International Journal of Applied Engineering and Technology ISSN: 2277-212X (Online)
Online International Journal Available at http://www.cibtech.org/jet.htm
2020 Vol. 10, pp.93-98/Nivedda et al.
***Research Article** (Open Access)*

ATM SECURITY USING IRIS AUTHENTICATION

Nivedaa GA., Ashif J., Bharani Shankar T., *Chandru S. and Krishna kumar J.
Department of Electronics and Communication Engineering
SRM TRP Engineering College, Tiruchirappalli, TN, India
**Author for correspondence*: *chandrusudharsan55@gmail.com*

ABSTRACT

The dawn of monetary transactions has brought about a new economic and technological reform around the world. Along with the continuous development of technology, security concerns are also increasing. ATM or Automated Teller Machine, which helps in transaction of money anytime, and anywhere, faces the threat of fraud and theft, and thus, there is a need for high security to provide safety to the consumer market. Iris technology, which uses the iris pattern of an individual as an identity proof, is the best method to address and eradicate the threats involved in ATM transactions. This project basically explains advantages of iris recognition system over the traditional biometric system along security techniques used for ATM.

***Keyords:** ATM, Iris, Recognition, Authentication, security*

INDRODUCTION

Transaction system has seen a certain development since the early age. The number of ATM card holders has also increased. As progress in science has also accelerated the number of unlawful pursuit and cyber-crimes like ATM card skimming. In spite of continuous warning by the bank authorities, customers tend to disclose their confidential information to the fraudsters and hence become their victims. The fraudsters victimize the customers by intercepting their PIN through fraud text messages and emails. The customer's account becomes easily accessible when they share their account's PIN through these emails or messages. With the development of computer network technology and e-commerce, the self-service banking system has got extensive popularization with the characteristic offering high-quality 24 hours service for customer. However, the financial crime case rises repeatedly in recent years, a lot of criminals tamper with the ATM terminal and steal user's credit card and password by illegal means. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer. How to carry on the valid identity to the customer becomes the focus in current financial circle. Traditional ATM systems authenticate generally by using the credit card and the password, the method has some defects. Using credit card and password can not verify the client's identity exactly. Biometrics deals with automated methods of recognizing a person based on physiological characteristics such as face, fingerprints, hand geometry, iris, retinal, and vein. Biometric authentication technique based on iris patterns is suitable for high level security systems. Iris is the annular ring between the pupil and the sclera of the eye. The structure of iris is fixed from about one year in age and remains constant over time. It exhibits long-term stability and infrequent re enrolment requirements. The variations in the gray level intensity values distinguish two individuals. The difference exists between identical twins and even between left and right eye of the same person. As the technology is iris pattern-dependent, not sight dependent. Thus, the necessity of advancements in technology and ATM systems are needed to implement in order to stop such skimming activities. Many of the banks are starting to implement a second level of authentication system. Further advancements are to be implemented to be at par with the skimming technologies.

LITERATURE SURVEY

[1] C. Rathgeb and A. Uhl, The fuzzy commitment scheme has been leveraged as a means of biometric template protection. A statistical attack against the fuzzy commitment scheme is presented. Comparisons of different pairs of binary biometric feature vectors yield binomial distributions, with standard deviations bounded by the entropy of biometric templates. In case error correction consists of a series of chunks helper data becomes vulnerable to statistical attacks. Error correction codewords are bound to separate parts of a binary template among which biometric entropy is dispersed.

[2] A. F. Sequeira, H. P. Oliveira, J. C. Monteiro, J. P. Monteiro, and J. S. Cardoso, Biometric systems based on iris are vulnerable to several attacks, particularly direct attacks consisting on the presentation of a fake iris to the sensor. The development of iris liveness detection techniques is crucial for the deployment of iris biometric applications in daily life specially in the mobile biometric field. In this paper we present a brief description of the methods and the results achieved by the six participants in the competition.

[3] N. Erdogmus and S. Marcel, The problem of detecting face spoofing attacks (presentation attacks) has recently gained a well-deserved popularity. Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. In this paper, we inspect the spoofing potential of subject-specific 3D facial masks for 2D face recognition.

[4] Souradeep Ganguli, Advanced ATM System Using Iris Scanner We are augmenting a fingerprint sensor of FIM3030 series to the RFID card with a small power supply connected to the card. This acts as our level one security check. Thefingerprint given as input to the card is cross verified with the database created by the bank. A message is sent to the registered card holder if there is a mismatch between the input fingerprint and the fingerprint in the database. If the security check has a clearance, the system further goes on with the level-2 security check i.e. the IRIS scanner. IRIS isthe only part of our body which doesn’t change from birth till our death. So IRIS being the most secured biometric system that we have used in our proposed system. The banks need to design a database consisting of the information of the IRIS of the customers, which is to be verified at the ATM counters by the help of IRIS scanner. If the scanned data does not match with the bank’s database, immediately a message gets delivered to the registered mobile number of the user. The system has to localize the inner boundaries of the iris (pupil and limbs). Further, subordinates detect and exclude eyelashes, eyelids and spectacular reflections. As a result, a set of the complex number will generate that carry local amplitude and phase information about the iris pattern.

EXISTING SYSTEM

For the traditional ATM system customer recognition systems depend only on bank cards and passwords. For solving the bugs of traditional ones, the designs a new ATM terminal recognition system is designed. By using biometric system we can ensure the secure, safe, and improved system for banking. The iris recognition systems have recently shown very high accuracies in verifying an individual’s identity. For Iris detection of person we can split this method into following parts which are: Image acquisition, segmentation, encoding and matching. The results of this system are very efficient for ATM transactions. use for retinal identification is very rare in literature. Landmark based methods for retinal registration were presented in using vessel bifurcations and crossover points as feature points. Another retinal registration method based on location of optic disc was presented by. A cross correlation coefficient based retinal identification was done in They first registered the input image and then matching is done by correlating the vascular pattern. Bevilacqua et al. proposed a vascular bifurcation and cross over point based system for retinal authentication. The comparison was done by means of accumulation matrix.

DISADVANTAGES

- In now a days technology, biometric is easily breakable

- The pupil gets strings at bright surface and larger at dark surface, so that we can’t make a proper scanning in existing system
- In the face recognizing system, photo also give access to further proceeding on any security system

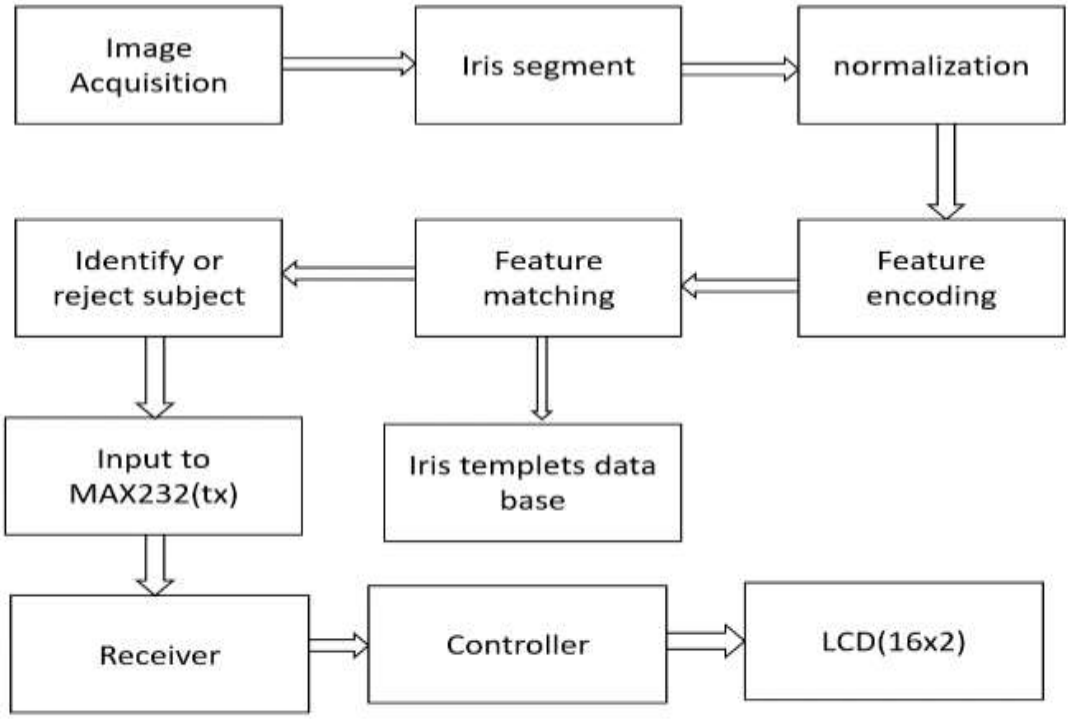
PROPOSED SYSTEM

Iris recognition is the process of recognizing a person by analyzing the random pattern of iris .The iris is a muscle within the eye that regulates the amount of light entering the eye by controlling the size of pupil The system is to be composed of a number of sub-systems, which corresponds to every stage of iris recognition technique. The stages involved in iris recognition are: Image Acquisition – capturing the eye image using Cmos camera, Segmentation – locating the iris region in an eye image. , Normalization - creation of a dimensionally consistent representation of the iris region, Encoding – creating a template containing only the most discriminating features of the iris[4], Database Enrollment – storing up of all the iris patterns of the users, Matching - involves matching up of iris pattern with the stored one, and Recognition – proper matching and recognition is done

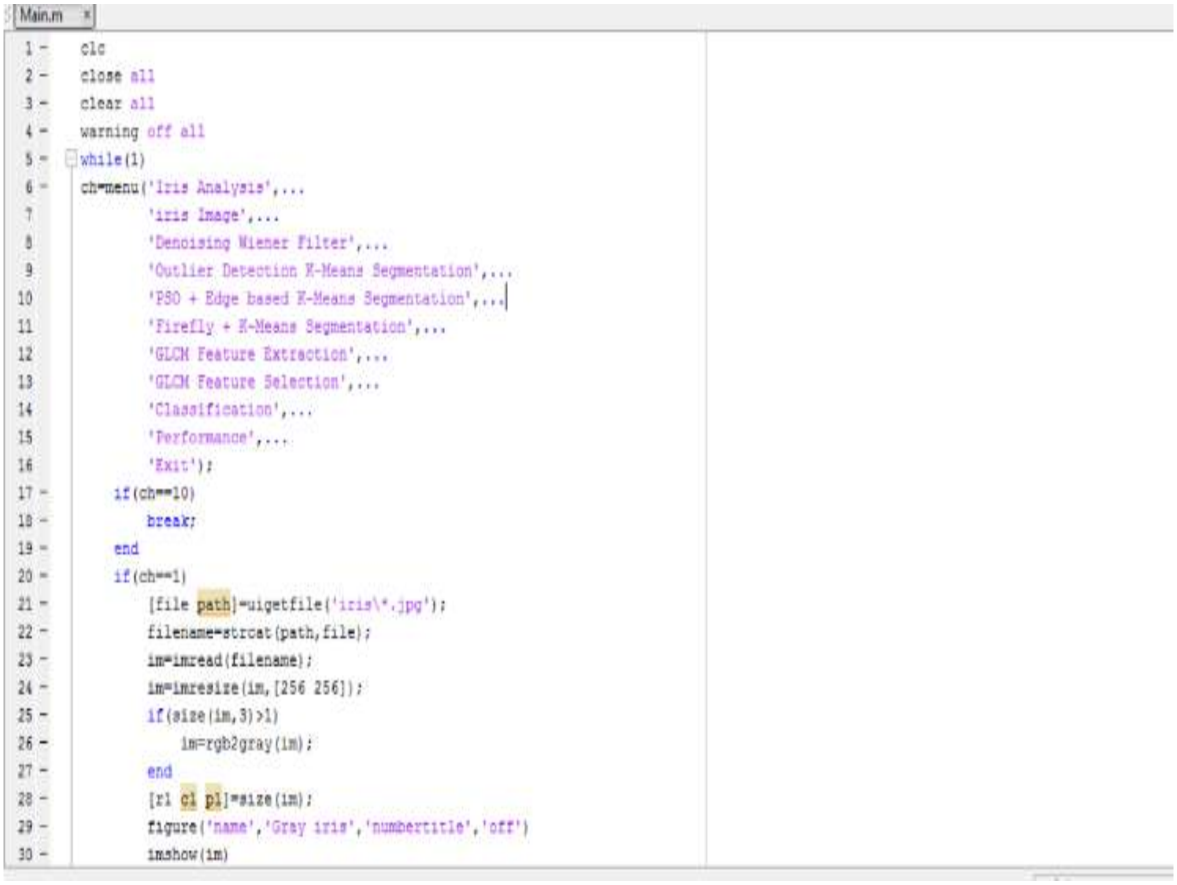
ADVANTAGES

- It will take measure on radius of total eye from the center of the pupil in three different ways, and it gives authorization from previously collected database
- It is used in any other security system using this type of authorization(ex. Wallets, Home security, etc,.)
- The acquisition of human retina is not as simple as for other biometrics like fingerprints, face, irisetc and the fundus cameras are also very expensive

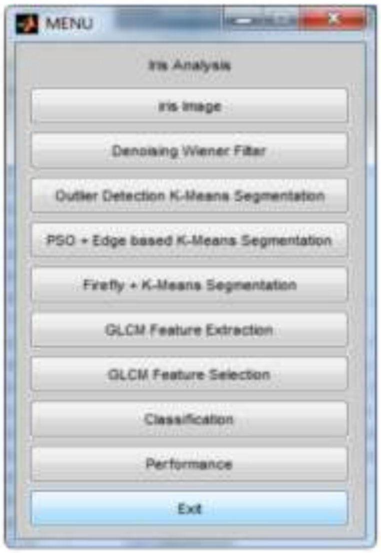
ARCHITECTURE DIAGRAM

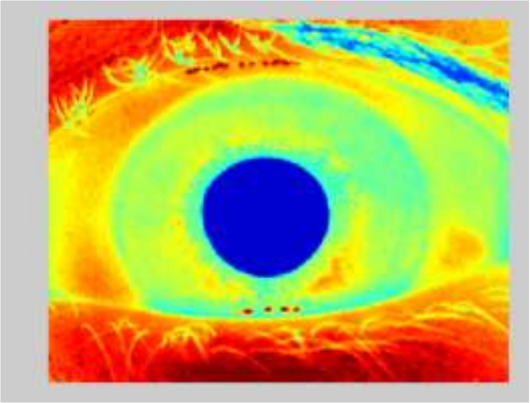


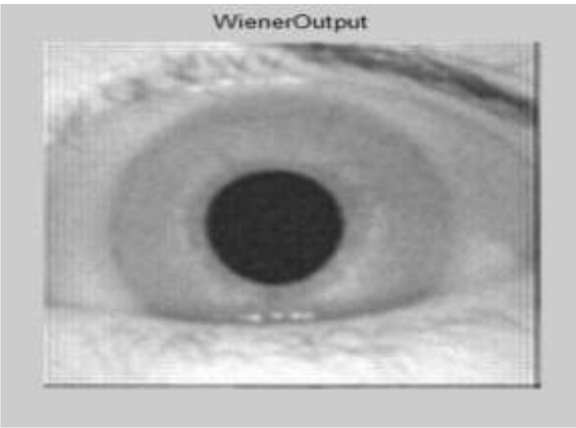
EXPERIMENTAL RESULT

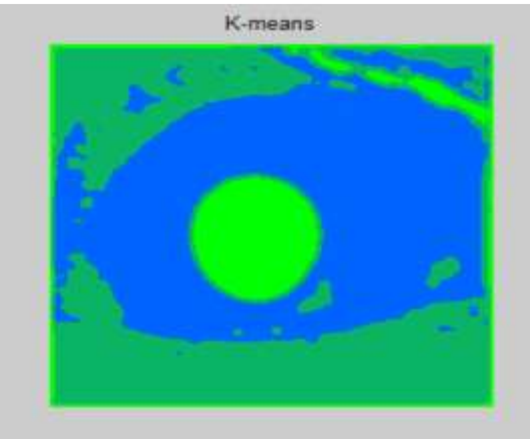


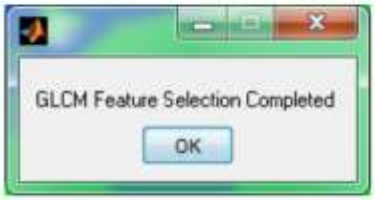
```
clc
close all
clear all
warning off all
while(1)
ch=menu('Iris Analysis',...
        'iris Image',...
        'Denoising Wiener Filter',...
        'Outlier Detection K-Means Segmentation',...
        'PSO + Edge based K-Means Segmentation',...
        'Firefly + K-Means Segmentation',...
        'GLCM Feature Extraction',...
        'GLCM Feature Selection',...
        'Classification',...
        'Performance',...
        'Exit');
    if(ch==10)
        break;
    end
    if(ch==1)
        [file path]=uigetfile('iris\*.jpg');
        filename=strcat(path,file);
        im=imread(filename);
        im=imresize(im,[256 256]);
        if(size(im,3)>1)
            im=rgb2gray(im);
        end
        [r1 c1 p1]=size(im);
        figure('name','Gray iris','numbertitle','off')
        imshow(im)
```

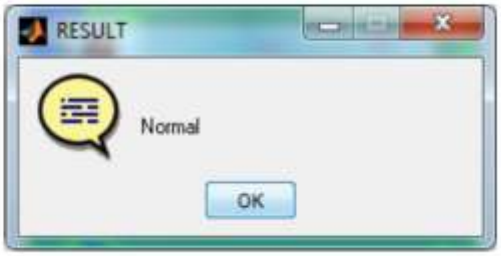




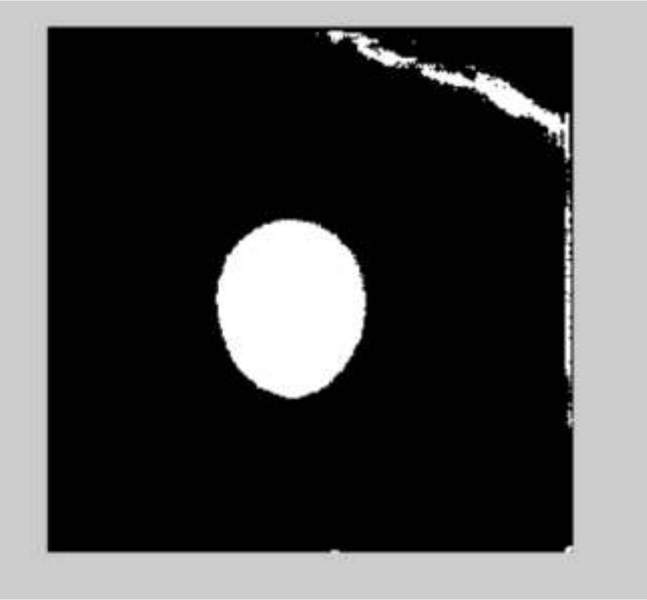





GLCM Feature Selection Completed


RESULT

Normal



CONCLUSION

Our networks use classic convolution operations that can be viewed as linear and non-linear image processing operations. When stacked, these operations essentially extract higher level representations, named multiband images, whose pixel attributes are concatenated into high-dimensional feature vectors for later pattern recognition. Iris recognition is the process of recognizing a person by analyzing the random pattern of iris .The iris is a muscle within the eye that regulates the amount of light entering the eye by controlling the size of pupil .The system is to be composed of a number of sub-systems, which corresponds to every stage of iris recognition technique. The stages involved in iris recognition are: Image Acquisition – capturing the eye image using Cmos camera, Segmentation – locating the iris region in an eye image. , Normalization - creation of a dimensionally consistent representation of the iris region, Encoding – creating a template containing only the most discriminating features of the iris[4], Database

Enrollment – storing up of all the iris patterns of the users, Matching - involves matching up of iris pattern with the stored one, and Recognition – proper matching and recognition is done

REFERENCES

Prabhakar S., S. Pankanti, and A. K. Jain, **(2003).** *Biometric recognition:Security and privacy concerns, IEEE Security and Privacy*, **1**(2) 33-42.

Das Ravi, **(2007)**.*Retinal recognition Biometric technology in practice ,Keesing Journal of Documents & Identity*, **22**, 11-14.

Simon C., Goldstein I., (1935). *A New Scientific Method of Identification, New York State Journal of Medicine*, **35(**18) 901-906.

Tower P., (1955). *The Fundus Oculi in Monozygotic Twins: Report of Six Pairs of Identical Twins, Archives of Ophthalmology* **54**, 225-239.

Staal J., M. D. Abramoff, M. Niemeijer, M. A. Viergever and B. van Ginneken,(2004). *Ridge-based vessel segmentation in color images of theretina, IEEE Trans. Med. Imag*., **23**(4) 501-509,.

Soares J. V. B., J. J. G. Leandro, R. M. Cesar, H. F. Jelinek and M. J. Cree., (2006). *Retinal vessel segmentation using the 2-D gabor wavelet and supervised classification", IEEE Trans. on Med. Imag*, **2**, (9), 1214-1222,

Mishra S., A. Jain, S. Kumar and A. Goyal, (2017). *Enhanced ATM security system using GSM, GPS and Biometrics, IJETR*, **7**(8), 34-35, August.

Jaiswal A.M., M. Bartere, (2014). *Enhancing ATM security using Fingerprint and GSM technology, IJCSMC*, **3**,(4), 28- 32, April.

Hatekar A., H. Babani, T. Kakde, N. Wadhwa, *Fingerprint basedsecurity system using GSM module, Int. Journal of Engineering Research and Application*, **7**(5) (part 2), 31-34.

Sivakumar T, G. Askok, K. Sai Venuprathap, **(2013).** *Design and implementation of security based ATM theft monitoring system", International Journal of Engineering Inventions*, **3**(1), 01-07, August.

Lim S., K. Lee, O. Byeon and T. Kim, *Efficient iris recognitionsystem by optimization of feature vectors and classifier", Etri Journal*.

Soffel V, (2003). Asynchronous interfaces overview: UART and LIN bus, Micro Controller Pros Corporation, May 12.