004
G09

T330

Verification of Identity Using Multimodal Biometric Fusion

A thesis submitted in partial fulfillment of the requirements for award of the degree of Doctor of Philosophy

Minakshi Gogoi
Registration No. 009 of 2014

School of Engineering
Department of Computer Science & Engineering
Tezpur University
September 2014

"TO KNOW WHAT YOU KNOW
AND KNOW WHAT YOU DON'T KNOW
IS THE CHARACTERISTIC OF ONE WHO KNOWS
AND IS A TRUE KNOWLEDGE"

- CONFUCIUS

DEDICATED

To

My sons Dhritiraj & Deboprit

Acknowledgement

I would like to express a deep sense of thanks and gratitude to my research guide Prof. Dhruba Kr. Bhattacharyya of Tezpur University for his guidance and personal supervision in an atmosphere of dignity and confidence and extending all kinds of help. He always evinced keen interest in my work.

I take this opportunity to express my appreciations to all the members of my doctoral research committee and other faculty members for their constructive suggestions through out the research work. My sincere thanks go to Prof. S. M. Hazarika, Head, Department of computer Science & Engineering for his coordination in extending every possible facilities for the completion of this work. I am grateful to all the technical and non-technical members of the Department for their support.

I am also grateful to GIMT, Azara, Guwahati, for providing me the opportunity to carry out the research work.

I am also highly indebted to my parents, husband and my loving sons Dhritiraj & Deboprit for their extreme support to carry out the work and my co-sisters who find great pleasure in my success.

Last but not the least; I would like to thank all those who had helped directly or indirectly towards the completion of this research and the almighty for everything.

Minakshi Gogoi

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING
TEZPUR UNIVERSITY

NAPAAM, TEZPUR - 784028

CERTIFICATE

This is to certify that the thesis entitled *"Verification of Identity Using Multimodal Biometric Fusion"* submitted by Minakshi Gogoi, bearing Registration No. **009 of 2014** to Tezpur University in the Department of Computer Science and Engineering under the school of Engineering in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science and Engineering has been examined by us on .....25/3/15........ and found to be satisfactory.

The committee recommends for award of the degree of Doctor of Philosophy.

Signature of

Nabendu Chaki
25/3/15

Principal Supervisor

External Examiner

Date : 25/3/15

Department of
Computer Science and Engineering
Tezpur University
NAPAAM, TEZPUT - 784028

CERTIFICATE

This is to certify that the thesis entitled *"Verification of Identity Using Multimodal Biometric Fusion"* submitted to the Tezpur University in the Department of Computer Science and Engineering under the school of Engineering in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science and Engineering is a record of research work carried out by Minakshi Gogoi, bearing Registration No. **009 of 2014** under my supervision and guidance.

The thesis as a whole or part thereof is not submitted to any other University or institutions for the award of any degree or diploma.

I wish her all success in life.

Signature of Research Supervisor

(Dhruba Kumar Bhattacharyya)
Designation : Professor
School : Engineering
Department : Computer Science and Engineering

DECLARATION

I hereby declare that the research work entitled **"Verification of Identity Using Multimodal Biometric Fusion"** submitted to the Tezpur University in the Department of Computer Science and Engineering under the school of Engineering is based on bona fide work carried out by me and no part of this thesis has been submitted for the award of any other degree or diploma.

(Minakshi Gogoi)

Date : 23/01/2015

CONTENTS

List of Figures

List of Tables

Abstract

Biometric is the science and technology of measuring and analyzing data related to human characteristics and traits, that may be physiological or behavioral. The candidate biometric modalities include iris, fingerprint, faces, palmprint, keystrokes, signatures etc.

Biometric system may be of two types: single modal systems and multiple modal systems. Single modal systems perform person recognition ,based on a single biometric modality and are affected by problems like noisy sensor data, intra-class variations, distinctiveness and non-universality. A multimodal system,that combines evidence from multiple biometric modalities can alleviate those problems of single modal ones.

Consolidating evidence obtained from multiple biometric traits, known as fusion, is a critical part in multiple modal systems, and it may be integrated at several levels like feature level fusion, matching score level fusion and decision level fusion. Among biometric modalities, iris, fingerprint and palmprint are more secure and hence make it more feasible to apply a multi-modal identification system based on these traits for security applications. Therefore, this dissertation proposes an algorithm of fingerprint recognition and explored the effectiveness of other biometric traits like iris and palmprint. In addition, a novel decision level fusion approach has been developed that can dynamically select the number of modalities, which have been tested by a virtual multimodal database and proved to be more reliable and robust than systems that rely on a single modality.

Chapter 1

INTRODUCTION

With the rapid rise in the ubiquity and the sophistication of computer and communication technology, the demand for reliable, simple, flexible and secure system has been increasing tremendously. The increasing growth of technical skill of the enemies and criminals poses several challenging issues for network applications attempting to render services to only enrolled users. The traditional methods of establishing a person's identity uses knowledge-based security like passwords. However, it suffers from several serious limitations. Biometric is a measure to identify an individual based on his or her physiological or behavioral characteristics and is capable of distinguishing reliably an authorized person from an imposter. It is considered to be an efficient means of remedying the various problems arising from the traditional authentication means.

1.1 Research Background

Identity verification or identity proofing is a process used to confirm the identity of a person in instances when the person is not able to show his or her identity. Identity verification is a real-time, electronic process that validates the information provided by a person. Based on the level of assurance needed, there are several levels of identity verification. For example, sometimes it is needed to confirm that an identity is real and there are no fraud flags associated with it. Or, in some instances high assurance is needed that someone is who they say they are. Identity verification can be used in any situation where it is not possible to check a customer's ID in person. Many organizations use identity verification to confirm consumer identities online or authorizing any account change activity.

Password – based systems and its demerits : An authentication system must be simple, cost effective, efficient and socially acceptable. The password-based system is *the cheapest and simplest technology as it requires elementary software resources.* In traditional password-based system, effective passwords are traditionally characterized by a long and alternated sequence of numbers and symbols. Therefore, they are often found difficult to remember. Moreover, most password-based systems are found vulnerable, and can be compromized by mounting a careful online or offline dictionary attack, or by extracting the information to the person itself. Regardless of their authentication type, passwords also can be shared. Hence, with the traditional password-based system some times, it becomes difficult to ensure the certainty of the actual user of the system.

Biometrics and its significance : A biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological or behavioral characteristic possessed by the person. Significance of a generic biometric system are their security, accountability and convenience.

- Security : Biometric systems offer a high degree of security than typical password-based authentication method, since biometric characteristics cannot be guessed or stolen. Also, biometric characteristics are not shared.

- Accountability: A biometric-based recognition system is able to keep track of the user's activities, e.g., it is possible to know who has been doing what, at a given time.

- Convenience: Biometric system can be used to simplify verification process where access privileges are necessary. Instead of possessing multiple tokens or passwords, a single biometric characteristic can be sufficient to confirm the identity of a person.

Base on the application, a biometric system can operate in two modes: (i) Verification-there is a one to one comparison of a captured biometric with a stored template to verify the individual identity. It involves the process of accepting or rejecting the claimed identity. Major applications are in smart card deployment. (ii) Identification-a one-to-many comparison of the captured biometric against a biometric database to identify an individual.

Identity verification using biometric measures : A generic identity verification system, using biometric measure(or measures)have five components, namely (i)sensor, (ii)feature extractor, (iii)template database, (iv)matching module and (v)decision module. Figure 1-1 depicts the basic modules in the schematic diagram of a biometric system.

- Sensor: A sensor scans the biometric trait of a user and it is the interface between the user and the verification system.
- Feature extractor : Feature values are extracted by processing the data acquired from the sensor module.
- Template database : A repository of prototype biometric trait of the legitimate users of the verification system.
- Matching module : It is responsible for generation of a score based on matching between the candidate biometric trait(s) and the prototype traits(s).
- Decision module : It is responsible to provide the final decision (accept/reject)based on the respons(es) given by the matching module.

A major advantage of using biometrics in verifying identity of a person is that the information are unique for each individual and that it can identify the individual in spite of significant variations over time. In addition to that biometric is a technique that can reliably provide all the requirements of security services such as authentication, privacy, authorization, data integrity and non-repudiation.

Despite of having several favorable advantages, one major disadvantage of biometric is the cost incurred in the deployment of a biometric system. Different biometric

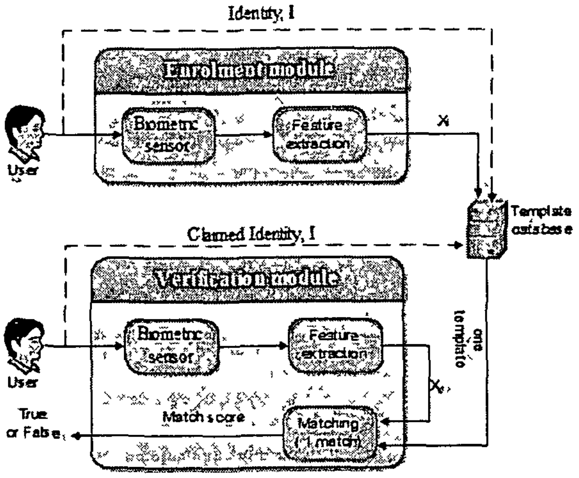


Figure 1-1: Block diagram of a biometric verification system

devices have different range of cost. Identification using biometrics may face the problem of non-universality due to the limited population coverage.

Multimodal biometrics : Today, biometric fusion is a popular practice to increase the reliability of identity verification. However a unimodal biometric system has been often found susceptible to non-universality and spoof attacks. To overcome it, information from different biometric sources are combined forming a multimodal biometric system.

Multibiometric is a sub-discipline within the domain of biometrics to establish identity. The problem of biometric recognition is a great challenge in terms of expectations of high matching accuracy, scalability and ease of usability in a variety of applications. A multibiometric system can be accomplished by fusion of multiple traits of an individual, or multiple feature extraction, or matching algorithms operating on the same biometric and multimodal fusion of different biometric traits.

The challenges of an unimodal system that leads to the multibiometric systems [76] are:

(i) Due to temporary inferences in the biometric trait such as scars in the fingerprint, changes of voice due to cold and due to unfavorable environmental conditions like in the face recognition and voice recording, noise may occur resulting an incorrect label of an individual as an imposter thereby increasing the false reject rate (FRR) of the system,

(ii) Intra-class variations occur due to incorrect interaction of users with the sensor of unimodal system,

(iii) Inter-class similarities may occur in systems used by a large number of users, where there might be more mismatch of features by multiple users of different identity,

(iv) Non-universality problem arises when not all users in the population able to produce the same type of features,

(v) Spoof or reply attack may occur due to an imposter's attempt to mimic the traits like signature and voice which are behavioral in nature and physical traits like fingerprint by inscribing ridge-like structures.

Types of Multibiometrıc System : Depending on the sources of evidence, a multibiometric system can be classified into one of the following six categories [4]: multisensor, multialgorithm, multi-instance, multisample, multimodal, and hybrid.

(i) Multisensor systems: Multisensor systems employ multiple sensors to capture a single biometric trait of an individual. The use of multiple sensors, in some instances, can result in the acquisition of complementary information that can enhance the recognition ability of the system

(ii) Multialgorithm systems: In some cases, invoking multiple feature extraction and/or matching algorithms on the same biometric data can result in improved matching performance. Multialgorithm systems consolidate the output of multiple feature extraction algorithms, or that of multiple matchers operating on the same feature set. These systems do not necessitate the deployment of new sensors and, hence, are cost effective compared to other types of multibiometric systems. But on the other hand, the introduction of new feature extraction and matching modules can increase the computational complexity of these systems.

(iii Multi-instance systems: These systems use multiple instances of the same body trait and have also been referred to as multiunit systems in the literature.

(iv) Multisample systems: A single sensor may be used to acquire multiple samples of the same biometric trait in order to account for the variations that can occur in the trait, or to obtain a more complete representation of the underlying trait.

(v) Multimodal systems: Multimodal systems establish identity based on the evidence of multiple biometric traits.

(vi) Hybrid systems: The term hybrid system is described by Chang et al. [23] to describe the system that integrates a subset of five scenarios.

Advantages and disadvantages of multibiometric systems : A multibiometric system achieves higher recognition accuracy than a unibiometric system. It is advantageous due to the following points[4].

(i) Facilitates the filtering or indexing of large-scale biometric databases.

(ii) Multibiometric systems address the issue of non-universality (i.e., limited population coverage) encountered by unibiometric systems. A certain degree of flexibility is achieved when a user enrolls into the system using several different traits while only a subset of these traits is requested during authentication based on the nature of the application under consideration and the convenience of the user.

(iii) Multibiometric systems also help in the continuous monitoring or tracking of an individual in situations when a single trait is not sufficient.

(iv) A multibiometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation. The notion of fault tolerance is especially useful in large-scale authentication systems involving a large number of subjects (such as a border control application).

Factors in designing a multibiometric system : The factors that impact the design and structure of a multibiometric system are [4]:

- Cost benefits: The tradeoff between the added cost and the improvement in matching performance is a cumbersome work to find out. The cost is a function of the number of sensors deployed, the time taken to acquire the biometric data, the storage requirements, the processing time of the algorithm and the perceived (in) convenience experienced by the user.

- Acquisition and processing sequence: Depending upon the needs data corresponding to multiple information sources (e.g., modalities) be acquired simultaneously or at different time instances in a serial fashion. The information acquired can be processed sequentially or simultaneously.

- Sources of biometric information: Determination of appropriate sources of information that can be used in a multibiometric system that are relevant to the application at hand.

- Types of information: The types of information or attributes (i.e., features, match scores,decisions, etc.) to be fused have to be decided and the impact of correlation among the sources of information on the performance of the fusion system have to be determined.

- Fusion methodology: The information presented by multiple biometric sources are combined depending on the fusion scheme. The performance gain obtained using different fusion methodologies in order to determine the optimal one is to predict.

Fusion and Its types : Recently, works on the fusion of multimodal biometrics are gaining significant importance due to their effectiveness in terms of cost and efficiency. In the past few years, several novel methods have been introduced to address this important problem. Based on our study as mentioned in our work [9] several levels of fusion approaches can be found in the literature.

In *sensor level* fusion, Raghavendra et al.(2010) [40] consider biometric sensor fusion technique using PSO for face and palmprint images. The authors use decomposition technique based on wavelet transformation. They select the most discriminative wavelet coefficients from the images to produce a fused image. Singh et al.(2008) [41] use visible and infrared face images and verification. It decides based on match scores by using multiple SVMs to learn both the local and global properties of the multi-spectral face images at different granularity levels and resolution.

In *representation level* fusion, Nagar et al.(2009) [42] consider fusion of different features into a single multi-biometric template by converting different biometric representations into a common representation space using various embedding algorithms. Rattani et al.(2007) [43] use integrated feature sets obtained from multiple biometric traits like fingerprint and iris.

Whereas in *dynamic classifier selection*, Giacinto et al.(1999) [44] select classifier for each unknown pattern, that is more likely to classify it correctly. In another attempt, Giacinto et al.(2000) [45] design a multiclassifier selector for each pattern. It ensures that at least one classifier identifies the patterns correctly. In order to select this classifier, the training patterns with the same behaviour are considered and the classifier with the highest accuracy is chosen.

In $matching\ score-based$ fusion, Kittler et al.(1998) [46] introduce a rule-based method to combine the classifiers in a probabilistic Bayesian framework on the basis of the Bayes theorem and by using a hypothesis it obtains the ways to merge the modalities (sum, product, max, min). It is established by the authors based on experimental results that the *sum rule* outperforms the remainder due to its robustness to errors made by the individual classifiers. Fierrez-Aguilar et al. (2003) [47] provide a supervised method which shows that a fusion strategy using a support vector machine (SVM) can outperform a fusion algorithm using the *sum rule*.

In $class\ rank-based$ fusion, Rukhin et al. (2005) [48] propose a fusion technique based on a minimum distance method for combining rankings from several biometric algorithms.

In *decision level* fusion, Veeramachaneni et al. (2008) [12] use a decision-level fusion for correlated biometric classifiers based on likelihood ratio test (LRT) and the Chair Varshney rule (CVR).

Decision level fusion in multibiometric verification : The term decision level fusion describes the establishment and evaluation of an ensemble based system and it sums up a variety of methods that rely on the usage of some small classifiers and their combination. Decisions are made by combination of the responses given by a number of classifiers. In case of multibiometric verification using decision level fusion, decision are taken using appropriate fusion rules. S. Prabhakar and A.K. Jain (2000)[5] propose a design scheme for decision-level fusion in biometric verification for classifier combination. Four different fingerprint matching algorithms are combined using the proposed scheme to improve the performance of a fingerprint verification system. Analysis of the results provide some insight into the various decision-level classifier combination strategies.

1.2 Motivation

Based on our limited survey we identify several factors that motivate us to design an effective multibiometric system are :

(i) Biometric representation : Biometric may be represented based on their large intra-class variability and large inter-class similarity, because every individual biometric have their own characteristics. Intra-class variations occur due to incorrect interaction of users with the sensor of unimodal system, whereas inter-class similarities may occur in systems used by a large number of users, where there might be more mismatch of features by multiple users of different identities.

(ii) Accuracy : The aim of biometric is to enhance security. But due to noisy input, a biometric sample may not always offer correct decisions and can make either false match or false non-match errors. The three primary underlying reasons as can be found in[2] are:

(a) Information limitation: The individual information in a biometric pattern samples may be limited or less discriminative then any other biometric. Inconsistent method of data acquisition may result in information limitation.

(b) Representation limitation: In order to retain all invariance and discriminative information of a biometric, an ideal scheme of representation is necessary, so that true features are represented, thus improving the accuracy.

(c) Invariance limitation: In order to improve the matching accuracy, the pattern matchers have to correctly model the invariance relationship in different patterns from the same class

(iii) Scalability : In case of unimodal biometric verification, large population coverage does not matter, since it essentially involves query matching with a single template. Whereas, in case of multimodal biometric verification, with a large population coverage of (say size N) needs to compare the query with N identities sequentially. Thus inherently increasing the chances of false match rate and reducing the throughput of the system. Hence, it demands for an effective approach to address the scalability issue.

(iv) Biometric system security and privacy: Biometric system security is a challenging issue due to the template aging and update.

(v) Soft biometric: Soft biometrics provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate them. e.g., ethnicity, skin color, hair color, height and weight.

Based on the study, the following observations have been made.

- In case of unimodal biometric , its authentication has been shown to be effective in a controlled environment and its performance can degrade in the presence of a mismatch between training and testing conditions.

- A multimodal biometric system comprises of several modality experts and a decision module. Hence, the error rate is low, since it uses complimentary discriminative information.

- A multimodal biometric system is more robust as degradation in performance of one modality can be compensated by another modality.

- In case of multi-biometric system, fusion of evidences obtained from multiple biometric is a critical part. The key to successful multibiometric system is an effective fusion scheme and may be consolidated at several levels like feature level fusion, matching score level fusion, rank level fusion and decision level fusion. Among all of the above fusion approaches as extensively studied in the literature [9], the decision level fusion is relatively more effective, yet understudied problem having a high potential for efficient consolidation of multiple unimodal biometric systems.

- The decision level fusion involves the selection of optimal fusion rule(s) and the selection of individual biometric sensor point for their matching scores dynamically. Some of the classical approaches that employ an optimal fusion are: deterministic methods, probabilistic method and evolutionary computation method like Ant Colony Optimization (ACO) [3], Swarm Intelligence [25], Bacteria Foraging and Genetic Algorithm [24]. But all these methods are not free from the aforesaid limitations.

1.3 Research goals

It is aimed to achieve the following objectives.

1. To study the effectiveness of various biometric traits such as fingerprint, iris and palmprint for identity verification.
2. To study and explore the usefulness of decision level fusion of multimodal biometric traits for effective identity verification.
3. To explore the effectiveness of optimization techniques such as SA, ACO and PSO to
   (a) select appropriate rules for fusion and
   (b) select dynamic threshold for individual trait matching score.
4. To validate the approach using benchmark datasets in terms of global false acceptance rate (GFAR) and global false rejection rate (GFRR).

1.4 Major contributions

In this thesis, a systematic study has been carried out and attempts have been made to solve problems that score level fusion techniques faced. In score level fusion of different modalities, the performance is adversely affected by the fusion strategies. The score level fusion involves matching scores from the different sensors, and the fusion of these scores by sum, product and weighted sum rules. I explore the possibility of optimal fusion rule selection for fusion of multimodal biometrics. Several effective methods for decision level fusion of biometrics using appropriate optimization technique have been introduced. A brief about the explored fusion techniques are discussed below.

In this work, effectiveness of the fusion method has been established using several benchmark databases using Simulated Annealing approach [10]. Simulated annealing is an annealing process in metallurgy which reduces defects by controlling cooling of materials. SA statistically guarantees to find an optimal solution and it has its ability and flexibility to approach global optimality [10]. The selection of a proper set of parameters for SN is a multi-objective decision making optimization problem. Initially the matching scores for individual biometric classifiers are computed. Next, a SN-based procedure is followed to simultaneously optimize the parameters and the fusion rules for fingerprint, iris and palmprint biometrics. An experimental verification of the convergence nature of the simulated annealing method with the worst case behavior for optimum rule selection is analyzed and a comparative result of the method with the Ant Colony Optimization technique is also given.

In this work, we have explored an effective method for decision level fusion of fingerprint and iris biometrics using binary ant colony optimization(ACO) technique to identify the imposter instances [9]. ACO is an evolutionary method. The selection of a proper set of optimization parameters for ACO is a multi-objective decision making optimization problem. Initially the matching scores for individual biometric classifiers are computed. Next, a ACO-based procedure is followed to simultaneously optimize the parameters and the fusion rules for fingerprint and iris biometrics. The proposed method has been found to perform satisfactorily on several benchmark datasets. However, sometimes it may not converge as it updates the pheromone based on its current best possible path [11]. Further operation on dynamic sets often leads to complex scenario, which is a major issue on the scalable datasets of multi-modal biometrics. Hence there is a need to explore Simulated Annealing approach for fusion of multi-modal biometrics as it has many advantages while comparing with its other counterpart.

The task of multimodal biometric system is to minimize the (global) cost by selecting (i) the appropriate score level combination rule, (ii) its parameters and (iii) the decision threshold. The multi-dimensional search among the various combination rules and their weight parameters to optimize the global cost is achieved by the particle swarm optimization (PSO) approach. It uses binary particle swarm optimization (BPSO) to compute and optimize the parameters and fusion rules. Initially the appropriate parameters (thresholds) for individual biometric classifiers are selected based on their matching scores. Next, a BPSO based procedure is followed to simultaneously optimize the parameters and the fusion rules. The biometric thresholds are continuous. In such model, a fusion rule takes an integer value which suffers slow convergence. Moreover the fusion rule is a binary number having a length of $\log_2 p$ bits, where $p=2^{2^N}$, with a real value varying from $0\leq f\leq p-1$. For binary search spaces, the binary decision model as described in [12] is being used. A binary decision model works better for moving through the decision fusion space. Hence the effectiveness of the method is being compared with the BACO based approach [8].

In the present study, the work is focused on the development of an effective method for combination of multimodal biometric data. Iris, fingerprint and palmprint biometrics have been found better as compared to other available traits due to their accuracy; reliability and simplicity, which make them promising solution to the society. The features of individual iris, fingerprint and palmprint traits are extracted from their preprocessed images. These features of a query image are compared with those of stored template to obtain the matching scores as in [7]. It shows the utility of adaptive multimodal biometric fusion on the real biometric samples using the Bayesian fusion rule for score level fusion. We have investigated the adaptive combination of iris, fingerprint and palmprint biometric on publicly available benchmark databases and the results have been found satisfactory.

1.5 Organization of the thesis

- Chapter 2 gives a background of the study. It discusses in details about the biometric modalities, their preprocessing, proximity mesures etc. It considers the issue of performance evaluation in biometric systems, by presenting some state-of-the-art criteria and metrics used to evaluate the performance of a biometric verification system.

- Chapter 3 describes a fingerprint verification scheme and its experimental results.

- Chapter 4 describes an iris-based identity verification scheme and its experimental results.

- Chapter 5 describes a palmprint-based verification scheme and its experimental results.

- Chapter 6 reports some multimodal verification schemes and their experimental results.
- Chapter 7 finally summarizes the work with concluding remarks. It also reports several scopes for future research.

Chapter 2

BACKGROUND AND RELATED WORK

2.1 Background

The biometric modalities may be of different types based on the physiological or behavioral characteristics of human. The various biometric modalities can be broadly categorized into three: physical biometric, behavioral biometric and chemical biometric. Physical biometric involves some form of physical measurement. The behavioral biometrics are usually temporal in nature and involve measuring the way of performing a certain activities, whereas chemical biometric is a recent field that involves measuring some chemical cues of human being. Different types of biometrics modalities are :

- DNA Matching (Chemical biometric): It is based on the analysis of segments from DNA.
- EAR (Physical biometric): It uses the shape of the ear of an individual.
- Iris recognition (Physical biometric): It uses the features found in the iris to identify an individual.
- Retina recognition (Physical biometric): It uses the patterns of veins in the back of the eye to accomplish recognition.

- Face Recognition (Physical biometric): It uses the facial features or patterns for the authentication or recognition of an individuals' identity.
- Fingerprint recognition (Physical biometric): It uses the ridges and valleys(minutiae) found on the surface tips of an individual's finger.
- Finger Geometry Recognition (Physical/Spatial biometric): uses 3D geometry of the finger of an individual.
- Gait (Behavioral biometric): An individual's walking style or gait is used to determine identity.
- Hand Geometry Recognition (Physical/spatial biometric): The geometric features of the hand like length of fingers and the width of the hand are used to identify an individual.
- Signature Recognition (Behavioral biometric): The authentication of an individual by the analysis of handwriting style, in particular the signature.
- Voice (Auditory biometric): The use of the voice as a method of determining the identity of a speaker for access control.
- Speech (Auditory biometric): Recognizing what is being said or who said.

2.1.1 Basics of Fingerprint

Fingerprints are considered to be one of the most popular biometric authentication and verification measures because of their high acceptability, ability and uniqueness [32]. Here immutability refers to the persistence of the fingerprints over time whereas uniqueness is related to the individuality of ridge details across the whole fingerprint image. Automatic fingerprint identification comprises of feature extraction, fingerprint classification and fingerprint matching. The effectiveness of feature extraction depends on the quality of the images, representation of the image data, the image processing models, and the evaluation of the extracted features. At the first stage of the fingerprint classification process, the image is only represented as a matrix of

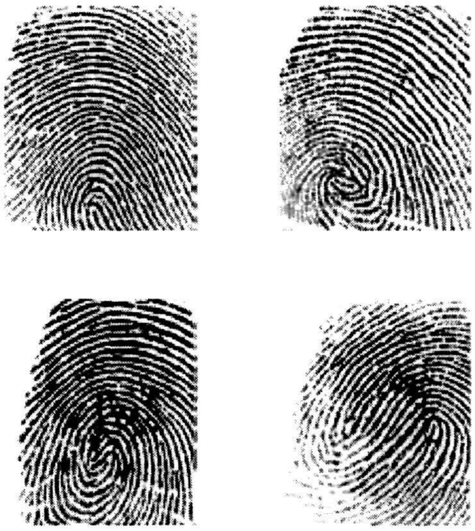


Figure 2-1: Examples of Fingerprint images

grey scale intensity values. Feature extraction is a process through which geometric primitives within images are isolated in order to describe the image structure, i.e. to extract important image information and to suppress redundant information that is not useful for classification and identification processes. Thus fingerprint features and their relationships provide a symbolic description of a fingerprint image. Fingerprint classification is an important step in any fingerprint identification system because it significantly reduces the time taken in identification of fingerprints especially where the accuracy and speed are critical. Examples of Fingerprint images are shown in Figure 2-1.

2.1.2 Basics of Iris

Iris when treated as a biometric trait has excellent recognition performance. Iris patterns are unique due to their complex environmental and genetic processes. Even two identical twins have different iris patterns. Iris verification involves analyzing features found in the colour ring of tissue that surrounds the pupil. In case of iris, the most discriminating features of iris pattern is the phase information. A complex iris

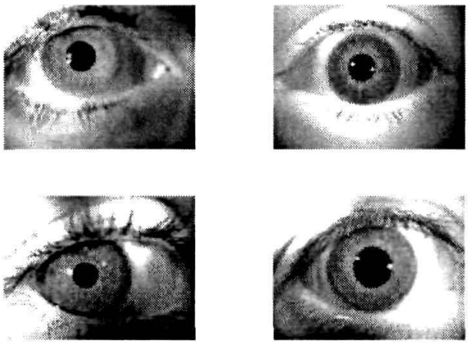


Figure 2-2: Examples of Iris images

pattern can contain many distinctive features like ridges, crypts, rings and freckles [50]. Among all eye related biometrics, iris scanning is less intrusive and iris scanner requires no close contact between user and camera. Some popular applications for iris biometrics can be employee verification and immigration process at airports or seaports etc.

A generic iris recognition system consist of the steps like (i) Preprocessing, (ii) Localization, (iii) Normalization, (iv) Encoding and (v) Iriscode comparision (Matching). Example of Iris images are shown in Figure 2-2.

2.1.3 Basics of Palmprint

Biometric verification using palmprint has emerged as a promising one. It is a new biometric modality which is getting wide acceptance. Palmprint not only has the unique information available as on the fingerprint but has far more amount of details in terms of principal lines, wrinkles and creases. Studies have revealed that the palmprint contains mainly three types of information namely texture information, line information, and appearance based information. Example of palmprint images are shown in figure 2-3.

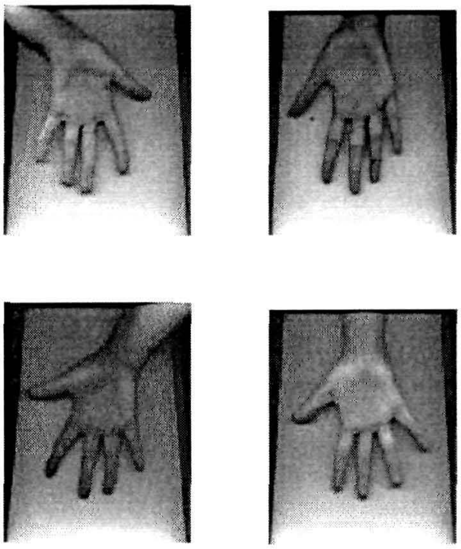


Figure 2-3: Example of Palmprint images

2.1.4 Fusion types

Fusion is performed to build a unified biometric decision based on the information collected from different biometric sources. The unified result must guarantee the best performance possible and take into account the efficiency of the solution. Information fusion in multi-biometrics take into account the nature of biometric information sources as well as the level of fusion suitable for the application. Biometric information fusion can occur at four major levels namely, sensor level, feature level, score level, and decision level.

- Sensor level fusion: In sensor level fusion information produced by several sources can be combined optimally.
- Feature level fusion: In feature level fusion, feature vectors are created by capturing the data from each sensor. Biometric information are combined either by concatenation or by applying a weighted summation before applying to pattern classifier module as shown in Figure 2-4. The feature vectors can be homogeneous or nonhomogeneous. In case of homogeneous feature vectors (e.g. feature vectors of multiple fingerprint impressions) a single resultant feature vector is

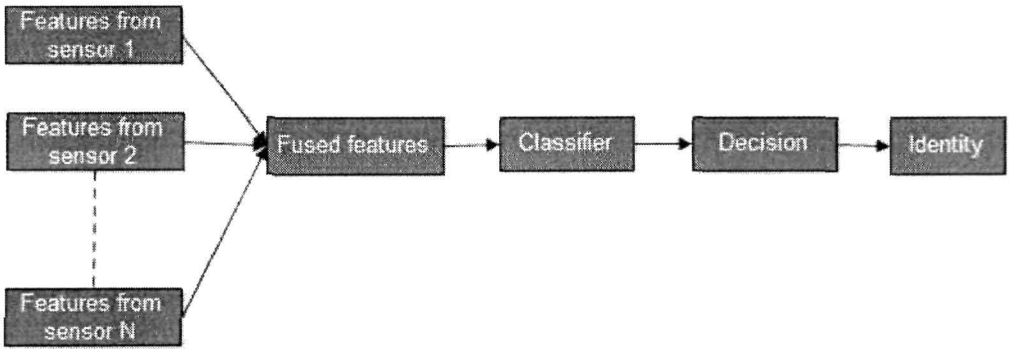


Figure 2-4: Block diagram of a feature level fusion

created from the same modality. Whereas in case of non-homogeneous feature vectors, feature vectors from different modalities are combined to form a single feature vector. Fusion at feature level is difficult in practice because : (i) the feature sets of multiple modalities may be incompatible (e.g., eigen-coefficients of face and Mel-frequency cepstral coefficients (MFCCs) of voice); (ii)the relationship between the feature vectors of different biometric sensors may not be known.

- Matching score level fusion: In score level fusion, the feature vectors from each biometric modal are extracted and are passed to their individual matching algorithms, which attempt to match them against previously captured templates. The matching scores provides the quality of each match. The biometric matchers provide a set of possible matches along with the matching scores which are then combined, resulting a decision. To ensure meaningful combination of scores, scores have to transform to a common domain first. Output of matching scores contain the richest information about the input pattern. The block diagram of the matching score level fusion is shown in Figure 2-5.

- Decision level fusion: In decision level fusion, individual decisions for each biometric are fused and fusion is carried out with the help of some rules like 'AND'

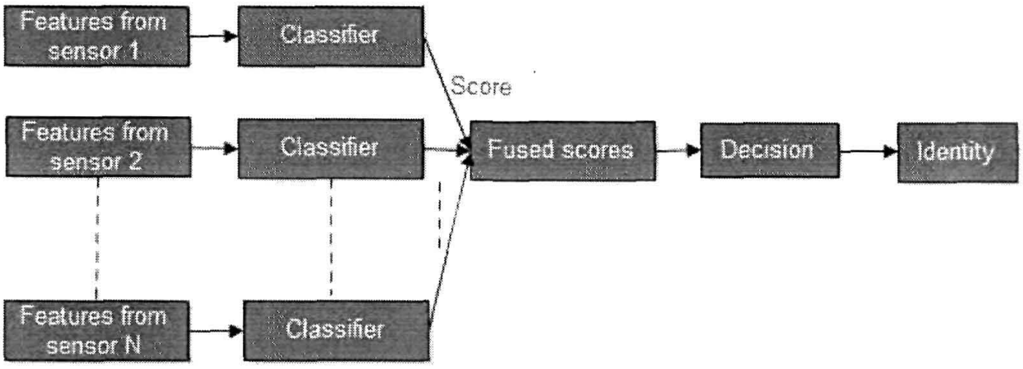


Figure 2-5: Block diagram of a matching score level fusion

or 'OR', majority voting, Bayesian decision fusion etc. The challenges with the decision level fusion are the least features or scores of different modalities. The block diagram of the matching score level fusion is shown in Figure 2-6.

2.1.5 Fusion techniques

In this section we discuss two basic approaches:

1. Simple approach :

   - Product(AND) rule: In multimodal verification system, product rule (or 'AND' rule is a simplest method to combine the decision output of different multimodal subsystems. When the input samples of both the subsystems match with the train data template, the output of AND rule is the match. In case of fusion by 'AND' rule, the false acceptence rate(FAR) of fused system is lower than the FAR of individual matcher [4].

   - Sum(OR) rule: Sum or OR rule is another simplest method to combine the decision output of different multimodal matchers. The output of the OR rule is a 'match' if any one of the individual input sample of the

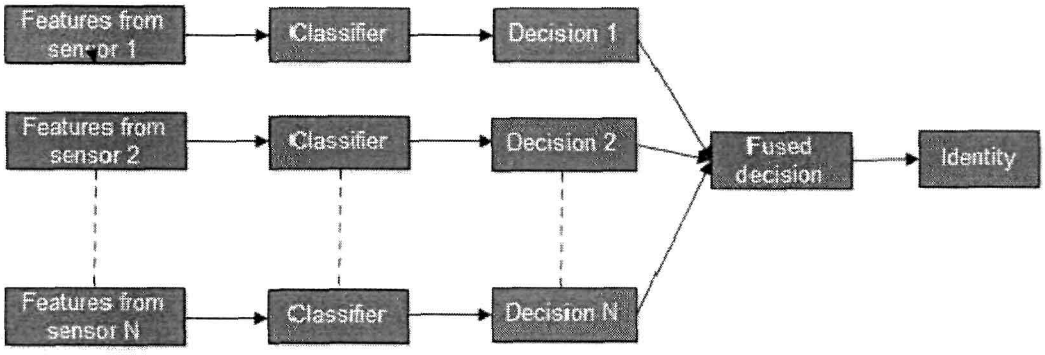


Figure 2-6: Block diagram of a decision level fusion

decision module matches with the train data template. In case of 'OR' rule the fusion systems false rejection rate(FRR) is more than the FRR of individual matchers. But if the two matchers have different decision, it may be difficult to get the correct output of the fusion system.

- Majority voting rule: The majority voting rule is another common and simplest rule derived from the sum rule for decision level fusion. In multimodal verification system, input samples are assigned to the individual matchers and identifies whether the majority of the matchers agrees to match or not. Out of R input samples if at least k are identified as matched then final output of the decision level is 'match' , where 'k' matchers agree that identity as in equation 2.1 [32].

$$k = \begin{cases} \frac{R}{2} + 1, \text{if R is even and} \\ \frac{R+1}{2}, \text{if R is odd} \end{cases} \tag{2.1}$$

The major drawback in majority voting is that all the biometric matchers are treated or weighted equally. But in real world scenario, that may not be always feasible, so weighted majority voting rule selectin is used.

- Weighted majority voting : In weighted majority voting rule, the weights w_k are assigned based on the reliability of fusion subsystems obtained during training process and k is the number of times the subsystem is matched.

$$S_{j,k} = \begin{cases} 1, \text{if output of the } j^{th} \text{ matchers is in class } w \\ 0 \text{ otherwise.} \end{cases} \tag{2.2}$$

  The discriminant function using weighted voting is given by the equation 2.3.

$$g_k = \sum \omega_j S_j, k \tag{2.3}$$

  Where ω_k is the weight assigned to the j^{th} matcher.

2. Evolutionary approach: These techniques are employed to determine the optimal fusion strategy and the corresponding fusion parameters. Various available evolutionary approaches for biometric fusion are genetic algorithm (GA), particle swarm optimization (PSO) and ant colony optimization (ACO).

   (a) GA: Genetic algorithms(GAs) are developed by John Holland, his students and colleagues in 1960-70. Holland presented the genetic algorithm as as abstraction of biological evolution. In GA the problem solutions are represented as genomes or chromosomes [24]. The GA is an optimization and search technique based on the principles of genetics and natural selection. A GA allows a population composed of many individuals to evolve under specified selection rules to a state that maximizes the fitness or minimizes the cost function.

   GA Operators: The Genetic Algorithms create a population of solutions and apply genetic operators like

   - Reproduction: Generates a population of candidates (chromosomes) in some region of the space; i.e. exploration.
   - Crossover: This operator randomly chooses a locus and exchanges

the subsequences before and after that locus between two chromosomes to create two offspring for the next generation.

- Mutation: Simulate small random variation of the genotype. Mutation can occur with some probability, usually very small (e.g., 0.001).
- Selection: According to the fitness function, this operator selects chromosomes for reproduction. The fitter is the chromosome, the more times it is likely to be selected to be reproduced.

Advantages and disadvantages: GA has a number of advantages [24].

- Optimizes with continuous or discrete variables,
- Simultaneously searches from a wide sampling of the cost surface,
- It can quickly scan a vast solution set.
- For an optimization problem, GAs are capable to find the global optimum solution in a multi-dimensional space without worrying about local minima.

GA has some drawbacks too: - The major disadvantage of GA is that the algorithm uses a very large amount of processing time .

(b) PSO: Particle Swarm Optimization (PSO) was formulated by Edward and Kennedy in 1995. The thought process behind the algorithm was inspired by the social behavior of animals, such as bird flocking or fish schooling. PSO is similar to the continuous GA in that it begins with a random population matrix. Unlike the GA, PSO has no evolution operators such as crossover and mutation. The rows in the matrix are called particles [24]. They contain the variable values and are not binary encoded. Each particle moves about the cost surface with a velocity. The particles update their velocities and positions based on the local and global best solutions. The PSO algorithm updates the velocity vector for each particle then adds that velocity to the particle position or values. Velocity updates are influenced by both the best global solution associated with the lowest cost ever found by a particle and the best local solution associated with the lowest cost in the present population. If the best local solution has a cost less than the cost of the current global solution, then the best local solution replaces the best global solution. Two major advantages of PSO are: (i)it is easy to implement (ii) there are few parameters to adjust.

(c) ACO: Ants can find the shortest path to food by laying a pheromone (chemical) trail as they walk. Other ants follow the pheromone trail to food. Ants that happen to pick the shorter path will create a strong trail of pheromone faster than the ones choosing a longer path. Since stronger pheromone attracts ants better, more and more ants choose the shorter path until eventually all ants have found the shortest path.

2.1.6 Identity verification using multilevel decision level fusion

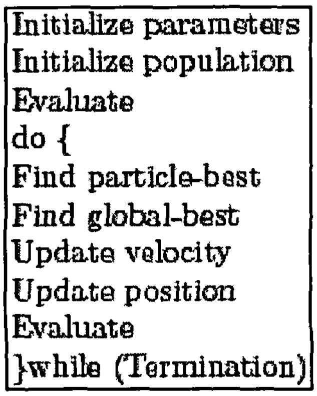
It is an abstract level fusion. They only provide the result of matching in the form of whether the user is genuine or imposter. With decision level fusion, there are different rules that can be used to identify an user. Majority voting rule was given by Lam and Suen [52]. Xu et al. proposed weighted voting based on Dempster-Shafer theory [53]. AND/OR rules were given by Daugman for decision making [54].

2.1.7 Optimization techniques for fusion of biometrics

In this section, we discuss three popular optimization techniques, which have been used in the multimodal verification system for an optimum performance.

1. PSO: In a PSO algorithm, as introduces by Kennedy (2001) [25], population is initiated randomly with particles and evaluated to compute fitness together with finding the best value of each individual so far (particle-best) and best particle in the whole swarm (global-best). The pseudo code of the general PSO algorithm [25] is reported in Figure 2-7.

2. ACO: Ant colony optimization (ACO) is a nature-inspired optimization algorithm [3] [30], motivated by the natural phenomenon that ants deposit pheromone



```
Initialize parameters
Initialize population
Evaluate
do {
Find particle-best
Find global-best
Update velocity
Update position
Evaluate
}while (Termination)
```

Figure 2-7: Pseudo code of the general PSO.

on the ground in order to mark some favorable path that should be followed by other members of the colony. The first ACO algorithm, called the ant system, was proposed by Dorigo et al. [57]. ACO has been widely applied in various problems [31].

ACO aims to iteratively find the optimal solution of the target problem through a guided search (i.e. the movements of a number of ants) over the solution space, by constructing the pheromone information. The main characteristic of ACO algorithm is that, at each iteration the pheromone values are updated by all the k ants those have built a solution in the iteration itself. Each ant chooses its possible solutions randomly from the available possible values. Two important parameters in ACO are 'pheromone constant' (Q) and 'evaporation factor' (ρ<1).

3. SA: Simulated Annealing(SA) is a mathematical analogy to a cooling system which can be used to sample highly nonlinear multidimensional functions. In the early 1980s, the method of simulated annealing (SA) was introduced by Kirkpatrick and coworkers (1983), based on the ideas formulated in the early 1950s (Metropolis, 1953). This method simulates the annealing process in which a substance is heated above its melting temperature and then gradually cooled to produce the crystalline lattice which minimizes its energy probability distribution. This crystalline lattice, composed of millions of atoms perfectly aligned,

is a beautiful example of nature finding an optimal structure. However, quickly cooling or quenching the liquid retards the crystal formation, and the substance becomes an amorphous mass with a higher than optimum energy state. The key to crystal formation is carefully controlling the rate of change of temperature. The algorithmic analog to this process begins with a random guess of the cost function variable values. Heating means randomly modifying the variable values. Higher heat implies greater random fluctuations. The cost function returns the output, f, associated with a set of variables. If the output decreases, then the new variable set replaces the old variable set. If the output increases, then the output is accepted with probability that

$$P = exp^{(f_{old}-f_{new})/T} > r \tag{2.4}$$

where r is a uniform random number and T is a variable analogous to temperature. Otherwise, the new variable set is rejected. Thus, even if a variable set leads to a worse cost, it can be accepted with a certain probability. The new variable set is found by taking a random step from the old variable.

Applications of SA: SA was started as a method or tool for solving single objective combinatorial problems, these days it has been applied to solve single as well as multiple objective optimization problems in various fields. The problems may have continuous or discrete variables. SA has been greatly used in operational research problems. Application of SA does not restrict to optimization of nonlinear objective function, these days it has been applied for many other purposes. Bell et al (1987) have used it to cluster tuples in databases. They have attempted to use SA in circuit board layout design and it suggests that it would be advantageously applied to clustering tuples in database in order to enhance responsiveness to queries.

2.1.8 Discussion

Information fusion is a key issue in a multimodal biometric system. Sensor level fusion has limited use in commercial applications due to their compatibility problems. It is rare that different sensors are compatible. Also fusion at feature level is not always guaranteed feasible, because the feature sets extracted from different biometric modalities are not compatible to each other. Also resulting feature vectors may result in a feature vector with very large dimensionality. Combination at matching score level is relatively easy to use. The main problem of score level fusion is to obtain the score weights of different modalities.

In our work we have make an appropriate use of the three important biometrics i.e. fingerprint, iris and palmprint in developing an effective multibiometric verification system by deriving the benefits of decision level fusion and optimization technique. The details of the schemes developed based on these biometrics, fusion and optimization techniques are reported in the succeeding chapters.

Next chapter describes a fingerprint classification and verification method and their experimental results.

Chapter 3

FINGERPRINT CLASSIFICATION AND VERIFICATION

3.1 Introduction

Fingerprints are the most widely used biometrics for the verification of user identity because of their high acceptability, immutability and uniqueness [56]. Here immutability refers to the persistence of the fingerprints over time whereas uniqueness is related to the individuality of ridge details across the whole fingerprint image. Fingerprints are commonly employed in biometric systems such as civilian and commercial devices for user identity proof. Another widespread use of fingerprints are in forensic science to support criminal investigations.

3.1.1 History of fingerprints

User identification through fingerprint biometric is a quite matured technique over the past century and experts have developed accurate procedures for determining the similarity of two prints. However, proficiency has been achieved at the cost of efficiency. It is surprising that the problem is still far from solved. A brief history of the science of fingerprints and applications are reported as follows:

1823 J. E. Purkinje, professor of anatomy at the University of Breslau, published his thesis discussing nine fingerprint patterns.

1858 W. J. Herschel, a British Administrator in Hoogly district in India used fingerprints on civil contracts

1880 Dr. Henry Faulds, a Scottish doctor in Tokyo, Japan recognized the importance of fingerprints as a means of identification and devised a classification method. In 1880, he published an article in the Scientific Journal, "Nature"(nature), mentioning printer ink as a method for obtaining fingerprints for personal identification.

1882 Gilbert Thompson of the U.S. Geological Survey in New Mexico, used his own thumb print on a document to help prevent forgery, which is the first known use of fingerprints in the United States.

1882 Alphonse Bertillion, French anthropologist, devised a method of classifying and identifying people known as Bertillion System.

1891 Juan Vucetich, an Agentine Police Officials made the first fingerprinting of criminals.

1892 Sir Francis Galton, a British Anthropologist published the first book on fingerprints, establishing the individuality and permanence of fingerprints and defines the first classification system for fingerprints. According to his calculations, the odds of two individual fingerprints being the same were 1 in 64 billion. he also identified the characteristics by which fingerprints can be identified as minutiae is also known as Galton details.

1901 Sir Edward Henry, an Inspector General of Police in Bengal, India developed the first official system of classifying fingerprints in India and eventually spread throughout the world.

1905 U.S. Military adopts the use of fingerprints soon thereafter, police agencies began to adopt the use of fingerprints

1908 The first official fingerprint card was developed.

1924 Formation of ID Division of FBI.

1980 First computer data base of fingerprints Automated Fingerprint Identification System, (AFIS) was developed. Presently there are nearly 70 million cards, or nearly 700 million individual fingerprints entered in AFIS.

2012 INTERPOL's Automated Fingerprint Identification repository exceeds 150,000 sets fingerprints for important international criminal records from 190 member countries.

2014 America's Largest Database, AFIS repository in America is operated by the Department of Homeland Security's US Visit Program, containing over 120 million persons' fingerprints, many in the form of two-finger records.

2014 The world's largest database, the Unique Identification Authority of India, also known as 'Aadhaar' operates the world's largest fingerprint(multi-modal biometric) system with over 560 million fingerprint, face and iris biometric records. The Aadhaar project has the ambitious goal of eventually providing reliable national ID documents for 1.2 billion Indian residents.

3.1.2 Fingerprint as a biometric

Fingerprint verification is a pattern recognition problem. Fingerprint patterns are compared with the help of developed algorithms and similarity between them is used to verify identity. Automatic fingerprint verification comprises of feature extraction, fingerprint classification and fingerprint matching. The effectiveness of feature extraction depends on the quality of the images, representation of the image data, the image processing models, and the evaluation of the extracted features. At the first stage of the fingerprint classification process, the image is only represented as a matrix of grey scale intensity values. Feature extraction is a process through which geometric primitives within images are isolated in order to describe the image structure, i.e., to extract important image information and to suppress redundant information that are not useful for classification and identification processes. Thus fingerprint features and their relationships provide a symbolic description of a fingerprint image. Fingerprint classification is an important step in any fingerprint verification system because it significantly reduces the time taken in identification of fingerprints especially where the accuracy and speed are critical. To reduce the search and space complexity, a systematic partitioning of the database into different classes is highly essential. Fingerprint matching is done generally at two levels: at coarse level, fingerprints are classified into six distinct groups viz., whorl, arch, tented arch, left loop, right loop or twin loop and at fine level, matching is performed by extracting minutiae i.e., ridge ending and branching points. Global ridge shape provides important clues about the global pattern configuration of a fingerprint image. One of the most desirable features of a fingerprint representation and verification method is transformation invariance under translation, rotation and scaling. This indicates that the problem of identifying fingerprints is of a topological nature, rather than geometrical.

3.2 Prior related work

Based on our survey related to fingerprint classification [7], it has been observed that there exist different classification methods based on the features of fingerprints. The structural features present structural classification approaches, which are mostly based on syntactic pattern matching and graph matching. Also there exist various heuristic approaches based on singularities and ridge structures. In the neural network approach, the existing applications of neural networks can also be applied.

Based on our study, it has been observed that the classification methods are of eight major categories as follows.

A. Structural approach: The structural classification approaches classify input fingerprints based on the interrelationships of low-level features. It uses syntactic and graph based pattern matching approach.

i) Syntactic pattern matching: In syntactic pattern recognition an analogy is drawn between the structure of the input data and the syntax of a language. The input data is represented by a sequence of primitives which is considered to be a sentence of a language. Every class has an associated set of rules (or grammar) that describes how to build new sequences (sentences). Classification is performed by determining which grammar most likely produces a given input sequence.

ii) Graph matching: In this approach, two graphs are given as input, graph matching algorithms attempt to determine whether or not the graphs are isomorphic. For each fingerprint class, a model graph is created that has a structure typical of that class.

B. Heuristic rule approach: In this automated fingerprint classification approach, the knowledge of human experts is codified using a system of heuristic rules based on the singularity features, ridge features or a combination of singularity and ridge features.

i) Singularity structure-based approach: Since singularities are local features they are very sensitive to noise. Having detected a fingerprints' singularities (core and delta points), heuristic rules based on their number and location can be used to classify fingerprints accurately.

ii) Global ridge structure-based approach [60]: Use the calculation of orientation fields to represent the global geometric shape of fingerprints based on analyzing the global geometric shape of the fingerprint. Twin loops can be recognized by the fact that they are the only global geometric shape that has two turns with opposite signs.

iii) Singularities and global ridge structure-based approach: The singularities perform very poorly on noisy images. The global ridge structure features are also difficult to deal with the large intra class variations and small interclass variations of fingerprint classes. Some systems overcome these limitations by using both singularities and ridge structures.

C. Neural approach: The research work of the applicability of neural networks to fingerprint classification began in the early 1990s and became one of the most commonly used classifiers for fingerprint classification systems. Researchers have developed different neural based classification approaches.

i) The neural approach developed by NIST for the FBI in 1990 [61]: This research formed the basis for the PCASYS system (Pattern-level Classification Automation System for Fingerprints) [62] PCASYS uses the core of loops, the upper core of whorls and a well-defined feature of arches and tented arches. The fingerprintŠs directional image is registered with respect to the centre of the fingerprint image. The dimensionality of the orientation field is reduced using the KL transform. Next, a probabilistic neural network (PNN) is used to classify the feature vector.

ii) The neural approach based on wavelet features: Wavelets form the basis of the FBI's fingerprint image compression scheme [63]; however, wavelets are sensitive to rotations and translations. A feed-forward neural network with a single hidden layer was trained to classify feature vectors consisting of 64 wavelet coefficients.

iii) The neural approach based on SOM: SOM's are based on Kohonen learning and are used for dimensionality reduction. A modified version of SOM also used that includes a certainty parameter to handle fingerprints [7]. The features being used for classification are the fingerprint's orientation field and some certainty measures.

iv) The neural approach based on fuzzy-network classifier: It combine the advantages of fuzzy logic techniques and neural networks and offer algorithms for learning and classification. The neural network is used to automatically generate fuzzy logic rules during the training period. It is based on singularity features that include the number of core and delta points, the orientation of core points, the relative position of core and delta points and the global direction of the orientation field. The authors Mohamed and Nyongesa [66] point out that noise and preprocessing errors lead to an intra class variation among fingerprints.

D. Combining structural and statistical features: Structural features are extracted from the orientation field using a line tracing algorithm. Prominent flow lines are represented by strings of symbols that encode information about their endpoints and curvature. A three-layer feed-forward artificial neural network with six sub networks (one for each class) is used for classification.

E. Clustering approach:It uses a k-means based classifier. An unlabeled feature vector is assigned to the most common class of its three-nearest neighbors. Using clustering and three-nearest neighbors is certainly more powerful than simply using a single nearest neighbor, and it still has a low computational complexity. Clustering was performed on 500 samples, each labeled as either a whorl, left loop, right loop or arch. The features used were the orientation vectors in the area surrounding a fingerprint's core. Through experimentation, the authors found that using nine clusters had the best performance, and these clusters were found using a k-means clustering algorithms.

F. Using multi-space KL transform: The KL transform reduces the dimensionality of a feature space while minimizing the average mean-squared error. The multi-space KL (MKL) transform is a generalization of the KL transform that uses multiple subspaces for classification [68]. One subspace is trained for each fingerprint class and fingerprints are characterized by their distances to the subspaces. MKL has a strong ability to distinguish the fingerprint classes.

G. Support vector machines (SVMs): SVMs are based on statistical learning theory. SVMs are binary classifiers that work by finding the optimal separating hyper plane in the feature space [69]. One advantage of SVMs is their strong ability to classify vectors with high-dimensions. SVMs are applied to the problem of fingerprint classification using the FingerCode representation of the fingerprint. SVMs are a powerful classifier and good results were presented.

H Hybrid classifiers: Uses a two-stage classifier based on FingerCodes. The algorithm first uses a k-nearest Neighbour classifier to determine the two most likely classes of the fingerprint. SVMs have been shown to be well suited for classifying FingerCodes [69], so by using SVMs instead of neural networks the accuracy of this system may be improved further. Classes are determined by the two most common classes of the knearest neighbours to the vector in the feature space. During the second stage, the fingerprint's class is determined by a neural network trained specifically to distinguish those two classes.

3.3 Proposed Method of Fingerprint Classification and Verification

3.3.1 Background of our work

Real-time image quality assessment can greatly improve the accuracy of identification system. The good quality images require minor preprocessing and enhancement. Conversely, low quality images require major preprocessing and enhancement. To test a fingerprint recognition algorithm, large databases of sample images are required to estimate error. But collecting large databases of fingerprint images is not a trivial task both in terms of money and time. An automatic recognition of people based on fingerprints requires that the input fingerprint be matched with a large amount of fingerprints in a database. To reduce the search space and hence the computational complexity, it is desirable to classify these fingerprints in an accurate and consistent manner so that the input fingerprint be matched against an appropriate subset of fingerprints in the database.

3.3.2 Proposed method

3.3.2.1 Conceptual Framework: The flow diagram of the proposed fingerprint verification method is depicted in Figure 3-1.

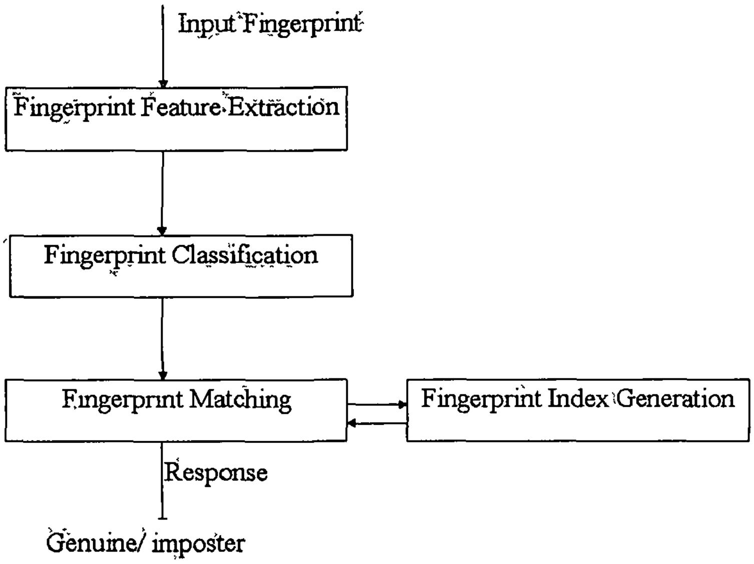

Input Fingerprint
Fingerprint Feature Extraction
Fingerprint Classification
Fingerprint Matching
Fingerprint Index Generation
Response
Genuine/ imposter

Figure 3-1: Flow diagram of the proposed fingerprint verification method

3.3.2.2 Feature Extraction: One of the fundamental step before classification is the core point extraction. This step is particularly important since a reference center is required in order to correctly compare two fingerprints. Automated core detection can only find the most likely center of the image without regard whether there is a meaningful core exists or not. Furthermore, the alignment according to the core point only partially remedies the misalignment of two fingerprints.

The fingerprint feature vector generation phase consists of five steps. Initially the block direction of the image is estimated. Next, the certainty value associated with each block is calculated. Then the segmentation of the fingerprint image is carried out so that noisy and corrupt parts that do not carry valid information are deleted. Meanwhile, the core point to be taken as the reference center is extracted. Then a 16x16 block direction surrounding the core are identified towards construction of the feature vector.

i) Block Direction Estimation: The block direction estimation program operates on the gray level fingerprint image and then obtains an approximate direction for each image block with size 16x16. The technique found in [71] was used to calculate the horizontal and vertical gradients of each pixel and then combines all the gradients within the block to get an estimated direction. It has large consistency with the ridge flows of the original fingerprint image in most testing cases.

ii) Finding Certainty Values: The certainty values are computed simultaneously during the direction estimation as adopted by [64]. The certainties are the magnitudes of vectors representing the flow directions of ridges in a grid for the extracted information on flow direction for the grid. The certainty vectors are of the same size as the block directional image. All the directions are then normalized into the domain from 0 to, and the certain values are in the interval from 0 to 1.

iii) Segmentation: An inevitable problem after step I is that after discarding the image areas the background noise may not be eliminated completely. It is needed to extract the tightly bounded fingerprint region from the image. To achieve high accuracy we accomplish (i) the segmentation task by techniques like histogram equalization, image enhancement and coarse segmentation by Fourier transform, image binarization and (ii) interesting region location by morphological operations.

iv) Finding of core or reference point: This step is particularly important since a reference center is required in order to correctly compare two fingerprints images. We used a variant of [71] to detect the core point. Unlike [71] map all the block directions to an interval from 0.5 to 05.8 our experimentation, we consider 0.5 or the corresponding value of the core.

v) Regulate the feature vector: we extract a 16x16 block centered at the core and then reconstruct it as a 1x256 vector. The parts of the block in the background region or outside the image region will not affect the vector values in further process. The same operations are enforced to the certainty vector.

3.3.2.3 Classification: Fingerprint classification is a technique to assign a fingerprint into one of the several pre-specified types. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then at a finer level, it is compared to the subset of the database containing that type of fingerprints only. Fingerprints are classified into six categories: arch, tented arch, left loop, right loop and whorl and twin loop as in the Figure 3-2. Details

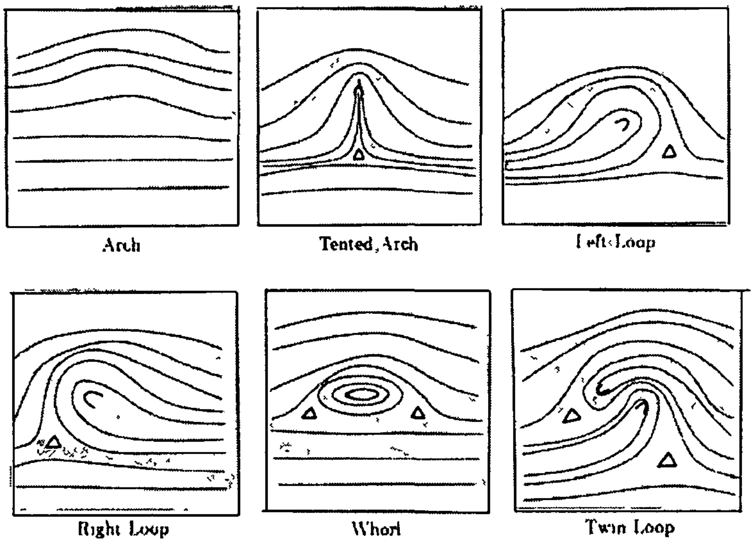


Figure 3-2: Fingerprint Classification

about the coarse level classification and fine level matching is reported below.

A. Coarse level classification using MSOM

Algorithm for self organizing map: Assume that output nodes are connected in an array of and the network is fully connected (all nodes in input layer are connected to all nodes in output layer), as shown in Figure 3-3. In this type of neural network, the learning rate is kept large at the beginning of training epochs and decreased gradually as learning proceeds.

SOM has been used in this work as a basic classifier, where each fingerprint image is described by 256x256 pixels divided into 16x16 blocks. The orientation of each block is used as input to the neural network so the input layer consists of 256 nodes. Each image can fall into one of the

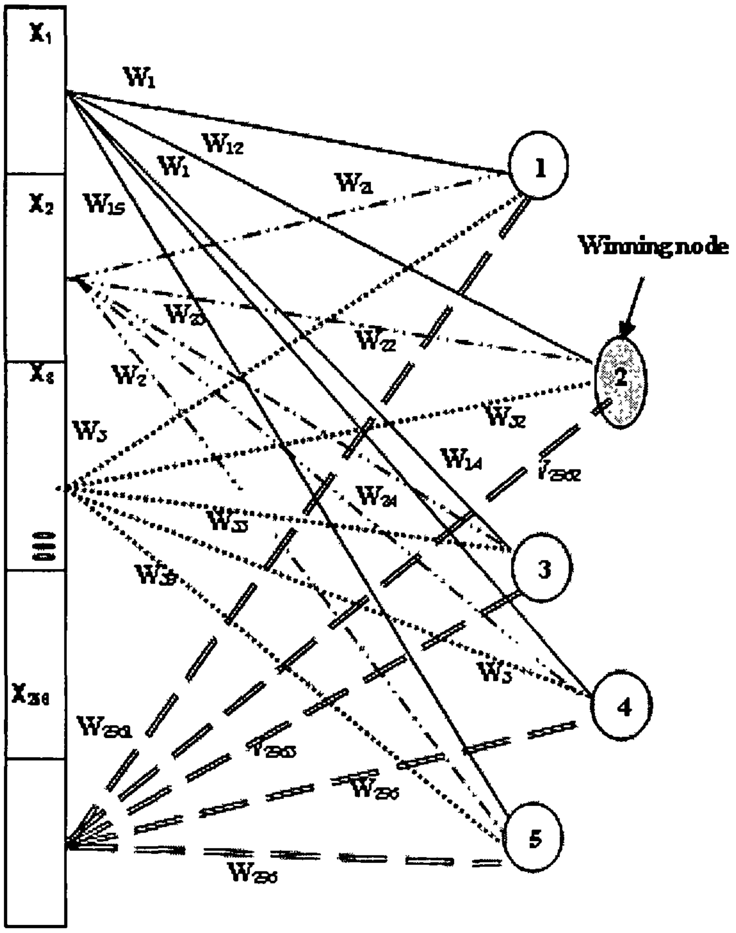


Figure 3-3: Basic structure for a well-trained fingerprint SOM, where winning node is 2, so the input vector X is of class 2..

five classes (right loop, left loop, whorl, arch, tented arch), so the output layer consists of five nodes. The learning rate which we used is a = 0.5 and neighborhood radius R= 0. This process is designed to facilitate the identification process whenever the system is used, thus the searching time will be reduced as the system search only in one cluster. The learning algorithm [64], [65] of such network can be described as in Figure 3-4.

SOM construction and training Steps are as follows.

The neighborhood function is a window centered around the winning node d_{min}, whose radius decreases with time. In the implementation, the radiuses are simply set to decrease from the map size m to 1 during all the K runs. The learning rate function $L(t)$ is also a decaying function. It is kept large at the beginning of training and decreased gradually as learning proceeds.

```
1. Construct an $m \times m$ SOM and initialize all the weights.
2. Input a fingerprint vector: $\{x_1, x_2, ...x_{256}\}$.
3. Find the winning node $d_{min}$:,
$d_{min}$:=min$\{||x - w_i||\}$,
where $||.||$ denotes the Euclidean norm and $w_j$ is the weight vector connecting input nodes to output node $j$.
4. Update the weight vectors:
$w_{ij}(t+1) = w_{ij}(t) + L(t)[x_i(t) - w_{ij}(t)]N(j,t)$
Where $w_{ij}$ is $j^{th}$ component of the weight vector $w_j$,
L(t) is the learning rate and N(j,t) is the neighborhood function.
5. Repeat steps 2-4 till update is not significant.
```

Figure 3-4: Algorithm for the conventional SOM

Instead of original SOM algorithms for training and classification, the modified SOM algorithm using certainty vector as parameter, as depicted at [64] is also used for classification. Here each fingerprint is associated with a certainty vector c. The steps are shown in Figure 3-5.

```
1. Construct an $m \times m$ SOM and initialize all weights.
2. Input a fingerprint vector:
$X_c\{x_1, x_2, ...x_{256}\} = c \times X + (1-c) \times X_{avg}$
where $x_{avg}$ is the vector holding the average values $x_k$ ($k$ from 1-256) over the whole training sample space.
3. Find the winning node $d_{min}$
where: $d_{min}$=min$\{||c(x-w_j)||\}$
4. Update the weight vectors:
$w_{ij}(t+1) = w_{ij}(t) + L(t)[x_i(t) - w_{ij}(t)]N(j,t) x\ c_i$
where: $w_{ij}$ is $j^{th}$ component of the weight vector $w_j$.
L(t) is the learning rate and N(j,t) is the neighbor hood function.
5. Repeat 2-4 till Update is not significant.
```

Figure 3-5: Algorithm for the conventional MSOM

A free SOM toolbox [68] is adopted to assist in the classification.

Result of SOM and MSOM: For coarse level classification we have used FVC2000 and FVC2004 datasets and the results are shown in Table 3.1

Table 3.1: Results of coarse level classification for different map size

Algorithm	The Dataset and their accuracy % with different Map size				
	Training	Testing	5 x 5 map	8 x 8 map	8 x 8 map
SOM	60	20	88%	86%	92%
	200	40	90%	91%	94%
	600	40	91%	93%	94.6%
MSOM	60	20	89%	92%	93.47%
	200	40	91%	92.2%	95%
	600	40	93.3%	94%	95.52%

B. Fine Level grouping using Minutiae Clustering: Here the steps followed are

B.1 Minutiae Extraction: We have used CUBS fingerprint feature extraction tool [73] for minutiae feature extraction. This tool provides a graphical user interface for minutiae feature extraction and visualization. It also allows the user to manually identify new minutiae or remove spurious ones.

B.2 Minutiae clustering for fingerprint similarity metric : After extracting the feature point set N from a fingerprint, we have clustered the feature points using Kmeans algorithm with variable number of clusters. The procedure minutiaeCluster is shown in Figure 3-6.

Procedure minutiaeCluster( )

Input : Fingerprint minutiae M_i , core point $P_i(x, y)$, cluster no. m

Output: k representation of minutiae groups

```
1. For $i = 1$ to $n$
2. Read the minutiae $M_i$ for each class of fingerprints given by MSOM
3. Call KmeansFing($M_i$, m, $P_i$(x, y)) ; to identify k groups;
4. Next i.
5. Next, we report our minutiae graph generation technique.
```

Figure 3-6: Procedure for minutiaeCluster()

B.3 Graph generation over clustered minutiae space : After obtaining the clustered minutiae space, cluster-graphs are generated.

Procedure minutiaeGraph()

Input: Cluster centroids $C_i(x, y)$,

Output: Centroids distance matrix, D_{ij} and graph plot.

```
For i=1 to $m$ do
    Read the centroids $C_i(x, y)$ ;
    For j=1 to $m$ do
        Call DistMatrix($C_i$,$C_j$); to perform Euclidean distance
    Next j
Next i
For i=1 to $m$ do
    For j=1 to $m$ do
        Call minDist($D_{i,j}$)
        Draw graph $D_{i,j}$
```

Figure 3-7: Procedure for minutiaeGraph()

3.3.2.4 Index Generation: In the proposed system, a SOM based classification approach [64], is used for coarse level classification whereas, a graph-theoretic approach is used to analyze the process of fingerprint comparison for finer level matching. Finer level matching is supported by extraction of minutiae i.e. ridge ending and branching points.

From the minutiae graph, an index is generated for each fingerprint, which is unique, i.e., no two fingerprint images will have the same index. An index is generated based on four parameters:

(i) Number of vertex

(ii) Degree of each vertex

(iii) Highest degree.

(iv) Number of vertices with same degree.

The generated index for each minutiae graph is then saved to the database.

3.3.2.5 Matching : Fingerprint matching is done at two levels. At coarse level, fingerprints are classified into whorl, arch, tented arch, left loop, right loop and twin loop. Coarse level classification is good only for faster detection of the class type of a given input fingerprint. At finer level, matching is performed based on the minutiae (i.e. ridge ending and branching points) information.

3.4 Transformation Invariance

The proposed graph based index can be found to be advantageous due to its transformation invariance. To establish the proof of transformation invariance we adopt two approaches i.e.(a) graph-based and (b)distance-based. Next we report each of these approaches.

(a) Graph-based approach We are interested in establishing that two fingerprints which are similar must be matched correctly. To do that we observe the differences comparing the minutiae cluster graphs due to small perturbations in the seed points. To accomplish this, we consider the graph obtained from the minutiae feature point clusters.

Definition I: MinutiaeGraph The graph obtained from the minutiae clusters is referred as the MinutiaeGraph. This graph contains all the topological properties of the minutiae clusters. It tells which vertices are connected, but it does not contain any geometric measures, such as the lengths of the edges and angles they form at each vertex.

Definition II: Fingerprint Equivalence : Two fingerprints F and $F^{/}$ are equivalent, i.e. diff(F,$F^{/}$)=0, if their respective MinutiaeGraphs are isomorphic, else they are distinct.

Using isomorphism classes of minutiae graphs to compare fingerprints has the following advantages

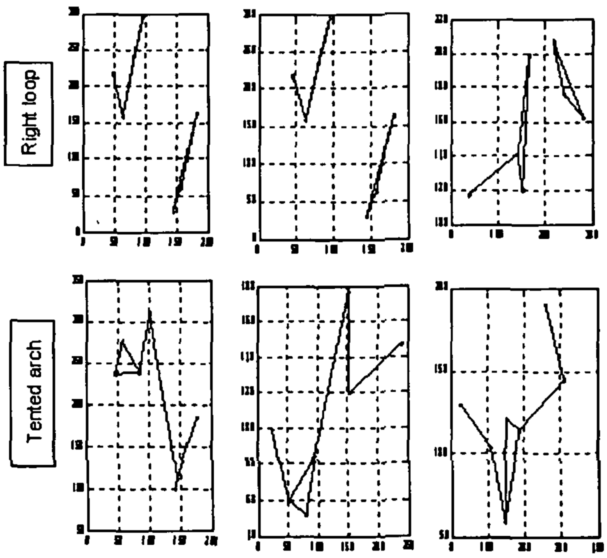


Figure 3-8: Three variations of two types, viz. right loop and tented arch fingerprints graph, proofing their isomorphism under rotation and translation invariance.

1. No effect on the comparison, due to any unintentional rotation, translation, or scaling factor while recording a fingerprint.
2. A slight perturbation in the location of minutiae points will result in a topologically equivalent minutiae graph.

The cluster graphs of each individual impression are tested for isomorphism, proving their transformation invariance. The graphs obtained from two types of fingerprint, each having three impression of each; represent the isomorphic graphs as shown in figure 3. Next we report the distance based approach.

(b) Distance based approach A distance measure for the purpose of object matching should have the following properties.

(1) It should have a large discriminatory power.

(2) Its value should increase with the amount of difference between the two objects. The operation of image matching consists of computing a measure of similarity between two images based on their features.

We have used Hausdorff distance and Modiffied Hausdorff distance (MHD) [74], [75] between two sets of minutiae maps (points) associated with the fingerprint and thus proving the invariance of different fingerprint impressions. Based on [74] we define the Hausdorff distance as follows.

Hausdorff distance: Given two finite point sets M$\bar{m}_1$,m$_2$,....,m$_p$ and N $\bar{n}_1$,n$_2$,.... n$_q$, the Hausdorff distance is defined as

$$H(M,N) = max(h(M,N), h(N,M)) \text{ where } h(M,N) = \max_{m \in M} \min_{n \in N} ||m - n|| \tag{3.1}$$

and ||.|| is the underlying norm on the points of M and N. The function h(M,N) is called the directed Hausdorff distance from M to N. h(M;N) in effect ranks each point of M based on its distance to the nearest point of N and then uses the largest ranked such point as the distance. The Hausdorff distance H(M,N) is the maximum of h(M , N) and h(N , M). Thus it measures the degree of mismatch between any two shapes described by the sets M and N. Our choice of Hausdorff distance is based on its relative insensitivity to perturbations in feature points, and robustness to occasional feature detector failure or occlusion [74].

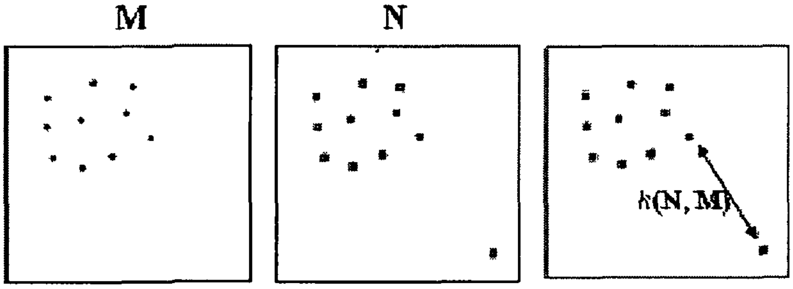


Figure 3-9: The directed Hausdorff distance is large just because of a single outlier.

3.5 Performance Evaluation

To evaluate the performance of the reported fingerprint classifier, we have test the false accept rate (FAR) against the accuracy of the method. FAR is a measure of the fingerprints that are accepted by a certain fingerprint class, while not belonging to that particular class. An example of an event that increases the FAR of a RL (right loop type) class is a non-RL, for instance LL, fingerprint being classified as a RL fingerprint. The FAR of a particular fingerprint class is mathematically modeled as in equation 3.2. The details of the environment used, dataset used and results are as follows:

(a) Environment used: The experiment was carried out on a workstation with Intel Dual-Core processor (1.86 GHz) with 1 GB of RAM. We used MATLAB 7.2 (R2006a) version in windows (64-bits) platform for the performance evaluation.

(b) Datasets used: In order to evaluate the performance of the classifier, dataset is used from FVC2000 and FVC2004.Also we have used a synthetic fingerprint generator SFinGe [89] to create at zero cost, large databases of fingerprints, thus allowing recognition algorithms to be simply tested and optimized. This synthetic fingerprint generator captures the main interclass and intra-class variations of fingerprints in nature are well enough [71]. The image size is of 300×300 pixels.

(c) Experiment Result and analysis: From the result of our experiment we have obtained and hence proved as shown in the Figure 3-8, the following two lemmas.

Lemmal: Graph-based feature index for any fingerprint image remains invariant subject to translation.

Lemma2: Graph-based feature index for any fingerprint image remains invariant subject to any rotational transformation.

$$FAR = (F/S) \times 100 \qquad (3.2)$$

Where F is the total number of fingerprints that are wrongly accepted and S is the total number of fingerprints that are to be recognized. For a good fingerprint classifier, the average FAR value should approach 0% and the value less than 20% are sufficient. The results obtained can be depicted as in the Figure 3-8. From the figure we can see that our method has both better performance and efficient, therefore is more suitable for fingerprint verification application. As the FAR value approaches to 0%, the accuracy level approaches to 100%

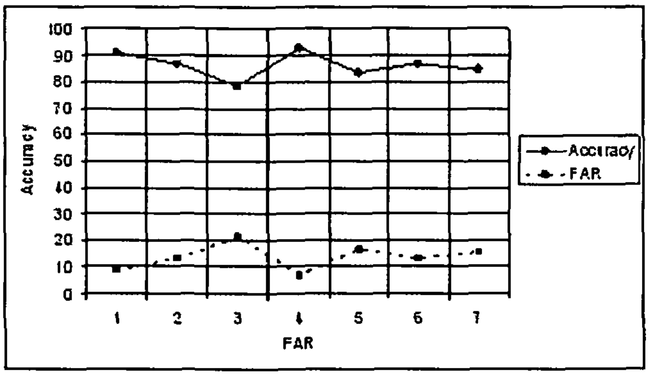


Figure 3-10: FAR vs. Accuracy of MSOM based fingerprint classification

3.6 Discussion

A limited survey on some of the popular fingerprint classification methods was carried out and found capable of identifying four or five classes with an accuracy level of (80-95)%.

The proposed fingerprint classification method works with an accuracy level of 95.52 % for coarse level classification and presents a new approach for graph based fine level matching of fingerprints and their template generation. Also we have reported two techniques, viz. graph based and distance based approach, for proofing robustness of various fingerprints.

Although fingerprint classification and matching techniques have developed drastically over times, there are scopes for developments which will make the process more efficient and accurate. A multiple SOM based approach can be used to enhance the performance.

Next chapter describes an iris authentication scheme and its experimental results.

Chapter 4

IRIS RECOGNITION AND VERIFICATION

Iris is a colored ring-shaped organ in the front part of the eye. It is visible from the outside of the body allowing it to be easily imaged and well protected from external modifiers [81]. The ease of imaging makes iris an ideal biometric. The iris structure is formed in 3^{rd} to 8^{th} month of gestation(prenatal) period and pigmentation can continue after birth. The whole process is considered to be random, unique, chaotic and only dependent on initial conditions in the embryonic mesoderm [83]. Due to this random, unique and chaotic nature and easy acquisition of this contact-less image, the iris is considered as a strong biometric.

The iris is the most visible and distinguishable part of the human eye due to its texture and vibrant color. Iris color have mostly melanin pigment but blue iris is of absence of pigment. The average thickness and diameter ratio of iris is of 0.5mm to

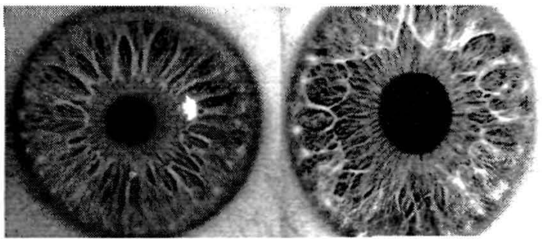


Figure 4-1: Iris Structure [82]

12mm [84]. Iris recognition is the process of recognizing a person by analyzing the iris that possess a high degree of randomness and uniqueness set by combinatorial complexity [81]. Automatic recognition of Iris biometric is relatively safe, accurate and works with high speed without high accuracy [78], [79] due to its complex pattern of many distinctive features like arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette. An ideal iris structure is shown in Figure 4-1.

The automated iris recognition is relatively a young area of research, and patented only since 1994 [81]. But the idea of using iris for personal identification came into light in 19^{th} century. A brief history of the science of Iris and applications are reported as follows :

1885 Alphonse Bertillon had the idea of using iris for personal identification based on color and pattern type.

1936 Frank Burch, an ophthalmologist proposed the idea of using iris patterns as a method to recognize an individual.

1985 Dr. Leonard Flom and Aran Safir, two ophthalmologist had gave the idea that no two iris patterns are alike. They got patent for their iris identification concept in 1987

1993-1995 Dr. Daugman, Dr. Flom and Safir worked together for the Defense Nuclear Agency to test and deliver a prototype unit.

1994 Dr. Daugman received patent for his automated iris recognition algorithm.

The four basic advantages of using iris as a biometric are:

- Iris patterns possess a high degree of randomness and uniqueness set by combinatorial complexity.
- Encoding and matching are reliable and fast.
- Iris codes very compact to store (hundreds of bytes).
- Changing pupil size can confirm it is a real iris.

4.1 Prior related work

Many methods have been proposed for iris recognition. Daugman [54] has excellent performance on a diverse database of many images. A method for personal verification based on automatic iris recognition was given by Wildes [86]. A method for iris feature extraction based on zero-crossing representation of 1-D wavelet transform was given by Boles et al. [77]. The comparisons of the steps for preprocessing iriscode used in the different recognition methods as shown as below

Preprocessing	Segmentation	(a) Wildes approach: An automatic iris segmentation based on circular Hough transform was used to deduce the radious and entre co-ordinates of the pupil and iris regions .
		b) Daugman's Integro-differential Operator approach: Daugman makes use of an integro-differential operator for locating the circular iris and pupil regions, and also the arcs of the upper and lower eyelids. The integro-differential operator is defined as 5
	Normalizaion	(a) Daugman's Rubber Sheet Model[1]: This method maps each point within the iris region to a pair of polar coordinates (r,è) where r is on the interval [0,1] and è is angle [0,2ð].
		(b) Wildes et. al.'s Image Registration approach: geometrically warps a newly acquired image, into alignment with a selected database image [4]. When choosing a mapping function to transform the original coordinates, the image intensity values of the new image are made to be close to those of corresponding points in the reference image. The mapping function must be chosen so as to minimise].

4.2 Background of the work

Iris recognition steps comprise four basic steps such as (1) image acquisition, (2) iris preprocessing, which includes localization; segmentation and normalization, (3) feature extraction or encoding, (4) iriscode comparison or matching. Next we discuss each of these steps in detail.

4.2.1 Image acquisition

One of the main problems of iris recognition is image acquisition. A low quality sample, may result in a faulty verification. In order to extract a sufficient amount of detail the iris section in the eye image should be no less than 70 pixels [81]. With a high resolution camera of average diameter of size 12mm, the details of the collarette pattern of iris can be captured. Many commercial products have in their products dual lens, one for localization of iris in the scene and another for narrowing the focus to the target image thus providing a high resolution snapshots of the image.

Illumination is another problem in image acquisition, as the illumination angle will determine the dark and light parts of the image and two different classes be generated by the same iris at two different illumination angle. Monochrome CCD camera with near infrared illumination are used for this purpose.

In case of CASIA Iris database a special camera that operates in the infrared spectrum of light, not visible by the human eye is used.

4.2.2 Iris preprocessing

The task of iris preprocessing is executed in three steps, viz. (i) localization, (ii) segmentation and (iii) normalization

i) Localization: In this step, the iris region in an eye image is located. The iris region can be approximated by the region between two boundaries, one for the iris/sclera boundary and another for the iris/pupil boundary. The boundary region of an iris can be easily viewable in Figure 4-2.

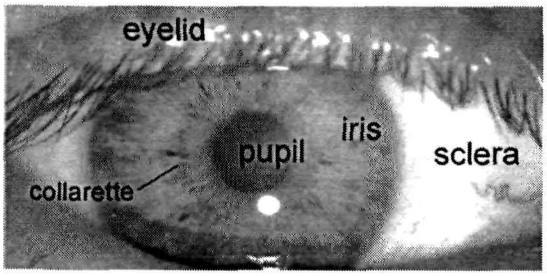


Figure 4-2: Boundary of an Iris

The Hough transform is a standard method for detecting the primitive geometric objects like lines, circles present in an image. But due to its limitations, to deduce the radius and coordinate center of the pupil and iris regions of an iris image, the circular Hough transform is used [85].

AS the pupil is located within the iris region only, the circular Hough transform is applied on the iris/sclera boundary first and then in the iris/pupil boundary, instead of the entire eye image. For the CASIA iris database as the values of the iris radius, known to be 90 to 150 pixels and the pupil radius ranges from 28 to 75 pixels, the circular boundary detection process provides the radius and x and y coordinates for both circles.

ii) Segmentation: The purpose of segmentation step is to separate the input iris image into several components making it feasible to extract features easily. To isolate and exclude the artifacts like eyelids and eyelashes as well as locating the circular iris region an effective technique is needed. The circular Hough transform can be used for detecting the iris and pupil boundaries [85]. The pupil is the largest black area in the intensity image. Hence by using a suitable threshold of the intensity image, its edge can be easily detected from the binary image.

iii) Normalization: Normalization of iris region is needed to transform the region into fixed dimensions so as to allow comparisons. Daugman's famous rubber Sheet Model is used for iris normalization where the segemnted iris region is resampled to a fixed-size rectangular image by mapping the extracted iris region into a normalized coordinate system by defining the iris location by two coordinates (r, θ), such that $0 \leq r \leq 1$ and $0 \leq \theta \leq 360^0$.

4.2.3 Encoding or Feature extraction

In this step, iris patterns are created. The most discriminating feature of iris pattern is the phase information. Extraction of the phase information is done using 2D Gabor wavelets according to Daugman (2004)[14]. In this step, the 2D normalized pattern is broken into a number of 1D signals, and these signals are convolved with 1D Gabor wavelets. Each row of the 2D normalised pattern corresponds to a circular ring on the iris region. The angular direction corresponds to columns of the normalized pattern is taken rather the radial one, since maximum independence occurs in the angular direction.

Gabor wavelet: Gabor wavelets are useful tools to detect edges, corners and blobs of images. Gabor wavelets are series of mutually similar Gabor functions created by dilation and shift from one elementary Gabor function, i.e,

$$g_{\alpha,\xi,a,b}(x) = |a|^{-\frac{1}{2}} g_{\alpha,\xi}(\frac{x-b}{a}) \tag{4.1}$$

for $a \in \Re^+$ (scale) and $b \in \Re$ (shift).

The idea behind the 2-D Gabor wavelet is that the wavelet can be used to decompose the data in the iris region into components that appear at different resolutions. A series of wavelet filters is applied to the 2D iris region for each of the resolutions. Encoding of the wavelet pattern provide a compact and discriminating representation of the iris patterns.

4.2.4 Iriscode comparison or matching

Matching a pair of iris images means to measure how different they are or to decide whether they belong to the same individual or not. The bitwise comparison of iriscode can be made using the Hamming Distance(HD).

- Hamming distance was chosen as a metric for recognition by Daugman since bit-wise comparisons were necessary. Two templates are considered to have been generated from the same iris if the Hamming distance produced is lower than a set Hamming distance which is defined as

$$HD = \frac{1}{M}\sum_{j=1}^{M} X_j(XOR)Y_j \tag{4.2}$$

and calculates the amount of different bits in binary sequences X and Y over total number of M bits by the sum of the exclusive-OR between X and Y. As matching incorporates noise masking, so that only significant bits are used in calculating the Hamming distance between two iris templates. Only those bits in the iris pattern that correspond to 0 bits in noise masks of both iris patterns will be used in the calculation. The Hamming distance will be calculated using only the bits generated from the true iris region,and this modified Hamming distance formula as given by Daugman is as

$$HD = \frac{||(templateA(XOR)templateB)\bigcap maskA \bigcap maskB||}{||maskA \bigcap maskB||} \tag{4.3}$$

where *templateA* and *templateB* are two iris templates to be matched and *maskA* and *maskB* are the corresponding masks specifying which bits of the templates belong to the valid region of iris.

The goal of our research is to perform the pattern matching of iris template with Weighted Euclidean distance and also with the Jaccard distance and by their fusion with the hamming distance so that verification accuracy is more.

- Weighted Euclidean distance (WED): It is a measure of similarity of collection of values between two iris templates. The WED is defined as

$$WED(k) = \sum_{i=1}^{N} \frac{(f_i - f_i^k)^2}{(\delta_i^k)^2} \tag{4.4}$$

Where

f_i : ith feature of unknown iris

f_i^k : ith feature of iris template k

δ_i^k : standard deviation of the ith feature in iris template k

The unknown iris template is matched with the iris template k if WED is minimum at k.

- Jaccard distance(JD): It is a distance measure between binary feature vector given by P. Jaccard is defined as

$$JD(\imath, k) = \frac{x^T y}{x^T y + x^T Y + X^T y} \tag{4.5}$$

The value of JD ranges from 0 to 1.

4.3 Work done

The biometric verification problem is a classification problem that classifies from two given randomly selected biometric samples, whether they belong to the same person or not. The flow diagram of iris verification is as shown in Fig. 4.3 below.

First features are extracted using Daugman method of iris code detection [81] from iris. The Iris recognition system followed by image segmentation based on the Hough transform called localization of circular iris and pupil region, occluding eyelids and eyelashes and reflections. The extracted iris region was then normalised into a rectangular block with constant dimensions. Finally encoding is done by extracting the phase data from 1D Log-gabor filters and quantised to give the unique pattern of the iris into a bit-wise biometric template.

Let $x : \{x_1, x_2, ...x_d\}$ and $y : \{y1, y2, ...yd\}$ denote two feature sets extracted from iris biometrics. Let c(x) denote the class of the person that x belongs. As the matching is based on distance measure, two distributions are generated viz. intra-distance (or within person) that occurs when c(x)=c(y) and inter-distance (or two different person) when c(x) $\neq$ c(y). So by assuming that the distributions are normal , it is easy to find the decision threshold to minimize the FAR and FRR.

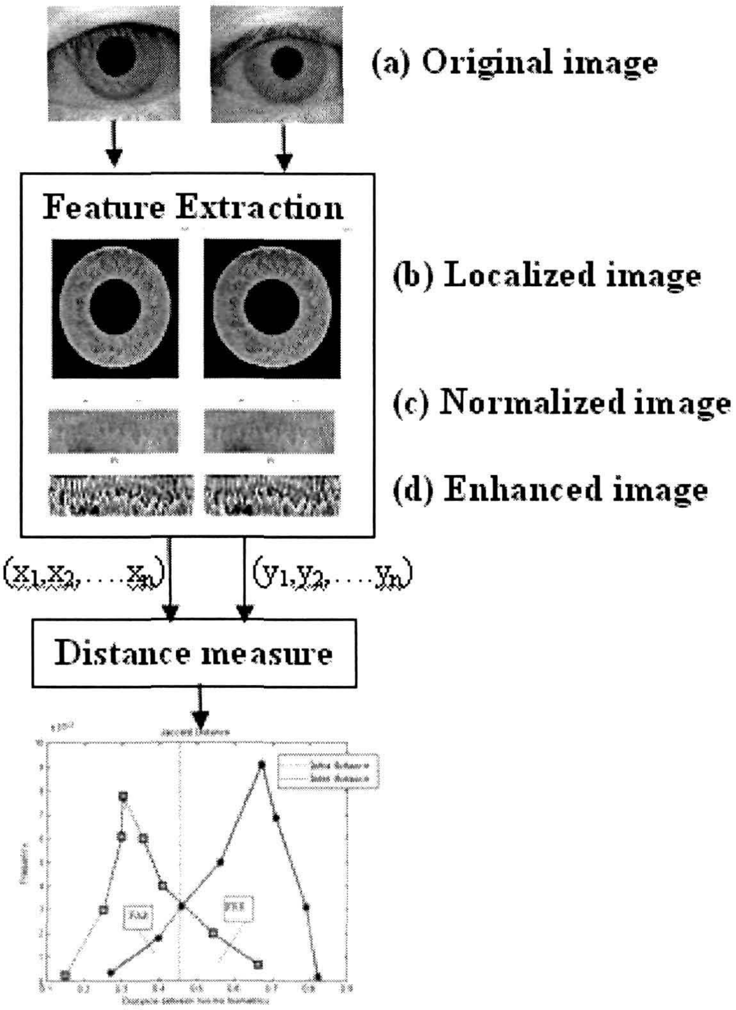


Figure 4-3: Iris verification model

The Iris code comparison or matching is done to check if the two irises belong to the same person or not , hence a distance measure give the intra distance distribution tends to be close to 0 while the inter distance distribution tends to be far from 0. The goal of this research is to perform and extending the pattern matching techniques using different distances like(i) Jaccard distance, (ii) Weighted Euclidean Distance, (iii) Hamming distance and comparing their results individually and by their classifier fusion.

The expression for classifier fusion for similarity measure is given by

$$f(x) = \begin{cases} 1, & \text{if } WED < t_b \\ HD, & \text{if } t_b \leq WED \leq t_a \\ 0, & \text{if } WED \geq t_a. \end{cases} \tag{4.6}$$

4.4 Performance Evaluation

AS iris biometric verification involves a distance or similarity measure between two samples of the same class and between samples of two different classes, the feature distance between the two iris biometric samples can be classified as intra-person (identity) or inter-person (non-identity). The two distributions from the intra-person and inter-person distances have some overlap with each other.

The performance protocol given by [56] is used to measure the accuracy of the iris verification system. To evaluate similarity measures for binary features, we chose two types of errors, False Accept Rate (FAR) and False Reject Rate (FRR). For a stored template T and input template I to be verified if $H0$ and $H1$ represent null and alternate hypotheses, $H0$ and $H1$ are defined as:

$H0{=}I \neq T$, if input I is not from the same person as the original template.

$H1{=}I = T$, if input I is from the same person as the original template.

Also the decision variables $D0$ and $D1$ are represented as

$D0$: The person is not claimed to be.

$D1$: The person is the claimed identity one.

Mathematically the conditional probability of an event A for a given event B is defined as

$$P(A|B) = \frac{P(B|A).P(A)}{P(B)} \tag{4.7}$$

Hence, the FAR and FRR are defined as:

$$FAR = P(D1|H0 = True) \tag{4.8}$$

$$FRR = P(D0|H1 = True) \tag{4.9}$$

4.4.1 Environment used

The experiments were carried out on a workstation with Intel dual-core processor (1.86 GHz) with 1 GB of RAM. We used MATLAB 7.2 (R2006a) version in windows (64-bits) platform for the performance evaluation.

4.4.2 Datasets used

We have used one benchmark dataset for iris trait. The details about the datasets are given in Table 4.1. The iris dataset ia available in [91]. For the verification experiments, the datasets are divided into two parts training and test sets. The results are generated using K-folded errors validation method

Table 4.1: Iris dataset details

Dataset types	Training	Test
Iris CASIA V.1	324	432

4.4.3 Experimental Result and analysis

1. Experiment 1. In this section, a comparison of experimental results are made by using several similarity measures. From iris dataset(CASIA V.1), we obtain the matching scores for different iris images and the corresponding error rates

are generated using different threshold values. After obtaining the matching scores of different iris, the error rates are generated using different threshold values.

From the result of our experiment we have obtained ROC curves as shown in Figure 4-4. The FAR and FRR values are reported in Table 4.2. It can be seen from the table as well as from the figure that result is satisfactory. The ROC curve for the CASIA V.1 Iris dataset is depicted in Figure 3.

Table 4.2: FAR/FRR values of CASIA V.1 dataset

Threshold	FAR	FRR
0.3200	0.0007	44.5988
0.3400	0.0007	33.5648
0.3600	0.0021	23.6883
0.3800	0.0100	16.8210
0.4000	0.0436	12.1142
0.4200	0.3358	8.7191

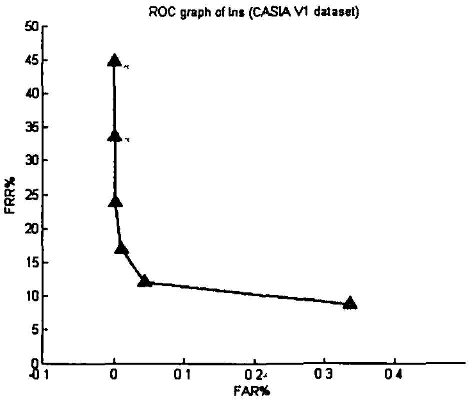


Figure 4-4: ROC curve of Iris biometric (CASIA) dataset.

2. Experiment 2: In order to extend the proposed model, we have again divided the entire samples into two sets: intra-class distance sets and inter-class distance sets by randomly selecting two iris data from the same subject and from two different subjects respectively. We prepared three datasets(DB1,DB2,DB3) from CASIA

V.1 of intra-distance and inter-distance data for both training and testing, each of size 1000 as given in Table 4.3.

Table 4.3: Datasets used for cross-comparison of samples

Samples	Dataset types			
	Class	DB1	DB2	DB3
Training	Intra class	500	600	400
	Inter class	500	400	600
Testing	Intra class	500	400	600
	Inter class	500	600	400

In this section, we compared the experimental results obtained by using different distance measures. From the two created sample sets, intra-class distance and inter-class distance sets as given in Table 4.3, the Iris verification model is tested.
The FAR and FRR values with recognition rates are reported in Table 4.4. It can be seen from the table as well as from the figures that results are satisfactory. Each scalar distance value is classified into intra or inter person class by comparing with the threshold values as depicted in the three distribution curves in Fig. 4.5., Fig. 4.6 and Fig. 4.7 with respect to three distances Hamming, Jaccard and Weighted Euclidean distances are shown respectively.

Table 4.4: Performance of the various distance measures

Method	CASIA V.1 dataset								
	Datal			Data2			Data3		
	FAR	FRR	Rate(%)	FAR	FRR	Rate(%)	FAR	FRR	Rate(%)
HD	0.33	0.91	95.5	0.51	0.8	96	0.56	0.73	95.8
JD	0.29	0.40	95.7	0.65	0.9	95	0.3	0.9	95.3
WED	0.41	1.2	93	0.58	1.1	93.5	0.67	.11	92.8

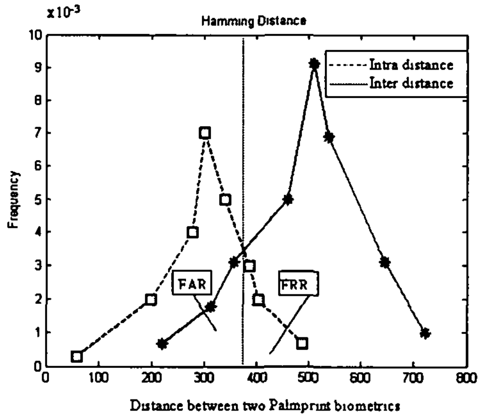


Figure 4-5: Distribution curves for Inter class and Intra class w.r.t. hamming distance.

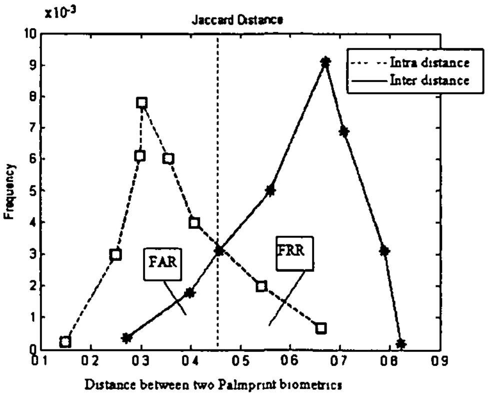


Figure 4-6: Distribution curves for Inter class and Intra class w.r.t. Jaccard distance.

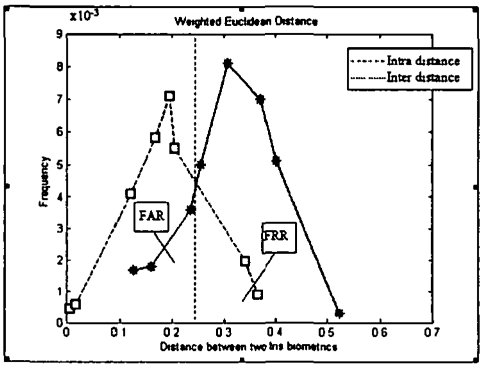


Figure 4-7: Distribution curves for Inter class and Intra class w.r.t. Weighted Euclidean distance.

4.5 Discussion

A cross-comparison was performed to build the distribution of imposter and genuine match scores.

We attempted to draw distribution curves for both imposter and genuine for Daugman's approach using Hamming distance, Jaccard distance, Weighted Euclidean distance by calculating Inter-class and Intra-class distributions. Selecting and designing a distance measure is a difficult task as Iris biometric verification involves measure of binary feature vector distances and verification of the identity of a person.
The curves also depict the optimization of threshold values of the individual match scores of a person with effective to specific application data.

In the next chapter, we are describing a palmprint based verification scheme and its experimental results.

Chapter 5

PALMPRINT RECOGNITION AND VERIFICATION

Palmprint is a hand-based biometric, rich of information presented in friction ridge impression. It provides information of the raised portion of the epidermis (the outermost layer of skin) containing ridge structure, ridge characteristics and ridge flow details. Due to its uniqueness and permanence characteristics, like fingerprint, it is also used for over a century as a trusted media for user identity proof. But due to the restrains in live-scan technologies and its computing capabilities, it is automated slowly than other competing biometric measures.

A palmprint can be either an online image or offline image taken with paper or ink respectively. Palmprint recognition uses the palm region of a person as a biometric for identifying or verifying identity of the person. The palm is the inner surface of our hand from the wrist to the root of fingers.

Earlier in 19^{th} century, in many instances, palmprint examination was the only method of distinguishing illiterate person from each other. But automated palmprint recognition is relatively young. A brief history of the science of palmprint biometric and its applications are reported as follows :

1997 - First palmprint identification is made in Nevada. The bloody palmprint, found on a letter left at the scene of a stage coach robbery and murder of its dnver, was identified to Ben Kuhl.

1997 - A US company bought a palm system embedded with palm and fingerprint identification technology.

2004 - California along with other two states established state wide palmprint databases by submitting unidentified latent palmprint by the law enforcement agencies. Australia have the largest repository of palmprints in the world. The new Australian National Automated Fingerprint Identification system (NAFIS) includes 4.8 million palm prints.

Palmprints can be used for criminal, forensic or commercial applications like

(i) It is used in medical diagnosis like genetic disorders and downs syndromes to detect genetic abnormality.

(ii) At the crime scenes, palmprints are often found as part of the unprotected hand or sometime may be due to slipping of offender's gloves during the commission of the crime and thus exposing part of the unprotected hand..

(iii) In Chinese culture, there is a "Fortune telling' for the indication of past and future based on the palmprints.

The palmprint provides large quantity of information and have many advantages. It deals with more stable physical characteristics and hence more stable biometric. It is mostly an acceptable biometric due to its permanence and uniqueness. Even identical twins have different principle lines, wrinkles, minutiae, datum point features and texture images [98]. The basic advantages [93], [94] of using palmprint as a promising biometric are its

- High distinctiveness
- Permanence
- High performance

- Non-intrusiveness
- Low-resolution imaging
- User-friendliness
- Low price palmprint devices, and
- High stability

However, the palmprint has a serious disadvantage also. The palmprint may undergo changes depending on the type of work the person is doing over a long duration of time.

A palmprint basically shows certain skin pattern of a palm, composed of many physical characteristics like lines, points, and texture of the skin. The palmprint epidermis may be as thick as 0.8 mm comparing to other part of our body which is 0.07 to 0.12 mm thick. In response to continuous pressure and friction after birth, the epidermis gradually becomes thicker. Palm in general contains three flexion creases (i)Permanent creases (principal lines), (ii) secondary creases (wrinkles) and (iii) ridges . These three major flexions are genetically dependent [91].

In this work we have concentrated on a palmprint verification method. The method exploits a ROI(Region of Interest) detection technique and a classification method. The classification method works based on various similarity measures for the matching scores obtained at various threshold values. The performance of the method was established using benchmark datasets and the results have been found satisfactory. Next, we describe the prior related work.

5.1 Prior related work

Personal verification using palmprint biometric has received considerable attention and numerous approaches have been proposed in the literature.

Use of Sobel and Morphological operations of palmprint was found to be suitable in many network-based applications analyzed by Chin Chuan Han et al [94]. In this paper they have suggested region extraction steps to obtain a square region in a palm table which is called ROI. A method of locating and segmenting the palm print into ROI using elliptical half-rings has been reported by Poon et al [100] to improve the identification.

The use of ROI while applying correlation filter classifiers for palmprint identification and verification has been reported by Pablo Hennings [101]. In this work three different regions of pixel sizes: 64×64, 96×96, 128×128 has been used. Two reference points were first determined from the hand geometry, and square regions are extracted after aligning these two points with the vertical axis.

J.Z. Wang, J. Li, and G. Wiederhold have proposed an integrated region matching (IRM) scheme which allows for matching a region of one image to several regions of another image and thus decreases the impact of inaccurate segmentation by smoothing over the imprecision. The scheme is implemented as SIMPLIcity system [102].

Ying-Han Pang et al. have used various moments (ZM, PZM and LM) as feature descriptors [103]. In the first stage of their experiment a localization of palm print region has been implemented as per methodology given by Tee Connie et al. [104]. Different methods in palmprint feature extraction using ROI has been analyzed by Kasturika et al [105].

5.2 Background of the work

Palmprint recognition steps comprise four basic steps such as (i) image acquisition, (ii) palmprint preprocessing, (iii) feature extraction or encoding, (iv) palmcode comparison or matching. Figure 5-1 shows a generic palmprint verification system. Next we discuss each of these steps in detail.

5.2.1 Image acquisition

In this step, a sensor scans the palmprint of the user and acts as the interface between the user and the verification system. The palmprint image acquisition may be off-line or on-line. In case of off-line verification, all palmprint samples are inked, which

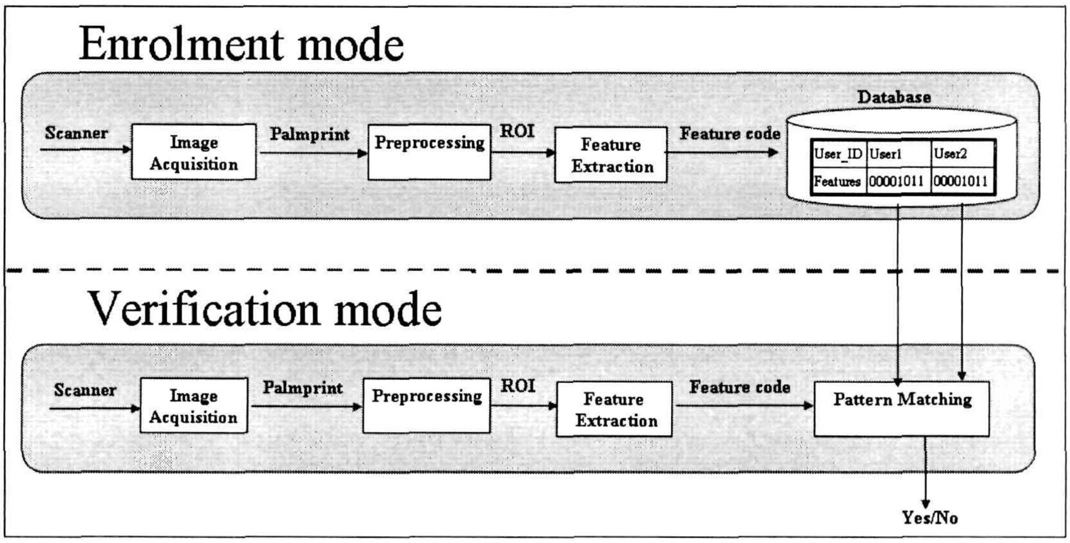


Figure 5-1: A palmprint verification system

are then transmitted into a computer with a scanner. Whereas, in case of on-line identification, the samples are captured with a palmprint scanner which is connected to a computer for storage.

5.2.2 Palmprint preprocessing

Palmprint preprocessing involves alignment of different palmprints under the same coordinate system so that the expected area of each palmprint, called ROI can be extracted for use in feature extraction and matching. Many ROI detection algorithms involve the detection of key points between fingers. In general, palmprint preprocessing have five steps, (i) binarization, (ii) contour detection of the finger and/or palm region, (iii) detecting the key points, (iv) establishing a coordinate system and (v) extracting the central parts. The details of the steps are as follows :

(i) Binarization: Image thresholding operation is used to obtain a binary palmprint image. As image background is stable(black), after computing a threshold value, can be subsequently used for other images.

(ii) Contour detection of the finger and/or palm region: Here, we obtain the binary image countour by first applying the canny edge detection method [99] and then finding the boundary of the image.

(iii) Key points detection: The key points detection of the hand boundary is useful for proof of transformation invariance of the palmprint representation. The key point detection algorithms are of different types. It may be of (a) finger-based, (b) bisector based and (c) tangent based.

(iv) Establishing a coordinate system: To establish the coordinate system using finger-based key point detection, Han proposes one approach, based on the index, middle and ring fingers [95]. This is a wavelet based multiple finger approach that uses a set of predefined boundary points on the three fingers to construct lines in the middle of the three fingers so that the lines from index and ring fingers are used to set the orientation of the coordinate system and the line from the middle finger is used to set its position. Another approach given by Han et al. [94] is based on the middle finger that uses a wavelet to detect the finger trip and the middle point in the bottom finger and draw a line passing through these two points. In the tangent-based approach, two convex curves are drawn as a boundary, one from index finger and middle finger and other from ring finger and last finger. The intersection points between the tangent to these curves give the key points for establishing the coordinate system. In case of bisector-based approach [97], [96], a line is drawn between the center of gravity of a finger boundary and the middle of its start and end points. Their intersection points give a key point.

(v) Extracting the ROI: The goal of ROI detection is to obtain a sub-palmprint image for feature extraction and to eliminate the variation caused by rotation and translation.

The details of our preprocessing steps are shown in the Figure 5-6 to Figure 5-5.

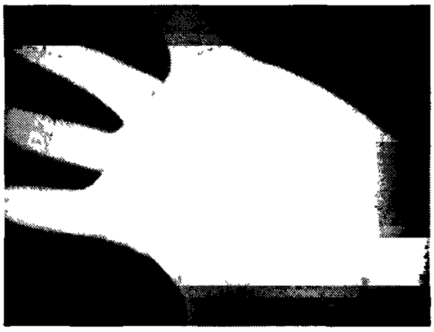


Figure 5-2: An original palmprint image

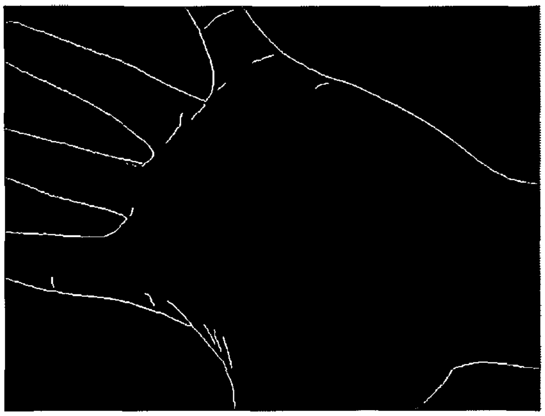


Figure 5-3: Binarization of the image

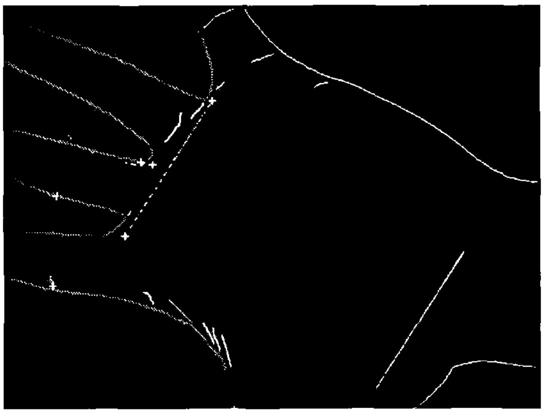


Figure 5-4: Contour and co-ordinate point detection of the image

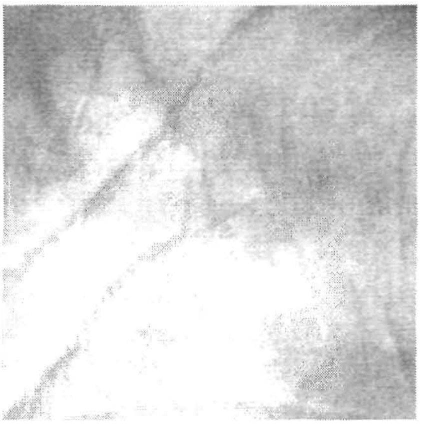


Figure 5-5: ROI of the image

5.2.3 Palmprint Feature extraction

Palmprint contains large number of different types [91] of features as depicted in the Figure. 5-6 and Figure 5-7 for both the off-line and on-line images. The features that are used to identify a person uniquely can be divided into three different categories.

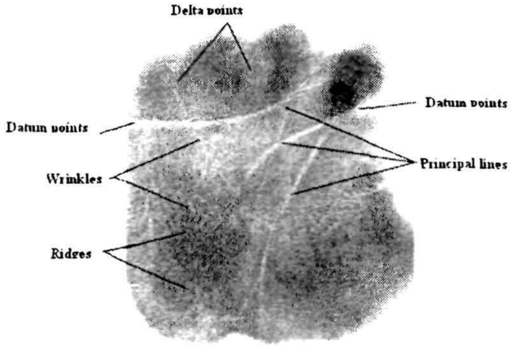


Figure 5-6: Palmprint features definition (off-line). Source [92]

1. Point features: These are the features that can be obtained from palmprint images with high resolution.

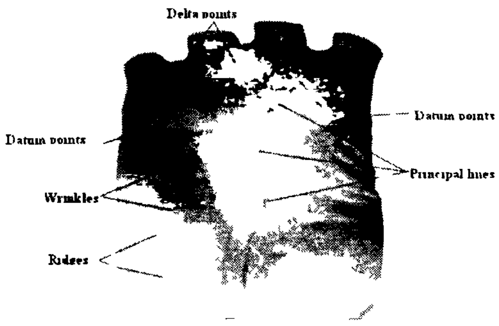


Figure 5-7: Palmprint features definition(on-line). Source [92]

- Datum Points features: These are two end points obtained by using the principal lines. They provide a stable way to register palmprints by intersecting both sides of a palm. Distance between these two points give the size of a palm.
- Delta point features: A delta point is the center of a delta-like region in the palmprint. In general they are in the finger root region. They provide unique and stable measurements for palmprint recognition.
- Ridge features (Minutiae details): The ridge structures of a palm region are the outer cellular layer of the skin and permanent thickening of the epidermis. Minutiae details of ridge section give finer details about palmprint as another measure for identity verification.

2. Line features: These features include three relevant palmprint principal lines, due to flexing the hand and wrist in the palm, and other wrinkle lines and curves (thin and irregular).

    - Principal-line features: They are the flexure creases that may vary from person to person. Physiological characteristics like location and form of principal lines in a palmprint are useful for identifying or verifying individuals as over time these features vary.
    - Wrinkle features: Wrinkles are the lines to provide the skin with a certain amount of stretchability. In a palmprint, there are many wrinkles, which

are different from the principal lines in that they are thinner and more irregular, so more detailed features can be obtained. These features provide the skin with classification details of coarse level and also fine level so that more details can be achieved.

3. Texture features: Palmprint are rich of texture information. These are the geometry features like width, length and area of a palm's shape. According to the palm's shape, we can extract the corresponding geometry features easily. The texture features have advantages over other features that, images can be obtained at low spatial resolution and hence can be smaller in size and the system is less sensitive to noise.

Out of these features, the point features can be obtained only from inked palmprint with high resolution whereas both inked and inked-less palmprint provide all the features [91].

5.2.4 Palmcode comparison or matching

Matching a pair of palmprint means to measure how different they are or to decide whether they belong to the same individual or not. As our goal is to verify palmprint by classifying between imposter and genuine users, pattern matching can be performed using the Hamming Distance(HD). The effectiveness of the method is done with the help of other distance measures also. The details of the distance measures that are used are as follows:

- Hamming Distance (HD) was chosen as a metric for recognition since bit-wise comparisons were necessary. Two templates are considered to have been generated from the same palmprint if the HD is less than a user specified threshold value which is defined as

$$HD = \frac{1}{M}\sum_{j=1}^{M} X_j (XOR) Y_j \tag{5.1}$$

and calculates the amount of different bits in binary sequences X and Y over total number of M bits by the sum of the exclusive-OR between X and Y.

- Weighted Euclidean Distance (WED) is a measure of dissimilarity of collection of values between two palmprint templates. The WED is defined as

$$WED(k) = \sum_{i=1}^{N} \frac{(f_i - f_i^k)^2}{(\delta_i^k)^2} \tag{5.2}$$

  Where

  f_i : i^{th} feature of unknown palmprint

  f_i^k : i^{th} feature of palmprint template k

  δ_i^k : standard deviation of the i^{th} feature in palmprint template k

  The unknown palmprint template is matched with the palmprint template k if WED is minimum at k.

- Jaccard distance(JD) is a distance measure between binary feature vector given by P. Jaccard is defined as

$$JD(i,k) = \frac{x^T y}{x^T y + x^T Y + X^T y} \tag{5.3}$$

  The value of JD ranges from 0 to 1.

Although in the literature, there are many proximity measures for binary data handling, we have chosen these three proximity measures because of the following reasons.

- In case of Hamming distance(HD), it is easy to implement and two palmcode pattern generated from two similar palmprint will be of highly correlated in nature. Moreover, it has faster response and established for wide range of application domains of binary data. But for two binary pattern of genuine or imposter classification, if the HD provides equal weights to all responsible bits in the binary palmcode, the performance of the system may degrade.

- More reasonable way is to put different weight for different elements of the binary descriptors. Assigning the weight would not effectively put all the measurements on the same scale in case of WED. As WED is used for numeric data only, converting the binary feature vectors to a numeric one, it is used as a proximity measure. It is giving a good result from the benchmark CASIA V1. palamprint dataset we have used in our palmprint verification method.

- To compare and test our result with another binary feature vector measure we have adopted JD because it is also used for a wide range of application domains of binary data handling and its responses are faster.

5.3 Motivation

The motivation of this research is to develop

i) a palmprint verification method using a 2-D circular Gabor filter and to generate a feature code (PF_Code) from the extracted ROI. For each location in the region of interest, Gabor response is converted into a binary format. This can be considered as a feature reduction method, as Gabor response will be 1 or 0. Afterwards, pattern matching is done using hamming distance.

ii) a classifier to support the verification system for two randomly selected palmprint samples, whether they belong to the same person or not based on the distance measures using different distances like HD, WED and JD and by designing a fusion rule for classification using HD, WED and JD.

5.4 Palmprint recognition for personal verification: Proposed Method

In this work, a method has been developed for verification of identity using palmprint information. It follows three basic steps for palmprint recognition: (i) apply an adjusted circular Gabor filter initially to the preprocessed palmprint images, (ii) Codify the signs of the filtered images as a feature vector, and (iii) Measure the difference between two plamprint representations using the normalized hamming distance. It also provides robustness against varying brightness and contrast in images. In biometric research, Gabor filters have been applied to feature extraction iris, face and fingerprint recognition.

To support palmprint based classification, a palmprint featurecode(PF-code) is generated where the proposed method for palmprint verification comprises of distinct stages as shown in Figure 5-9 for algorithm of PF_code computation as depicted in Figure 5-8.

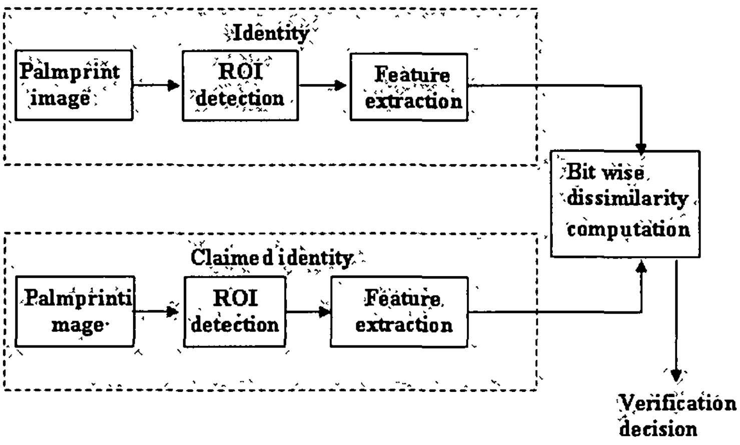


Figure 5-8: Proposed palmprint verification system

5.4.1 Our method

After detection of ROI, segmentation and normalization (size and orientation) steps, we calculate a set of palmprint texture features.

As the proposed method has been developed with reference to generated features of palmprint image, a method called PF_code is proposed, the short review of which is given in the following algorithm.

To generate a meta representation called PF_code based on the feature extraction for palmprint image we develop a routine called PF_code() which is shown in Figure 5-9 For illustration of working of our method let us assume that x : $\{x_1, x_2, ...x_d\}$ and y : $\{y_1, y_2, ...y_d\}$ denote two feature sets generated from palm-

```
Input a palm image.
Extract ROI.
Obtain a palmprint vector: $\{x_1,x_2,..x_{256}\}$ from ROI.
Apply an adjusted circular Gabor filter:
$G(x,y,\theta,u,\sigma) = \frac{1}{2\pi\sigma^2}exp\left\{-\frac{x^2+y^2}{2\sigma^2}\right\}exp\{2\pi i(ux\cos\theta + uy\sin\theta)\}$
Obtain feature vector, PF_code as the sign of the filtered image.
Measure and find out the difference between two PF_code using distance measures.
```

Figure 5-9: Algorithm for PF_code computation

print biometrics. Let c(x) denotes the class of the person that x belongs to. As the matching is based on distance measurê, two distributions are generated viz. intra-distance (or within person) that occurs when c(x) = c(y) and inter-distance (for two different persons) when c(x) $\neq$ c(y). So by assuming that the distributions are normal, we find a decision threshold to minimize the FAR(False Acceptance Rate) and FRR(False Rejection Rate).

As the palmprint code comparison or matching is done to check if the two palmprint belong to the same person or not, hence a distance measure give the intra distance distribution tends to be close to 0 while the inter distance distribution tends to be far from 0.

We calculate Hamming distance of the palmprint template. However for evaluation of the effectiveness of the method we also test with the other proximity measures like Weighted Euclidean distance(WED) and the Jaccard distance(JD).

5.4.2 Effective verification using classifier fusion

To improve the matching performance, a classifier based on decision level fusion is designed with the fusion of different proximity measures.

Based on an experimental study we decide the expression for decision level fusion for those chosen dissimilarity measures as follows:

$$f(x) = \begin{cases} 1, & \text{if } WED < t_b \\ HD, & \text{if } t_b \leq WED \leq t_a \\ 0, & \text{if } WED \geq t_a. \end{cases} \tag{5.4}$$

Here we have used only HD and WED because of the superior performance over other synthetic and benchmark dataset.

5.5 Performance evaluation

The performance protocol given by [56] is used to measure the accuracy of the palmprint verification system. To evaluate similarity measures for binary features, we chose two types of errors, false accept rate (FAR) and false reject rate (FRR). For a stored template T and input template I to be verified, if H_0 and H_1 represent null and alternate hypotheses, H_0 and H_1 are defined as:

H_0=$I \neq T$, if input I is not from the same person as the original template.

H_1=$I = T$, if input I is from the same person as the original template.

Also the decision variables D_0 and D_1 are represented as

D_0: The person is not claimed to be.

D_1: The person is the claimed identity one.

Mathematically, the conditional probability of an event A for a given event B is defined as

$$P(A|B) = \frac{P(B|A).P(A)}{P(B)} \tag{5.5}$$

Hence, the FAR and FRR are defined as:

$$FAR = P(D_1|H_0 = True) \tag{5.6}$$

$$FRR = P(D_0|H_1 = True) \tag{5.7}$$

In order to check validity of the sample data taken for training and testing, we use a k-fold cross-validation method. It is a generalization approach which partitions data into disjoint subsets of size n/k and then trains, validates and takes average over the k partitions where n is the total number of training data points.

The algorithm use for cross validation check is shown in Figure 5-10. K-fold cross-validation has several advantages such as (i) the method with the highest cross-validation accuracy is chosen, (ii) cross validation generates an approximate estimate of how well the classifier will do on 'unseen' data and (iii) by averaging over different partitions it is more robust than just a single train/validate partition of data.

```
for i=1:k
train on 90% of data,
Acc(i)= accuracy on other 10 %
end
CrossValidationAccuracy = 1/k $\sum_i$ Acc(i)
```

Figure 5-10: Algorithm for k-fold cross validation

5.5.1 Environment used

The experiments were carried out on a workstation with Intel dual-core processor (1.86 GHz) with 1 GB of RAM. We used MATLAB 7.2 (R2006a) version in windows (64-bits) platform for the performance evaluation.

5.5.2 Datasets used

We have used CASIA(V1) palmprint dataset for verification of palmprint. The dataset contains 312 subjects and total 5502 samples. The samples are of 8-bit gray-level JPEG files. The palmprint dataset is available in [90].

For the verification experiments, the datasets are divided into two parts training and test sets. The results are generated using k-fold error validation method. The dataset used for cross-comparison of samples is as shown in the Table 5.1

Table 5.1: Datasets used for cross-comparison of 300 subjects and 8 samples

Class	Data sample types	
	Samples	DB per k fold
Intra class	Training	216
	Testing	24
Inter class	Training	216
	Testing	24

5.5.3 Experimental results and analysis

In this section, we carry out two different experiments to evaluate the performance of our method.

Experiment 1: A randomized k-fold cross validation method is adopted by dividing the 2400 palmprint images into k parts on a per subject basis.

From the CASIA V.1 Palmprint dataset, we have taken 2400 samples of 300 subjects containing 8 samples per subjects and divided entire samples into two partitions of 1200 and 1200 samples of intra class and inter class palmprint samples for balanced classification.

The k-fold cross validation was performed for k=5 as also given in [80] and selecting 90% of data for training and selecting 10% of data for testing for each of the k-fold or partition for both Intra class and Inter class. Hence for each fold, we have taken 216 training samples and 24 testing samples for each of intra class and inter class subjects. The details of the data samples are as shown in the Table 5.1.

A comparison of experimental results are made by using cross-validation with k=5. From palmprint dataset (CASIA V.1), we obtain the matching scores for different palmprint images and the corresponding error rates are generated using different threshold values for each of the filter level of the Gausian filter.

From the result of our experiment we have obtained ROC curves for this method in terms of FAR and FRR for palmprint biometric as shown in Figure 5-11. The FAR and FRR values are reported in Table 5.2 with best values among all the five sets of data samples. It can be seen from the table as well as from the figure that result is satisfactory.

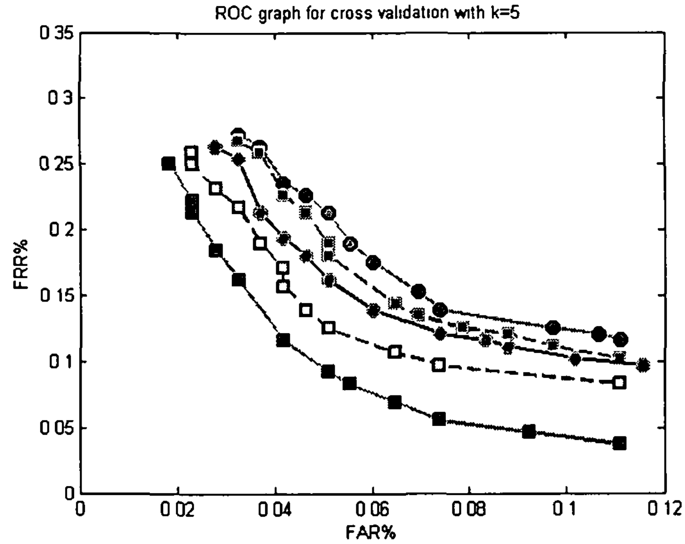


Figure 5-11: ROC curve of Palmprint verification (CASIA V1) dataset

Experiment 2: In order to extend the proposed model, in this section we compared the experimental results obtained by using different distance measures also. From the two created sample sets, intra-class distance and inter-class distance sets as given in Table 5.1, the Palmprint verification model is tested. Each scalar distance value is classified into intra or inter person class by comparing with the threshold values as depicted in the three distribution curves in Figure. 5-12, Figure. 5-13 and Figure. 5-14 with respect to three distances Hamming, Jaccard and Weighted Euclidean distances are shown respectively.

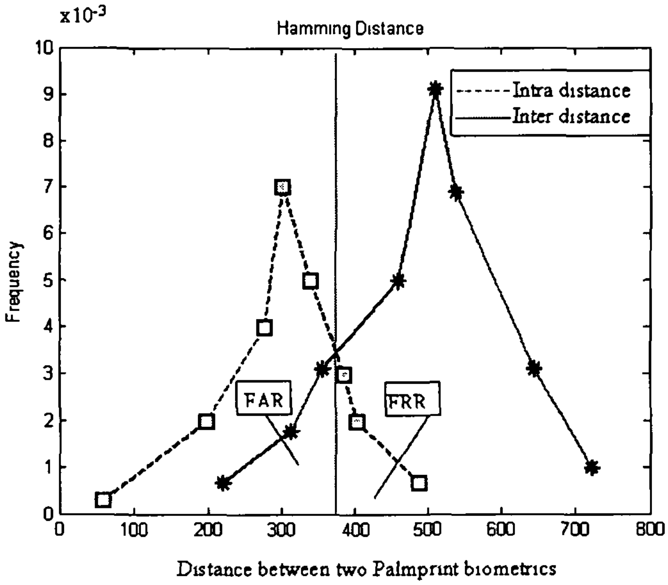


Figure 5-12: Distribution curves for Inter class and Intra class w.r.t. hamming distance.

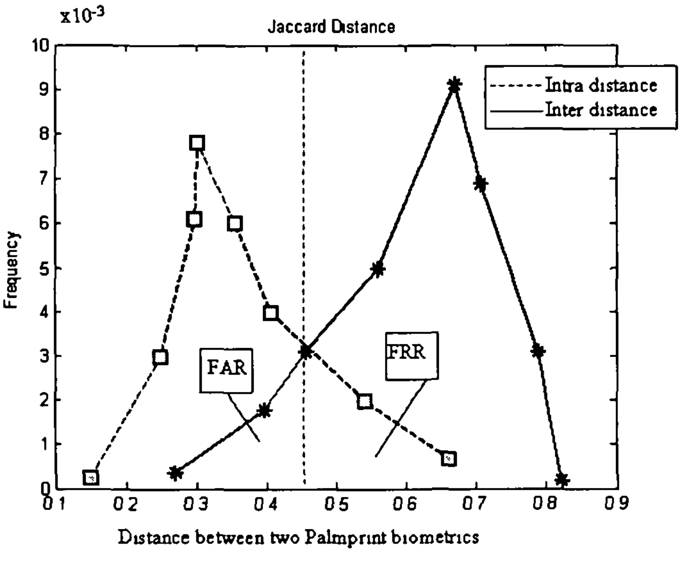


Figure 5-13: Distribution curves for Inter class and Intra class w.r.t. Jaccard distance.

Table 5.2: FAR/FRR values of Palmprint V.1 dataset

Filter No.	FAR	FRR
1	0.0185	0.25
2	0.0231	0.2222
3	0.0231	0.213
4	0.0278	0.1852
5	0.0324	0.162
6	0.0417	0.1157
7	0.0509	0.0926
8	0.0556	0.0823
9	0.0648	0.0694
10	0.0741	0.0556
11	0.0926	0.0463
12	0.1111	0.037

Table 5.3: Performance of the various distance measures

Distance Measures	Palmprint(CASIA V.1) data sample recognition rate for each k														
	DB1(k=1)			DB2(k=2)			DB3 (k=3)			DB4 (k=4)			DB5 (k=5)		
	FAR	FRR	%	FAR	FRR	%	FAR	FRR	%	FAR	FRR	%	FAR	FRR	%
HD	0.33	0.91	94.8	0.51	0.8	95	0.56	0.73	95.04	0.61	0.8	95.06	0.72	0.8	95.2
JD	0.29	0.40	94.7	0.65	0.9	95.1	0.3	0.9	95.03	0.7	0.5	95.1	0.7	.85	95.2
WED	0.41	1.2	93.8	0.58	1.1	93.5	0.67	1.1	93.9	0.8	0.09	94.4	0.7	0.89	94.9

5.6 Discussion

A cross-comparison was performed to build the distribution of imposter and genuine match scores. We attempted to draw distribution curves for both imposter and genuine using Hamming distance, Jaccard distance and Weighted Euclidean distance by calculating inter-class and intra-class distributions. To select an appropriate and unbiased distance measure is a difficult task as texture-based palmprint biometric verification involves measure of binary feature vector distances and verification of the identity of a person.

The curve also depicts the optimization of threshold values of the individual match

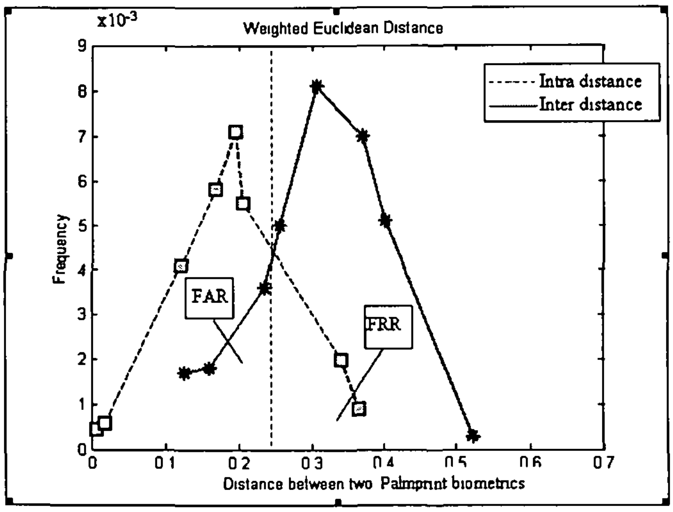


Figure 5-14: Distribution curves for Inter class and Intra class w.r.t. Weighted Euclidean distance.

scores of a person with effective 'to specific application data. As in case of biometric verification, higher the matching score, higher the similarity between them. Access to a biometric system is granted only, if the biometric pattern to be verified is higher than a certain threshold. If we increase the threshold, there will be reduced FAR but more FRR. A common variation is obtained using normal deviation scales on both axes which is a linear graph that eliminates the differences for higher performances.

From the distribution graph we obtained, as in Figure. 5-12, Figure. 5-13 and Figure. 5-14 the matching threshold assessment for classification of genuine or imposter class can be made easily.

In the next chapter, our work is emphasized on the multimodal biometric fusion work with our developed fingerprint, iris and palmprint verification model.

Chapter 6

BIOMETRIC VERIFICATION USING MULTIMODAL FUSION

Although in the recent past, a good number of unimodal biometric verification systems have been developed, none of them are totally free from some important limitations such as non-universality and susceptibility to spoof attack. Multibiometric is a new subdiscipline within the domain of biometric which combine information from different biometric sources to establish identity. The problem of biometric recognition is a great challenge in terms of expectations of high matching accuracy, efficient scalability and ease of usability in a variety of applications. A multibiometric system can be accomplished by fusion of multiple traits of an individual, or multiple feature extraction, or matching algorithms operating on the same biometric and multimodal fusion of different biometric traits.

A multibiometric system can have a variety of scenarios for information fusion like multi-sensor, multi-algorithm, multi-instance, multisampling and multimodal. All the scenarios are based on single trait except multimodal where evidence is obtained from different biometric traits.

A multibiometric system enhances recognition accuracy than an unibiometric system. It provides other facilities as listed below [4].

- Facilitates the filtering or indexing of large-scale biometric databases.

- Multibiometric systems address the issue of nonuniversality (i.e., limited population coverage) encountered by unibiometric systems. A certain degree of flexibility is achieved when a user enrolls into the system using several different traits while only a subset of these traits is requested during authentication based on the nature of the application under consideration and the convenience of the user.
- These systems also help in the continuous monitoring or tracking of an individual in situations when a single trait is not sufficient.
- A multibiometric system may also be viewed as a fault tolerant system which continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation. The notion of fault tolerance is especially useful in large-scale authentication systems involving a large number of subjects (such as a border control application).

The factors that impact the design and structure of a multibiometric system are [4]:

- Cost benefits: An appropriate tradeoff between the added cost and the improvement in matching performance is highly essential. The cost is a function of the number of sensors deployed, the time taken to acquire the biometric data, the storage requirements, the processing time of the algorithm and the perceived (in)convenience experienced by the user.
- Sources of biometric information : Determining the sources of information those can be used in a multibiometric system and are relevant to the application at hand.
- Acquisition and processing sequence: Depending upon the needs, data corresponding to multiple information sources (e.g., modalities) be acquired simultaneously or at different time instances in a serial fashion. The information acquired can be processed sequentially or simultaneously.

- Types of information: The types of information or attributes (i.e., features, match scores, decisions, etc.) are to be fused have to be decided and the impact of correlation among the sources of information on the performance of the fusion system have to be determined.

- Fusion methodology: The information presented by multiple biometric sources are combined depending on the fusion scheme. The performance gain obtained using different fusion methodologies in order to determine the optimal one is to predict.

Depending on the sources of evidence, a multibiometric system can be classified into one of the following six categories [4] : multisensor, multialgorithm, multi-instance, multisample, multimodal and hybrid.

- Multisensor systems: Multisensor systems employ multiple sensors to capture a single biometric trait of an individual. The use of multiple sensors in some instances, can result in the acquisition of complementary information that can enhance the recognition ability of the system

- Multialgorithm systems: In some cases, invoking multiple feature extraction and/or matching algorithms on the same biometric data can result in improved matching performance. Multialgorithm systems consolidate the output of multiple feature extraction algorithms, or that of multiple matchers operating on the same feature set. These systems do not nècessitate the deployment of new sensors and, hence, are cost-effective compared to other types of multibiometric systems. But on the other hand, the introduction of new feature extraction and matching modules can increase the computational complexity of these systems.

- Multi-instance systems: These systems use multiple instances of the same body trait and have also been referred to as multiunit systems in the literature.

- Multisample systems: A single sensor may be used to acquire multiple samples of the same biometric trait in order to account for the variations that can occur in the trait, or to obtain a more complete representation of the underlying trait.

- Multimodal systems: Multimodal systems establish identity based on the evidences of multiple biometric traits.
- Hybrid systems: Chang et al. use the term hybrid to describe systems that integrate a subset of the five scenarios discussed above

6.1 Prior related work

Based on our study as mentioned in our work [9] we revealed the different levels of multibiometric systems with their uses as in the Table 6.1. Recently, works on the fusion of multimodal biometrics are gaining significant importance due to their effectiveness in terms of cost and efficiency. In the past few years, several novel methods have been introduced to address this important problem.

Based on our study, it has been observed that the fusion works can be classified into six major categories as (i) sensor level, (ii) representation level, (iii) dynamic classifier selection, (iv) matching score-based, (v) class rank-based and (vi) decision level fusion. A general comparision of these methods is shown in Table 6.1.

We enumerate the following observations based on our study:

i) In the past, several effective supervised and unsupervised methods have been introduced to address the multimodal biometric fusion problem. Most methods have been established using fingerprint and iris images.

ii) Methods for multi-biometric fusion can be broadly classified into six categories based on their flexibility on the measure, metric and level of representation used. A major issue with most of these methods is the increase in false alarms. Special attempts have been made to improve the detection accuracy, and hence to minimize the false alarms.

iii) Appropriate use of optimization techniques have proven to be useful in improving the performance of such multi-sensor based methods. However, deciding the appropriate set of parameters/thresholds is the challenging task in such optimization techniques.

Table 6.1: Biometric fusion methods and their uses

Approaches	Descriptions/methods used
Sensor level (Raw data)	The authors [40] consider biometric sensor fusion technique using PSO for face and palmprint images. The authors [41]have fused visible and infrared face images and verification decision is made using match score fusion.
Representation or Feature level	The author [42] have considered fusion of different features into a single multi-biometric template. The author [43] have used integrated feature sets obtained from multiple biometric traits like fingerprint, iris.
Dynamic classifier selection	The author [44] have aimed to select, for each unknown pattern, the classifier that is more likely to classify it correctly. The author [45]also considered to design an multiclassifier selector for each pattern.
Matching score or Confidence level	The author [46] introduce a rule-based approach to consider the task of combining classifiers in a probabilistic Bayesian framework based on the Bayes theorem and hypothesis. The author [47], provided a supervised approach which shows fusion strategy using a support vector machine (SVM).
Class Rank-based (Class rank)	The author [48] propose fusion based on a minimum distance method for combining rankings from several biometric algorithms
Decision (abstract level)	The authors [22] introduce decision-level fusion for correlated biometric classifiers

6.2 Background of the work

Our work is focused on the development of an effective method for combination of multimodal biometric data. Iris, fingerprint and palmprint biometrics have been found better as compared to other available traits due to their accuracy, reliability and simplicity, which make them promising solution to the society. The aim of our work is to achieve the following objectives.

(a) To study and explore the usefulness of decision level fusion of multimodal biometric traits for effective identity verification.

(b) To explore the effectiveness of optimization techniques such as SA(Simulated Annaling), ACO(Ant-Colony Optimization) and PSO(Particle Swarm Optimization) for selection of appropriate rule for fusion and dynamic threshold selection of individual traits matching score.

(c) To validate the approach using benchmark datasets in terms of global false acceptance rate (GFAR) and global false rejection rate (GFRR).

Next, we provide some fundamentals of ACO which has been found as an effective optimization technique for handling multi-biometric verification problem.

6.2.1 ACO: An effective optimization technique

Ant colony optimization (ACO) is a nature-inspired optimization algorithm [3][30], motivated by the natural phenomenon that ants deposit pheromone on the ground in order to mark some favorable path that should be followed by other members of the colony. The first ACO algorithm, called the ant system, was proposed by Dorigo et al. [57]. ACO has been widely applied in various problems[31].

ACO aims to find the optimal solution of the target problem iteratively through a guided search (i.e. the movements of a number of ants) over the solution space, by constructing the pheromone information. The main characteristic of ACO algorithm is that, at each iteration the pheromone values are updated by all the k ants those have built a solution in the iteration itself. Each ant chooses its possible solutions randomly from the available possible values. Two important parameters in ACO are 'pheromone constant' (Q) and 'evaporation factor' (ρ<1). The pseudo_code of an ACO algorithm is given in Figure 6-1

```
Initialize parameters
Initialize positions of totally K ants
Initialize pheromone matrix $\tau(0)$
$n = 1$
$k = 1$
repeat
    Consecutively move the $k^{th}$ ant for $L$ steps, by selecting a probabilistic rule.
    Update the pheromone matrix $\tau(N)$.
    Make the solution decision according to the final pheromone matrix $\tau(N)$.
    n=n+1;
    k=k+1;
until n=N and k=K
```

Figure 6-1: Pseudo code of an ACO

The selection of a proper set of optimization parameters for ACO is a multi-objective decision making optimization problem. Initially, the matching scores for individual biometric classifiers are computed. Next, an ACO-based procedure is followed to simultaneously optimize the parameters and the fusion rules as given in [9]. It shows the utility of adaptive multimodal biometric fusion on the real biometric samples using the Bayesian fusion rule for score level fusion. We have investigated the adaptive combination of iris, fingerprint and palmprint biometric on publicly available benchmark database using a Binary ACO(BACO) and the results have been found satisfactory.

Binary ACO(BACO): The idea behind the proposed binary ACO based method is that the biometric thresholds are continuous. In such model, a fusion rule takes an integer value which suffers slow convergence hence the need for binary ACO (BACO) algorithm, where FAR of each biometric is evolved instead of thresholds. The fusion rule is a binary number having a length of $\log_2$p bits, where p=2^{2^N}, with a real value varying from 0$\leq f \leq p-1$. For binary search spaces, the binary decision model as described in [12] is being used. A binary decision model works better for moving through the decision fusion space.

6.2.2 Particle Swarm Intelligence(PSO)

PSO was formulated by Edward and Kennedy in 1995 [51]. It is one of the evolutionary optimization methods inspired by social behaviour of animals like bird flocking or fish schooling, which is similar to other methods like Genetic Algorithm. Unlike the GA, PSO has no evolution operators like crossover and mutation. In PSO algorithm, each member is called 'particle' and each particle flies around in the multi-dimensional search space with a velocity, which is constantly updated by the particle's own experience and the experience of the particle's neighbors. Since its inception, PSO has been successfully applied to optimize various continuous nonlinear functions.

In a PSO algorithm, population is initiated randomly with particles and evaluated to compute fitness together with finding the best value of each individual so far (particle-best) and best particle in the whole swarm (global-best). The pseudo code of the general PSO algorithm [51] is reported in Figure 6-2. The symbols and notations used to describe the rest of the work are reported in Table 6.2. The basic elements of PSO algorithm are described in brief.

```
Initialize parameters
Initialize population
repeat
    Find particle-best
    Find global-best
    Update velocity
    Update position
    Evaluate
until Termination
```

Figure 6-2: Pseudo code of a PSO

1. Particle: The i^{th} particle of the swarm is represented by a d-dimensional vector and can be defined as $x_i^k=[\lambda_{i1}^k, \lambda_{i2}^k, \ldots\ldots \lambda_{id}^k]$, where λ s are the optimized

Table 6.2: Symbol used with meaning

Symbol	Meaning
λ	Optimized parameters
x_i	i^{th} Particle of swarm
k	Number of iteration
d	Number of dimension
X	Set of n^{th} particle of swarm
PBest	Best value of the particle
V	Velocity of particle
v	Velocity with respect to dimension
GBest	Best postion among all particles in the swarm
ω	Inertia weight(value ranges from 0 to 1) and provide a balance between global and local search abilities of the algorithm
S	Sigmoid function that limit the value of the probability V to the range [0,1]
PBest	Best value of a perticle
FAR	False acceptance rate
FRR	False rejection rate
GFAR	Global false acceptance rate

parameters and $\lambda_{id}{}^{k}$ is the position of the ith particle w.r.t. dth dimensions, k is the iteration.

2. Population: X^{k} is the set of n particles in the swarm at iteration k, i.e. X=[x$_1{}^{k}$, x$_2{}^{k}$,...., x$_n{}^{k}$].

3. Velocity: V$_i{}^{k}$ is the velocity of particle i at iteration k. It can be described as V$_i{}^{k}$ = [v$_{i1}{}^{k}$, v$_{i2}{}^{k}$,...,v$_{id}{}^{k}$] where v$_{id}{}^{k}$ is the velocity with respect to dth dimension.

4. Particle-best: PBest$_i{}^{k}$ is the best value of the i^{th} particle, obtained until iteration k. The best position associated with the best fitness value of the ith particle obtained so far is called particle best and is defined as
PBest$_i{}^{k}$ = [pbest$_{i1}{}^{k}$, pbest$_{i2}{}^{k}$,.....,pbest$_{id}{}^{k}$] with the fitness function
f(PBest$_i{}^{k}$).

5. Global-best: GBest^{k} is the best position among all particles in the swarm, which is achieved so far and can be expressed as
GBest^{k} = [gbest$_1{}^{k}$, gbest$_2{}^{k}$,.....gbest$_d{}^{k}$], with the fitness function f(GBest^{k}).

6. Termination criterion: The search is terminated when the number of iteration reaches a predetermined value or a maximum number of iteration.

A particle in PSO moves to a new position in multi-dimensional solution space depending upon the particle's best position (local best position), PBest$_i{}^{k}$ and the global best position, GBest^{k}. The PBest$_i{}^{k}$ and GBest^{k} are updated after each iteration, whenever a suitable, i.e. lower cost, solution is located by the particle. The velocity vector of each particle represents/determines the forthcoming motion details. The velocity update equation of a particle of PSO for instance (t+1) can be represented as follows:

$$V_i^k(t+1) = \omega V_i^k(t) + c_1 r_1 (PBest_i^k(t) - x_i^k(t)) + c_2 r_2 (GBest^k(t) - x_i^k(t)) \qquad (6.1)$$

where ω is the inertia weight between 0-1 and provide a balance between global and local search abilities of the algorithm. The accelerator coefficients c$_1$ and c$_2$ are positive constants, called cognitive parameter and social parameter respectively and r_1 and r_2 are two random numbers in 0-1 range. The corresponding position vector is updated by using equation(2)

$$X_i^k(t+1) = X_i^k(t) + V_i^k(t+1) \tag{6.2}$$

Binary PSO as an optimization problem for fusion of biometrics :

In PSO the particles are better represented as discrete binary variables and such problems require that these binary particles be evolved to obtain an optimal solution. The position vector for each particle in binary PSO can have a value either 0 or 1 on each dimension. The formula for calculating the velocity update in binary PSO remains the same as real valued version, except that $\mathrm{PBest}_i{}^k$, $\mathrm{X}_i{}^k$ and GBest^k in equation (1) are binary valued. The velocity $\mathrm{V}_i{}^k$ for binary PSO represents the probability of bit $\mathrm{X}_i{}^k$ taking the value 1. A sigmoid function S is employed to limit the value of the probability $\mathrm{V}_i{}^k$ to the range [0, 1]. Therefore the position vector of a particle in binary PSO is updated as follows:

$$X_i^k(t+1) = 1 \text{ for } r_3 \langle S(V_{ik}(t+1))\ 0 \ \text{ otherwise} \tag{6.3}$$

Where

$$S(V_{ik}(t+1)) = \frac{1}{1 + exp(-V_{ik}(t+1))} \tag{6.4}$$

and r_3 is a random number in the interval [0, 1] with uniform distribution. The binary PSO algorithm used in this fusion approach of iris and fingerprint trait is to make choice of sensors, dynamically selecting threshold and the fusion rule selection to maximize the accuracy or minimize the accuracy error given by [12] is :

6.2.3 Simulated Annealing(SA)

Simulated Annealing is a mathematical analogy to a cooling system which can be used to sample highly nonlinear multidimensional functions. In the early 1980s, the method of simulated annealing (SA) was introduced by Kirkpatrick and coworkers (1983), based on the ideas formulated in the early 1950s (Metropolis, 1953). This method simulates the annealing process in which a substance is heated above its melting temperature and then gradually cooled to produce the crystalline lattice which minimizes its energy probability distribution. This crystalline lattice, composed of millions of atoms perfectly aligned, is a beautiful example of nature finding an optimal structure. However, quickly cooling or quenching the liquid retards the crystal formation, and the substance becomes an amorphous mass with a higher than optimum energy state. The key to crystal formation is carefully controlling the rate of change of temperature. The algorithmic analog to this process begins with a random guess of the cost function variable values. Heating means randomly modifying the variable values. Higher heat implies greater random fluctuations. The cost function returns the output, f, associated with a set of variables. If the output decreases, then the new variable set replaces the old variable set. If the output increases, then the output is accepted with probability that

$$P = exp^{(f_{old}-f_{new})/T} > r \tag{6.5}$$

where r is a uniform random number and T is a variable analogous to temperature. Otherwise, the new variable set is rejected. Thus, even if a variable set leads to a worse cost, it can be accepted with a certain probability. The new variable set is found by taking a random step from the old variable.

Applications of SA: SA was started as a method or tool for solving single objective combinatorial problems, these days it has been applied to solve single as well as multiple objective optimization problems in various fields. The problems may have continuous or discrete variables. SA has been greatly used in operational research problems. Application of SA does not restrict to optimization of nonlinear objective function, these days it has been applied for many other purposes. Bell et al (1987) have used it to cluster tuples in databases. They have attempted to use SA in circuit board layout design and it suggests that it would be advantageously applied to clustering tuples in database in order to enhance responsiveness to queries. Some of the methods that SA find applications are listed below in Table 6.3.

The parameters in SA are T (temperature) and S (energy function S). The Pseudo code of the general SA is given in Figure 6-3

```
1: Select starting temperature and initial parameter values
2: Randomly select a new point in the neighborhood of the original
3: Compare the two points using the Metropolis criterion.
4: Repeat steps 2 and 3 until system reaches equilibrium state ie to repeat the
   process $N$ times for large $N$
5: Decrease temperature and repeat the above steps, stop when system reaches
   frozen state.
```

Figure 6-3: Pseudo code of a SA

The flow diagram of SA is shown in Figure 6-4.

Approaches of SA

SA was started as a method or tool for solving single objective combinatorial problems, these days it has been applied to solve single as well as multiple objective optimization problems in various fields. The problems may have continuous or discrete variables. SA has been greatly used in operational research problems.

6.2.4 Fusion and multimodal fusion

The unimodal biometric system may fail when the biometric data available is noisy or due to unavailability of biometric template. Multibiometric is a new sub-discipline within the domain of biometrics to establish identity. The problem of biometric verification is a great challenge in terms of expectations of high matching accuracy, efficient scalability and ease of usability in a variety of applications. Rose and Jain identify some of the challenges of an unimodal system that leads the motivations for multibiometric systems [4] are: (i) Noise- Due to temporary inferences in the biometric trait thereby increasing the False Reject Rate (FRR) of the system, (ii)

Table 6.3: Applications of Simulated Annealing

Applications	Author/Descriptions/methods used
1.(i) Graph partition (ii) Graph coloring and number partitioning problems. (iii) Travelling salesman problem	Johnson et al.(1989-1991)illustrated simulated annealing and highlighted the effectiveness of several modifications to the basic simulated annealing algorithm.
2.(i) Single machine, (ii) Flow shop and (iii)Job shop scheduling	Here Koulamans et al.(1994) found that an increased number of iterations combined with increased number of searches at each iteration can result in solutions with a higher probability of converging to the optimal solution
3.(i) Maximum likelihood joint channel and data estimation, (ii) Infinite-impulse-response filter design and (iii) Evaluation of minimum symbol-error-rate decision feedback equalizer.	Chen and Luk (1999) proposes an adaptive simulated annealing algorithm as a powerfull global optimizatio tool for addressing difficult non-linear optimization problems.
4. School time tabling problem.	Abramson et al. (1999)Use the scheduling problem to highlight the performance of six different cooling schedules viz. the basic geometric cooling schedule, a scheme that uses multiple cooling rates, geometric reheating, enhanced geometric reheating, nonmonotonic cooling, and reheating as a function of cost.
5.Airline crew-pairing problem based on an algorithm run-cutting formulation.	Emden-Weinert and Proksch (1999) found that the algorithm run-time can be decreased and solution quality can be improved by using a problem-specific initial solution, relaxing constraints, combining simulated annealing with a problem-specific local improvement heuristic, and by conducting multiple independent runs.
6.The multiobjective optimization of constrained problems	Suman(2002, 2003) has proposed two different SA-based approaches, WMOSA and PDMOSA.

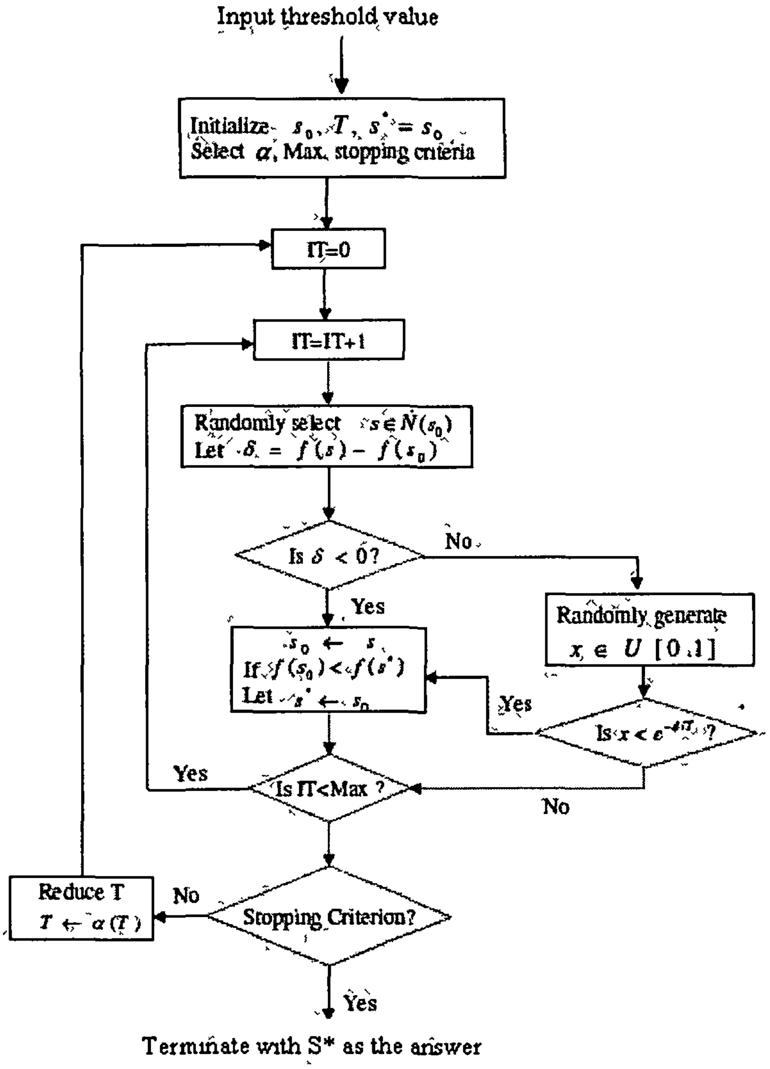


Figure 6-4: Flow diagram of Simulate Annealing

Intra-Class variations occur due to incorrect interaction of users with the sensor of unimodal system, (iii) Inter-Class similarities may occur in systems used by a large number of users, where there might be more mismatch of features by multiple users of different identity, (iv) Non-Universality problem arises when not all users in the population able to produce the same type of features, (v) Spoof or reply attack may occur due to an imposters attempt to mimic the traits like signature and voice which are behavioral in nature and physical traits like fingerprint by inscribing ridge-like structures. A multibiometric system can be accomplished by fusion of multiple traits of an individual, or multiple feature extraction, or matching algorithms operating on the same biometric and multimodal fusion of different biometric traits.

6.2.5 Discussion

In order to achieve an effective verification method that can mitigate the problem with unimodal biometric system, we have decided to extend our unimodal biometric system with fingerprint, iris and palmprint to a multimodal biometric verification system by their fusion. In the next section our developed multimodel biometric system is reported.

6.3 Biometric verification using multimodal fusion

A method using BACO, BPSO, SA is proposed in our multimodal biometric fusion approach of iris, fingerprint, palmprint traits (i) to make choice of sensors, (ii) to dynamically select threshold and (iii) to select fusion rule to maximize the accuracy or minimize the accuracy error. The algorithm quantifies different security level by associating error rates: global false acceptance rate (GFAR) and global false rejection rate (GFRR) given by [12] are depicted in the Table 6.4. The problem is to develop an effective decision level fusion method based on a score combination function f which accepts individual scores obtained from each sensor to identify an instance X_i either as genuine or imposter w.r.t. a decision threshold.

The block diagram of the proposed method is shown in Figure 6-5. As shown in

Table 6.4: Fusion rules

Error	Fusion rule selected	
	AND	OR
GFAR	FAR1*FAR2	FAR1+FAR2-FAR1*FAR2
GFRR	FRR1+FRR2-FRR1*FRR2	FRR1*FRR2

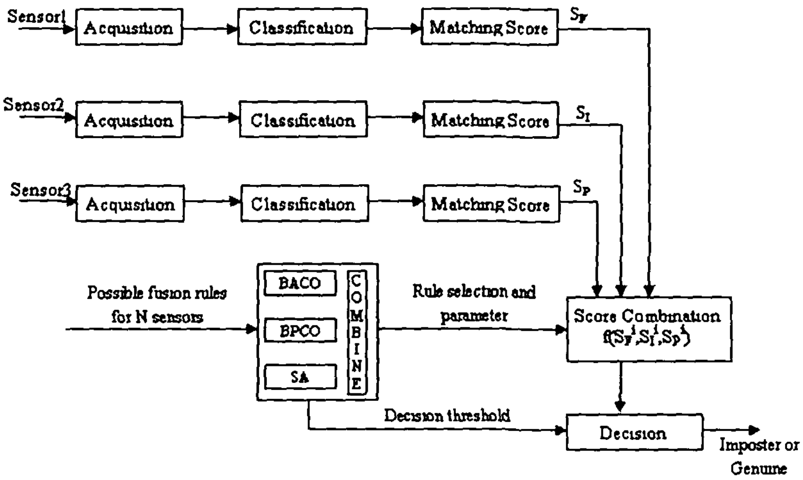


Figure 6-5: Block diagram of the proposed multimodal system

the figure, the method accepts the match scores from the individual sensors and uses a combination function f to combine the scores, hence to decide the genuiness of an input instance.

The multimodal biometric data from fingerprint, iris and palmprint biometrics are used to extract the corresponding F_F and F_I feature vectors. These feature vectors are employed to generate the matching scores S_F and S_I from the corresponding templates acquired during the registration. The risk of attack on a biometric system can be varying and therefore it is critical to provide multiple levels of security. The security requirement in Bayesian sense, is quantified with two parameters; the global cost (0, 1) of falsely accepting an imposter C_{FA} and the global cost (0,1) of falsely rejecting or accepting a genuine user C_{FR} from the installed biometric system. These two costs can be employed to adequately quantify the desired performance. The total error cost, E to be minimized by the multimodal biometrics system is the weighted sum of $GFAR$ and $GFRR$ as given by [12] is

$$E = C_{FA}GFAR(\eta) + C_{FR}GFRR(\eta) \text{ where } C_{FA} + C_{FR} = 2 \tag{6.6}$$

where $GFAR(\eta)$ is the global or the combined false acceptance rate and $GFRR(\eta)$ is the combined false rejection rate at decision threshold η from the multimodal biometric system. The task of multimodal biometric system as shown in Figure 6-6 is to minimize the (global) cost E, i.e the accuracy error for the system given by equation 2, by selecting (i) the appropriate score level combination rule, (ii) its parameters and (iii) the decision threshold. The multidimensional search among the various combination rules and their weight parameters to optimize the global cost E is achieved by the ant colony optimization (ACO) approach.
We discuss the basic steps of the proposed method as depicted in Figure 6-5.

1. *Data Acquisition* : A virtual multimodal database derived from the CASIA palmprint image database [90], CASIA iris image database [90] and FVC fingerprint image database [88] is used to evaluate the performance of the said method. The multimodal database consists of 108 users obtained by randomly pairing the first 108 users in the FVC database with the users in the CASIA database for iris and palmprint images.

   As the adopted database contains fingerprint and iris database, the fingerprint database is used from two databases: FVC2000 and FVC2004 [28] and the synthetic dataset we have created using tools [29]. The image size is of 300*300 pixels. We have used [30] dataset for the iris database. For the verification experiments, the datasets are divided into two parts training and test sets. The training set contains 48 subjects from FVC and synthetic fingerprint database and CASIA iris database. The test set contains 60 subjects from the same fingerprint and iris database. CASIA V1 and FVC are well-known public domain iris database and fingerprint database. The FVC database contains 36 subjects and 108 images. The synthetic database contains 36 subjects and 108 images (3 per subject). The CASIA iris database contains 108 subjects and 756 images

(7 per subject). The multimodal biometrics recognition system is evaluated in the two sets.

2. *Feature extraction* : Palmprints are rich of texture information. Palmprint's texture features are extracted with the help of an adjusted circular Gabor filter to the preprocessed palmprint images. In case of iris, the most discriminating features of iris pattern is the phase information. Extraction of the phase information is done by using 2D Gabor wavelets according to Daugman (2004)[54]. In case of fingerprint feature extraction, two salient features, i.e. core and reference points. An algorithm developed by Hong et al.(1998) [35]is used to detect the core point but with a slight difference that maps all the block directions to the interval from -0.5 to 0.5 and then simply regards the value 0.5 corresponds to the core.

3. *Matching* : We use individual matching mechanism for each sensor output, which are discussed in the relevant chapters above.

4. *Combination function f* : This function accepts match scores, i.e., S_P, S_I and S_F respectively , from palmprint, iris and fingerprint module and computes $f(S^i_P,S^i_F,S^i_I)$ using the rules and parameter provided by SA or BACO or PSO in the 'COMBINE' submodule. This module takes the input from combination function, f and the 'COMBINE' module to decide the class of a given input instance X_i either as genuine or imposter. It uses the decision threshold given by the 'COMBINE' module comprises of BACO submodule to decide the class of X_i

6.4 Multimodal decision level fusion of fingerprint and iris using BACO

In this work we provide the solutions for fusion of iris and fingerprint for the range of costs $1.7-1.98$. The algorithm ran the BACO 100 times for the same cost. The detail

Table 6.5: Ant colony optimization parameters

No of ants	No of dimensions	No of rules	Pheromone constant(Q)	Evaporation factor(R)
8	2	4	0.01	0.05

Table 6.6: Selection of rules against different C_{FA}

C_{FA}	Probabilities of rule chosen by ACO			
	Iris only	Fingerprint only	AND rule	OR rule
1.70	0	0	0	100
1.72	0	0	0	100
1.74	0	0	0	100
1.76	0	0	0	100
1.8	0	0	0	100
1.82	0	0	0	100
1.84	0	0	0	100
1.86	0	0	0	100
1.88	94	0	0	6
1.9	95	0	0	5
1.92	100	0	0	0
1.94	100	0	0	0
1.96	100	0	0	0
1.98	100	0	0	0

about the parameters used is given on the Table 6.5. It can be observed from Table 6.6 that as the value of C_{FA} approaches more towards the maximum value (i.e.,value less than 2), the sensor 1 (i.e., Iris) is dominant in the sensor suite of fingerprint and iris. The solutions consist of the rule and the sensor operating point defined by its false acceptance rate(FAR) and false rejection rate(FRR). From the error rates of the sensors and their distributions, the sensor thresholds are computed. In Table 6.6, we summarize the results showing a range of costs and the probable rules selected. The 'OR' rule is more probable when the cost of false acceptance is low i.e., less than 1.9. Due to sensor 1's dominance, the system simply ignores the sensor 2's (Fingerprint) decisions with higher range of costs.

Based on our experiential study, it has been observed that our method performs significantly well over several benchmark datasets. However, due to lack of benchmark datasets with high dimensionality we couldn't evaluate its performance with the increase dimensionality. We aim to use other biometric traits and to explore the possibility of developing a faster approach with high detection accuracy.

6.5 Multimodal decision level fusion of fingerprint and iris using BPSO

The multi-dimensional search among the various combination rules and their weight parameters to optimize the global cost is also achieved by the particle swarm optimization (PSO) approach. It uses binary particle swarm optimization (BPSO) to compute and optimize the parameters and fusion rules. Initially the appropriate parameters (thresholds) for individual biometric classifiers are selected based on their matching scores. Next, a BPSO based procedure is followed to simultaneously optimize the parameters and the fusion rules. The biometric thresholds are continuous. In such model, a fusion rule takes an integer value which suffers slow convergence.

Table 6.7: Results of BPSO algorithm on Fusion module of Iris and Fingerprint

$X_i^{d=1}$	$X_i^{d=2}$	F_i=AND	F_i=OR	GFAR	GFRR(1.0e+003*)	E_{AND}	E_{OR}
0	0	0	0	-18	0.5734	23.1442	-3.5131
0	0	0	0	-15.3334	0.9284	63.7072	33.6670
0	0	0	0	-12.6577	0.8920	65.1470	38.2560
0	0	0	0	-7.3283	0.9398	80.0584	57.4329
0	0	0	0	-4.6568	1.0423	95.3801	73.5848
1	0	0	1	-0.0200	-1.2657	126.6057	-05.5301
1	1	1	1	0.1163	0.9558	95.8028	79.9829
1	1	1	1	0.4478	0.6947	70.3226	59.1694

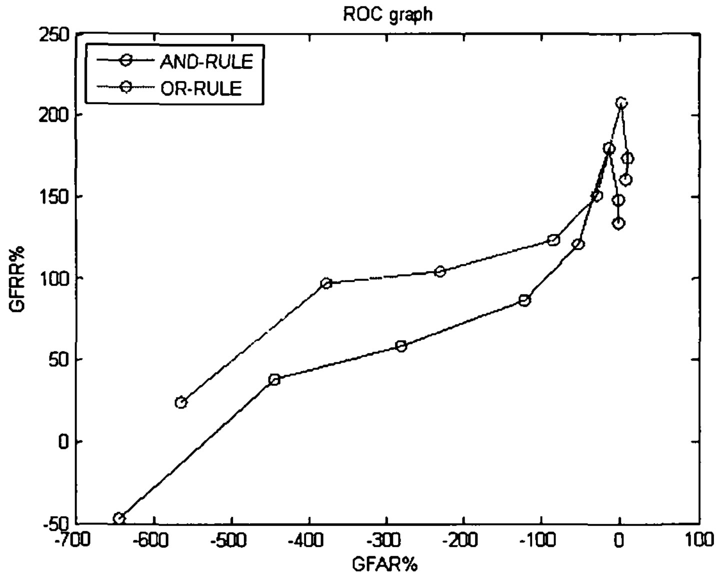


Figure 6-6: GFAR vs. GFRR curve for AND rule and OR rule of Iris CASIA dataset and Fingerprint, FVC dataset

Discussion

The theory as stated above says that, the value of the objective function as in Equation 6.6 should be minimum. From the result of BPSO, as in the Table 6.7, it is clear that the best rule for fusion module at a particular operating point of the sensor depends on the minimum value of expected error, which also resemble with GFAR Vs. GFRR results of individual recognizer as shown in Figure 6-6.

The choice of operating point to initialize the particles of the binary PSO fusion module is a key factor. New method can be approached to select the different operating points.

6.6 Multimodal decision level fusion of fingerprint and iris using SA

SA is an annealing process in metallurgy which reduces defects by controlling cooling of materials. SA statistically guarantees to find an optimal solution and it has its ability and flexibility to approach global optimality .

The selection of a proper set of parameters for SA is a multi-objective decision making optimization problem. Initially the matching scores for individual biometric classifiers are computed. Next, a SA-based procedure is followed to simultaneously optimize the parameters and the fusion rules for fingerprint and iris biometrics.

The objective is to perform decision level fusion of iris and fingerprint, at matching score level architecture using Simulated Annealing optimization problem. The features of individual iris and fingerprint traits are extracted from their preprocessed images. These features of a query image are compared with those of stored template to obtain matching scores. The individual scores generated after matching are passed to the fusion module where optimal fusion rules and decision thresholds are chosen automatically using simulated annealing(SA) technique. An experimental verification of the convergence nature of the simulated annealing method with the worst case behavior for optimum rule selection is analyzed and a comparative result of the method with the ant colony optimization technique is also given here.

As the decisions made by the biometric sensors are binary based on their presence or absence, they need to be fused by some binary fusion rule. One of the tasks of decision level fusion is to select an optimal fusion rule that minimizes the total errors of the system.

An effective framework for the adaptive combination of multimodal fingerprint and iris biometric data is proposed [60]. In our work, biometric thresholds are continuous. Here, a fusion rule takes an integer value which suffers slow convergence hence the need for binary Simulated Annealing algorithm, where FAR of each biometric is evolved instead of thresholds. The fusion rule is a binary number having a length of $\log_2$p bits, where p=2^{2^N}, with a real value varying from $0\leq f\leq p-1$. For binary search spaces, the binary decision model as described in [107] is being used. A binary decision model works better for moving through the decision fusion space.

The proposed method is depicted in Figure 6-7. As shown in the figure, the method accepts the match scores from the individual sensors and uses a combination function f to combine the scores, hence to decide the genuiness of an input instance.

In this work we provide the solutions for fusion of iris and fingerprint for the range of costs 1.6 – 2.0. We run the BSA 100 times for the same cost for each temperature ranging from high to low. In Table 6.8, we summarize the results showing a range of costs and the probable rules ie. whether I(Iris), F(Fingerprint), AND rule or OR rule is selected against different threshold points . It seems to be obvious from table that the dynamic selection of threshold point is effective with regard to less randomness of the rules i.e. it is showing that at threshold point 4 for almost all values of C_{FA} the rule selected is same. The result is that the sensor 1 (i.e., Iris) is dominant in the sensor suite of Fingerprint and Iris. The solutions consist of the rule and the sensor operating point defined by its false acceptance rate(FAR) and false rejection rate(FRR). From the error rates of the sensors and their distributions, the sensor threshold are computed. Due to sensor 1's dominance, the system simply ignores the sensor 2's (Fingerprint) decisions with higher range of costs and when the selected sensor threshold point is tight.

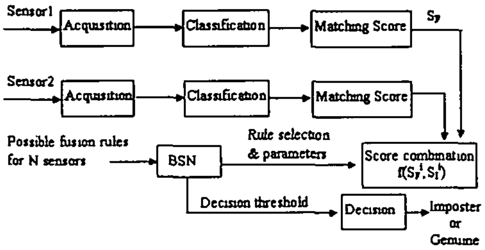


Figure 6-7: Block diagram of the proposed system using binary simulated annealing (BSA)

Experimental verification of the convergence nature of SA

Simulated Annealing maintains a current assignment of values to variables randomly. If the assignment does not increase the number of conflicts, the algorithm accepts the assignment and there is a new current assignment. Otherwise, the assignment is accepted with some probability, depending on the temperature and how much worse it is than the current assignment. The current assignment is unchanged if the change is not accepted. The parameter T, temperature in SA is to control how

Table 6.8: Selection of rules against different C_{FA} at different threshold points, where 'I', 'F', 'A' and 'O' stands for Iris, Fingerprint, And rule and Or rule respectively.

C_{FA}	The Rule chosen by SA at different threshold															
	Point1				Point2				Point3				Point4			
	I	F	A	O	I	F	A	O	I	F	A	O	I	F	A	O
1.6			√				√				√		√			
1.62			√				√				√		√			
1.64			√				√				√		√			
1.66				√			√				√		√			
1.68				√			√				√		√			
1.70				√			√				√		√			
1.72				√			√				√		√			
1.74				√			√				√		√			
1.76				√			√				√		√			
1.80				√			√				√		√			
1.82				√			√				√		√			
1.84				√			√				√		√			
1.86				√			√				√		√			
1.88				√				√			√		√			
1.9				√				√			√		√			
1.92				√				√			√		√			
1.94				√				√			√		√			
1.96				√				√			√		√			
1.98				√				√			√				√	

Table 6.9: Probability of acceptence of rule at different temperatures,T

T	Probability of acceptance			
	1.2- worse	3.5- worse	5.8- worse	6.5- worse
10	0.88	0.7	0.55	0.51
0.94	0.25	0.02	0.0017	0.0007
0.5	0.07	0.0006	0	0
0.3	0.02	0	0	0
0.25	0.0061	0	4.5562*e-011	1.7893*e-012
0.2	0.0018	0	1.3747*e-013	2.4527*e-015
0.17	0.0005	4.0362*e-010	4.1479*e-016	3.362*e-018
0.15	0.0001	1.1661*e-011	1.2515*e-018	4.6085*e-021
0.1	4.5400*e-005	3.3691*e-013	3.7761*e-021	6.3172*e-024

many worsening steps are accepted. Table 6.9 shows the probability of accepting worsening steps at different temperatures. Our goal is to minimize the cost of the multimodal biometrics system that we have obtained using the Bayesian cost E as in equation 6.6. If A is the current assignment of a value to each variable, $E(A)$ is the evaluation of assignment A to be minimized. As simulated annealing selects a neighbour at random by giving a new assignment $A^{'}$, if $E^{'}(A) \leq E(A)$, it accepts the assignment and $A^{'}$ becomes the new assignment. Otherwise, the assignment is only accepted randomly with probability $exp^{(E(A)-E(A^{'}))/T}$. The assignment is more likely to be accepted if $E(A^{'})$ is close to $E(A)$. At higher temperature, the exponent will be close to zero, and so the probability will be close 1. As the temperature approaches zero, the probability approaches zero and the exponent approaches $-\infty$. In the Table 6.9 $k-$worse means that $E(A^{'}) - E(A) = k$. i.e. when the temperature is 10(T=10), a change with k-worse=1.2 will be accepted with probability $e^{-0.12}$ approx 0.88, a change that is 3.5 will be accepted with probability $e^{-0.35}$ approx 0.7. Similarly when the temperature is reduced to 0.5, i.e. T=0.5, accepting a change with k=1.2 will occur with probability $e^{-1.2}$ approx 0.07. If the temperature is 0.1, a change that is one worse will be accepted with probability e^{-10} approx. In this temperature, it is essentially only performing steps that improve the value or leave it unchanged. With higher temperature, i.e T=10, the algorithm tends to accept steps that only worsen a small amount; it is not accepting a very large worsening steps. But as the temperature is slowly reduced the occurrences of the worsening steps are very less. With T=0.1, it is very rare that it chooses a worsening step.

6.6.1 Discussion

Fusion of fingerprint and iris biometric using the SA, BACO and BPSO methods individually are giving good result, thus proven to be a good solution for binary decision model that works better for moving through the decision fusion space of genuine or imposter classification of multimodal biometric verification.

In order to increase the possibility and scalability of the method with more numbers of traits, our model of two traits is extended with more number of trait like palmprint, thus performing analysis with the possible rule selections, which are reported on the next sections below.

6.7 Multimodal decision level fusion of Fingerprint, Iris and Palmprint using BACO and SA

In this work, effectiveness of the fusion method has been established using several benchmark dataset of different traits using SA and BACO approach.

6.7.1 Fusion of Fingerprint and Iris biometrics using SA and BACO

Here we have combined fingerprint and iris traits and used both simulated annealing and ant colony optimization technique to select best rule of fusion and results are obtained as shown in Table 6.10.

- From the Table it can be seen that SA performs better than ACO.

- Iris at a particular cost of false acceptance is sufficient to be prove as better trait than fingerprint.

A dynamic rule selection for fusion at dynamically selected threshold points with different cost of false acceptance is also obtained and results are as shown in Table 6.11.

Table 6.10: Rule selection for fusion of Iris and Fingerprint

C_{FA}	Probabilities of rule selected							
	SA				BACO			
	I	F	AND	OR	I	F	AND	OR
1.70	0	0	100	0	0	0	0	100
1.72	0	0	100	0	0	0	0	100
1.74	0	0	100	0	0	0	0	100
1.76	0	0	100	0	0	0	0	100
1.80	0	0	100	0	0	0	0	100
1.82	0	0	100	0	0	0	0	100
1.84	0	0	100	0	0	0	0	100
1.86	0	0	100	0	0	0	0	100
1.88	0	0	0	100	94	0	0	6
1.9	0	0	0	100	95	0	0	5
1.92	0	0	0	100	100	0	0	0
1.94	0	0	0	100	100	0	0	0
1.96	0	0	0	100	100	0	0	0
1.98	0	0	0	100	100	0	0	0

6.7.2 Fusion of Iris and Palmprint using SA and BACO

From the experimental study on the fusion of iris and palmprint with SA and ACO approach for biometric verification as reported in Table. 6.12 , it is observed that

- The SA approach has been found more effective than BACO based approach
- At higher CFA value (>1.7), the palmprint individually has been found sufficient for verification. It saves the cost of fusion significantly.

Table 6.11: Dynamic rules selection with threshold point selection

C_{FA}	Rules at different threshold points															
	Point1				Point2				Point3				Point4			
	I	F	A	O	I	F	A	O	I	F	A	O	I	F	A	O
1.6			√				√				√		√			
1.62			√				√				√		√			
1.64			√				√				√		√			
1.66				√			√				√		√			
1.68				√			√				√		√			
1.70				√			√				√		√			
1.72				√			√				√		√			
1.74				√			√				√		√			
1.76				√			√				√		√			
1.80				√			√				√		√			
1.82				√			√				√		√			
1.84				√			√				√		√			
1.86				√			√				√		√			
1.88				√				√			√		√			
1.9				√				√			√		√			
1.92				√				√			√		√			
1.94				√				√			√		√			
1.96				√				√			√		√			
1.98				√				√			√				√	

6.7.3 Fusion of Palmprint and Fingerprint using SA and BACO

For fusion of palmprint and fingerprint with the algorithm of SA and ACO, verification by palmprint with SA is sufficiently enough to work as unimodal system than fusion with fingerprint using ACO method with their convergence nature as reported in Table. 6.13

6.7.4 Fusion of Iris, Palmprint and Fingerprint using SA for identity verification

For the fusion of three biometric modalities that is iris, fingerprint and palmprint, it has been observed that Sum (OR) and Product (AND) fusion rules are more effective

Table 6.12: Rule selection for fusion of Iris and Palmprint

C_{FA}	Probabilities of rule selected							
	SA				BACO			
	I	P	AND	OR	I	P	AND	OR
1.70	8	33	59	0	0	0	100	0
1.72	0	100	0	0	0	0	100	0
1.74	0	100	0	0	0	0	100	0
1.76	0	100	0	0	0	0	100	0
1.80	0	100	0	0	0	0	100	0
1.82	0	100	0	0	0	0	100	0
1.84	0	100	0	0	0	0	100	0
1.86	0	100	0	0	0	0	100	0
1.88	0	100	0	0	0	0	100	0
1.9	0	100	0	0	0	0	100	0
1.92	0	100	0	0	0	0	100	0
1.94	0	100	0	0	0	0	100	0
1.96	0	100	0	0	0	0	100	0
1.98	0	100	0	0	0	0	100	0

with generated 17 rules as can be found that in Table 6.14

From the result as shown in the table, it obvious that palmprint based verification with SA dominates other traits due to their effectiveness.

6.7.5 Fusion of Iris, Palmprint and Fingerprint using BACO for identity verification

For the fusion of three biometric modalities that is iris, fingerprint and palmprint it has been observed that with 17 rules as found in Table 6.15, the Sum (OR) and Product (AND) fusion rules are more effective. From the result as shown in Table 6.15, it is obvious that palmprint based verification with BACO requires Iris trait to be verified with either palmprint or fingerprint based trait for identity verification of a person.

Table 6.13: Rule selection for fusion of Palmprint and Fingerprint

C_{FA}	Probabilities of rule selected by							
	SA				BACO			
	P	F	AND	OR	P	F	AND	OR
1.70	100	0	0	0	0	0	100	0
1.72	0	0	100	0	0	0	0	100
1.74	0	0	100	0	0	0	0	100
1.76	0	0	100	0	0	0	0	100
1.80	0	0	100	0	0	0	0	100
1.82	0	0	100	0	0	0	0	100
1.84	0	0	100	0	0	0	0	100
1.86	0	0	100	0	0	0	0	100
1.88	0	0	0	100	94	0	0	6
1.9	0	0	0	100	95	0	0	5
1.92	0	0	0	100	100	0	0	0
1.94	0	0	0	100	100	0	0	0
1.96	0	0	0	100	100	0	0	0
1.98	0	0	0	100	100	0	0	0

6.8 Performance Evaluation

We evaluate the performance of our method in light of three well-known and one synthetic datasets.

(a) Environment Used :The experiments were carried out on a workstation with Intel dual-core processor (1.86 GHz) with 1 GB of RAM. We used MATLAB 7.2 (R2006a) version in windows (64-bits) platform for the performance evaluation.

(b) Datasets used :We have used *five* datasets out of which *three* benchmark, and *one* synthetic dataset for fingerprint trait, *one* benchmark dataset for iris trait and *one* benchmark dataset for palmprint. The detail about the datasets are given in Table 6.16. The fingerprint FVC2000 and FVC2004 are available in [88]. The synthetic dataset was created using tools [89], where each image size is of 300 × 300 pixels. The iris dataset ia available in [90]. For the verification experiments, the datasets are divided into two parts training and test sets using

Table 6.14: Rule selection for fusion of Iris(I), Palmprint(P) and Fingerprint(F) by SA

C_{FA}	Rules with probabilities of selection																
	S1(I)	S2(F)	S3(P)	S1+S2	S1+S3	S2+S3	S1.S2	S1.S3	S2.S3	(S1.S2)+S3	(S1.S3)+S2	(S2.S3)+S1	(S1+S2).S3	(S1+S3).S2	(S2+S3).S1	S1.S2.S3	S1+S2+S3
1.70	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.72	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.74	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.6	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.80	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.820	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.84	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.86	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.88	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.90	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.92	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.94	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.96	0	0	100	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1.98	0	0	58	0	0	0	0	0	42	0	0	0	0	0	0	0	0

k-fold cross validation method with k=5. For iris dataset, i.e. CASIA V.1, we obtain the matching scores for different iris images, the corresponding error rates are generated using differnt threshold values. The ROC curve obtained for AND and OR rule selection of Iris CASIA and Fingerprint FVC dataset is shown in Figure 6-6. The FAR and FRR values are reported in Table 6.7. It can be seen from the table as well as from the figure that result is satisfactory.

6.9 Discussion

In our developed multimodal biometric verification modal we have found that

(i) The simulated annealing based method of biometric fusion outperforms its other counterpart method of particle swarm optimization and ant colony based method.

(ii) Decision level fusion of traits acceptability by user for identity verification can be

Table 6.15: Rule selection for fusion of Iris(I), Palmprint(P) and Fingerprint(F) by BACO

C_{FA}	Rules with probabilities of selection																
	S1(I)	S2(F)	S3(P)	S1+S2	S1+S3	S2+S3	S1.S2	S1.S3	S2.S3	(S1.S2)+S3	(S1.S3)+S2	(S2.S3)+S1	(S1+S2).S3	(S1+S3).S2	(S2+S3).S1	S1.S2.S3	S1+S2+S3
1.70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.72	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.80	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.82	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.84	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.86	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.88	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.90	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.92	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.94	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.96	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0
1.98	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	0	0

possible with good recognition rate. (iii) The modal is userfriendly as an user can select any one or more number of choices of biometric traits of its choice.
(iv) The model can be extended to more number of choices of traits in future.

In the next chapter we are reporting the conclusion and future prospect of the developed model.

Table 6.16: Datasets used for multimodal fusion of Fingerprint, Iris and Palmprint

Samples	Dataset types				
	Fingerprint		Fingerprint	Iris	Palmprint
	Real		Synthetic	Real	Real
	FVC 2000	FVC 2004		CASIA V.1	CASIA V.1
Training	200	200	200	324	1000
Test	100	100	100	432	1000

Chapter 7

CONCLUSION AND FUTURE WORK

In this chapter we report our concluding remarks based on our experience and finally attempts to highlights some future research directions.

7.1 Conclusion

A biometric system recognizes a person by determining the authenticity of a specific physiological or behavioral characteristic possessed by the person. Biometric systems offer a high degree of security than typical password-based authentication method, since biometric characteristics cannot be guessed or stolen. Moreover, biometric characteristics are not shared. At a given time, it is possible to keep track of user's activities through a biometric-based recognition system. The present study is concentrated on to develop a automatic biometric based identity verification system which is expected to open a new vistas in the cutting edge technologies. This could be taken as a de-facto standard towards the development of identity verification model in case of other biometric traits.

Despite of having several favorable advantages, the identity verification using a biometric may face the problem of non-universality due to the lack of population coverage. To challenge with a unimodal system, the present study leads to the development of multibiometric system for verification of user identity. In the present study, the effectiveness of the identity verification by multimodal biometric using fingerprint, iris and palmprint biometric traits are explored.

Among the six chapters embodied in this thesis, the Chapter 1 outlines the history and advancement of biometric researches and the objective and methodology of the present study. The biometric system and their pros and cons that necessitates for designing a multi-biometric system and their related works are described in Chapter 2.

The fingerprint verification for user identity proof has been discussed in Chapter 3. This chapter also describes about the coarse level classification and fine level matching of fingerprints using their minutiae details. A limited survey on some of the popular fingerprint classification methods was carried out and found capable of identifying four or five classes with an accuracy level of (80-95)%.

It is observed in the present study as mentioned in Chapter 3 that the proposed fingerprint classification method works with an accuracy level of 95% for coarse level classification and presents a new approach for graph based fine level matching of fingerprints and their template generation. Also we have reported two techniques, viz. graph based and distance based approach, for proofing robustness of various fingerprints. Although fingerprint classification and matching techniques have developed drastically over times, there are scopes for developments which will make the process more efficient and accurate. A multiple SOM based approach can be used to enhance the performance.

Chapter 4 deals with the verification of user identity with Iris biometric. In the present study we have explored the idea and usefulness of considering the iris verification method for user identity proof. The method we have adopted for classification of generated iriscode is providing significant results that outperforms other iriscode matching techniques found on our limited survey of iris verification base method.

As different biometric traits have their own usefulness base on the application it necessitates to study more with more number of traits like palmprint for the deployment of multimodal biometric, which outperforms its other counterpart biometric traits due to its large number of feature space. In the present study, the classifier selection for fine level matching of feature code to obtain a matching score is also carried out and tested using three different proximity measures namely Hamming distance, weighted Euclidean distance and Jaccard distances, as discussed in Chapter 4 and Chapter 5. In the context of the present study with respect to palmprint biometric as discussed in Chapter 5 the following observations have been made corresponding to these three distance measures.

- Selecting an appropriate and unbiased distance measure for texture based palmprint verification can be made by drawing an imposter and genuine match scores.

- The distribution curve of imposter and genuine match scores depicts the possibilities of optimization of threshold values of the match scores specific to application data. Access to a biometric system is granted only, if the biometric pattern to be verified is higher than certain threshold. If threshold value is increased, the FAR value is reduced but FRR will be more. To eliminate the differences for higher performances a linear graph is drawn using normal deviation scale on both axes as depicted on the respective graphs of HD, WED and JD.

- The matching threshold assessment for classification of genuine or imposter class can be made easily.

Chapter 6 deals with the verification of user identity with the proposed multimodal biometric system that comprises of fingerprint, iris and palmprint traits. Based on our proposed method, the following observation have been made-

- In case of unimodal biometric, its verification has been shown to be effective in a controlled environment and its performance can degrade in the presence of a mismatch between training and testing conditions.

- A multimodal biometric system comprises of several modality experts and a decision module. Hence, the error rates is low, since it uses complimentary discriminative information.

- A multimodal biometric system is more robust as degradation in performance of one modality can be compensated by another modality.

- Simulated Annealing(SA) based decision level fusion scheme outperforms other counterpart method like PSO and ACO and provide the identify verification method a more prominent field of study comparing its other counterpart method as in SA only few parameters are to be adjusted.

In case of multi-biometric system, fusion of evidences obtained from multiple biometric is a critical part. The key to successful multibiometric system is an effective fusion scheme and may be consolidated at several levels like feature level fusion, matching score level fusion, rank level fusion and decision level fusion. Among all of the above fusion approaches as our limited survey the decision level fusion is relatively more effective, yet understudied problem having a high potential for efficient consolidation of multiple unimodal biometric systems.

Chapter 7 Finally summarizes the work with concluding remarks. It also represents several scopes for future research.

7.2 Future Work

The present work as embodied in the thesis, is a decision level fusion scheme for multimodal biometrics of fingerprint, iris and palmprint for verification of user identity. In the fusion of fingerprint, iris and palmprint biometrics, the individual scores of three modalities are passed to a decision-level fusion module, where parameters are optimized with the help of PSO, ACO and SA approaches. However, there are several scopes for extension of the present model. Some of the directions for future research are listed below.

- The present multimodal verification system can be extended towards development of a full-fledged user authentication system by incorporating other security aspects.

- The performance of the present classifier can be further enhanced by incorporating improved active learning approach.

- Appropriate use of an ensemble of classifiers can further improve the performance of the overall accuracy of the verification system.

- Development of a real-life test-bed with the facilities of generation of unbiased training and test samples for all types of biometric traits can help evaluating a verification system properly.

- Use of a soft-computing approach can help handling the inconsistencies and imprecision in the datasets.

- Hardware implementation of the verification module can help providing a real time performance.

Author's Publication List

1. Gogoi, M., Bhattacharya, D.K. 'An effective Fingerprint Classification method using Minutiae Score Matching', *Journal of Computer Science and Engineering,* 1(1), http://arxiv.org/ftp/arxiv/papers/1006/1006.2804.pdf, 2010.
2. Gogoi, M., Bhattacharya, D.K. 'Fingerprint Classification using Minutiae Score', in *Proceedings of the National Conference on Trends in Machine Intelligence (NCTMI'11),* Tezpur University, 2011.
3. Gogoi, M., Bhattacharya, D.K. 'Fusion of Fingerprint and Iris biometrics using Binary Particle Swarm Optimization', in *Proceedings of the National Workshop on Network Security(NWNS'13)*, Tezpur University, 2013.
4. Gogoi, M., Bhattacharya, D.K. 'Fusion of Fingerprint and Iris biometrics using Binary Ant Colony Optimization', in *Third International Conference on Soft Computing for Problem Solving (SocPros 2013)*, IIT Roorkee, 2013.
5. Gogoi, M., Bhattacharya, D.K. 'Verification of identity using Multimodal biometric fusion', Communicating with an international journal, 2014.
6. Gogoi, M., Bhattacharya, D.K. 'Biometrics fusion, its needs and challenges: A survey', *International Conference on Green Energy and Smart Materials Through Science, Technology and Management (GESM'14)*, Organized by Faculty of Technology, Gauhati University and University of South Africa (UNISA), Florida Campus, ISBN:978-81-921779-0-8, 2014.
7. Gogoi, M., Bhattacharya, D.K. 'An Effective Method for Multi-biometric Fusion using Simulated Annealing', *International Journal of Computer Applications* (0975 8887) 95(25), June 2014.

Bibliography

[1] Jain A. K., Ross. A. Multibiometric Systems. Communications of the ACM, Special Issue on Multimodal Interface, 47(1), 34-40, January 2004.

[2] Jain A. K., Pankanti S. Biometrics Systems: Anatomy of Performance. IEICE Transactions Fundamentals, E84-D(7), 788-799, 2001.

[3] Dorigo, M.,Thomas, S. Ant Colony Optimization, MIT Press, Cambridge, 2004.

[4] Ross A., Nandakumar, K., and Jain, A.K. Handbook of Multibiometrics, Springer, New York, USA, 2006.

[5] S. Prabhakar, Jain, A.K. Decision-level Fusion in Biometric Verification. IEEE Trans. Patt. Anal. and Machine Intell, 2000.

[6] Gogoi, M., Bhattacharya, D.K. Fingerprint Classification using Minutiae Score, in Proceedings of the National Conference on Trends in Machine Intelligence (NCTMI'11), Tezpur University, 2011.

[7] Gogoi, M., Bhattacharya, D.K. An effective Fingerprint Classification method using Minutiae Score Matching, Journal of Computer science and engineering, 1(1), http://arxiv.org/ftp/arxiv/papers/1006/1006.2804.pdf, 2010.

[8] Gogoi, M., Bhattacharya, D.K. Fusion of Fingerprint and IRIS biometrics using Binary Particle Swarm Optimization, in Proceedings of the National Workshop on Network Security(NWNS'13), Tezpur University, 2013.

[9] Gogoi, M., Bhattacharya, D.K. Fusion of Fingerprint and Iris biometrics using Binary Ant Colony Optimization, in Third International Conference on Soft Computing for Problem Solving (SocPros 2013), 2013.

[10] Mahmoud, H.A., Ali, H.D. A simulated annealing technique for multi-objective simulation optimization, Applied Mathematics and Computation, 215(8), 3029Ũ3035, 2009.

[11] Zhao, P., Zhao. P., and Zhang, X. A New Ant Colony Optimization for the Knapsack Problem, Computer-Aided Industrial Design and Conceptual Design, CAIDCD '06. 7th IEEE International Conference, Hangzhou, DOI 10.1109/CAIDCD.2006.329439, 2006.

[12] Veeramachaneni, K., Osadciw, L.A., and Varshney, P.K. Adaptive Multi-modal Biometric Fusion Algorithm Using Particle Swarm, L.C. Smith College of Engineering and Computer Science, Electrical Engineering and Computer Science, 2003.

[13] Raghavendra, R. Rao, A., Kumar, G.H. Multimodal Biometric Score Fusion Using Gaussian Mixture Model and Monte Carlo Method, Journal of Computer Science and Technology, 2010.

[14] Singh, R., Vatsa, M., Noore, A. Integrated Multilevel Image Fusion and Match Score Fusion of Visible and Infrared Face Images for Robust Face Recognition, Pattern Recognition - Special Issue on Multimodal Biometrics, 41(3), 880–893, 2008.

[15] Nagar, A., Jain, A.K. On the Security of Non-Invertible Fingerprint Template Transforms, in Proc. IEEE Workshop on Information Forensics and Security, London, UK.

[16] Rattani, A., et al. Feature Level Fusion of Face and Fingerprint Biometrics, in Proc. 1st IEEE International Conference on Biometrics, Theory, Applications and Systems, 1–6, 2007.

[17] Giacinto, G., Roli, F. Methods for Dynamic Classifier Selection, in 10th International Conference on Image Analysis and Processing, Venice, Italy, 659–664, 1999.

[18] Giacinto, G. and Roli, F. Selection of Classifiers based on Multiple Classifier Behaviour, in Proceedings of the Joint IAPR International Workshops on Advances in Pattern Recognition, 2000.

[19] Kittler, J., et al. On Combining Classifiers, in IEEE Trans. Pattern Anal. and Machine Intell, 20(3), 226-239, 1998.

[20] Fierrez-Aguilar, J., Ortega-Garcia, J. and Gonzalez-Rodriguez, J. Fusion strategies in multimodal biometric verification, in IEEE International Conference on Multimedia and Expo, Los Alamitos, CA, USA : IEEE Computer Society, 5–8, 2003.

[21] Rukhin, L., Malioutov, I. Fusion of biometric algorithms in the recognition problem, Pattern Recognition Letter, 26, 679-684, 2005.

[22] Veeramachaneni, K. et al. Decision-level Fusion Strategies for Correlated Biometric Classifiers, in Proc. of IEEE Computer Society Workshop on Biometrics at the Computer Vision and Pattern Recogniton (CVPR) conference, Anchorage, USA, 2008.

[23] Chang, K.I., Bowyer, K.W., Flynn, P.J. An Evaluation of Multimodal 2D+3D Face Biometrics, IEEE Transactions on Pattern Analysis and Machine Intelligence , 27(4), 619Ũ624, April 2005

[24] Haupt, L.R. and Haupt, E.S. Practical Genetic Algorithms, 2^nd ed., Wiley Inderscience, 2004.

[25] Kennedy, J., Eberhart, R.C., Shi, Y.H. Swarm Intelligence, CA:Morgan Kaufmann, 2001

[26] Gogoi, M., Bhattacharya, D.K. Verification of identity using Multimodal biometric fusion, Communicating with an international journal, 2014.

[27] Phillips, P.J., et al. An Introduction to Evaluating Biometric Systems, IEEE Computer, 33(2), 56-63,2000.

[28] Jain, A.K., Ross, A., and Pankanti, S., Biometrics: A Tool for Information Security, IEEE Transactions on Information Forensics and Security, 1(2), 125 -143, June 2006.

[29] Jain, A.K., Nandakumar, K., Abhishek, N. Biometric Template Security EURASIP Journal on Advances in Signal Processing Special Issue on Biometrics, January 2008.

[30] Duan, H.B. Ant Colony Algorithms: Theory and Applications, Science Press, Beijing, 2005.

[31] Dorigo, M., Caro,G.D., Stutzle,T. Special Issue on Ant Algorithms, Future Generation Computer Systems, 16(1), June 2000.

[32] Maltoni, D., et al. Handbook of Fingerprint Recognition, Springer, New York, 2003.

[33] Maio, D., Maltoni, D. A structural approach to fingerprint classification, in Proc. ICPR 578–585, 1996.

[34] Karu, K., Jain, A.K. Fingerprint classification, Pattern Recognition. 29(3), 389–404, 1996.

[35] Hong, L., Jain, A. Classification of fingerprint images, in Proceedings of the 11th Scandinavian Conference on Image Analysis, Kangerlussuaq, Greenland, 1999

[36] Jain, A., Prabhakar, S., Pankanti, S. Matching and classification: a case study in the fingerprint domain. Proceedings of the Indian National Science Academy. 67(2), 67–85, 2001.

[37] Daugman, J. How Iris Recognition Works, IEEE Transactions on Circuits and Systems for video technology, 14(1), 2004.

[38] Jain, A.K., Prabhakar, S., Hong, L.: A multichannel approach to fingerprint classification. IEEE Trans Patt Anal Mach Intell. 21(4) (1999) 348–359

[39] Bhuyan, M.H., Saharia, S., Bhattacharyya, D.K. An Effective Method for Fingerprint Classification. IAJeT 1(3),89–97, ISSN 1997-6364, 2010.

[40] Raghavendra, R. Rao A., Kumar G. H. Multimodal Biometric Score Fusion Using Gaussian Mixture Model and Monte Carlo Method, Journal of Computer Science and Technology, 2010.

[41] Singh, R., Vatsa, M., Noore, A. Integrated Multilevel Image Fusion and Match Score Fusion of Visible and Infrared Face Images for Robust Face Recognition, Pattern Recognition - Special Issue on Multimodal Biometrics. 41(3), 880–893, 2008.

[42] Nagar, A., Jain, A.K. On the Security of Non-Invertible Fingerprint Template Transforms, in Proc. IEEE Workshop on Information Forensics and Security, London, UK

[43] Rattani, A., et al. Feature Level Fusion of Face and Fingerprint Biometrics, in Proc. 1st IEEE International Conference on Biometrics, Theory, Applications and Systems, 1–6, 2007.

[44] Giacinto, G., Roli, F. Methods for Dynamic Classifier Selection, in 10th International Conference on Image Analysis and Processing, Venice, Italy, 659–664, 1999.

[45] Giacinto, G. and Roli, F. Selection of Classifiers based on Multiple Classifier Behaviour, in Proceedings of the Joint IAPR International Workshops on Advances in Pattern Recognition, 2000.

[46] Kittler, J., On Combining Classifiers, IEEE Trans. Pattern Anal. and Machine Intell, bfseries 20(3), 226-239, 1998.

[47] Fierrez-Aguilar, J., Ortega-Garcia, J. and Gonzalez-Rodriguez, J. Fusion strategies in multimodal biometric verification, in IEEE International Conference on Multimedia and Expo, Los Alamitos, CA, USA : IEEE Computer Society, 5-8, 2003.

[48] Rukhin, L., Malioutov, I. Fusion of biometric algorithms in the recognition problem, Pattern Recognition Letter, 26, 679-684, 2005.

[49] Kumar, A., et al. Decision-level Biometric Fusion using Ant Colony Optimization, in Proc. of IEEE 17th International Conference on Image Processing, 2010.

[50] Kung, S.Y., Mak, M.W. and Lin, S.H. Biometric authentication, Prentice Hall, 2004.

[51] Dorigo, M., Maniezzo, V., Colorni, A. Ant system: Optimization by a colony of cooperating agents, IEEE Trans. on Systems, Man and Cybernetics, Part B, 26, 29-41, Feb. 1996.

[52] Lam, L., and Suen, C.Y. Optimal Combination of Pattern Classifiers, Pattern Recognition Letters, 16, 945-954, 1995.

[53] Xu, L., Krzyzak, A., and Suen, C.Y. Methods for Combining Multiple Classifiers and their Applications to Handwriting Recognition, IEEE Transactions on Systems, Man, and Cybernetics, 22(3), 418-435, 1992.

[54] Daugman, J., Combining Multiple Biometrics, http://www.cl.cam.ac.uk/users/jgdlOOO/combine/combine.html.

[55] Poh, N., Bengio, S., Database, protocols and tools for evaluating score-level fusion, Pattern Recognition, 39(2), 223Ű233, 2006.

[56] Maltoni D., Maio D., Jain A. K., Prabhakar A. Handbook of Fingerprint Recognition, Springer, New York, 2003.

[57] Dorigo, M., Maniezzo, V., Colorni, A. Ant system: Optimization by a colony of cooperating agents, IEEE Trans. on Systems, Man and Cybernetics, Part B, 26, 29-41, Feb. 1996.

[58] Gogoi, M., Bhattacharya, D.K. Biometrics fusion, its needs and challenges : A survey, International Conference on Green Energy and Smart Materials Through Science, Technology and Management (GESM'14), Organized by Faculty of Technology, Gauhati University and University of South Africa (UNISA), Florida Campus, ISBN:978-81-921779-0-8, 2014.

[59] Gogoi, M., Bhattacharya, D.K. An Effective Method for Multi-biometric Fusion using Simulated Annealing, International Journal of Computer Applications (0975 8887) 95(25), June 2014.

[60] Chong, M., et al., Geometric framework for fingerprint image classification, Patt Recog, 30(9), 1475Ũ1488, 1997.

[61] Standards, W.C.L., Massively parallel neural network fingerprint classification system, National Institute of Standards and Technology, NISTIR 4880, 1992.

[62] Candela, G., et al. PCASYSŮa pattern-level classification automation system for finger-prints, National Institute of Standards and Technology, NISTIR 5647, 1995.

[63] Federal Bureau of Investigation, WSQ gray-scale fingerprint image compression specification, Document IAFISIC-0110v2, 1993.

[64] Halici, U., Ongun, G. Fingerprint classification through self-organizing feature maps modified to treat uncertainties, in Proc IEEE 84(10), 1497-1512, 1996.

[65] Bernard, S., Boujemaa, N., Vitale, D., Bricot, C. Fingerprint classification using a Kohonen topologic map, In Proceedings of the International Conference on Image Processing, Thessaloniki,.Greece, October 2001.'

[66] Mohamed, S., Nyongesa, H., Automatic fingerprint classification system using fuzzy neural techniques, in Proceedings of the 2002 IEEE International Conference on Fuzzy Systems, Washington, DC, April, 2002

[67] SOM Matlab ToolBox. http://www.cis.hut.fi/projects/somtoolbox/.

[68] Cappelli, R., Maio, D., Maltoni, D. Fingerprint classification based on multi-space KL, In Proceedings of the Workshop on Automatic Iden-tification Advances Technologies, Summit, NJ, ,. [36]

[69] Vapnik, V. The nature of statistical learning theory, Springer, Berlin Heidelberg, New York,1995

[70] http://biolab.csr.unibo.it/sfinge.html

[71] Hong, L. Automatic Personal Identification Using Fingerprints, Ph.D. Thesis, 1998

[72] http://www.cubs.buffalo.edu/

[73] http://www.biometrics.idealtest.org/

[74] Rucklidge, W.J, Efficient Computation of the Minimum Hausdorff Distance for Visual Recognition, Ph.D. thesis, Cornell University, 1995.

[75] Dubuisson, M.P. and Jain, A.K. A modified hausdorff distance for object matching, in Proc. IEEE Int. Conf. on Pattern Recognition, 566-568, Sept. 1994.

[76] Jain, A.K., Ross, A. Multibiometric Systems, Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1), 34-40, January 2004.

[77] Jain, A.K., Ross, A. Multibiometric Systems, Communications of the ACM, Special Issue on Multimodal Interfaces, 47(1), 34-40, January 2004.

[78] Boles, W.W., Boashash. A Human Identification Technique Using Images of The Iris and Wavelet Transform, IEEE trans. Signal Processing, 46(4), 1185-1188, 1998.

[79] Choi, J., Kim, J., Cho, S., Marks, R.J. Iris recognition using wavelet features, Journal of VLSI Signal Processing, 38(2), 147-156, 2004.

[80] Kevin, W., Bowyer, X.L., Patrick, J.F. Experimental evaluation of iris recognition, In Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), volume 3, page 158, Washington, DC, USA, 2005.

[81] Wang, H., Biswanath, S., Madabuhshi A. Dscriminatively weighted multiscale local binary patterns: Applications in prostate cancer diagnosis on T2W MRI, In Proceedings of the 2013 IEEE 10th International Symposium on Biomedical Imaging:From Nano to Macro, San Francisco, CA, USA, April 7-11, 2013

[82] Daugman, J. Iris Recognition for personal Identification, The Computer Laboratory, University of Cambridge

[83] Daugman, J. University of Cambridge: Computer Laboratory: Webpage for John Daugman. http://www.cl.cam.ac.uk/users/igd1000/

[84] Flom L. and Safir A. Iris recognition system, U.S. Patent 4641349, February 03, 1987.

[85] Davis, R.L., Becherer, P.D. Techniques for improved soft lens fitting. Contact Lens Spectrum, no. 117, 2005.

[86] Masek, L. Recognition of Human Iris Patterns for Biometric Identification, Thesis, 2003

[87] Zhu, Y., Wang, Y.: Iris Image Acquisition System, Chinese Patent Application.

[88] http://www.bias.csr.unibo.it/fvc2004

[89] http://www.cubs.buffalo.edu: SFinge

[90] http://www.biometrics.idealtest.org

[91] Zhang, D. Palmprint authentication, kluwer academic publishers, 2004.

[92] Zhang, D., Shu, W. Two novel characteristics in palmprint veriÞcation: datum point invariance and line feature matching, Pattern Recognition 32, 691-702, 1999.

[93] Zang, D., Kong, W., You, J., Wong, M. Online Palmprint Identification, Pattern Analysis and Machine Intelligence 25(9), 1041-1051, 2003.

[94] Han, C.C., Cheng, H.L., Lin, C.L., and Fan, K.C. Personal Authentication using palmprint features, Pattern Recognition 36(2), 371-381, 2003.

[95] Han, C.C. A hand-based personal authentication using a coarse-to-fine strategy, Image and Vision Computing, 22(11), 909-918, 2004.

[96] Li, W., Zhang, D., Xu, Z. Palmprint identification by Fourier transform, International Journal of Pattern Recognition and Artificial Intelligence, 16(4), 417-432, 2002.

[97] Wu, X., Wang, K. and Zhang, D. HMMs based palmprint identification, Lecture Notes in Computer Science, Springer, 3072, 775-781, 2004.

[98] Kong, A., Zhang D., Lu, G. A study of identical twins palmprint for personal verification, Pattern Recognition, 39(11), 2149-2156, 2006.

[99] Gonzalez R. C., Woods R.E., Digital Image Processing: Addison-Wesley Pub (Sd),3^rd ed.

[100] Poon,C., Wong D.C.M., Shen H.C.,ŞA new method in locating and segmenting palmprint into Region-of-InterestŤ. ICPR 4, 2004, p 1051-4651.

[101] Hennings, P., Kumar, V. B.V.K. Palmprint Recognition Using Correlation Filter Classifiers, IEEE 2004.

[102] Wang, J.Z., Li, J., Wiederhold, G. SIMPLIcity: Semantics -Sensitive Integrated Matching for Picture LIbraries, , .IEEE Transactions on Pattern Analysis and Machine Intelligence, 23(9), 947-963, 2001

[103] Pang, Y. H., Andrew, T.B.J, David, N.C.L, San, H. F. Palmprint Verification with Moments, Journal of WSCG, 12(1-3), ISSN 1213-6972, Plzen, Czech Republic, February 2-6, 2003.

[104] Connie, T., Goh, M., Teoh, A., Ngo, D. An automated biometric palmprint verification system, 3rd Int. Symp. On Communications & Info. Tech. (ISCIT2003), 2(), 714-719, 2002.

[105] Ray, K. B., Misra, R. A New Method in Palmprint Features using Region-of-Interest, 3rd National Conference on Recent Trends in Communications computation and Signal Processing (RTCSP), Koimbator, Amrita ViswaVidyalayam University, 294-297, Mar 2011.