International Journal of Management, IT & Engineering
Vol. 7 Issue 5, May 2017,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CROSS SENSOR MULTIBIOMETRIC AUTHENTICATION SYSTEM

DharaHeble*

RupaliNikhare**

Abstract

Precise identification of claimed identity is very important to the operation of our increasingly electronically interconnected information society. As a rapidly evolving technology Biometrics has been widely used in forensics, such as identifying criminals and prison security, and has the good potential to be adopted in a very broad range of civilian applications. The proposed system is trained using neural network (NN) algorithm and support vector machine (SVM) to achieve sensor adaptability. The result of training gives the adaptive parameters which will be stored into database. These stored adaptive parameters will be used at the time of matching for verification. The output of the system will be whether to accept the claimed identity or to reject

.

Keywords:

Iris;
Fingerprint;
Multimodal;
Machine Learning;
Cross Sensor

Author correspondence:

DharaHeble,
Student, Information Technology (AI & Robotics), Master of Engineering
Pillai College of Engineering, Mumbai University
Email: dharaakolkar@gmail.com

* Student, Information Technology, Master of Engineering, Pillai College of Engineering, New Panvel, India

** Asst. Professor, Computer Engineering, Pillai College of Engineering, New Panvel, India

I. Introduction

Single biometric systems have limitations like uniqueness, high spoofing rate, high error rate, non-universality and noise, and have increased the necessity of the more strong and powerful authentication system. So, using multiple biometrics is recommended. Due to increasing popularity of biometrics authentication, new sensors are being developed for acquiring input from persons, so it is beneficial if sensors are interoperable. Instead of using pure image processing, if we apply some machine learning techniques to select the learning adaption parameters will reduce the complexity and duration to complete the recognition process.

The iris is a protected but an externally visible organ whose epigenetic patterns are stable throught the life. These characteristics make iris very attractive for use as a biometric for identifying individuals. The human iris is rich in features which can be used to distinguish between two eyes. These features and patterns can be used to Measure their spatial relationships to each other provides other quantifiable parameters useful to the identification process.

Fingerprint identification is one of the well-known biometrics, because of their uniqueness and consistency over time. Fingerprints have been used for identifying people for over a century. Due to advancements in computing capabilities these days identification using fingerprints becoming automated. A fingerprint is a unique pattern of ridges and valleys on the finger surface of an individual. A ridge is a single curved segment, and a valley is the area between two neighbouring ridges. The local ridge discontinuities are known as minutiae points.

1.1 Literature Survey

The paper[1] presents iris and fingerprint fusion system. Iris and fingerprint images are preprocessed to extract the ROIs (Regions of Interest). Then normalized data is given to the Gabor filters. The database contains five iris images and five fingerprint images of each person. The matching score is calculated through the Euclidean Distance calculation.

In paper[2], for fingerprint minutiae based matching, for face the eigenface approach is used.

Anatomical variations found amongst different people and the differences in their learned speaking habits manifest themselves as differences in the acoustic properties of the speech signal. Decision level fusion is used in this system.

Mohamad Abdolahi, Majid Mohamadi& Mehdi Jafari[3], presented a novel fusion strategy for personal identification using fingerprint and iris at the decision level fusion scheme. Hamming distance and fuzzy logic are used for decision.

2. Architecture of Cross Sensor Multibiometric Authentication System

The basic idea of this approach is to provide sensor adaptability and to provide high security using multi biometric concept i.e. Iris and Fingerprint.

Here, we focus on the sensor adaptability as it is not necessary that the sensor used at the time of enrolment is still being used by the system.

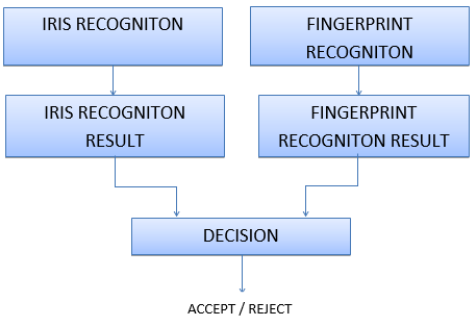

Figure 1. High Level Diagram of Proposed Approach

The System mainly contains 3 modules: Iris Recognition, Fingerprint Recognition and Decision Module

2.1. Iris Recognition

Iris Recognition module is responsible for the enrolment of users' iris, learning and sensor adaption and verification process of the user iris.

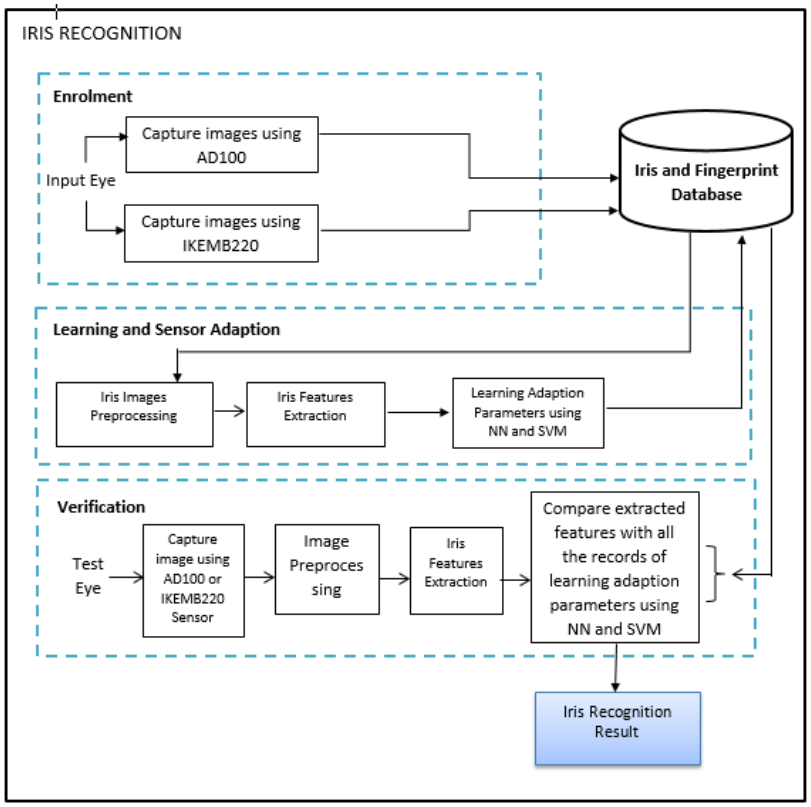

Figure 2. Iris RecognitionModule

2.2. Fingerprint Recognition

Fingerprint Recognition module is responsible for the enrolment of the users' fingerprint, learning and sensor adaption and verification process of the user fingerprint.

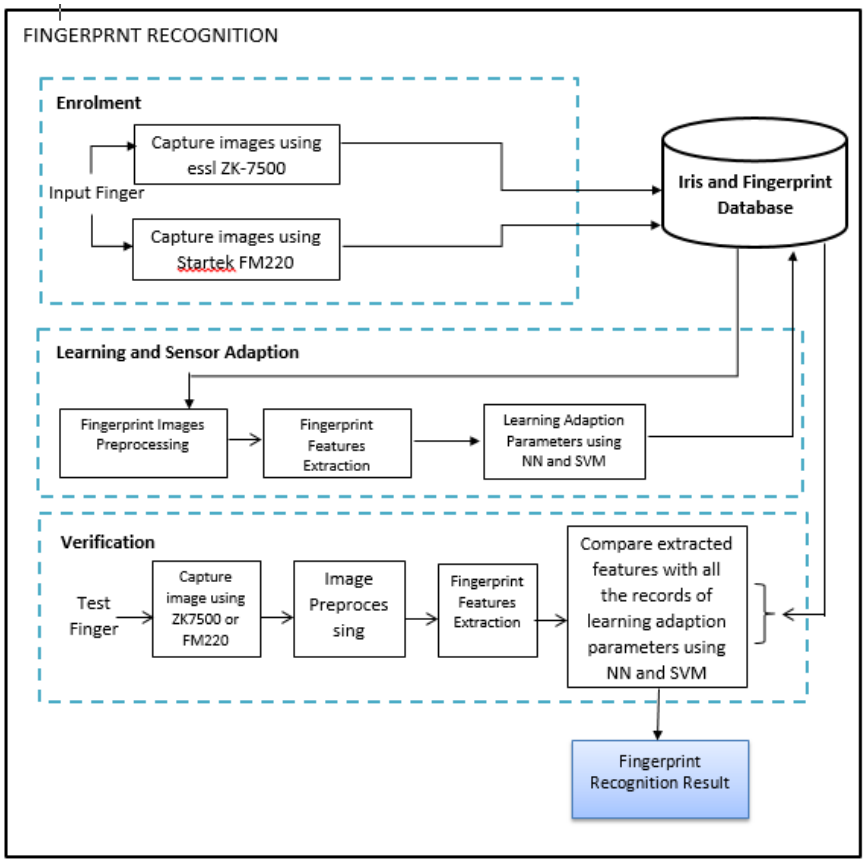

Figure 3. Fingerprint Recognition Module

2.3 Decision

Using the results of Fingerprint module and Iris module, decision about accepting or rejecting identity claimed is taken.

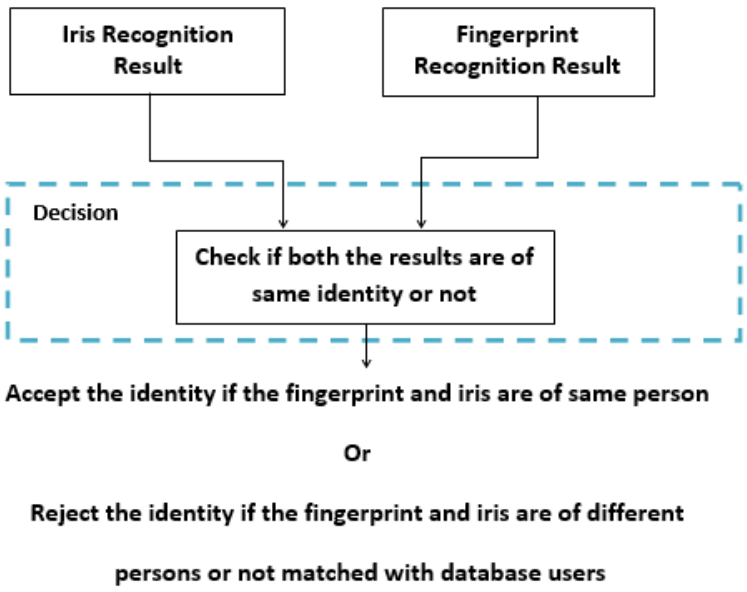

Figure 4. Decision Module

2.4 Algorithm

Input: Iris and Fingerprint images captured with respective sensors
Output: Accept/Reject the Identity Claim
Enrolment

1. Capture the Iris and Fingerprint image using respective Sensors
    a. Capture two Iris images using IG AD100 and IKEMB220 each.
    b. Capture three Fingerprint images using essl ZK7500 and Startek FM220
2. Store the Iris and Fingerprint Images into Database

Learning and Sensor Adaption

3. Training Iris Database
    a. Iris Images Preprocessing
        i. Localization
        ii. Segmentation
        iii. Normalization
    b. Extract Iris Features.
    c. Apply Neural Network algorithm and SVM algorithm on extracted features and save the adaption parameters in database.
4. Training Fingerprint Database
    a. Fingerprint Image Preprocessing
        i. Binarization
        ii. Thinning
    b. Extract minutiae from images using windowing technique
    c. Apply Neural Network algorithm and SVM algorithm on extracted minutiae and save the adaption parametersin database.

Verification

5. Capture the Iris and Fingerprint image using respective Sensors
6. Image Preprocessing
    a. Apply step 3a and 3b on the captured iris image.
    b. Apply step 4a and 4b on the captured fingerprint image.
7. Compare Extracted Features
    a. Compare extracted iris features using selected method with the adaption parameters saved in database, found using Neural Network and SVM.
    b. Find image of minimum hamming distance (hd)

Match Found	}	if hd< threshold
No Match		if hd> threshold

    c. Compare extracted minutiae using selected method with the adaption parameters saved in database, found using Neural Network
    d. Find the image of minimum Euclidian Distance (ed)

Match Found	}	if ed< threshold
No Match		if ed> threshold

8. Find the result for Iris matching and Fingerprint Matching
9. Decision
    a. Check whether the identity of the person is same for Iris and Fingerprint
    b. Accept the identity if the result of Iris recognition and Fingerprint recognition is of same and claimed identity, otherwise reject the identity.

3. Result and Analysis

This system is developed in Matlab 2013b. For the Fingerprint enrolment we have used two different sensors, i.e. essl zk-7500 and Startek FM220. We have taken fingerprint data of 100 volunteer users. For the Iris enrolment we have used the CSIR train database, which is used for "The ICB Competition on Cross-sensor Iris Recognition"[12]. From this database we have taken images of 100 different eyes.

Figure shows the images found during Iris features extraction.

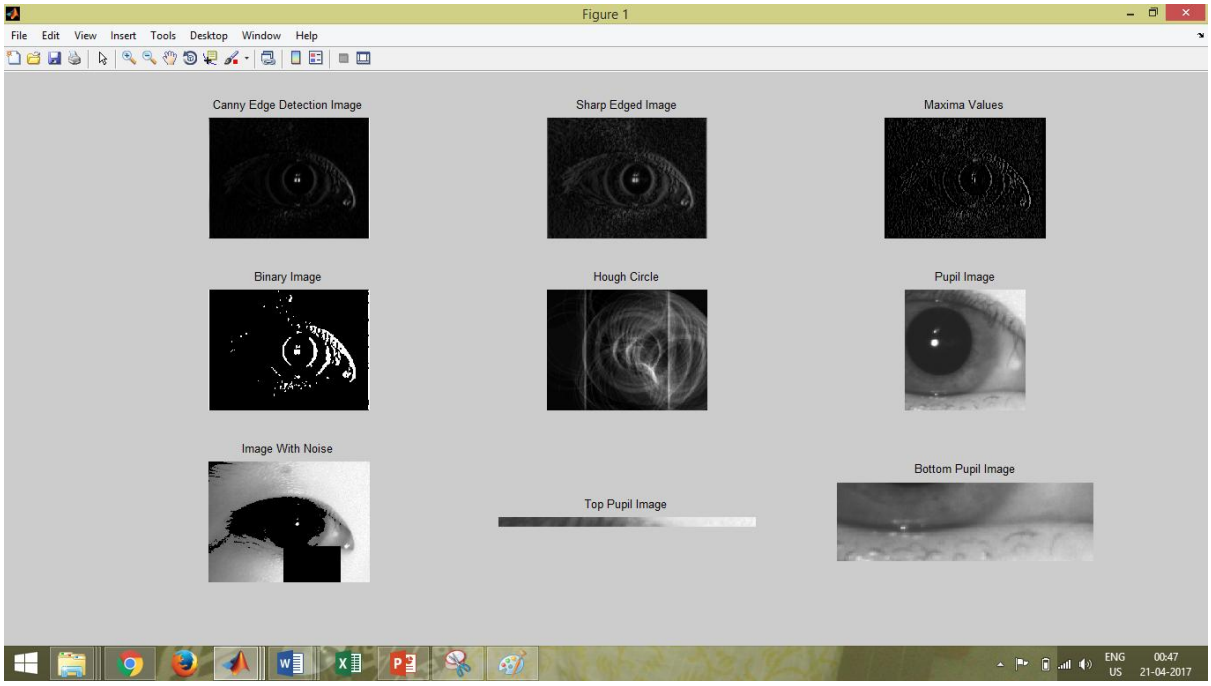

Figure 5: Iris pre-processing images

The below Figure shows the fingerprint pre-processing and minutiae extraction images.

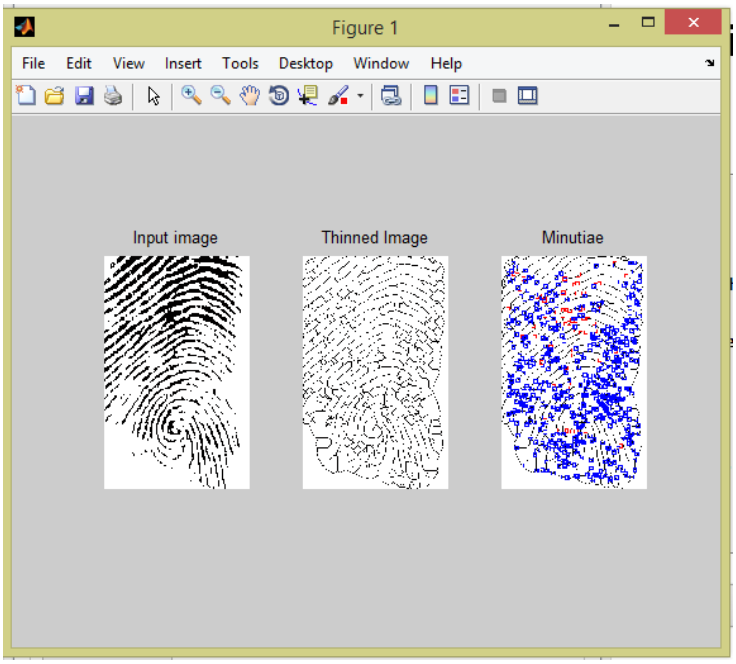

Figure 6: Fingerprint pre-processing and extracted Minutiae

The Figure shows the system input and result.

Verification Process is as follows:

Fingerprint

(a) Select the input Finger
(b) Select the Sensor from which the input is taken
(c) Select the verification method, i.e. Neural Network or SVM
(d) Click Finger Testing
(e) The result will be displayed.

Iris

(a) Select the input Iris
(b) Select the sensor from which the input is taken
(c) Select the verification method, i.e. Neural Network or SVM
(d) The result will be displayed

Decision

(a) Click on the Result button, it will display whether the User is Authorised user or not.

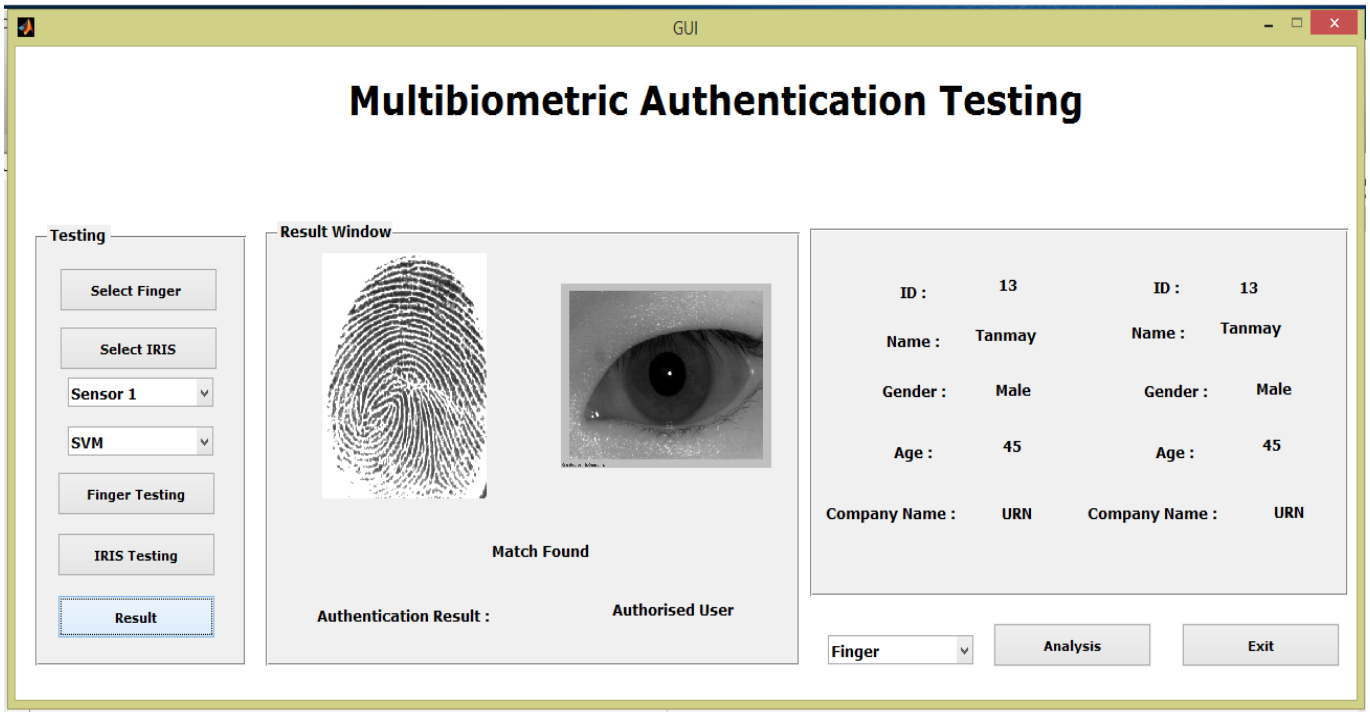

Figure 7: System Verification Module and Result

3.1 Analysis

System is tested on various positive (registered user) and negative (non-user) samples. Below are the findings of Precision, Accuracy, Recall and other measuring factors.

Terminology and Definitions Used in Analysis

TPR= True Positive Rate= TP/(TP+FN)

TNR= True Negative Rate = TN/ (TN+FP)

FPR= False Positive Rate = FP/(FP+TN)

FNR= False Negative Rate = FN/ (TP+FN)

Pr. = Precision = TP / (TP+FP)

Acc. = Accuracy = (TP+TN) / (TP+FP+FN+TN)

Table 1 Fingerprint Analysis

Fingerprint Sensor	SVM						NN					
	TPR	TNR	Pr.	FPR	FNR	Acc.	TPR	TNR	Pr.	FPR	FNR	Acc.
Zk7500	0.8	0.9	0.888	0.1	0.2	0.85	0.8	0.9	0.888	0.1	0.2	0.85
FM220	0.6	0.6	0.6	0.4	0.4	0.6	0.9	0.6	0.692	0.4	0.1	0.75

Table 2 Iris Analysis

Iris Sensor	SVM						NN					
	TPR	TNR	Pr.	FPR	FNR	Acc.	TPR	TNR	Pr.	FPR	FNR	Acc.
AD100	0.9	0.9	0.9	0.1	0.1	0.9	0.9	0.9	0.9	0.1	0.1	0.9
IKEMB220	0.9	1	1	0	0.1	0.95	0.9	1	1	0	0.1	0.95

Performance analysis graphs for Iris and Fingerprint are as follows:

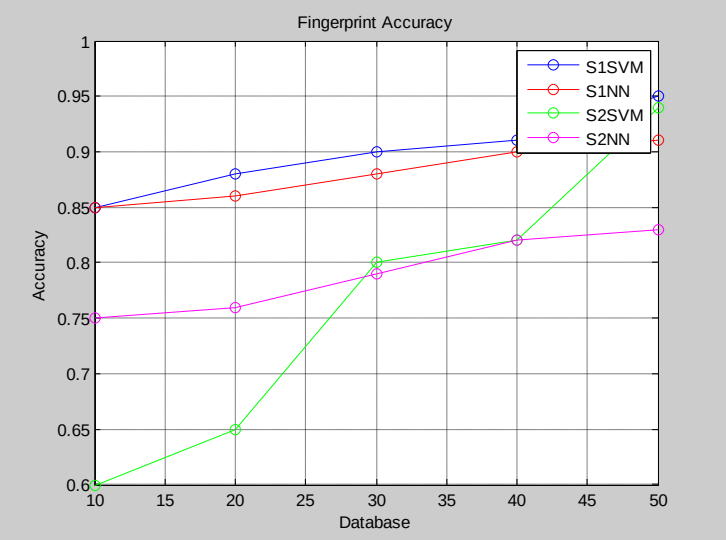

Figure. 8 Fingerprint Accuracy

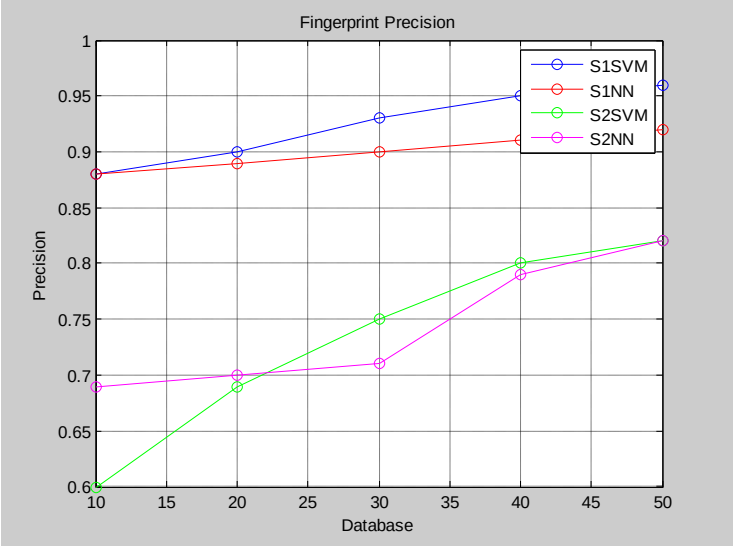

Figure 9 Fingerprint Precision

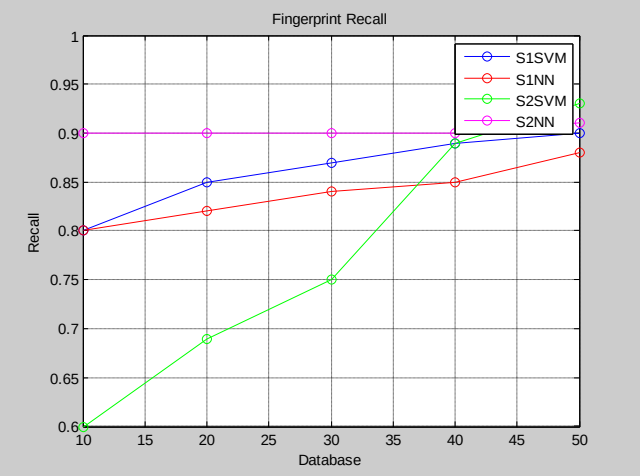

Figure 10. Fingerprint Recall

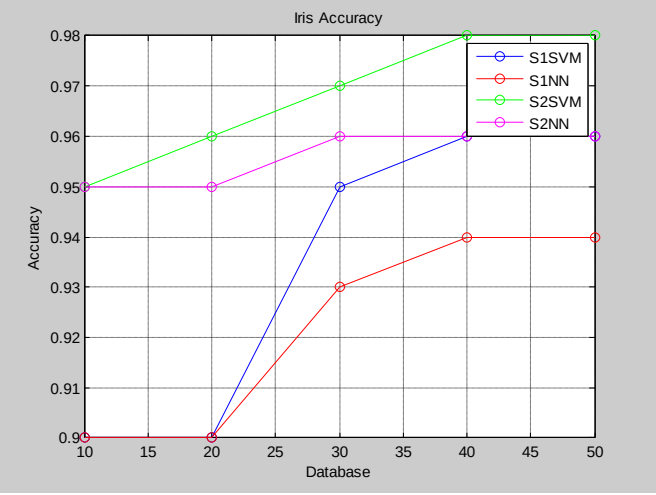

Figure 11. Iris Accuracy

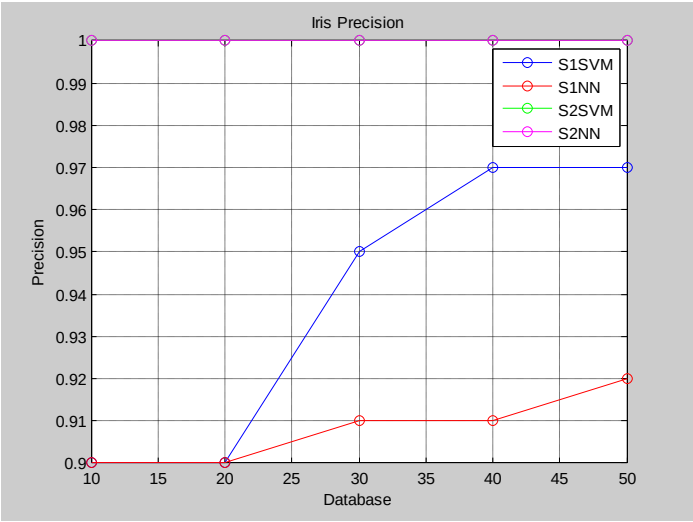

Figure 12Iris Precision

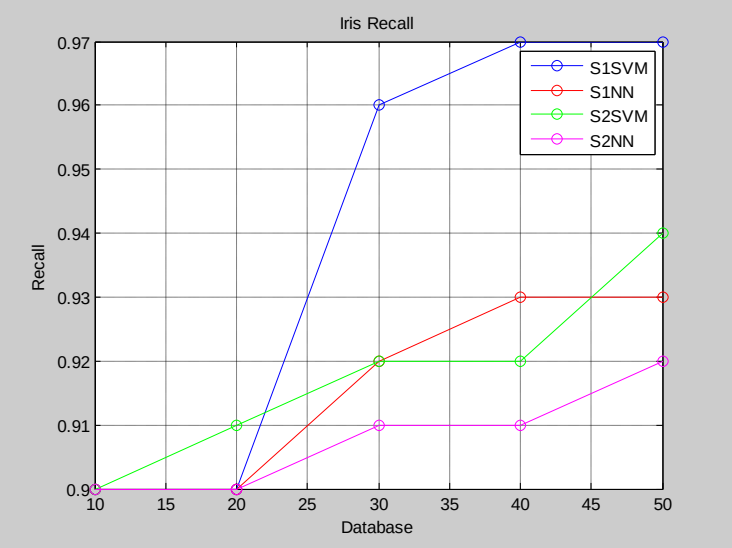

Figure 13.Iris Recall

4. Conclusion & Future Work

The Cross Sensor Multi Biometric Authentication Using Machine Learning is developed. The main focus revolves around the system adaption for cross sensor and using multi biometric to provide increased security. We presented the complete architecture for the development of cross sensor multi biometric system and several algorithms for this system.

Neural training algorithm and SVM are used to train the iris and fingerprint database for cross sensor adaption. Which reduces the efforts of features comparison while verification or identification. The goal of developing such an authentication system is to provide increased security where required, with sensor adaptability.

Neural Network and SVM both are good classifiers. For this system, SVM gives the better results than Neural Network.

For more efficient system we can take more samples of iris and fingerprint images of single user at the time of enrolment, which can result in more efficient learning and adaption parameters.

5. References

[1] Geethu S Kumar &C Jyothirmati Devi "A Multimodal SVM Approach for Fused Biometric Recognition" *(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3, 2014, 3327-3330)*

[2] Gajendra Singh Chandel&Ankesh Bhargava "Identification of People by Iris Recognition" *International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-4, March 2013*

[3] P.U.Lahane&Prof.S.R.Ganorkar "Fusion of Iris & Fingerprint Biometric for Security Purpose" *International Journal of Scientific & Engineering Research Volume 3, Issue 8, August-2012 1 ISSN 2229-5518*

[4] Mohamad Abdolahi, Majid Mohamadi& Mehdi Jafari "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic" *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013*

[5] Anil Jain, Lin Hong and Yatin Kulkarni "A multimodal biometric system using Fingerprint, Face and Speech"

[6] S. Sangeetha & N. Radha (2012) "A new Framework for Iris and Fingerprint Recognition Using SVM Classification and Extreme Learning Machine Based on Score Level Fusion" *Intelligent Systems and Control (ISCO), 2013 7th International Conference*

[7] Jaishanker K. Pillai, Maria Puertas and Rama Chellappa (2014) "Cross-Sensor Iris Recognition through Kernel Learning" *IEEE Transactions on Pattern Analysis And Machine Intelligence, Vol. 36, NO. 1, January 2014*

[8] Ryan Connaughton, Amanda Sgroi, Kevin Bowyer, and Patrick Flynn "A Multi-Algorithm Analysis of Three Iris Biometric Sensors" *IEEE Transactions on Information Forensics And Security 2012*

[9] Sunpreet S. Arora, MayankVatsa, Richa Singh and Anil Jain (2012) "On Iris Camera Interoperability" *978-1-4673-1228-8/12/2012 IEEE*

[10] Samir Nanavati, Michael Thieme, Raj Nanavati *"Biometrics Identity Verification in a Networked World"* Wiley Computer Publishing, 2002

[11] S.N. Sivanandam and S.N. Deepa *"Principles of Soft Computing"* Wiley India Publication

[12] http://biometrics.idealtest.org/2015/csir2015.jsp