Satwinder Singh, International Journal of Advanced Trends in Computer Applications (IJATCA)
Volume 2, Number 6, November - 2015, pp. 14-19
ISSN: 2395-3519

International Journal of Advanced Trends in Computer Applications
www.ijatca.com

IRIS BIOMETRIC AUTHENTICATION USING SIFT AND SVM

[1]**Satwinder Singh**
M.Tech (Scholar), CSE
RIET, Phagwara, India
satwinder_mehmi@yahoo.co.in
[2]**Er. Varinderjit Kaur**
AP, M.tech (CSE),
RIET, Phagwara, India
vari_rupi@yahoo.co.in

Abstract: *In the modern world, establishing the identity of a person is a critical task in any identity management system. Surrogate representations of identity such as passwords and ID cards are not sufficient for reliable identity determination because they can be easily misplaced, shared, or stolen. From past few years identification through biometric has been confirmed much more consistent in some specific manner for verifying the human identity. An upright biometrics is one that utilizes single feature which is extremely unique. So, in our work we have utilized Iris as it is one of the unique feature of an individual. In this work, a system is developed that can recognize human iris patterns and an analysis of the results is done. An innovative methodology has been utilized for execution of the framework. Some specific performance metric are evaluated like False Acceptance Rate, False Rejection Rate and Accuracy. The over-all work model took place in the MATLAB 7.10 environment.*

Index Terms: *Biometric, IRIS, SIFT, SVM, FAR, FRR, ACCURACY.*

1. INTRODUCTION

Biometric authentication systems verify a person's claimed identity from behavioral traits (signature, voice) or physiological traits (face, iris, and ear) [1, 13]. Biometric system can be constructed using more than one physiological or behavioral characteristic for identification and verification purposes [2]. These types of systems are developed for security purposes in various fields like crime investigation, e-commerce and military purposes [3]. Biometric system developed using fingerprint, hand geometry, they required the concerned human to make physical contact with a sensing device [13].
Most of the existing biometric systems developed were based on biometric features like (fingerprint, ear, face, iris and so on). Each biometric trait has its own strength and weakness [4, 5]. Some of the problem with fingerprint recognition system is fingerprint images have been observed to have poor ridge details [6]. Similarly, face recognition system fails due to variation in facial expression. Hence while developing biometric systems the choice of biometric traits is important in order to achieve better performance. Biometric systems available are face and ear [7, 8] face and fingerprint, palm print and face, etc. In this proposed work, iris will be chosen as biometric authentication.
Any physiological or behavioural feature may be used as a biometric verifier as long as it satisfies the following requirements:

Universality – every person must own this characteristic.

Distinctiveness – two persons possessing the same characteristic do not exist.

Permanence – the characteristic must be invariant for a time period as long as possible.

Collectability – indicates the fact that biometric may be quantitatively measured.

Performance – which refers to the accuracy of the tangible recognition, speed, robustness, as well as the prerequisites for touching a certain level of performance.

Acceptability – indicates the degree in which the given biometric characteristic is accepted by the users.

A normal biometric framework comprises of four principle segments, specifically, sensor, extractor, matcher and choice modules [9]. A sensor is utilized to secure the biometric information from a person. A quality estimation calculation is once in a while used to learn whether the obtained biometric information is adequate to be prepared by the resulting parts. At the point when the information is not of adequately top notch, it is generally re-procured from the client [10]. The element extractor gathers just the remarkable data from the procured biometric example to frame another representation of the biometric characteristic, called the list of capabilities. In a perfect world, the list of capabilities ought to be one of a kind for every individual (amazingly little between client similitude) furthermore invariant regarding changes in the distinctive examples of the same biometric quality gathered from the same individual (greatly little intra-client variability) [11]. The list of capabilities got amid enlistment is put away in the framework database as a layout. Amid confirmation, the list of capabilities removed from the biometric specimen (known as inquiry or info or test) is contrasted with the layout by the matcher, which decides the level of likeness (divergence) between the two capabilities [12, 14]. The choice module settles on the character of the client in light of the level of similitude between the format and the inquiry.

1.1 Components of Bio-Metric System

A biometric structure is constructed by means of the subsequent four foremost components:

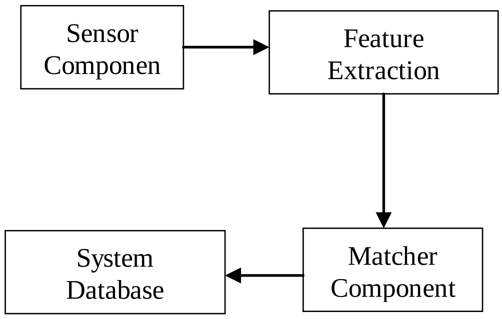

Figure 1: Biometric System Components.

1. *Sensor component* that invade the biometric records of a single person.
2. *Feature extraction component,* in this the attained biometric information is handled to take out a set of significant or prejudiced features.
3. *Matcher component,* in which the characteristics for the duration of acknowledgement are matched counter to the already deposited templates so that it can produce alike scores.
4. *System database component* that is used by the biometric structure to pile the biometric templates of the registered users. The registration module is in charge for registering peoples into the biometric structure database. For the duration of the enrolment stage, the biometric features of a solitary person is initially skimmed using a biometric reader to produce a digital demonstration (feature values) of the characteristic. The information seizure for the duration of the admission process may or may not be administered by a human being be contingent on the application. A quality check is in general accomplished to make sure that the attained example can be consistently administered by successive phases. In order to aid matching, the input digital illustration is further handled by a feature extractor to produce a compressed but communicative demonstration, called a template. Reliant on the application, the template may possibly be deposited in the principal database of the biometric structure or be documented on a smart card allotted to the individual.

2. METHODOLOGY

Iris recognition is done In MATLAB 7.10 environment using HCT, SIFT and SVM method. The following process will describe the iris recognition process.

2.1 Training Panel

Step 1 : *Upload Image.*

The images from UCI Machine learning algorithms iris image database are taken. It contains 8 images of one eye at two sessions. They are of 200kb .jpeg images.

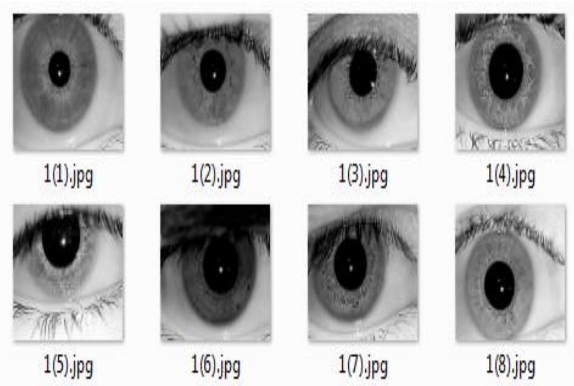

Figure 2: Iris Training Samples

Step 2 : *Edge Detection*

In this phase grey scale conversion has been done and edge detection. Edges characterize boundaries and are therefore a problem of fundamental importance in image processing. Edges in images are areas with strong intensity contrasts – a jump in intensity from one pixel to the next. Edge detecting an image significantly reduces the amount of data and filters out useless information, while preserving the important structural properties in an image. The Canny edge detection algorithm is known to many as the optimal edge detector [14].

Step 3 *:HCT For Localization*

The Hough transform can be applied to detect the presence of a circular shape in a given image. It is being utilized to discover any figure or else to find the iris in the human being's face [15].

Step 4 *:SIFT For Feature Extraction*

1st octave generation
2nd level pyramid generation
3rd level pyramid generation
Obtaining key point from the image
Key points plotting on to the image
Magnitude and orientation assignment to the key points
Forming key point neighborhoods
Finding orientation and magnitude for the key point
Forming key point Descriptors
Forming key point neighborhoods
Dividing into 4x4 blocks
Finding orientation and magnitude for the key point

Step 5 *: SVM for Training.*

```
function [itrfin] = multisvm( T,C,test )
itrind=size(test,1);
itrfin=[];
Cb=C;
Tb=T;
This while loop is the multiclass SVM Trick
        c1=(C==u(itr));
        newClass=c1;
        svmStruct                                    =
svmtrain(T,newClass,'kernel_function','rbf');
       try
        classes = svmclassify(svmStruct,tst);
       catch
        classes=rand;
        itrfin=classes;
        classes=1;
        end
```

2.2 Testing Panel

Step 6 *: Upload testing image*

The images from UCI Machine learning algorithms iris image database are taken for testing. It contains 4 images of one eye at two sessions.

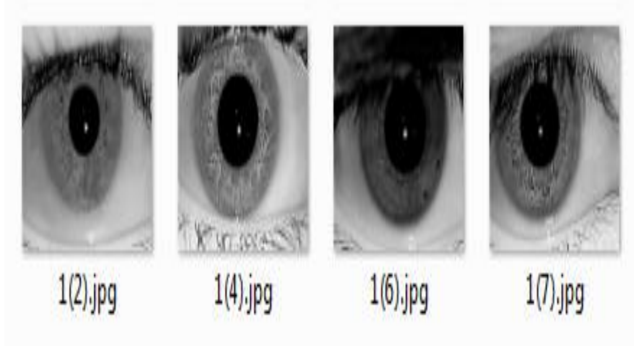

Figure 3: Iris Testing Samples

2.3 SIFT and SVM based Testing

```
load Test_data
load sift_features
[rows,cols]=size(data_new);
for i=1:rows
  Group(i)=i;
end
result=multisvm(data_new,Group,data_mysift(1,1:100)
);
```

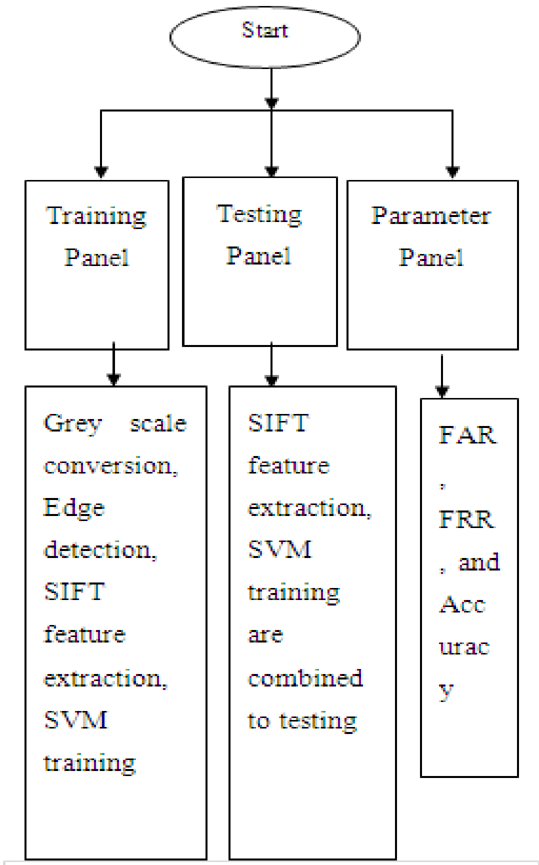

Figure 4: Flowchart of Proposed Work

3. RESULTS

The values in above table are obtained by implementing proposed work on 8 images taken from database randomly.

Table 1: Results value obtained

S. No.	False Rejection Rate	False Acceptance Rate	Accuracy
1.	0.0039206	0.0028389	99.4341
2.	0.0039344	0.0027403	99.4335
3.	0.003926	0.0027413	99.4416
4.	0.003944	0.0027395	99.3399
5.	0.003941	0.0027408	99.5326
6.	0.003841	0.0027393	99.4528
7.	0.003942	0.0027406	99.5286
8.	0.003842	0.0027606	99.4286

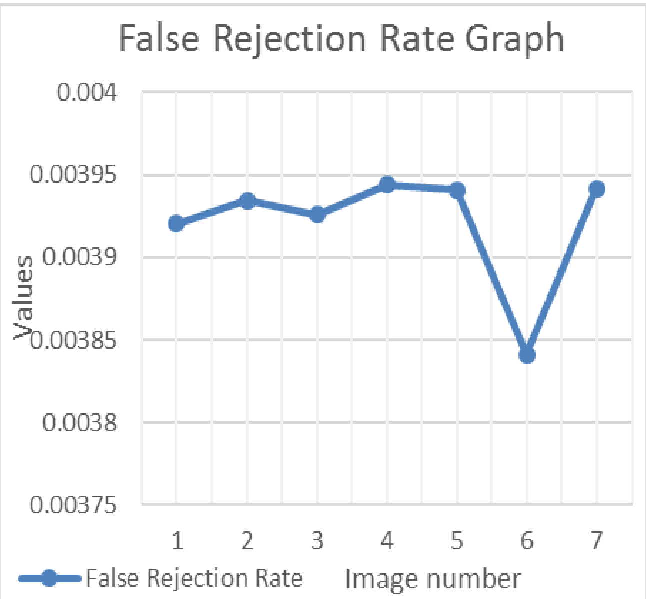

Figure 5: Graph of False Rejection Rate

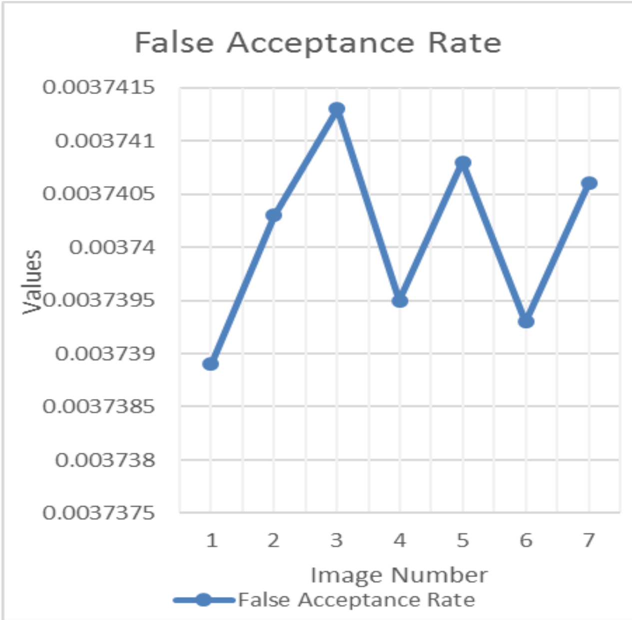

Figure 6: Graph of False Acceptance Rate

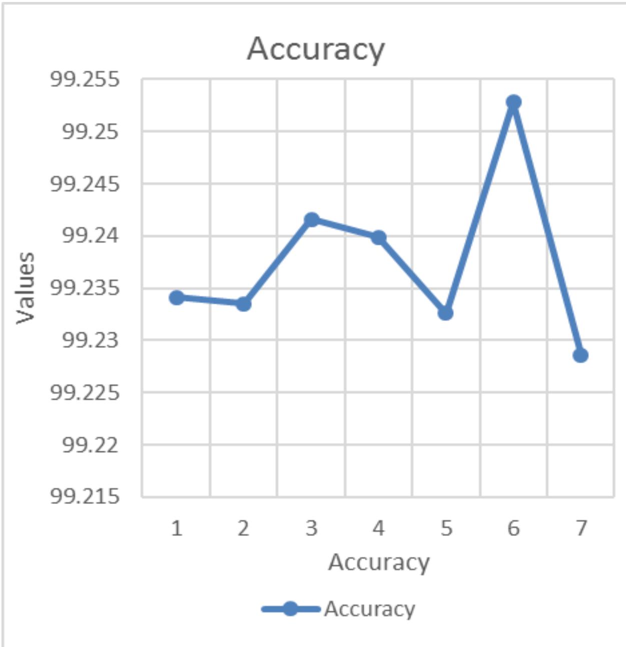

Figure 7: Accuracy parameter graph

In above graphs, we have taken values from above table and plotted graph individually of each parameter.

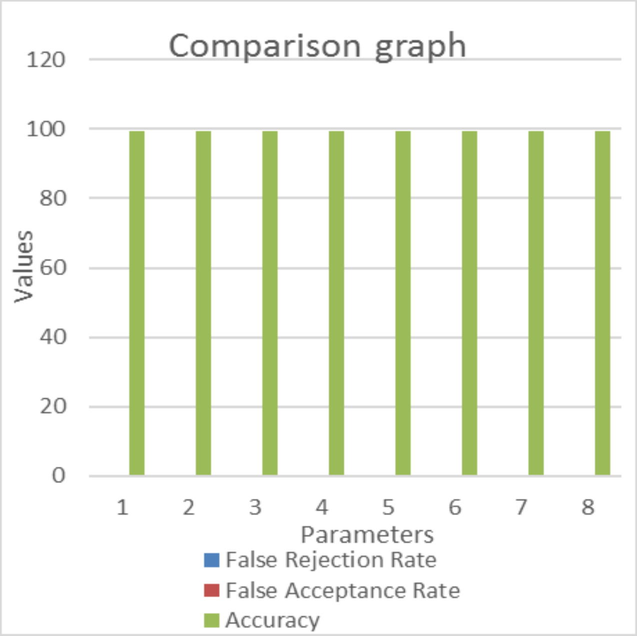

Figure 8: Error Rate, FAR, FRR and Accuracy Graph.

In above graph we have taken an average value of False Acceptance Rate, False Rejection Rate and Accuracy Graph. We also have shown the avg. value for every parameter such as:

False Acceptance Rate is 0.002841.
False Rejection Rate is 0.002641.
Accuracy is 99.4528.

Table 2: Comparison Table

Technique	Accuracy
Proposed	99.45
Euclidean	65
Mahalonobis	99.33

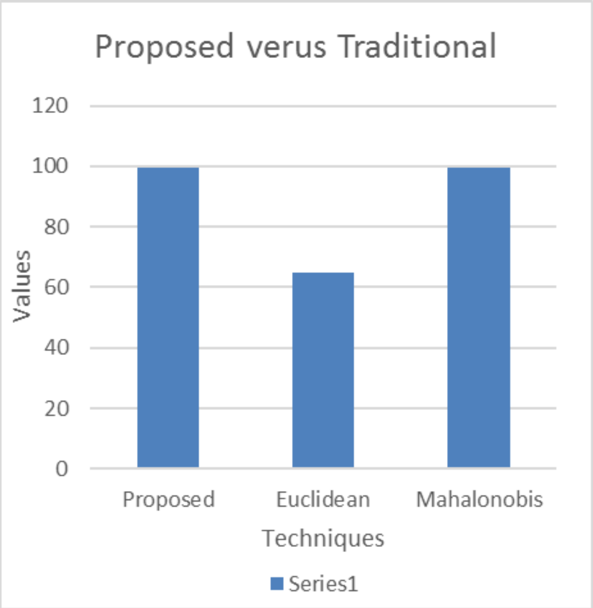

Figure 9: Proposed versus Traditional Approach

4. CONCLUSION

In the proposed system, a new technique is generated for feature extraction and matching of iris templates increase the accuracy of the authentication systems using SIFT and SVM. In this work, SIFT features are extracted for iris and this proposed method decreased the FAR as well as FRR, & has increases the system performance on the given data set having high accuracy. From the result evaluation, achieved average value of False Acceptance Rate is 0.002841, False Rejection Rate is 0.002641 and Accuracy is 99.4528.

Future works could go in the direction of using more robust modelling techniques against forgeries and hybrid fusion level can be used. Multimodal modalities can be used together to make forgeries more difficult. Also, the system should be tested on a larger database to validate the robustness of the model.

REFERENCES

[1] E.Sridevi, B.Aruna, P. Sowjanya, “An Exploration of Vascular Biometrics” IJECT (International Journal of Electronics & Communication Technology)Vol. 2, SP-1, Dec . 2011,ISSN : 2230-7109(Online) | ISSN : 2230-9543(Print) IJECT Vol. 2, SP-1, Dec . 2011 , pp.181-184.

[2] Jiali Cui, Yunhong Wang, JunZhou Huang, Tieniu Tan and Zhenan Sun, “An Iris Image Synthesis Method Based on PCA and Super-resolution”, IEEE CS Proceedings of the 17th International Conference on Pattern Recognition (ICPR’04), 23-26 August 2004, Cambridge, UK, Vol. 4, pp. 471-474.

[3] Elgamal, Mahmoud, and Nasser Al-Biqami. "An efficient feature extraction method for iris recognition based on wavelet transformation." International Journal of Computer and Information Technology 2.03 (2013): 521-527.

[4] Kefeng FAN, Qingqi Pei, Wei MO, Xinhua Zhao, and Qifeng Sun, “An Efficient Automatic Iris Image Acquisition and Preprocessing System”, Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation, June 25-28, 2006, Luoyang, China, pp. 1779-1784.

[5] Shi, Jin-Xin, and Xiao-Feng Gu. "The comparison of iris recognition using principal component analysis, independent component analysis and Gabor wavelets." Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on. Vol. 1. IEEE, 2010.

[6] Raja, Kiran B., R. Raghavendra, and Christoph Busch. "Binarized statistical features for improved iris and periocular recognition in visible spectrum."Biometrics and Forensics (IWBF), 2014 International Workshop on. IEEE, 2014.

[7] Lye Wi Liam, Ali Chekima, Liau Chung Fan and Jamal Ahmad Dargham, “Iris Recognition using Self-Organizing Neural Network”, IEEE 2002 Student

Conference on Research and Development Proceedings, Shah Alam, Malaysia, pp. 169-172.

[8] L.Ma, T. Tan, Y.Wang, and D. Zhang (2003), “Personal identification based on iris texture analysis,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(12), 1519–1533.

[9] B. J. Lei, Emile A. Hendriks, M.J.T. Reinders, “On Feature Extraction from Images”, Technical Report, MCCWS Project, Information and Communication Theory Group, Tudeft

[10] L. Masek (2003), “Recognition of human iris patterns for biometrics identification” , B. Eng. thesis, University of Western Australia, Perth, Australia.

[11] V. Dorairaj and N. Schmid, and G. Fahmy (2005), “Performance Evaluation of Iris Based Recognition System Implementing PCA and ICA Techniques,” in Proc. of the SPIE 2005 Symp. on Defense and Security, Conf. 5779, Orlando,.

[12] Jin-Xin Shi and Xiao-Feng Gu (2010),” The Comparision of Iris Recongnition Using Prinncipal Component Analysis , Independent Component Analysis and Gabor Wavelets”, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), 61-64.

[13] Jain A.K, Ross A. and Prabhakar S.(2004) “An Introduction to Biometric Recognition”, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and VideoBased Biometrics, Vol.14, No.1, pp.4–20.

[14] Kovoor, Binsu C., M. H. Supriya, and K. Poulose Jacob. "Iris Biometric Recognition System Employing Canny Operator." (2013): 65-74.

[15] Supriyanti, Retno, et al. "Detecting Pupil and Iris under Uncontrolled Illumination using Fixed-Hough Circle Transform." International Journal of Signal Processing, Image Processing and Pattern Recognition (IJSIP) 5.4 (2012): 175-188.