence in Probability

In the theory of probability, two occasions factually autonomous or stochastically free [74] if one event is not dependent on another. It applies to where two random variables are independent if the realization of one does not affect the probability distribution of the other. The concept of independence event extends to dealing with collections of more than two variables, in which case the events are pairwise independent of each or independent of each other. Events are naturally independent if each is independent to each other. We demonstrated this rule in our study by first evaluating performance of fingerprint as a single biometric system using false acceptance rate (FAR), false reject rate (FRR) and error equal rate (EER), and we moved on to use this rule to independently evaluate the performance of face as single biometrics system using the same evaluation.

3.2.3 Conditional Independence Probability.

In theory of probability, two occasions A and B are restrictively independent tending a third occasion Y decisively if the event or non-event of A and the event or non-event of B are autonomous events in their contingent distribution tending Y[75].

Let's consider three variables as per our study (i.e. fingerprint, face and finger given face as conditional distribution). Fingerprint is denoted by variable a , face b and finger given face c . conditional distribution of a given b and c , is

$$P(a|b,c)$$

If $P(a|b,c)$ does not depend on value b ,

We can write $P(a|b,c) = P(a|b)$, we therefore say that a is conditionally independent of b given c .

3. 3 Performance Evaluation Metrics Approach

It is important to assess the performance of biometrics systems in both research and application of the technology. This section discusses methodologies for evaluating biometrics systems with a review of different performance statistics. Biometrics comprises of two general biometrics applications that are verification and identification (these were fully discussed in chapter 1). Biometrics systems more often than not include circumstances in which there are no power over conditions, for example, lighting, (e.g. indoor or open air, in radiant or amid day) and this additionally includes level of noise(e.g. in school or in an eatery areas). This uncontrollable environment of usage results in unstable performance of, and hence becomes a major factor in showing down the acceptance of biometric-based authentication. The execution of biometric frameworks is an essential issue not just in high security applications in government associations, similar to legal sciences in crime examination, yet additionally in business applications like portable gadgets [76].

3.3.1 False Accept Rate (FAR)

The false acceptance rate, or FAR, is the measure of the probability that the biometric security framework will fraudulently acknowledge an entrance endeavor by an unauthorized client. FAR is donated by:

$$FAR(n) = \frac{\text{imposter scores surpass the limit } n}{\text{all fraudulent scores } n}$$

Where n is an extraordinary character. The overall FAR of a biometric framework can be calculated by the following formula,

$$FAR(n) = \frac{1}{N} \sum_{n=1}^N FAR(n). \quad (3.9)$$

Where N represents all personalities being assessed by the system. The FAR represent a factual value, and consequently is reliant on the size N of the personalities against which the biometric system is tried and additionally the quantity of fake endeavors made [1].

3.3.2 False Rejection Rate (FRR)

It is the frequency at which a biometric system rejects genuine user access. In simpler terms, it means failing to correctly match the provided input with the stored template. The false rejection rate, or FRR, is the measure of the probability that the biometric security framework will inaccurately dismiss an entrance endeavor by an approved client. It is denoted in this formula,

$$FRR = \frac{\text{genuine scores below the limit}}{\text{all genuine scores made}}$$

The general overall FRR of a biometric framework can be computed by finding the average using the following formula,

$$FRR(n) = \frac{1}{N} \sum_{n=1}^N FRR(n). \quad (3.10)$$

Like the FAR, the FRR represents to a statistical value reliant on the size N of the characters against which the biometric framework is tried and in addition the quantity of verification endeavors made. In this scenario, N is represented by both finger and face data sets classes. We used FRR to detect the images that were falsely rejected

even though they belong to that particular class. Details of the usage of FRR are provided in (Chapter 4).

3.3.3 Genuine Accept Rate (GAR)

The Genuine Accept Rate is the recurrence at which the biometric framework acknowledges a genuine client as credible. It is identified with the FRR through the formula,

$$\text{GAR} = 1 - \text{FRR}$$

Much like FAR and FRR, GAR is an important formula for measuring the performance biometric systems.

3.3.4 Equal Error Rate (EER)

The Equal Error Rate is an algorithm used to predetermine the threshold value for FAR and FRR. It is the value on ROC bend where the FAR and FRR are equivalent. When the value of EER is low, the biometric system would be considered to have a high accuracy. We used EER to find the average between the false acceptance rate and false rejection rate. Datasets for face and finger were used for training and testing of fingerprint, face and face given finger.

EER can be computed in Receiver Operating Characteristics (ROC) curve as depicted in Figure 9, it's a graphical plot that illustrates the performance of a binary classifier system as discrimination threshold is varied.

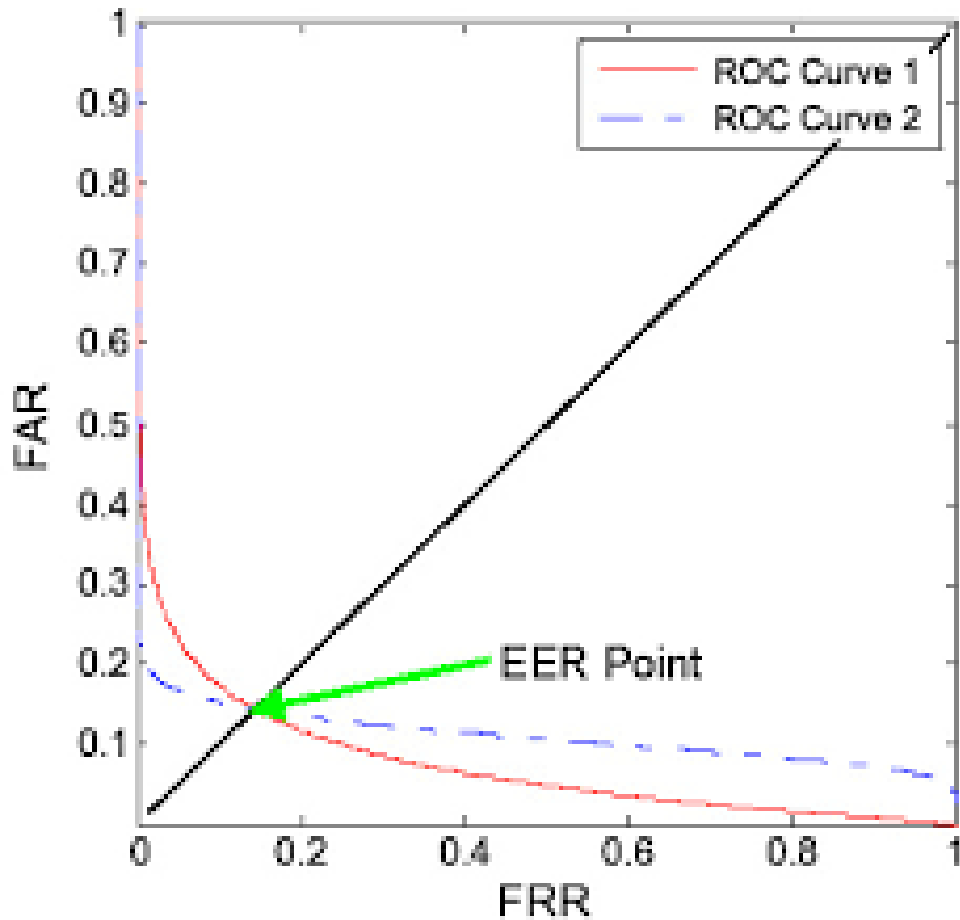


Figure 9: ROC curve indicating the Equal Error Rate (EER), where $EER = FRR = FAR$ [77]

The idea of Figure 9 is to measure the system performance against another system (the lower the better) by finding the equal (if not equal then at least nearly equal or have min distance) between false acceptance rate and false rejection rate (FRR, or missing rate).

CHAPTER FOUR

Presentation and Discussion of Results

4.1 Performance Analysis

This chapter of the dissertation outlines the evaluation of the proposed framework. The experiments were carried out to validate the proposed Framework as a proof of concept. The concepts to be proved in the framework have been discussed in the previous chapters; hence this chapter outlines the design of the experiments and the implications of those experiments.

4.2 Experiment Setup

The validation of the framework through the experiments was done on three sets of datasets (face datasets, finger dataset and the finger dataset given the face dataset). The coding of the experiments was performed on a dell machine that used the Intel i3 processor. The programming was done on MATLAB R2012b. The experiments were grouped into 3 categories; the face category in which the aim was to determine the false acceptance rate (FAR), false rejection rate (FRR) and finally the equal error rate (EER), next category was the fingerprint category and the final category was the fusion of the two categories using the probabilistic inference with the help Bayes network. To extract features for both face and finger Principal Component Analysis (PCA) was used as a primary feature extraction model that was embedded in our proposed framework. This feature extraction technique was used for both categories (i.e. face and finger). Figure 11 shows the features extracted by PCA from the face dataset. Data was trained and tested as shown in figure 11 below and was represented by the legend below;

Legend: * represents training data, ♦ represents testing data

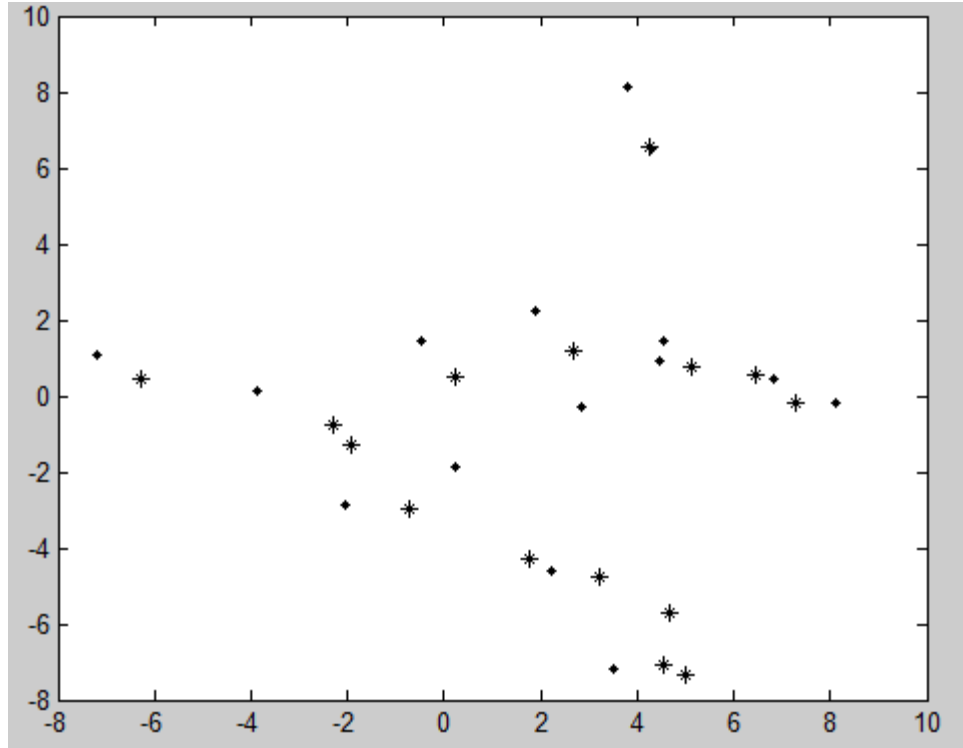


Figure 11: Principal component analysis feature extraction for face dataset

4.3 Face Analysis

From a set of 337 individuals from the Matrix Pie dataset we selected only 20 individuals for validating the framework. Each person has 20 images (totaling the number of images to 400). These images were divided into 2 groups of 10 where 10 of them were used as the training dataset and the rest were used as the testing dataset. The training dataset's main purpose was to extract features and estimate the location of the features. The testing data on the other hand, was used to ensure that the extracted features are at the right group. The KNN algorithm was implemented to make sure that the classification of the images according to their groups is correct. There are three measures that were obtained: the rate of false acceptance rate, false rejection rate and the equal error rate (as percentage). False acceptance rate ranges between 69 and 78, as shown in Figure 14. The false rejection rate ranges between 69 and 76. The equal error rate is around the same rate as both the FAR and FRR because EER is the average of the two. Figure 12

shows the results of training and testing the face dataset and each column represents the FAR, FRR and the EER, respectively. The error rate in actual fact ranged from 0.28 to 0.31 for both FAR, FRR and EER. As explained earlier there will be a total number of 20 classes (individuals) that were used to validate the model.

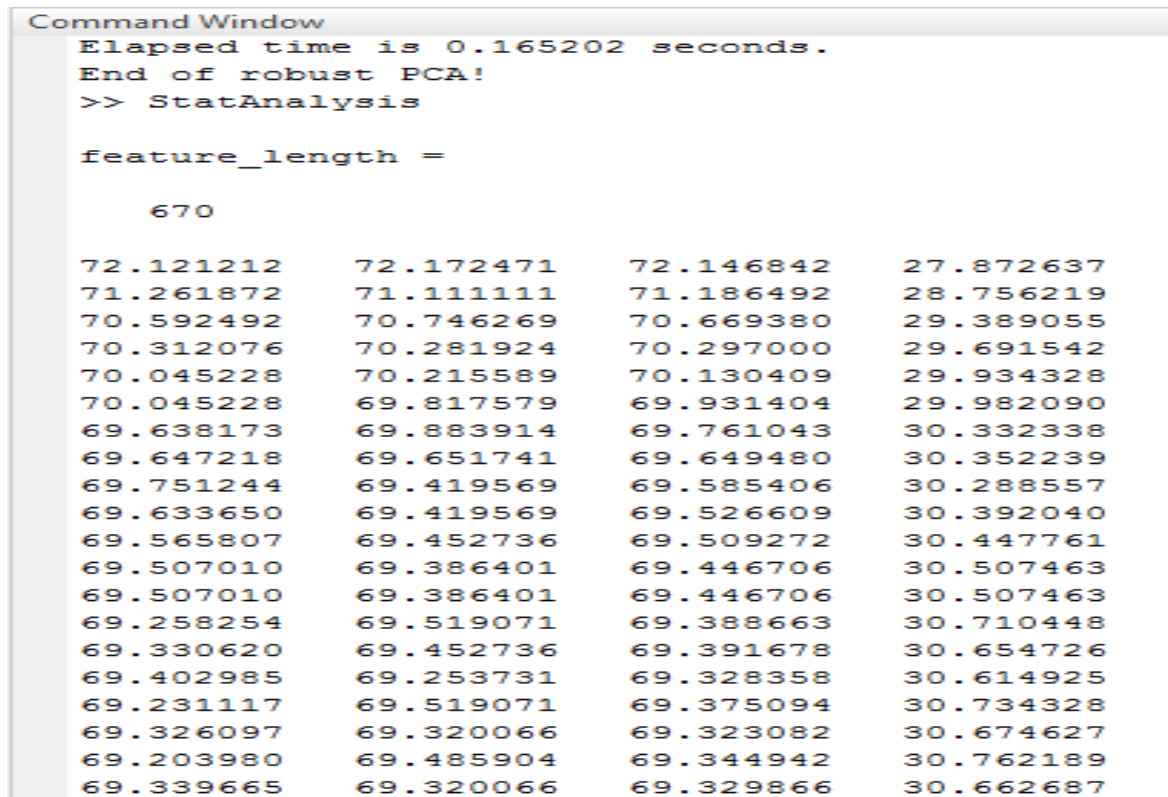


Figure 12: Total number of correctly classified images per class of face dataset pf 20 classes.

4.4 Fingerprint Analysis

The fingerprint dataset was a little different in terms of training and testing data. The data set had 20 individuals' fingerprints with only 10 images per person, which resulted in the total image count of about 200. Because of this difference had to adjust our training data size as well as the testing data size to 5. Hence the rate of false acceptance rate ranged between 80 and 81, the FRR ranged from 89 to 96 whereas the EER ranged between 85 and 89. Since the features in the fingerprint are mainly lines, the accuracy of the fingerprint will ultimately be higher than the

accuracy of face. Figure 13 shows the sample run of the fingerprint where the first column is the false acceptance rate for each of the 20 classes. The next column shows the false rejection rate whereas the next column represents the equal error rate.

```

^
End of robust PCA!
>> StatAnalysis

feature_length =

    670

96.352782    80.046434    88.199608    21.603980
94.263229    79.980100    87.121664    23.450746
93.023971    80.013267    86.518619    24.537313
92.047038    80.079602    86.063320    25.389055
91.486205    80.112769    85.799487    25.878607
90.988693    80.311774    85.650234    26.292537
90.622343    80.378109    85.500226    26.606965
90.265038    80.411277    85.338158    26.917413
89.998191    80.577114    85.287653    27.132338
89.686115    80.643449    85.164782    27.399005
89.459973    80.676617    85.068295    27.594030
89.292628    80.742952    85.017790    27.733333
89.156943    80.842454    84.999698    27.840796
89.030303    80.875622    84.952962    27.948259
88.872004    80.975124    84.923564    28.075622
88.758933    81.074627    84.916780    28.163184
88.645862    81.107794    84.876828    28.258706
88.568973    81.074627    84.821800    28.330348
88.478517    81.107794    84.793155    28.405970
88.388060    81.207297    84.797678    28.473632

```

Figure 13: The sample run of the fingerprint dataset of 20 classes of correctly classified images per class

4.5 Face Fused with Fingerprint

The fusion of the multimodal biometric system that has been performed, it is by using the Bayesian inference engine. The results of the fused Bayesian inference engine proved to have increased the accuracy significantly. The FAR of the fused biometric system ranged from 98 to 96, the FRR ranged between 96 and 99, which resulted in an increased EER (ranging between 98 and 99). The multimodal biometric training of this system ensured that for each class, the total percentage of wrongly classified images was between 1 and 2%.

4.6 Implications of fusion

The fusion of face and fingerprint has proved that the proposed framework will significantly increase the accuracy of either face only or finger only biometric system. The FAR of the multimodal biometric system proved it is higher which reflects that the falsely classified images in the entire data set are very low. If more features of face are misclassified the AND function will compensate for other errors. That is to say that, falsely rejected features have to be true for both face and finger resulting less rejected features. If the falsely rejected features are minimized the chances of misclassification are minimized hence there will be an increase in the accuracy of the framework. Figure 14 shows the FAR for face, finger and multimodal (finger given face).

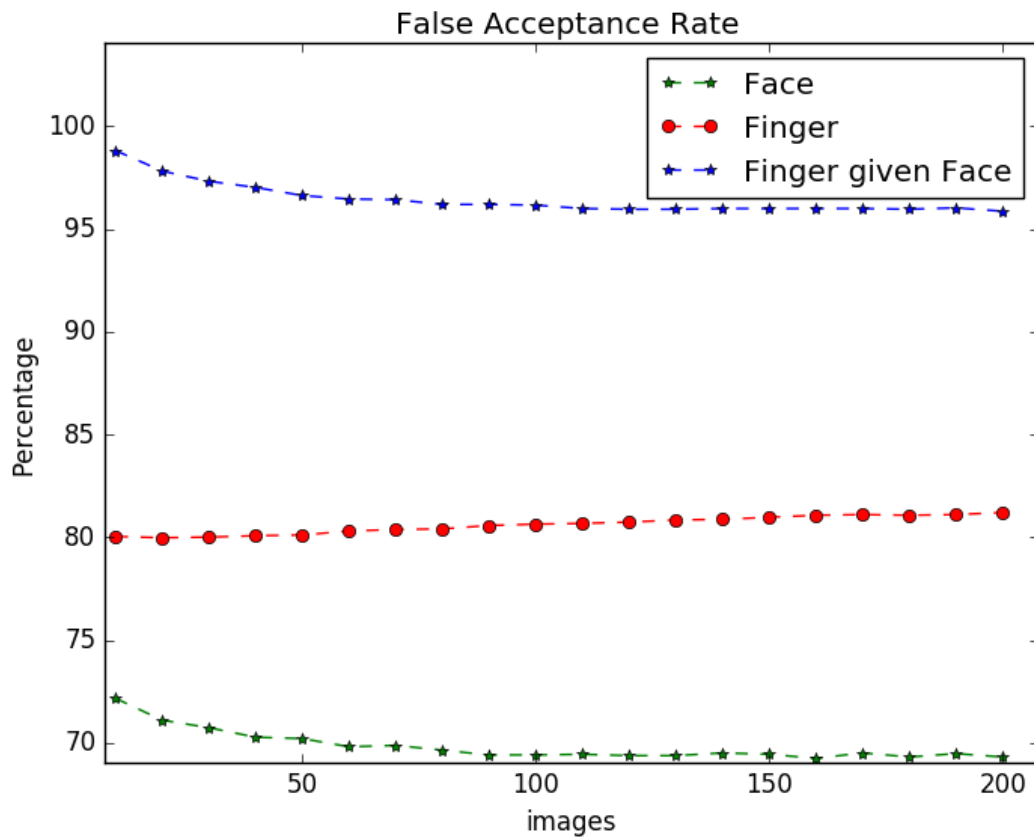


Figure 14: False Acceptance rate for Face dataset, Fingerprint dataset and multimodal biometric system.

To further explore the effects of fusion it is also necessary to explore the FRR, which is depicted by Figure 15. The purpose of the false rejection rate is to detect the images that were falsely rejected even though they belong to a particular class. The results show that the probability that the fingerprint will be correctly classified given that the image was correctly classified will be higher. The FRR of the fused system ranged between 96 and 99. This means that the FRR of the multimodal system ranges from 0.04 to 0.01. As explained earlier in the FAR the reason for this tremendous difference in the false rejection rate is because the face datasets has a lot of points of interest. All these points can be altered by a number of features such as pixel resolution (not enough pixels), face pose (face orientation), illumination and occluded facial areas. Due to these factors the face dataset training will yield only a less FRR as more images that do not belong to a certain class are accepted as a member of that class.

However, the points of interest in the fingerprint are mainly lines hence lines in image recognition are affected by few scenarios such as line orientation and line thickness hence the error of classification in these areas are very less hence the FRR of finger database will be higher as less features are needed for classification. To proof that the framework we proposed perform up to the standards required by the biometric community, it is very crucial that we also compare the equal error rate of both the finger and the face datasets.

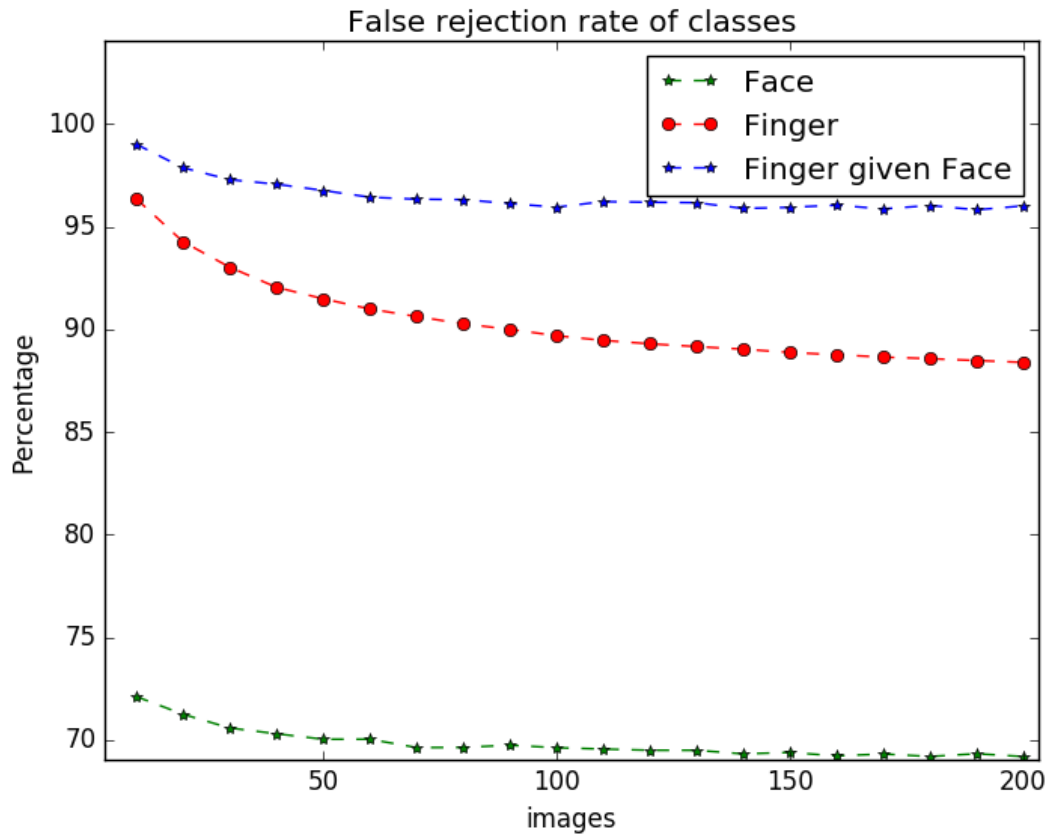


Figure 15: False Rejection Rate for Face dataset, Fingerprint dataset and multimodal biometric system.

Figure 16 shows the equal error rate that was explained in details in Chapter Three. The EER is measured at each class to determine the error equal rate per class, hence all the systems (single or multimodal biometrics systems) were used to determine the differences in the error equal rate and determine which method amongst either the multimodal or single biometric can yield a better result in terms of error equal rate. The face dataset training yielded the worst record in terms of error equal rate for the same reasons as explained earlier in this chapter. The same thing applied to the fingerprint dataset training, which will then yield the better results than the face data sets for the same reason as explained in the section of the false rejection rate. The most interesting part is to understand what impact the EER rate will have in single biometric and multimodal biometric system. The distribution of finger given face dataset yielded better results because the face

classes was determined then the AND function on the Bayesian network ensured that features in the face dataset were reduced hence the classification accuracy increased predominantly.

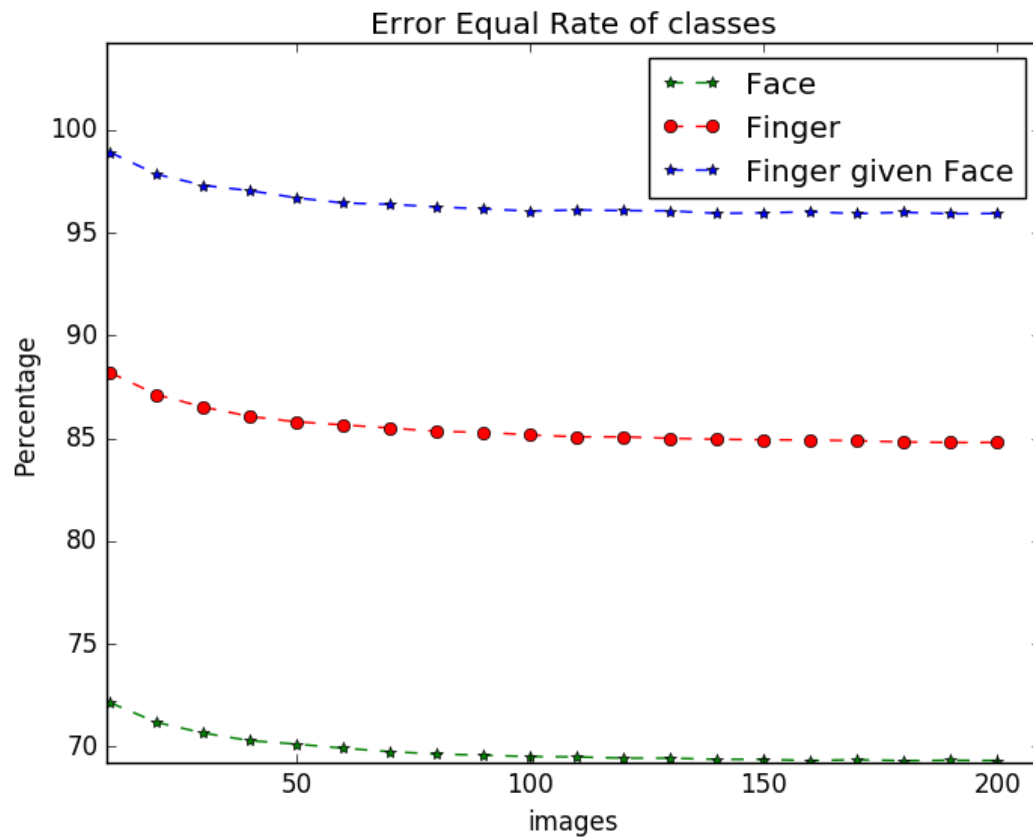


Figure 16: The Error equal rate of Face, Finger and fused (face + finger) dataset

CHAPTER FIVE

Conclusion

5.1 Conclusion

This thesis dealt with a broad topic of biometric recognition, which was then narrowed down to focus particularly on improving the security and accuracy of multimodal biometrics templates. Multimodal biometrics have been generally embraced in an assortment of large and little scale applications, for example, border post control, access controls and criminal investigations.

First, current existing approaches were reviewed with emphasis made on fusing two different biometrics modalities (face and fingerprint images since they have proven to be successful by different researches). However, even though so many approaches have been taken to improve the performance of biometrics systems, there are still gaps that needed to be improved using different technologies. The fused biometrics modalities proved to give a better performance as compared to a single biometrics system.

We thus proposed a new framework or an approach, based on Bayesian Networks (BN), especially dedicated to handle both fingerprints and face traits. The framework proposed therefore extends the concept of general multimodal biometrics frameworks, which needed to be improved. There are lots of factors considered before coming up with the relevant modalities to choose from through literature. The motivation for our choice of modalities, face and fingerprint was found by the wide use of the biometrics traits.

Our framework adopted the existing process of multimodal biometrics and hence applied Principal Component Analysis (PCA) and Bayesian Network (BN). The findings success of our thesis proved in terms of performance based on accuracy, our results shows a very good improvement of 0.01 Error Equal Rate (EER) and this comes from fused fingerprints with face images. There are a number of the key contributions of the thesis which can be summarized as follows:

- ❖ Our research framework was adopted from the general multimodal biometrics scheme.
- ❖ We developed a framework basing on the results fusion between face and fingerprints images using specifically probabilistic inference and we use the probability of finger given fac. With our BN we used fingerprints only, face and finger given face as our network classes as it is demonstrated in our chapter four. Our results demonstrated the feasibility and good performance of our approach by means of experiments and comparison with other approaches.

We started by running fingerprints datasets which gave an accuracy of 96%. While running our test, it has proven that finger prints gives a better accuracy results as compared to face because of feature factors, which are mainly lines hence gives better results. Face data was run as a single biometrics as well and it gave a bit low accuracy rate of 72% as compared to fingerprint results. This was mainly because face have so many features and the preprocessing take much longer hence reducing the accuracy rate.

We further ran our results to find the performance of fused face and fingerprint images which drastically gave us very promising results of 0.01 of Error Equal rate and accuracy rate of up to 99%. This proves our thesis gave a good results and it improved the results of a single biometrics systems. To the end we proposed a framework for multimodal biometrics security which fuses face and fingerprint images which improved authentication accuracy. We can also conclude that the obtained performance of recognition is better or improved from there results reported in literature, this is despite the use of Bayesian Network as our novel development. The execution of the displayed system was tentatively assessed utilizing two chimeric data storage.

REFERENCES

- [1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," vol. 14, no. 1, pp. 4–20, 2004.
- [2] S. Phadke, "The Importance of a Biometric," vol. 1, no. 4, pp. 128–132, 2013.
- [3] D. Shobha, "Biometric Cryptosystems : for User," pp. 4322–4326, 2015.
- [4] A. Jain, U. Uludag, and A. Ross, "Biometric Template Selection : A Case Study in Fingerprints," pp. 335–342, 2003.
- [5] U. Uluda, C. Researcher, and U. Manager, "Biometric Systems," 2014.
- [6] A. Annis Fathima, S. Vasuhi, T. M. Treesa, N. T. Naresh Babu, and V. Vaidehi, "Person authentication system with quality analysis of multimodal biometrics," *WSEAS Trans. Inf. Sci. Appl.*, vol. 10, no. 6, pp. 179–194, 2013.
- [7] D. Kaur, "Level of Fusion in Multimodal Biometrics : a Review," vol. 3, no. 2, pp. 242–246, 2013.
- [8] J. Wayman, A. Jain, D. Maltoni, and D. Maio, "An Introduction to Biometric Authentication Systems 1," pp. 1–20.
- [9] I. Kaur, N. Mann, and B. Verma, "Biometric Authentication in Computer Security," vol. 8491, pp. 58–62, 2016.
- [10] S. T. Fleming, "Biometrics Security," *IGI Glob.*, no. Figure 1, p. 6, 2005.
- [11] S. Patil, "Biometric Recognition Using Unimodal and Multimodal Features," pp. 6824–6829, 2014.
- [12] P. A. Kumari, G. J. Suma, A. Pradesh, and A. Pradesh, "A NOVEL MULTIMODAL BIOMETRIC SCHEME FOR PERSONAL AUTHENTICATION," vol. 2, no. 2, pp. 55–66, 2014.
- [13] M. C. Reddy, A. Pradesh, and A. Pradesh, "Biometric Quality on Finger , Face and Iris Identification," pp. 545–552.

- [14] A. H. Mir, C. Engineering, S. Rubab, and Z. A. Jhat, "Biometrics Verification : a Literature Survey," vol. 5, no. 2, pp. 67–80, 2011.
- [15] M. Abdolahi, M. Mohamadi, and M. Jafari, "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic," *Int. J. Soft Comput. Eng.*, vol. 2, no. 6, pp. 504–510, 2013.
- [16] A. Jagadeesan, T. Thillaikkarasi, and K. Duraiswamy, "Cryptographic Key Generation from Multiple Biometric Modalities : Fusing Minutiae with Iris Feature," vol. 2, no. 6, pp. 16–26, 2010.
- [17] K. Sasidhar, V. L. Kakulapati, K. Ramakrishna, and K. KailasaRao, "Multimodal Biometric Systems - Study to Improve Accuracy and Performance," *J. Comput. Sci.*, vol. 1, no. 2, p. 8, 2010.
- [18] P. Tigga and A. Wanjari, "A Survey on Template Protection Scheme for Multimodal Biometric System," vol. 4, no. 7, pp. 768–772, 2015.
- [19] G. Kaur, S. Bhushan, and D. Singh, "Fusion in Multimodal Biometric System : A Review," vol. 10, no. July, pp. 1–10, 2017.
- [20] V. Sireesha and S. Reddy, "Two Levels Fusion Based Multimodal Biometric Authentication Using Iris and Fingerprint Modalities," *Int. J. Intell. Eng. Syst.*, vol. 9, no. 3, pp. 21–35, 2016.
- [21] A. Dhanalakshmi, G. Arts, E. District, T. Nadu, F. Sensor, and F. Extraction, "Improved Person Identification System using Face Biometric Detection," vol. 1736, pp. 1731–1736, 2013.
- [22] S. Dutta, "Striking a balance between usability and cyber-security in IoT devices," no. May, 2017.
- [23] D. T. Meva, "Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication," vol. 66, no. 19, pp. 16–19, 2013.
- [24] R. Shyam and Y. N. Singh, "Identifying Individuals using Multimodal Face

- Recognition Techniques,” *Procedia - Procedia Comput. Sci.*, vol. 48, no. lccc, pp. 666–672, 2015.
- [25] G. Rajagopal and R. Palaniswamy, “Performance Evaluation of Multimodal Multifeature Authentication System Using K NN Classification,” vol. 2015, 2015.
- [26] C. Sunil, R. Maheshewari, and U. B. Shinde, “Review paper on applications of principal component analysis in multimodal biometrics system,” *Procedia - Procedia Comput. Sci.*, vol. 92, pp. 481–486, 2016.
- [27] M. Madane and S. Thepade, “Score Level Fusion Based Bimodal Biometric Identification Using Thepade ’ s Sorted n-ary Block Truncation Coding with varied Proportions of Iris and Palmprint traits .,” *Procedia - Procedia Comput. Sci.*, vol. 79, pp. 466–473, 2016.
- [28] S. N. Garg, R. Vig, and S. Gupta, “A Survey on Different Levels of Fusion in Multimodal Biometrics,” vol. 10, no. November, pp. 1–11, 2017.
- [29] W. Zhao, R. Chellappa, P. J. Phillips, and a Rosenfeld, “Face recognition: A literature survey,” *Acm Comput. Surv.*, vol. 35, no. 4, pp. 399–458, 2003.
- [30] S. Ribari, D. Ribari, and N. Paveši, “A BIOMETRIC IDENTIFICATION SYSTEM BASED ON THE FUSION OF HAND AND PALM FEATURES Faculty of Electrical Engineering , University of Ljubljana , Slovenia,” pp. 3–6.
- [31] S. Sakthivel, “Enhancing Face Recognition Using Improved Dimensionality Reduction and Feature Extraction Algorithms – an Evaluation With Orl Database,” *Int. J. Eng. Sci.*, vol. 2, no. 6, pp. 2288–2295, 2010.
- [32] S. Balakrishnama and a Ganapathiraju, “Linear Discriminant Analysis - a Brief Tutorial,” *Compute*, vol. 11, pp. 1–9, 1998.
- [33] S. K. S. Singh, M. P. Singh, D. Singhtise, and D. K. Singh, “A survey on network security and attack defense mechanism for wireless sensor networks,” *Int. J. Comput. Trends Technol.*, vol. 1, no. 2, pp. 9–17, 2011.

- [34] P. De Carrera, "Face Recognition Algorithms," *Master's thesis Comput. Sci. Univ. ...*, pp. 9–10, 2010.
- [35] L. Wiskott, J. M. Fellous, N. Krüger, and C. Von der Malsburg, "Face recognition by elastic bunch graph matching," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1296, no. July 1997, pp. 456–463, 1997.
- [36] T. Ahonen, S. Member, A. Hadid, and M. Pietik, "Face Description with Local Binary Patterns : Application to Face Recognition," no. June 2006, pp. 1–15.
- [37] Z. Guo, L. Zhang, and D. Zhang, "A completed modeling of local binary pattern operator for texture classification.," *IEEE Trans. Image Process.*, vol. 19, no. 6, pp. 1657–1663, 2010.
- [38] A. Jagadeesan and K. Duraiswamy, "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris," *Int. J. Comput. Sci. Inf. Secur.*, vol. 7, no. 2, pp. 028–037, 2010.
- [39] "Embryologic development of epidermal ridges and their configurations Embryologic Development of Epidermal Ridges," no. February 1991, 2016.
- [40] M. Kücken and A. C. Newell, "Fingerprint formation," *J. Theor. Biol.*, vol. 235, no. 1, pp. 71–83, 2005.
- [41] G. Iwasokun and S. Ojo, "Review and Evaluation of Fingerprint Singular Point Detection Algorithms," *Br. J. Appl. Sci. Technol.*, vol. 4, no. 35, pp. 4918–4938, 2014.
- [42] U. Rajanna, A. Erol, and G. Bebis, "A Comparative Study on Feature Extraction for Fingerprint Classification and Performance Improvements Using Rank-Level Fusion," pp. 1–21.
- [43] S. Nath, "Classification of fingerprints," *Pers. Identif. through fingerprints*, pp. 31–45, 2006.

- [44] Y. Yao *et al.*, “Combining at and structured representations for fingerprint classification with recursive neural networks and support vector machines,” *Pattern Recognit.*, vol. 36, pp. 397–406, 2003.
- [45] C. T. Hsieh, S. R. Shyu, and K. M. Hung, “An effective method for fingerprint classification,” *Tamkang J. Sci. Eng.*, vol. 12, no. 2, pp. 169–182, 2009.
- [46] “A Fuzzy Neural Network Fault Diagnostic System,” vol. 94, no. 1, pp. 9–13, 2014.
- [47] W. Wei, Z. Yang, and S. Wang, “Fingerprint Classification by Directional Fields.pdf,” no. 5, pp. 0–4, 2002.
- [48] S. Shah and P. S. Sastry, “Fingerprint Classification Using a Feedback-Based Line Detector,” vol. 34, no. 1, pp. 85–94, 2004.
- [49] N. Friedman and M. Goldszmidt, “Learning Bayesian networks with local structure,” *Learn. Graph. Model.*, pp. 421–459, 1998.
- [50] M. Scutari and R. Ness, “Bayesian Network Structure Learning, Parameter Learning and Inference,” 2018.
- [51] U. B. Kj, “Probabilistic Networks for Practitioners — A Guide to Construction and Analysis of Bayesian Networks and Influence Diagrams,” no. October, 2006.
- [52] M. Faizan, Z. Haque, and M. A. Ansari, “Characterizations of Distributions by Expected Values of Lower Record Statistics with Spacing,” *J. Mod. Appl. Stat. Methods*, vol. 16, no. 2, pp. 310–321, 2017.
- [53] J. R. Koiter, “Visualizing Inference in Bayesian Networks,” p. 125, 2006.
- [54] L. O. Gorman, “Comparing Passwords , Tokens , and Biometrics for User Authentication,” vol. 91, no. 12, pp. 2019–2040, 2003.
- [55] M. El-Abed, R. Giot, B. Hemery, J.-J. Schwartzmann, P. Lacharme, and C. Rosenberger, “Towards the Security Evaluation of Biometric Authentication Systems,” *Proc. 2011 Int. Conf. Secur. Sci. Technol. (ICSST 2011)*, vol. 4, no. 3, pp. 1–7, 2011.

- [56] L. An, M. Kafai, and B. Bhanu, "Dynamic bayesian network for unconstrained face recognition in surveillance camera networks," *IEEE J. Emerg. Sel. Top. Circuits Syst.*, vol. 3, no. 2, pp. 155–164, 2013.
- [57] N. Poh and S. Bengio, "A Score-Level Fusion Benchmark Database For Biometric Authentication," 2003.
- [58] K. Nandakumar and A. Dissertation, "Multibiometric systems: Fusion strategies and template security," 2008.
- [59] N. D. Sarier, "Biometric Cryptosystems : Authentication , Encryption and Signature for Biometric Identities Dissertation Mathematisch-Naturwissenschaftlichen Fakultät Rheinischen Friedrich-Wilhelms-Universität Bonn Neyire Deniz Sarier aus," 2011.
- [60] J. Muncaster and M. Turk, "Continuous Multimodal Authentication Using Dynamic Bayesian Networks."
- [61] A. M. Abdullah, R. Hikmat, and H. Aziz, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm," *Int. J. Comput. Appl.*, vol. 143, no. 4, pp. 975–8887, 2016.
- [62] I. A. Journal and I. Technology, "rs Fi t O in nl e P lic at," no. April, 2015.
- [63] B. Fu, S. X. Yang, J. Li, and D. Hu, "Multibiometric cryptosystem: Model structure and performance analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 4, pp. 867–882, 2009.
- [64] M. Kumar, "Digital Image Processing," *Satell. Remote Sens. GIS Appl. Agric. Meteorol.*, vol. 24, pp. 81–102, 2004.
- [65] L. Lu, Y. Zhou, K. Panetta, and S. Agaian, "Comparative study of histogram equalization algorithms for image enhancement," vol. 7708, p. 770811, 2010.
- [66] Q. For and N. Using, "M Odified H Istogram E Qualization for I Mage C Ontrast E Nhancement Using P Article," vol. 1, no. 5, pp. 13–27, 2011.

- [67] F. Edalat, "NIH Public Access," vol. 40, no. 6, pp. 1301–1315, 2012.
- [68] N. H. Barnouti and W. E. Matti, "Face Detection and Recognition Using Viola-Jones with PCA-LDA and Square Euclidean Distance," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 5, pp. 371–377, 2016.
- [69] J. Gunawardena, "Matrix algebra for beginners, Part II linear transformations, eigenvectors and eigenvalues," pp. 1–16, 2006.
- [70] S. Bhattacharya, "Fingerprint Recognition Using Global and Local Structures," vol. 3, no. 1, pp. 161–172, 2011.
- [71] J. Kim, B. Kim, S. Savarese, and A. Arbor, "Comparing Image Classification Methods : K-Nearest-Neighbor and Support-Vector-Machines," pp. 133–138.
- [72] G. Chetty and M. Wagner, "A Robust Spatio-temporal Face Modelling Approach Using 3D Multimodal Fusion for Biometric Security Applications," vol. 6944, pp. 1-5 BT-Proceedings of the SPIE 0277-786X, v.694, 2008.
- [73] R. Mattila, *Hidden Markov models: Identification, control and inverse filtering*. 2017.
- [74] "Introduction to Probability Theory and Statistics," pp. 2004–2008, 2008.
- [75] M. Strevens, "Stochastic Independence and Causal Connection." pp233- 294, 2015.
- [76] W. Cui, "A Scheme of Human Face Recognition in Complex Environments," p. 87, 2014.
- [77] K. A. Toh, J. Kim, and S. Lee, "Maximizing area under ROC curve for biometric scores fusion," *Pattern Recognit.*, vol. 41, no. 11, pp. 3373–3392, 2008.

List of Appendices

APPENDIX A

An algorithm for fused face and fingerprint using Bayesian Networks and Inference Engine

APPENDIX A.1: FUSED FINGER AND FACE

1. %K-Nearest-Neighbor-Classifer MatLab Code
2. function PredictedLabels=knn(k,TrainPattern,TrainLabel,TestPattern)
3. %k-nearest neighbor classifier
4. %Determines distances of all TrainPattern points from TestPattern points
5. %Outputs TrainLabel associated with nearest TrainPattern point
6. [rowTest,colTest]=size(TestPattern);
7. K=40;
8. M = moviein(K);
9. for row=1:rowTest(1,1)
10. S=size(TrainPattern);
11. N=S(1,1);

```
12. d=zeros(N,1);%creates specified space for distance column vector

13. hold off%releases previous plot

14. plot(TestPattern(row,1),TestPattern(row,2),'r*')%begins and holds new plot

15. title('Train Pattern Scatter Plot')

16. hold on

17. for i=1:N%creates distance column vector with N rows

18. x1=TrainPattern(i,1);

19. x2=TestPattern(row,1);

20. x=(x1-x2)^2;

21. y1=TrainPattern(i,2);

22. y2=TestPattern(row,2);

23. y=(y1-y2)^2;
```

```

24. d(i,1)=sqrt(x+y);

25. if TrainLabel(i,1)>0.5%creates scatter plot of train patterns with labels

26. plot(TrainPattern(i,1),TrainPattern(i,2),'bh')

27. else

28. plot(TrainPattern(i,1),TrainPattern(i,2),'kh')

29. end

30.end

31.M(:,row) = getframe(gcf);

32. legend('Test Pattern','Train Patterns and Labels',-1)

33. [cldvalues,clIndx]=sortrows(d);%determines closest distances and their indices

34. for j=1:N

35. CLTrainLabels(j,1)=TrainLabel(clIndx(j,1),1);

36. end

```

```
37. Closest_Train_Labels=CLTrainLabels(1:k(1,1),1);%displays "kth" closest labels

38. for r=1:k(1,1)

39. if Closest_Train_Labels(r,1)>0.5

40. PredictedLabels(r,1)={'Blue'};

41. else

42. PredictedLabels(r,1)={'Black'};

43. end

44. end

45. PredictedLabels

46. pause

47. end

48. disp('Creating AVI file...')
```

```
49. movie2avi(M,'k_classifier.avi','compression','Indeo5','FPS',1,'VideoName','k-  
nearest-neighbors');
```

```
50. disp('Done!')
```

```
51.
```

APPENDIX B.2: INFERENCE

The following source code is used for inference:

```
1. clear; close all; clc;
```

```
2. % Prior parameters
```

```
3. a = 9;
```

```
4. b = 15;
```

```
5. % Data
```

```
6. N = 10;
```

```
7. X = 9;
```

```
8. theta = linspace(0,1,100);
```

```
9. Y_prior = betapdf(theta,a,b);
```

```
10. Y_likelihood = nchoosek(N,X)*(theta.^X).*(1-theta).^(N-X);
```

```
11. Y_posterior = betapdf(theta,a+X,b+N-X);
```

```
12. h = figure(1);
```

```
13. subplot(3,1,1),
```

```
14. plot(theta,Y_prior,'LineWidth',3)
```

```
15. title('Prior','FontSize',20)
```

```
16.set(gca,'FontSize',20)
17.ylabel('pdf')
18.subplot(3,1,2),
19.plot(theta,Y_likelihoood,'m','LineWidth',3)
20.set(gca,'FontSize',20)
21.title('Likelihood','FontSize',20)
22.ylabel('likelihood')
23.subplot(3,1,3),
24.plot(theta,Y_posterior,'r','LineWidth',3)
25.title('Posterior','FontSize',20)
26.ylabel('pdf')
27.set(h,'Position',[1000 150 900 900])
28.set(gca,'FontSize',20)
29.xlabel('Theta')
```