Iris Recognition System: A Novel Approach For Biometric Authentication

Rohini Shelke
Dept. of Electronics and Telecommunication
Late G. N. Sapkal College of Engineering
Anjaneri, Nashik

Prof. S. B. Bagal
Dept. of Electronics and Telecommunication
Late G. N. Sapkal College of Engineering
Anjaneri, Nashik

ABSTRACT -Many of the researchers suggest that, Biometrics is the only solution for user identification and security issues. Incorrect use of the password and incorrect, intentional and involuntary application are a great safety void. These results occur mainly due to poor human judgment, negligence and lack of touch. Biometric eliminates all these types of security errors. In recognizing iris, system identification and verification is one of the most efficient methods. The goal of this proposed system is to analyze the performance of the iris. Iris segmentation uses shape, intensity, and position information for the pupil or iris position and normalizes the iris region by unfolding the circular region in a rectangular region. The extraction of the iris characteristics was performed using the GLCM biometry (gray scale matching matrix) and the HD dimension (Hausdorff dimension). The BGM algorithm (biometric graph matching) is used, which is used to match the graph between the training image and the biometric iris test. The BGM algorithm uses a graphic topology to define different functional values of iris models. A SVM (Support Vector Machine) classifier is used to distinguish between the genuine and the impostor. The results provide better performance and authentication than the existing method.

Keyword: SVM(Support Vector Machine), BGM(Biometric Graph Matching),Segmenation,IRIS

I.INTRODUCTION

Today, security measures for systems are increasingly important and useful. Authentication plays an important role in the line of defense, identity card and passport verification. There are three main types of authentication, such as password, card or token, biometric data. Biometrics is used to recognize the physical or behavioral characteristics of the person. There are different types of biometric data used, such as fingerprints, retina, facial recognition, voice pattern analysis, etc. Among all the biometric data, the iris is one of the best biometric data. Security is not good in many banking systems, financial transactions, sales and compliance with the law. Therefore confidentiality must be provided. Iris biometry is for personal identification before all features are verified with different techniques. Biometrics also provides a secure authentication and identification method, as they are difficult to replicate and steal. Behavioral characteristics include key dynamics, signature, voice model and physical characteristics including iris, palm, facial recognition. [1]Biometric system process through the collection and storage of biometric information and the comparison of biometric inputs with what is stored in the repository. Among all the varieties of existing physical characteristics, irises are one of the most perfect and precise physiological characteristics that can be used.

II.PROPOSED SYSTEM

Biometrics refers to the automatic identification of a person based on his unique physiological or behavioral characteristics. Behavioral biometry includes signatures, speech recognition, gait measurement and even key recognition[2]. Physiological biometry includes facial recognition, fingerprints, manual profiling, iris recognition, retinal scan, and DNA testing. Behavioral methods tend to be less reliable because they are easier to duplicate. Biometric methods based on physiological attributes are more reliable. Among these methods, iris recognition is gaining a lot of attention because it is accurate and reliable. To improve accuracy, most biometric authentication systems store different models per user to account for changes in biometric data. Therefore, these systems suffer from storage space and computational overload. To solve these problems, it is necessary to optimize the computational and storage complexities by creating a reliable iris sample model per user instead of maintaining multiple models. This paper presents a new approach to improve the performance of iris recognition systems.

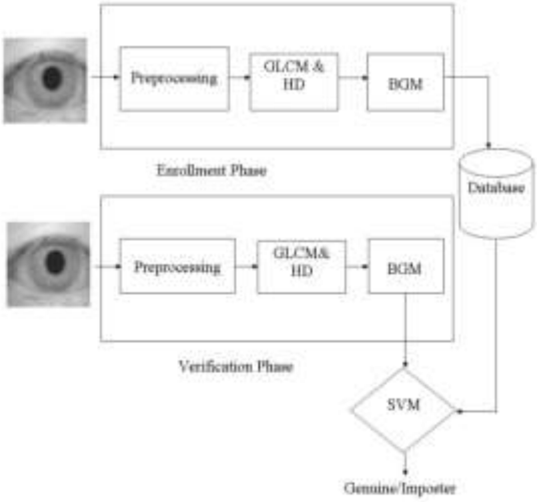

Fig .2.1 Block Diagram Of Proposed System

A]IRIS Segmenation

From the eye picture the iris part is isolated utilizing picture division. The edges of the iris internal and external limits are found and distinguished utilizing Canny edge detector.In watchful edge recognition the thresholding for the eye picture is done in a vertical course just, with the goal that the causes because of the eyelids can be diminished. The Hough transform is utilized for discovering the circles in the iris picture and diminishes a pixel on the limit of the circle. The area of the edge can be gotten even with the nonappearance of couple of pixels. It is likewise speedier since the limit pixels are lesser for calculation. The powerless edges of underneath edge is evacuated by the utilization of hysteresis thresholding. For each edge purpose of various radii circles is shaped. From all circles the greatest entirety is figured and is utilized to discover the circle radii and focus. The Hough transform is one all the more method for identifying the parameters of geometric items.

B]Iris Normaliztion

In standardization the iris area is standardized by changing over round into rectangular areas. Here, addition is utilized for unwrapping round power into polar force. Relocation of understudy focus from the iris base and span on the iris is ascertained.

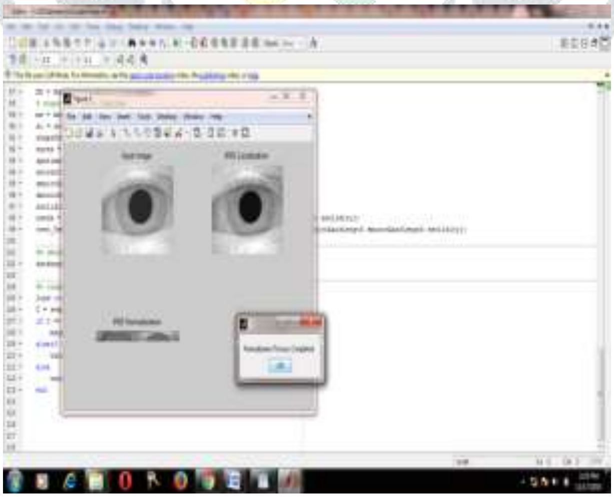

Figure 2.2. Standardized and segmented iris picture

In Fig 2.2 Segmented picture is acquired after the standardization of iris picture. Rings overlaying on unique iris picture are acquired by getting the pixel arranges for hover around iris and understudy. An iris coordinating framework has been displayed in light of the Biometric Graph Matching calculation. The iris picture was segmented. An arrangement of pictures are taken and discovering the highlights esteems. Expecting, the initial five estimations of the databases is validate and the following five qualities are thought to be unauthenticated. Preparing picture is contrasted and the test pictures. A spatial diagram was created from the surface, shading and shape highlight esteems and chart was plotted for the info picture and an arrangement of preparing picture. Contrast the both the chart with see if approved or unapproved individual.

III.Hausdorff Dimension by box counting method Algorithm

A quantitative examination of edge unpleasantness is done to delineate the level of harshness of info pictures. Usually known as the Hausdorff Dimension (H.D.), the calculation appeared in figure 3 gives the total border harshness as a fractal measurement. The fractal measurement portrays the intricacy of a protest; on account of gadgets displayed here, this calculation gives edge harshness which infers parasitic discharge locales for to a great degree unpleasant borders [3]. On Hausdorff Dimension scale, a measurement of 1 compares to a smooth line, while 2 suggests fractal many-sided quality like that of a Julia set, and in light of the fact that the gadgets introduced here are viewed as truncated fractals, the fractal measurement figured is bound by as far as possible, i.e. 1 < H.D. < 2. The calculation to accomplish this begins with an info electron micrograph picture transferred inside Matlab (figure 3), at that point the Canny calculation [4] is utilized to discover the edge inside the picture and superimposes a network of N squares over the edge, while checking the possessed squares that the edge goes through (upper right, N(s)). This is proceeded for an expanding number of squares and the fractal measurement (H.D) is given by the angle of the logarithm of the quantity of squares log N, over the quantity of squares possessed by the edge log N(s), as demonstrated by figure 3 (base) and condition (3):

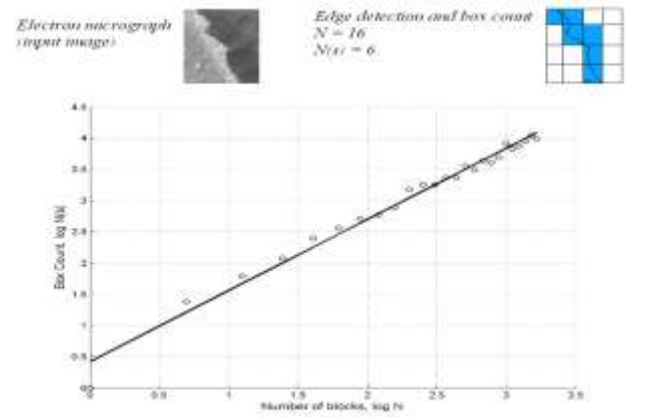

Fig.2.3Algorithm employed to calculate the Hausdorff Dimension.

$$H.D = \frac{\log N}{\log N(s)}$$

IV.Support Vector Machine (SVM)

SVM is connected for arrangement of information individuals. Information individuals or in information focuses there are two things which might be real or faker. The correct technique is to characterize the two information focuses is hyper planes. The edge signifies the greatest width in the hyper planes. The help vector is the informational indexes used to characterize the vectors. To separate among objects of unique class participations are known as hyper planes classifiers. Bolster Vector Machines are particularly to play out this sort of activity. On the off chance that the informational collections are not took into consideration isolating the hyper planes all things considered utilize delicate edge. It implies hyper planes that different huge numbers of the information focuses yet not all information focuses. To build ideal hyper planes, SVM applies an iterative preparing calculation which is utilized to diminish a blame acknowledgment. SVM bolsters grouping, relapse and furthermore it can deal with clear cut variable and numerous ceaseless. For absolute factors various sham factors are made with 0 and 1

V. RESULTS

In this project given information picture is portioned for restriction, standardization and dissected the component vector. Each testing iris is coordinated against each put away database format at each level. A veritable and fraud coordinating is characterized as the coordinating between iris highlights of preparing picture and iris highlights of test picture. Here, the parameters for the iris are ascertained. Furthermore, getting 97.5% proficiency .Total we had utilized 10 people iris picture. What's more, in this 1 to 7 is approved individual and 8 to 10 are nonauthorised individual. For database preparing I had utilized 30 pictures implies 3 pictures from every individual 3x10=30

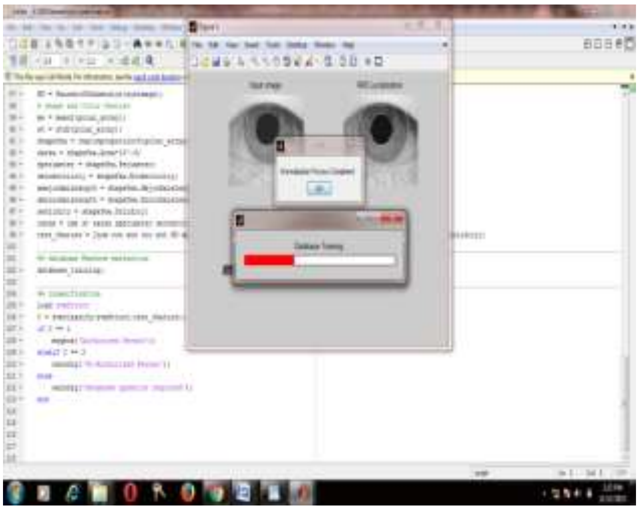

Fig.5.1 Database calculations

After iris segmenation and normalization database is tarined and for that waitbar is done for processing

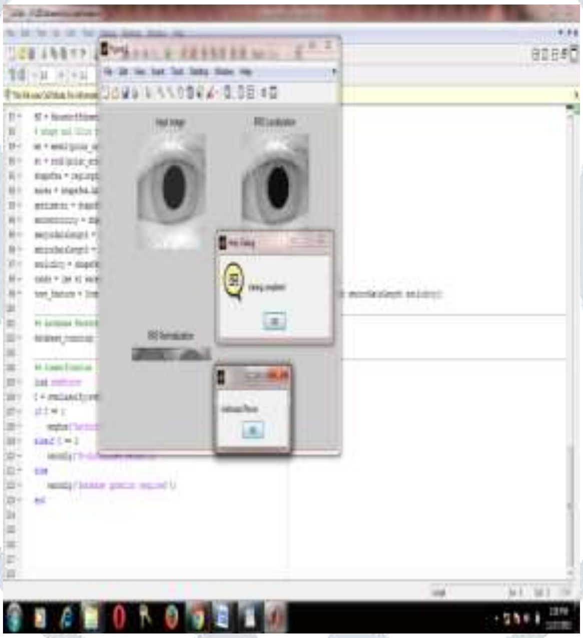

Fig.5.2 Person is authrized

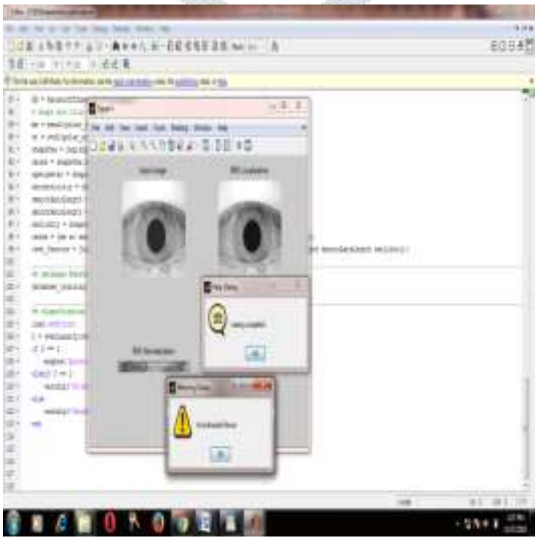

Fig.5.3 Person is not authorized

VI.CONCLUSIONS

In biometrics, iris is one of the easy to use on the grounds that without the individual contact the attributes of a man is effectively discover and furthermore give security and verification in a productive way. The proposed strategy includes the biometrics subtle elements is removed by utilizing two system, for example, GLCM (Gray Scale Co-event Matrix) and Hausdorff Dimension (HD). From GLCM surface highlights like vitality, differentiate, entropy, Correlation Coefficient, homogeneity are extricated. Shape highlights like standard deviation, mean and shape highlights like zone, edge minor pivot length, significant hub length, strength, flightiness are computed from Hausdorff Dimension (HD). What's more, contrasting both the incentive in a graphical portrayal in BGM. At long last, Support Vector Machine (SVM) is utilized to characterize whether the individual is approved or unapproved. In future work this impediment can be tended to by multimodal biometrics framework to consolidate both the biometric qualities got from one or modalities, for example, Palm print and iris which give abnormal state of security and distinctive secure applications.

REFERENCES

[1] Renu Bhatia "Biometrics and Face Recognition Techniques" International Journal Of Advanced Research In Computer Science And Software Engineering EURASIP Journal on Advances in Signal ProcessingVolume 3, Issue 5, May 2013 ISSN: 2277 128X

[2]Nakissa Barzegar ,M. Shahram Moin" Iris Recognition System Based on an Area Preserving Pointwise Level Set Segmentation Approach" EURASIP Journal on Advances in Signal Processing

[3] Yulin Si, Jiangyuan Mei, and HuijunGao, "Novel Approaches to Improve Robustness, Accuracy and Rapidity of Iris Recognition Systems" IEEE transactions on industrial informatics, vol. 8, no. 1, pp.110-117, February 2012.

[4] Seyed Mehdi Lajevardi, Arathi Arakala, Stephen A. Davis, and Kathy J. Horadam, "Retina Verification System Based on Biometric Graph Matching" IEEE Transactions on Image Processing, vol. 22, no. 9, pp.3625- 3635 September 2013.

[5] Hugo Proenca, "Toward Covert Iris Biometric Recognition: Experimental Results From the NICE Contests" IEEE Transactions On Information Forensics And Security, vol.7, no. 2, pp.798-808, April 2012.

[6] Ryan Connaughton, Amanda Sgroi, Kevin Bowyer, "A Multialgorithm Analysis of Three Iris Biometric Sensors" IEEE Transactions on Information Forensics And Security, vol.7, no.3, pp. 919-931, June 2012.

[7] Somnath Dey, "Iris Data Indexing Method Using Gabor Energy Features" IEEE Transactions on Information Forensics and Security, vol.7, no. 4, pp.1192-1203, August 2012.