CHAPTER – 1

INTRODUCTION TO BIOMETRIC TECHNOLOGY FOR IDENTIFICATION AND VERIFICATION

1.1 Introduction

As with the growth of Information Technology, the need of the security has became a prime issue in the area of IT. The security can be managed in number of ways. One way to improve security is by identifying or verifying the person with some technique. So, the basic idea is the identity of the person which can improve the security.

The term of identity is defined as “the quality or condition of being the same in substance, composition, nature, properties, or in particular qualities under consideration”. An identity is also defined as “a presentation or role of some underlying entity”.

In the case of a human being, this entity can have some physical features such as its height, weight or DNA, called attributes. The identity of this entity has also some attributes, such as a username, a social security number or particular authorizations and permissions.

Three approaches are available to prove a person’s identity and to provide “the right person with the right privileges, the right access at the right time”. These identity proving approaches, which establish the genuineness of the identity, are:

Something you have The associated service or access is received through the presentation of a physical object (keys, magnetic card, identity document etc.) in possession of the concerned person.

Something you know A pre-defined knowledge, as a password normally kept secret, permits to access a service.

Something you are Measurable personal traits, such as biometric measures, can also be used for identity prove.

A combination of these approaches makes the identity proof more secure. In day to day activities, the combination of possession and knowledge is very widespread. The use of the third approach, in addition to the others, has significant advantages. Without sophisticated means, biometrics is difficult to share, steal or forge and cannot be forgotten or lost.

1.1.1 Biometrics

The term “Biometrics” is derived from the Greek words “bio”(life) and “metrics”(to measure).[2] Biometrics is a term that encompasses “the application of modern statistical methods to the measurements of biological objects”. However, by language misuse, the term biometrics usually refers to automatic technologies for measuring and analyzing biological and anthropological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for identity prove. Biometrics refers to “Identifying an individual based on his or her distinguishing characteristics”.

Ideally the biometric characteristics used should satisfy the following properties:

- **Robustness** Over time, the characteristic should not change (Permanence), and thus have low intra-class variability.
- **Distinctiveness** Over the population, a great variation of the characteristic should exist (Uniqueness), and thus have large inter-class variability.
- **Availability** Ideally, the whole population should possess the characteristic (Universality).
- **Accessibility** The characteristic should be easy to acquire (Collectability).

The characteristics could be physiological or behavioral. Characteristics, which can be measured on a part of the body at some point in time (passive), are physiological biometrics. On the other hand, characteristics, which are learned or acquired over time (active), are called behavioral. For example, fingerprint, hand geometry and face are physiological biometrics, while dynamic signature, gait, keystroke dynamics and lip motion are behavioral once.

1.1.2 History of Biometrics

One of the basic examples of the use of biometrics is recognition of human by face. Other characteristics have been used throughout the history of civilization as a more formal means of recognition.

In a cave estimated to be at least 31,000 years old, the walls are adorned with paintings believed to be created by prehistoric men who lived there. Surrounding these painting are numerous hand-prints like their unique signature.

There is also evidence that fingerprints were used as a person's mark as early as 500 B.C. in Babylon.[1] Joao D. Barros wrote that early Chinese merchant used fingerprint to settle transactions.

By the mid-1800s, due to industry revolution and growth, there was a need to indentify people. With the influence of writings of Jeremy Betham and other Utilitarian thinkers, the courts of this time period began to codify concepts of justice that endure with us to this day. This created a need for formal system for identification with the use of identity traits. There were two approaches introduced in this duration. The first approach was the Bertillon system of measuring various body dimensions, which was originated in France. The other approach was the formal use of fingerprints by police departments. This method was used in South America, Asia and Europe. By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records. The first robust system for indexing fingerprints was developed in India by Azizul Haque for Edward Henry, IGP of Bengal, India. This system was called the Henry System.

The biometric systems began to emerge in the latter half of the 20th century, coinciding with the emergence of computer systems. The emerging field experienced an explosion of activity in the 1990s and began to surface in everyday applications in 2000s.

1.1.3 Use of Biometrics

A biometric system is essentially a pattern-recognition system. Such a system involves three aspects: data acquisition and preprocessing, data representation, and decision-making. It can thus compare a specific set of physiological or behavioral characteristics to the characteristics extracted beforehand from a person, and recognize this last one. The digital representation recorded in a database, which describes the characteristics or features of a physical trait, is defined as a template. It is obtained by a feature extraction algorithm. Biometric systems are traditionally used for three different applications: physical access control for the protection against unauthorized person to access to places or rooms, logical access control for the protection of networks and computers, and time and attendance control.

An authentication procedure can be performed in two modes by a biometric system:

1. *Identification*

This method consists in selecting the correct identity of an unknown person from a database of registered identities (Figure 1.1). It is called “one to many” matching process, because the system is asked to complete a comparison between the person’s biometrics and all the biometric templates stored in a database. The system can take either the “best” match, or it can score the possible matches, and rank them in order of similarity.

Two modes are possible, positive and negative identification. The positive identification tends to determine if a given person is really in a specific database. Such a method is applied when the goal is to prevent multiple users of a single identity. A negative identification determines if a given person is not in a “watch list” database. Such a method is applied for example when the goal is to identify persons registered under several identities.

2. *Verification*

This method consists in verifying whether a person is who he or she claims to be (Figure 1.2). It is called a ”one to one” matching process, as the system has to complete a comparison between the person’s biometric and only one chosen template stored in a centralized or a distributed database, e.g. directly on a chip for an identity document. Such a method is applied when the goal is to secure and restrict specific accesses with obviously cooperative users.

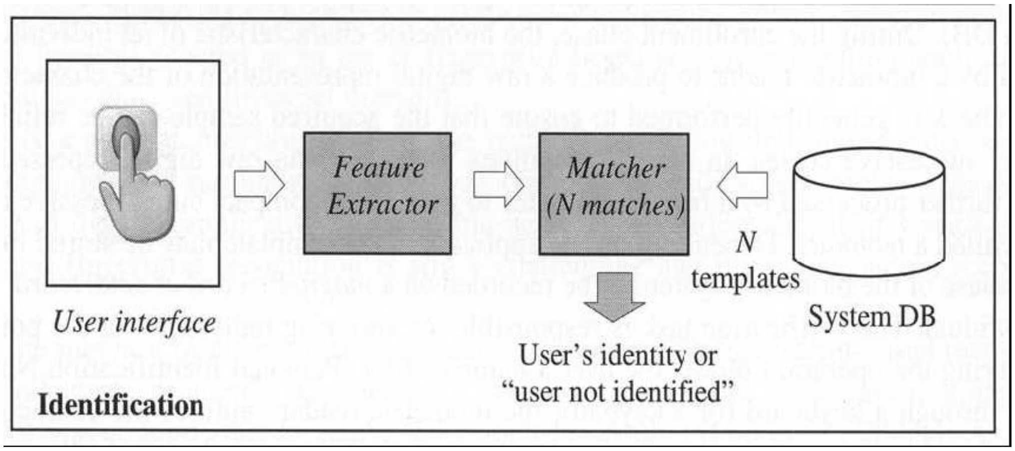

Figure 1.1 Identification

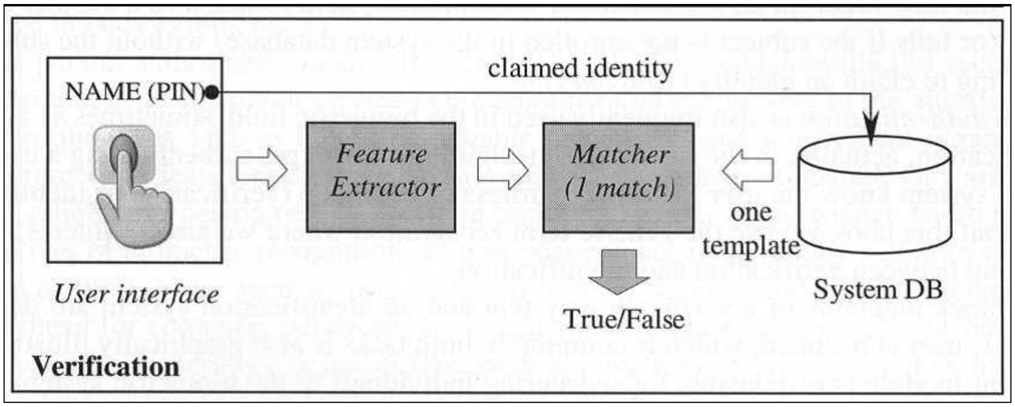

Figure 1.2 Verification

1.1.4 Properties of Biometric System

Besides the basic properties that a biometric has to satisfy, some additional properties have to be considered in a biometric system:

- **Performance** All the factors that influence and affect the accuracy and the computational speed of a biometric system.
- **Acceptability** The population should accept the fact that the characteristic is taken from them.
- **Circumvention** The ability of a system to resist against potential threats and spoof attacks.
- **Exception handling** The ability to complete a manual matching process in the case of an impossibility of features' extraction and modality use for certain persons.
- **System Cost** All the costs of the system components, in adequate and normal use.

1.1.5 Applications of Biometrics

As we have seen the basic applications of biometrics. Biometrics is used for both identification and verification. In other words, we can say that biometric systems are used in authentication and authorization. Now a day, fingerprint and facial recognition technologies are used widely for the identity purpose. The other technologies like iris and retina scanning is used in the areas where higher security is needed. The physiological traits are used widely. While among the behavioral traits, voice recognitions is used widely. DNA recognition is used for forensic purpose.

The Government of India has started the project “UID” for unique identity card of each Indian. This card will contain fingerprint data of the person. This will be the largest collection of fingerprints in the world. The person will be able to use this card anywhere in India to prove his/her identity. Similar types of projects are already implemented in European countries and in America. At the places where high security is needed, biometric identification is widely used. E.g. Airport and borders of the countries are the places of such importance. Even banks are implementing the use of biometrics traits for person authentication in their ATMs in rural areas where persons are illiterate. Fingerprint and facial recognition systems are specially used for attendance management. The public deployment of surveillance technology uses CCTV cameras through which we can identify the person with criminal background and who can do some destructive work in the area. In some countries, the facial recognition is used in voter’s registration. Iris scan technology is used for card less transaction with ATM. London’s Heathrow Airport has implemented Iris scan technology for clearance of immigration of visitors.

Voice recognition is not so widely used like fingerprint and facial recognition. A curfew enforcement system using voice-scan was adopted by the New York City Department of Corrections. Bacob, a Belgian financial institution, became the first European bank to provide a system for customers to make secure transactions by telephone. In Australia, Timemac Solutions has used Nuance voice-scan and speech recognition technology to allow stockholders to trade shares via telephone.

Hand-scan has been deployed in a number of interesting large-scale applications. In the United States, frequent international travelers can utilize the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS), permitting them to bypass waiting lines in the airport. Using Recognition Systems hand-scan technology, the system has been in place since 1993. In 1998, Ben-Gurion Airport in Tel Aviv, Israel, installed a similar system using hand-scan technology to allow Israeli citizens to circumvent lines when traveling internationally.

Retina-scan technology is best deployed in high-security environments where user convenience is not a priority, particular those involving employees in military, power plant, or sensitive laboratory environments. In the mid-1990s, the state of Illinois actually piloted retina-scan technology as a means of deterring and detecting duplicate welfare recipients.

The other rarely used biometric technology is signature scanning. There are few real-world deployments of signature-scan technology outside of standalone PC and PDA authentication for individual users. Charles Schwab & Co. began to allow customers elective use of a signature-scan system for new account applications.

1. 2 Statement of the problem

Title of the present study is: “Study the Issues and Solutions of Multimodal Biometric Authentication System Based on Fingerprint and Facial Recognition with Neural Network Approach”

In present study the authentication is performed with multimodal biometric traits. There are several biometric traits: Fingerprint, Facial, Iris, Retina, Hand geometry, Voice, Key stroke, and DNA. Here in this study fingerprint and facial recognition both are used for person authentication.

The proposed system uses the approach of neural network for reduction of error rate with help of back propagation. Threshold values need to be adjusted to reduce FAR and FRR. The scores of fingerprint and facial recognition are input to the neural network and output is the authentication of the person in terms of Yes or No. Weights of each trait need to be adjusted in hidden layers in neural network. And based on the rate of false rejection, back propagation is to be applied for weight adjustment.

1.3 Objective of the study

The principle objective of the present study is

- **To design and develop Multimodal Biometric Authentication System with more accuracy and cost effectiveness with compare to Unimodal Biometric Systems.**

To achieve this objective some sub-objectives were also formed, which are given below:

1. Study of concepts of face recognition and fingerprint recognition and methods.
2. Developing platform for capturing face and fingerprint samples of users for creation of database.
3. Creation of master face database and master fingerprint database.
4. Designing and developing multimodal IDE for implementation of unimodal biometrics systems using face and fingerprint recognition, multimodal biometric system using face and fingerprint recognition, multimodal biometric system using face and fingerprint recognition using neural network approach.
5. Designing and developing unimodal biometric face recognition system and performance evaluation.
6. Designing and developing unimodal biometric fingerprint recognition system and performance evaluation.
7. Study of existing multimodal biometric system and designing and developing multimodal biometric system using face and fingerprint recognition.
8. Designing neural network architecture with back propagation to adjust weights values as per the accuracy needs. (Weights will be adjusted automatically with reference to the result and accuracy limits)
9. Designing and developing multimodal biometric system using face and fingerprint recognition with neural network approach (with weight adjustment).
10. Comparing the results of Unimodal Biometric systems (Face and Fingerprint), Multimodal Biometric system and Multimodal Biometric system with neural network approach.

1.4 Rationality of the study

Importance of the study can be identified as:

1. With the help of this multimodal biometric system, we can minimize the error rate present with unimodal biometric technologies like fingerprint and facial recognition.
2. This model will be cost effective, because it will need fingerprint scanner and webcam for registration.

3. Neural network model will help to maintain the weight of important trait for authentication.
4. Backpropagation in the neural network model will adjust the weights of traits based on false rejection. This will in turn minimize the FRR and FAR.
5. The same model will also be useful to create multimodal biometric systems with other traits like palmprint, hand geometry, voice and keystroke recognition.
6. This system will be useful for authentication in areas where it is hard to capture any single trait and perform authentication. It will be possible to identify the person even if any one trait is not clear.

1.5 Scope of the study

“Biometrics” word is used to describe different identification techniques for a human. Here in this system, two biometrics traits are used to identify the person; they are fingerprint and face recognition. Rather than using a single trait, here two traits are used to increase the success ratio. Multibiometrics can be used in many different ways. This system is going to use multimodal biometric system. The study is distributed among different software components, which are developed with MATLAB.

The system contains easy to use GUI for register and enrolls the fingerprint and face sample. The system will capture the fingerprint sample and face sample, which will be used to generate template of the features of a human. This template is stored in .dat file on permanent basis for comparison in future. The template generated at authentication time is compared with template in database.

Here the fingerprint and face recognition softwares are created as per the need of the system. The system uses fingerprint capturing tool and webcam to capture face image. These tools will actually reduce the cost of the system.

1.6 Limitations of the study

1. This software is using webcam to capture the front face image, which may be of lower resolution.

2. As here the system is using the fingerprint and face recognition system designed by the researcher with the help of open source face and fingerprint code, so with compare to Unimodal COTS tools, accuracy of each tool may be compromised.
3. There are limitations in testing environment, so some aspects cannot be covered.

1.7 Literature review of the study

The main objective of the present study is “To develop multimodal biometrics using fingerprint and face recognition with neural network architecture”. The researcher has studied a lot of related literature to understand the related work in this area. This study has cleared the idea of the work. Here is the brief of literature review.

1.7.1 A glance over related literature

Multimodal biometric systems (Hong et al., 1999)[12], are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the strict performance requirements imposed by various applications (Hong and Jain, 1998)[11]. Multimodal systems address the problem of non-universality: it is possible for a subset of users to not possess a particular biometric. Multibiometric fusion refers to the fusion of multiple biometric indicators. Such systems seek to improve the speed and reliability (accuracy) of a biometric system (Hong and Jain, 1998) by integrating matching scores obtained from multiple biometric sources. A variety of fusion schemes have been described in the literature to combine various scores. These include majority voting, sum and product rules, k-NN classifiers, SVMs, decision trees, Bayesian methods, etc.[13].

Some of the earliest multimodal biometric systems utilized face and voice features to establish the identity of an individual (Brunelli and Falavigna, 1995)[14]. Physically uncorrected traits (e.g., fingerprint and iris) are expected to result in better improvement in performance than correlated traits (e.g., voice and lip movement).The below given tables show examples of multimodal biometric systems.

Modalities fused	Authors	Level of fusion	Fusion methodology
Face and voice	Brunelli and Falavigana, 1995	Match score and rank	Geometric weighted average; HyperBF
	Kittler et al.,1998	Match score	Sum, product, min, max and median rules
	Ben-yacoub et al., 1999	Match score	SVM, Multilayer perceptron, C4.5 decision tree, Fisher's linear discrimination, Bayesian classifier
	Bigaun et al., 1997	Match score	Statistical model based on Bayesian theory
Face, voice and lip movement	Frischholz and Dieckmann, 2000	Match score, decision	Weighted sum rule, majority voting
Face and fingerprint	Hong and Jain, 1998	Match score	Product rule
	Snelick et al., 2005	Match score	Sum rule, weighted sum rule
Face, fingerprint and hand geometry	Ross and Jain, 2003	Match score	Sum rule, decision trees, discriminant function
Face, fingerprint and voice	Jain et al., 199b	Match score	Likelihood ratio
Face and iris	Wand et al., 2003	Match score	Sum rule, weighted sum rule, fisher's linear discrimination , neural network
Face and gait	Shakhnarovich et al., 2001	Match score	Sum rule
	Kale et al., 2004	Match score	Sum and product rules
Face and ear	Chang et al., 2003	Sensor	Concatenation of raw images
Face and palmprint	Feng et al., 2004	Feature	Feature concatenation
Fingerprint, hand geometry and voice	Toh et al., 2004	Match score	Weighted sum rule
Fingerprint and hand geometry	Toh et al., 2003	Match score	Reduced multivariate polynomial model
Fingerprint and voice	Toh and Yau,2005	Match score	Functional link network
Fingerprint and signature	Fierrez-aguilar et. al.,2005c	Match score	SVM in which quality measures are incorporated
Voice and signature	Krawczyak and Jain,2005	Match score	Weighted sum rule

Table – 1.1 Multimodal Biometric Systems[5]

Artificial Neural Network (ANN) is a powerful tool to approximate functions. It has been used to approximate the functional relationship between motion capture data and the parameters of pre-defined facial deformation models. The neural network approach has also been used in Fingerprint recognition for classification.

Leung, Engeler, and Frank (1990) introduced a neural network-based approach where a multi-layer perceptron analyzes the output of a rank of Gabor filters applied to the gray-scale image. The image is first transformed into the frequency domain where the filtering takes place.

Maio and Maltoni (1998b)[3] used a shared-weights neural network to verify the minutiae detected by their gray-scale algorithm (Maio and Maltoni, 1997).

Statistical tools such as Support Vector Machines (SVM), Linear Discriminant Analysis (LDA), Principal Component Analysis (PCA), Kernel methods, and Neural Networks have been used to construct a suitable set of face templates. Here the concept of neural network was adopted by Jonathan Howell et al. for classification of human face.

Morishima et al. (1998) used ANN to learn a function, which maps 2D marker movements to the parameters or a physics-based 3D face deformation model. This helped to automate the construction of physics based face muscle model, and to improve the animation produced. ANN has been used to learn the correlation between facial deformation and other related signals. For example, ANN is used to map speech to face animation [Lavagetto, 1995, Morishima and Yotsukura, 1999, Massaro and et al., 1999].

By conducting experiments on a population approaching 1,000 individuals, Snelick, Uludag, Mink, Indovina and Jain (2005) demonstrated that the multimodal fingerprint and face biometric system, which combines the two biometric traits at the matching score level, was significantly more accurate than any individual biometric systems.

Fusion at the matching score level can be carried out using three distinct approaches. The first approach treats fusion as a classification problem (Ma, Cukic, & Singh, 2005) whereas the second approach treats fusion as a combination problem. The third approach, namely the density-based approach, treats fusion at the matching score level as a density-based score fusion problem, which is based on the likelihood ratio test and explicit estimation of genuine and impostor match score densities (Griffin, 2004).In the first approach, the matching score outputs of the individual biometric traits are first concatenated to form a feature vector. This feature vector is then classified into one of two classes: genuine user or impostor. This is also referred to as classifier-based score fusion (Nandakumar, Chen, Dass and Jain, 2008).

A number of studies (Dass, Nandakumar, & Jain, 2005; Kittler, Hatef, Duin, & Matas, 1998; Poh & Bengio, 2006; Ross & Jain, 2003; Schmid, Ketkar, Singh, & Cukic, 2006; Snelick Uludag, Mink, Indovina, & Jain, 2005; Vielhauer & Scheidat, 2005) have demonstrated that the matching score level fusion strategy can lead to a higher accuracy than the single biometric system.

In the second approach, the individual matching scores are combined to generate the final matching score which is then used to make the final decision. The density-based approach has the following advantage: If the score densities can be estimated accurately, it is able to achieve optimal performance at any desired FAR.

A normalization step is used to normalize the matching scores generated from different biometric traits and then the normalized scores are integrated to obtain the final matching score. One reason that the normalization step is adopted is the matching scores of multiple biometric traits may not be homogeneous. A variety of normalization procedures have been proposed for matching score level fusion (Snelick, Uludag, Mink, Indovina, & Jain, 2005). The normalized matching scores will be further integrated to produce the final matching score for personal authentication by using different approaches. Face has highest user acceptance and its acquisition is most convenient to users (Prabhakar, Pankanti, & Jain, 2003).

The matching scores generated from different biometric traits are used as inputs of a neural network classifier. Because each user has its claimed identity, the claimed user identity is also used as a feature to neural network classifier. The trained neural network classifies the user as a genuine user or impostor. David Zhang et. al. suggested neural network based classification approach for face and palmprint recognition in multimodal biometrics[5][7]. The matching scores from the face and palm print are used as inputs to train a feed-forward neural (FFN) network.

In Fingerprint recognition, because of the large variety and possibilities in authentic fingerprint features, the problem of effectively selecting and combining features to differentiate spoofs is unique to the MSI technology. One way to select and create conglomerate features is through multivariate data-driven learning techniques, such as neural networks or discriminate analysis (Duda et al., 2001). In Hill (2001), a neural network classifier is adopted to predict the fingerprint class.

There have been several neural network-based approaches; for example, the work of M. T. Leung et al., which uses a multilayer perceptron for minutiae extraction by analyzing the output of a bank of Gabor filters applied to the gray-scale fingerprint images. Also, another neural network approach is presented by W. F. Leung et al., where a three-layer perceptron is trained to extract the minutiae from the thinned binary images. Some neural network-based techniques can provide good results when applied to very high-quality fingerprint images, but most are not robust enough to handle noisy images.

In the process of Fingerprint classification, we can use the concept of neural network. Several neural network approaches have been proposed in the literature: Most are based on multilayer perceptrons and use the elements of the directional image as input features. Kamijo presents an interesting pyramidal architecture constituted by several multilayer perceptrons, each of which is trained to recognize fingerprints belonging to different classes.

Jain et al. adopt a two-stage classification strategy: AK-nearest-neighbor classifier is used to find the two most likely classes from a FingerCode feature vector; then a specific neural network, trained to distinguish between the two classes, is exploited to obtain the final decision. A total of 10 neural networks is trained to distinguish between each possible pair of classes.

It is possible to use backpropagation neural network approach for fusion. Here the class probabilities for all the classifiers are combined in a neural network, trained to output the true class on the training set.

The use of fuzzy neural network (FNN) as a recognition system to detect the minutiae pattern has been proposed by A. Wahab and his teammates.

With the aim of overcoming some of the problems related to fingerprint image binarization and thinning (e.g., the presence of spurious minutiae in the case of irregular ridge edges), some authors have proposed direct gray-scale extraction methods.

Djamel Bouchaffra & Abbes Amira Suggested fusions with support vector machine (SVM) for face and fingerprint recognition at fusion level. Kevin Octavius Sentosa et. al.

proposed sum rule based and SVM based fusion for fingerprint, face and fingervein modalities for performance evaluation of score level fusion. Anil K. Jain, Karthik Nandakumar, Xiao guang Lu and Unsang Park suggested to use soft biometric traits in addition to primary traits of face and fingerprint. Fawaz alsaade proposed a fusion of face and voice biometrics at match score level and adopted neural network concept.

Wang et al., 2003 consider the match scores resulting from face and iris recognition modules as a two dimensional feature vector and use Fisher's discriminant analysis and a neural network classifier with radial basis function to classify the 2-dimensional match score vector into "genuine" and "impostor" classes.

Luan Fang-jun, LI Kai and Ma Si-liang suggested multimodal biometric system with combination of signature, voice and face recognition[9]. They adapted neural network back propagation approach for fusion and performance was improved.

Henry Pak-Sum Hui, Helen M. Meng and Man-Wai Mak defined a multibiometrics verification that was fully adaptive to variability in data acquisition using fuzzy logic decision fusion. The system used fuzzy logic to dynamically alter the weight of three biometrics (Face, Fingerprint and Speech). They achieved improvement of 42.1% in overall EER relative to weighted average fusion.

Actually the neural network approach has been adopted at the feature extraction step mostly. No. of projects were implemented with neural network approach at fusion level. Input to the multilayer feed forward neural network can be implemented by applying the scores and ranks generated by the output of different traits. There is an option to implement match score and rank level fusion with fingerprint and face recognition and comparing results and still there could be an option to suggest a hybrid fusion method with these two biometric traits in multimodal biometric systems.

1.7.2 Review of related literature

From the literature review, the researcher has found that there is a scope to do some research work in the area of multimodal biometric system using fingerprint and face recognition. The work has been carried out with these modalities, but without neural network back propagation approach. The work was carried out with fuzzy logic. With the help of neural network back propagation approach, we can improve the quality in some challenging environments by adjusting the weights as per the need of accuracy. Also some of previous systems were developed with COTS approach, which is costlier one. This system will try to reduce the cost, so small organizations can afford such systems.

1.7.3 Salient features of the present study

1. The present work will help to improve the performance of the biometrics authentication mechanism.
2. The cost will be less with compare to commercial products available in the market.
3. The present work will help to improve the authentication even in the absence of one trait, as two biometric traits are used in this system.
4. The present work accommodates neural network approach to adjust the weights and thus reducing the error rate of the system.
5. The present system will be effective in any kind of environment.

1.8 Glossary of the terms

FMR	False Match Rate
FNMR	False Non Match Rate
FTE	Failure To enroll
FTA	Failure to Acquire
EER	Equal Error Rate
AFIS	Automated Fingerprint Identification Systems
API	Application Programming Interface
B2B	Business-to-Business
B2C	Business-to-Consumer
FRR	False Reject Rate
FAR	False Accept Rate
NIST	National Institute of Standards and Technology
COTS	Commercial Off The Shelf
FFN	Feed Forward Network

1.9 Summary of the remaining chapters

Here are the details about the remaining chapters:

Chapter 2:

Understanding the concepts of fingerprint recognition system, referring the history and working of fingerprint recognition, classification of fingerprint, feature extraction in fingerprints, fingerprint matching and applications of fingerprint recognition.

Understanding the concepts of face recognition and referring the history of face recognition. Getting the concepts of working of face recognition, elaborating face recognition algorithms, explaining the applications of face recognition.

Chapter 3:

Various unimodal biometric systems other than face and fingerprint recognition, limitations of unimodal biometric systems, creation of database for fingerprint and face recognition system, preparing model for master database creation, building unimodal face recognition system, performance evaluation of face recognition system, building unimodal fingerprint recognition system, performance evaluation of fingerprint recognition system

Chapter 4:

Introduction to multibiometric techniques, types, advantages, different fusion techniques, score normalization, building multimodal biometric system using face and fingerprint recognition, performance evaluation

Chapter 5:

Introduction to neural network, types of NN structures, NN backpropagation, applications of NN in biometrics and multibiometrics, building multimodal biometric system using face and fingerprint recognition using neural network approach with weight adjustment, performance evaluation

Chapter 6:

Comparing performances of unimodal biometric face and fingerprint recognition systems, multimodal biometric system using face and fingerprint recognition and multimodal biometric system using face and fingerprint recognition using neural network approach with weight adjustment. Deriving conclusion

References

[1]”Dermatoglyphics”, Hand Analysis, International Institute of Hand Analysis, 24 January, 2005.

[2] “Biometrics History”, National Science and Technology council, 7 August, 2006

[3] Maltoni, Maio, Jain, and Prabhakar, “Handbook of Fingerprint Recognition”, Springer-Verlag ,2003

[4] A. K. Jain and S. Z. Li, “Handbook of Face Recognition”, Eds. New-York: Springer-Verlag, 2005.

[5] Zhang, D., Nandkumar K., and Jain, A., “Handbook of MultiBiometrics”, Springer, 2006

[6] Anil K. Jain, Ruud Bolle , Sharath Pankanti, “Biometrics, Personal Identification in Networked Society: Personal Identification in Networked Society”, Kluwer Academic Publishers, Norwell, MA, 1998

[7] Zhang D. et. al, “Advanced pattern recognition technologies with applications to Biometrics”. Medical Information science Reference, 2009

[8] Ratha N, Bolle, R,”Automatic Fingerprint Recognition Systems”.Springer,2004

[9] Luan Fang-jun, Li Kai, Ma Si-Hang, ”Multimodal Identity Verification Based on Improved BP Neural Network”, 2nd International Congress on Image and signal Processing,2009

[10] Ratha N., Govindraju, V.,”Advances in Biometrics-Sensors, Algorithms and Systems ”, Springer, 2008

[11] Hong, L., Jain, A.K., “Integrating faces and fingerprints for personal identification.” IEEE Trans. PAMI 20 (12), 1295–1307, 1998

[12] Hong, L., Jain, A.K., Pankanti, S., “Can multibiometrics improve performance?” In: Proc. AutoID_99, Summit, NJ, USA. pp. 59–64, 1999

[13] Arun Ross, Anil Jain, “Information fusion in biometrics”, Pattern recognition letters, pp. 2115-2125, 2003

[14] Brunelli, R. and Falavigna, D., “Person Identification Using Multiple Cues.” IEEE Transactions on Pattern Analysis and Machine Intelligence, 17(10):955-966, 1995

[15] Henry Pak-Sum Hui, Helen M. Meng, Man-Wai Mak, “Adaptive Weight Estimation in Multi-Biometric Verification using Fuzzy Logic Decision Fusion”, ICASSP, 2007