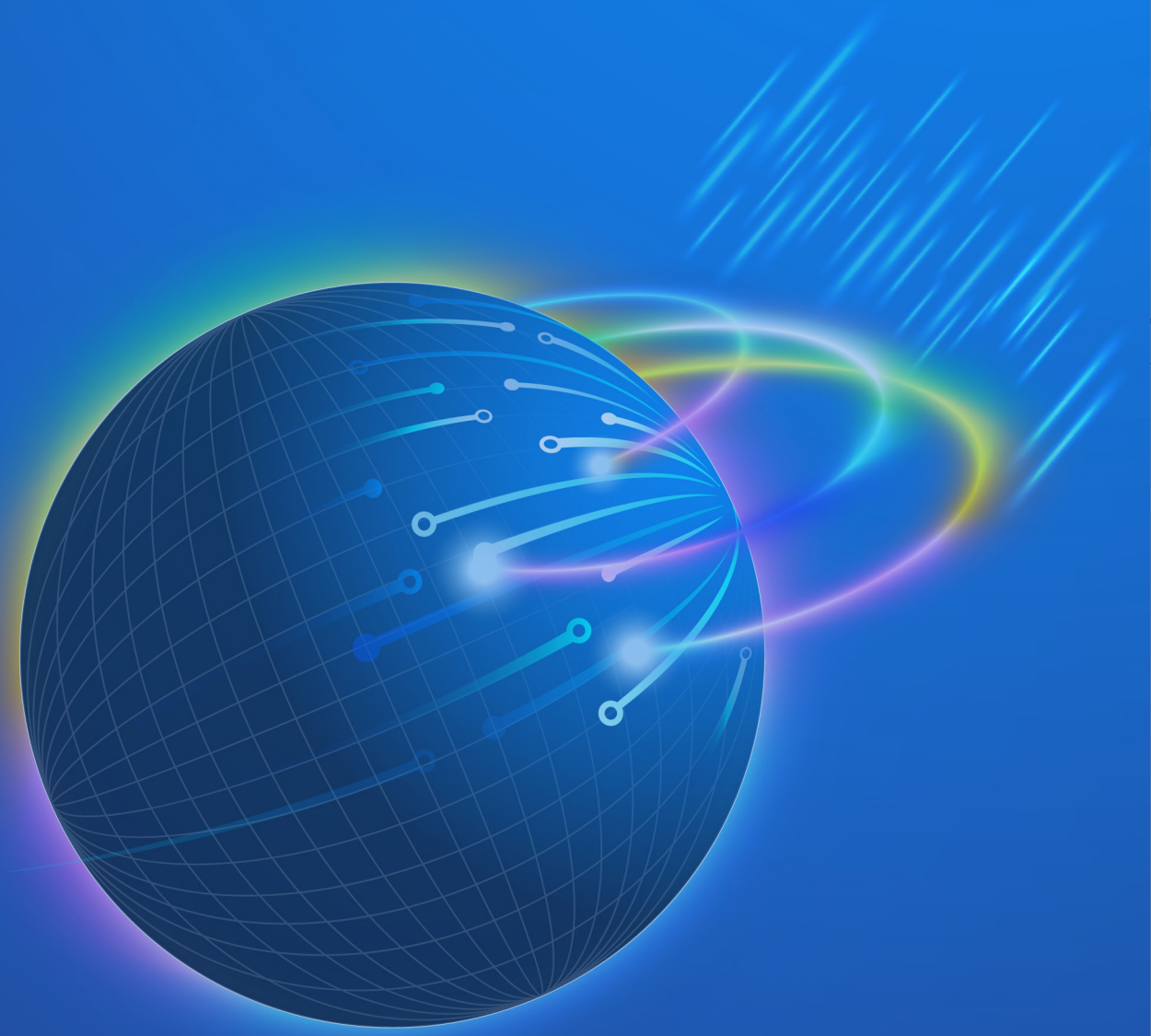
AMERICAN JOURNAL OF
GEOSPATIAL TECHNOLOGY (AJGT)
ISSN: 2833-8006 (ONLINE)
VOLUME 3 ISSUE 1 (2024)



PUBLISHED BY
E-PALLI PUBLISHERS, DELAWARE, USA

American Journal of Geospatial Technology (AJGT)

Volume 3 Issue 1, Year 2024
ISSN: 2833-8006 (Online)
DOI: https://doi.org/10.54536/ajgt.v3i1.2967
https://journals.e-palli.com/home/index.php/ajgt

Enhancing Atm Security System by Using Iris (Eye) Recognition

Irum Ashraf[1*]

Article Information

Received: May 10, 2024

Accepted: June 12, 2024

Published: June 15, 2024

Keywords

Image Preprocessing, Segmentation, Normalization, Feature Extraction

ABSTRACT

Newly invented Iris recognition which is a part of biometric identification,offering and purposing an antique method for personal identification, authentication and security by analyzing the random pattern of the iris. By using iris recognition system recognizes the identification of a person from a captured image by comparing it to the human iris patterns stored in an iris template database. The iris template database has been carried out by using three steps the first step is segmentation. Hough transform is used to segment the iris region from the eye image of the CASIA database. The noise and blurring due to eyelid occlusions, reflections is eliminated in the segmentation stage. The third step is normalization. A technique based on Hough Transform was employed on the iris for creating a dimensionally steady and compatible representation of the iris region. The last step and fourth step is feature extraction. In this Local Binary Pattern and Gray level Cooccurrence Matrix are used to extract the features. At last template of the new eye image captured will be compared with the iris template database using Probabilistic Neural Network.

INTRODUCTION

About 25,000 accounts are opened on the daily according to the RBI report around the world. In the past transaction cannot be done in emergency situation due to crowd and it also takes more time so John Shepherd invented ATM (Automated Teller Machine). Due to increase in the user account made to change the banking system. As users and customers increased drastically , fraudulent act also increased equally so banking system has given more importance to security system which is prior of the customers and users requirement. Hence the requirement for banking security is increased with the passage of time. Biometric system measures the antique specifications of a person so that no one can break the system. Because of this feature of Biometric, this idea evolved in banking systems and sectors. Biometric includes Iris recognition, sound recognition, face features recognition and fingerprint/thumb recognition. Among all those types of Biometrics used, Iris recognition transaction through ATM card it the easiest and simple, all of the customers and users are depend on card system. But at the same time ATM cards pin or password can be easily traced and account can be accessed. It is important to keep the record transaction reports made by use. To overcome these defaults. card less system is should be created by using Red-tacton. Red-tacton uses the surface of the human body as a safe, high speed network transmission path. As per newly invented iris system recognition, It also provides a complete and reliable security system to the users as it allows access to only those individuals whose iris is matched with the database and deny access to all others very reliably. This system has four stages: First is the Image Acquisition. In this image is taken with proper illumination, distance and other specifications affecting image quality and its other features. This step is important because image quality plays an important role in iris Localization step.Another Second is Image Segmentation in which iris is recognition. In this step of feature extraction stage, antique specifications from the segmented iris has been extracted to create an iris performa or template.Moreover this template is used for Iris recognition.However fourth one is matching with an original image taken and saved in database. On this stage it is to be verified that the iris matches image saved in data based or if it doesn't matches then its rejected. Iris recognition is an automatic method of biometric identification that uses an antique specification of evey single user.Iris an internal organ of our body that is visible from outside whose patterns are complex random patterns which are most unique and stable.

Howeve overall biometric technologies used for human authentication is one of the most authentic and accurate for securing banking and ATM system. Iris recognition is one of the stable and reliable out of other biometric techniques such as face recognition, finger recognition, hand and finger geometry, just because of its special and non- invasiveness of the iris pattern. The iris region, the part between the pupil and the white sclera provides many minute visible characteristics such as freckles, cornea stripes ,furrows, crypts which are unique for each individual(Daugman, 1993). If it comes to the eye matching, both of our eyes doesn't match with each other. However the chance of matching two people with same specification is almost zero which makes the system more frequent and stable when it comes to the security matter.

[1] Grand Asian University, Sialkot, Pakistan
[*] Corresponding author's e-mail: irum.ashraf@gaus.edu.pk

Figure 1: Biometric Technologies

Figure 2: Iris Recognition

LITERATURE REVIEW

Patented algorithm uses Iris recognition system which was developed by John Daugman BY using integro differential operator in his algorithm to find inner and outer boundaries of Iris, including the detection of upper and lower eyelid boundaries.For normalization Daughman's rubber sheet model is used where in the circular Iris region is unwrapped into rectangular block of fixed dimension. Feature extraction is performed using 2- D Gabor and hamming distance later on which is used for code matching. 1 in 4 million is the theoretical false match probability in this method. Yang Hu *et al(*Hu, Sirlantzis, & Howells, 2016) has suggested a method for optimal generation of iris codes for iris recognition. This suggested method has been verified later that the traditional iris code is the solution of an optimization problem, where the distance between the feature values and the iris codes has been reduced. This method also proves that more frequent iris codes can be obtained for the optimization problem by adding somevintial terms to the objective function. The two additional objective terms have been investigated; the first objective term which exploits the spatial relationships of the bits in different positions of an iris code. The second objective allivates the effects of less reliable bits in iris codes By individually or in a combined scheme these two objective terms are applied For the optimization problem. International Journal of Engineering Research & Technology (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV9IS070414 (This work is licensed under a Creative Commons Attribution 4.0 International License.) Published by : www.ijert.org Vol. 9 Issue 07, July-2020 999 Smereka(Smereka, 2010) , proposed a method with the capability of reliable segmenting non-ideal images, which is affected with the issues like blurring, specular reflection, occlusion, lighting variation, and off-angle images. For pre-processing the image Haar wavelet transform and contour filter were used and to detect the edges of the iris Circular Hough Transform and Hysteresis thresholding is used . ICE database was used for experiment to check the performance. Rai *et al.*(Rai & Yadav, 2014), who proposed a method for code matching based on combination of two algorithms for achieving better accuracy and speed rate. Circular Hough transform is used to isolate the iris image and then to find the blurring and the zigzag collarette region after that verifying and isolating the eyelids and eyelashes by using parabola detection technique and trimmed median filters. 1-d Log Gabor filters and Haar wavelets are used to isolate features from the zigzag and blurr collarette region of iris. To support vector machine and hamming distance approach by which Extracted features were recognized. Experimental results shows better recognition rate when features were extracted from the specific region of the iris, where more complex patterns are available followed by combining support vector machines and Hamming distance approach for feature recognition. Sunil S Harakannanavar1 *et al.* (Harakannanavar *et al.*, 2018), suggested a method were the iris and pupil boundaries are determinded by using circular Hough transform and normalization is performed by using Dougmans rubber sheet model. The fusion is performed in patch level. For performing fusion, the image is converted in to 3×3 patches for mask image and converted rubber sheet model. Patch conversion is done by sliding window technique. So that local information for individual pixels can be extracted. The final features of iris images are extracted by block based empirical mode decomposition as low pass filter to analyse iris images. Finally the database images and the test image are compared using Euclidean Distance (ED) classifier.

A facial system has been proved as one of the the most securedmethod of all biometric systems. For high level security entirely depending on the system even to help fighting against hacker (Babaei, Molalapata, & Pandor, 2012). Requirement of this identification system is simple camera, scanner, ATM within security systems that require an identity check. This system obtained by

Chinese Academy of Sciences Institute of Automation CASIA (Raghavendra, 2012). IRIS implementation encoded by 1D Log-Gabor filters and phase quantizing output produce a bit-wise biometric template. The Hamming distance was chosen as a matching metric and results show that the proposed approach has a faster operation and good recognition performance (Rao, Kulkarni, & Reddy, 2012) By comparing two digital eye images are capable by using new type of ATM system with Iris Recognition and universal subscriber module . IRIS image and the 'template' of 'IRIS' is to be compared to those in the database (Raj, 2013). In this, we have tried to find a solution of drastically increase in fraud through ATM by finger biometrics which is possible if account holder is physically present in the ATM booth. Thus, it isolates illegal transactions at the ATM points without the knowledge of the authentic owner (Aru & Gozie, 2013). In this,the given concepts of face recognition methods & its applications. In the future, 2D & 3D Face Recognition and large-scale applications such as passport, ID, any service, etc. (Parmar & Mehta, 2014).Biometrics refers to the quantifiable data related to human characteristics. For identification and access control Biometric identification is used in computer science as a form. It is also used to identify individuals in groups that are under surveillance (Betab & Sandhu, 2014).Automatic Teller Machine (ATM) in future will have biometric authentication techniques to A Review on an ATM with an Eye Koushik S *et al.* 4 © Eureka Journals 2018. All Rights Reserved. ISSN: 2581-5105 verify identities of customer during transaction. From this, it has been known that biometric ATM systems is highly secure with the information of body part such as IRIS which is easy to maintain and operate with lower cost (Malviya, 2014). Biometric technology is proven and capable of high levels of accuracy and speed. With smart cards biometric authentication is highly secured and is a stronger method for verification as it is uniquely bound to individuals. It is easy to maintain and operate with lower cost(Sunehra, 2014).The important step is to locate a dominant opensource appearance identification program that is used for local feature analysis and that is based on facial verification. This plan must be applied on various multiple systems, involving Windows and Linux variants (Suganya & Sunitha, 2015).This research has focused on the single biometric trait for recognition and authentication. This purpose is to implement the biometric security system based on iris and palm print recognition using wavelet packet transform and WLD with steganography technique for authentication purpose (Kamble & Nikumbh, 2015).The face of each individual is antique. Algorithms for face recognition usually use the distinguish between different faces. Such facial features can be the shape and the distance of the eyes, eyebrows, lips, chin or nose (see [JHP00]). A lot of research has been done in this area in this paper (Das & Debbarma, 2011).Iri Recognition biometric Uniqueness may save us from the card theft, Duplication, misplacement anddisclosure of password to the unknowns. No excuses for RF/Magnetic Cards forget password. No need to further invest on the Cards Cost as IRIS biometric is much safer. Biometrics allow for increased and frequent security, accountability while tracing and deterring fraud. Proposed method is suitable for the ATM users without the need to carry ATM card because our eyes going with us(Sainis & Saini, 2015). The Automated Teller Machine has made life of people easier and the banking industry functions. The best case is still be that the biometric machine password only your body that is IRIS recognition method So transaction can only be carried out possible due to your physical appearance (Mane, Rajeshirke, & Kumbhar, 2017). New uses like electronic identification cards, which are validated with automation, emerge the possible harm don't to a separate cannot be paid back to account, it must be prevented biometrics itself is not the solution to this problem. It just provides means to treat the possible user candidates uniquely(Bowyer, Hollingsworth, & Flynn, 2008) ATM provides great services in densed populated countries to save time . This identifies a model for the modification of existing ATM systems to economically incorporate fingerprint scanning PLUS blood group; and, outlines the advantages of using such system (Gyamfi, Mohammed, Nuamah-Gyambra, Katsriku, & Abdulah, 2016).Many crimes are tampered by stealing someone's password and card which is easier to access the account of user. Traditionally ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects which caused a lot of the problems for the customers. So we use biometric(Lim, Lee, Byeon, & Kim, 2001). This explains verifying methods which was inputting owner password which is send by the controller. The security features were enhanced largely for the stability and reliability of owner recognition (Patil, Wanere, Maighane, & Tiwari, 2013). Iris recognition is a very benefical and useful technique. Iris recognition is highly accurate technique due to its specifications and features. This technique is tremendously applicable. This technique has increased privacy and identity(Bhagat, Singh, Khajuria, & Student, 2017) for the user. We are able to understand the meaning of biometrics, its different types in briefing after going through the features and specifications. Also, we have studied the facial recognition meaning and techniques. In the end we will be able to know a good knowledge about the facial recognition (Goel, Kaushik, & Goel, 2012). Biometrics is an automatic recognition of a person based on her physiological characteristics and facial recognition. We have learnt so many thing about biometricr, this is the future of banking system (Gupta & Sharma, 2013). In this, it proves that how a person can be identified and verified by a numerous of ways but instead of carrying bunch of keys or remembering things as passwords. we International Journal of Current Research in Embedded System & VLSI Technology 5 Vol. 3, Issue 1 - 2018 © Eureka Journals 2018. All Rights Reserved. ISSN: 2581-5105 can use us as living password, which is called biometric recognition technology (Srivastava, 2013).Though there

are some flaws of facial system, there is a scope in India. This scheme can be effectively and frequently carried out in ATM's , identifying duplicate voters, passport and visa verification, driving permit verification, comparable and other written tests, in authorities and personal sectors (Garg & Singh, 2014).ATM with Adhaar Card is more secure in comparison with other biometric system. As above mentioned proposed conceptual model, it has been concluded that ATM with Adhaar card systems is highly secured as it provides information of body part i. e. , face recognition from three. Different angles. In the end of this paper, we will be able to acquire a good knowledge about the facial recognition (Gulmire & Ganorkar, 2012)

Figure 3: Techniques and tools for perpetrating ATM frauds

METHODOLOGY

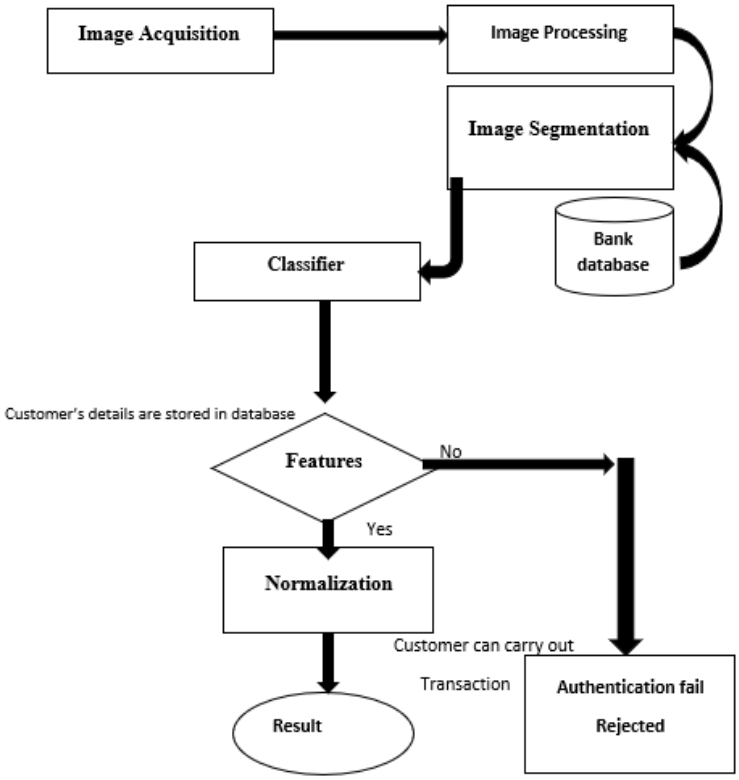


Figure 4: Proposed Approach & Methodology

Fig.4 Block diagram of iris recognition system First, the image is acquired from source. Then preprocessing techniques are applied to the images. The preprocessing is done to remove noise and blurr from images which makes the images more reliable for the training process. Pre-processing techniques involve resizing, reduction in noise and image contrast. Later the image set will be split into 2 sets: train set and validation set. The train set will be used for training the model. During the training phase, the model will learn the parameter and will try to classify the images into the five different classes. Once the training is complete, the parameters were tuned to make the model more accurate and sizeable. Once the model of optimum accuracy is obtained, the made model was used to predict some sample images from validation set and PNN was used to access the performance.

Data Acquisition

The data for training of a model was obtained from a CASIA database v3. There were 22035 images in dataset. Highly unbalanced data was obtained through this process.For matching purpose we have had 20

images in our project. For DATA PRE-PROCESSING median filtering was applied as the noisy images have been received. Canny edge operator is used for image preprocessing purpose, histogram equalization, threshold function for eyelid occlusion & to detect reflection.

Segmentation

Segmentation is a step where non useful regions is being removed from outside of the iris. Iris boundaries and pupil boundaries are being determined during segementation and after that converting this part to a suitable template in normalization stage.

Algorithm

Pupil Detection Input: Eye Image Output

Pupil Centre and its radius

i. linear thresholding method is used to create binary image of the input eye. The minimum pixel value of the given image is taken as threshold value.

ii. To remove the smaller parts, median filtering and morphological operations are performed on the binary image to get the clean region of Iris for matching.

iii.We use region properties to Calculate the centred of the pupil region .

iv. We perform the following operations to determine the radius of pupil:

• Count the number of 1s present on the Horizontal line from centroid to the left side.

• Count the number of 1s present on the vertical line from centroid to the top side.

• The radius of pupil is calculated by taking the average.

v. From the calculated centroid and radius segment the pupil region from the eye image. ALGORITHM

Iris Detection Input

Eye image with detected pupil region and its centre. Output: Iris centre its radius. International Journal of Engineering Research & Technology (IJERT) http://www.ijert.org ISSN: 2278-0181 IJERTV9IS070414 (This work is licensed under a Creative Commons Attribution 4.0 International License.) Published by : www.ijert.org Vol. 9 Issue 07, July-2020 1000

From both side of the detected pupil we Select two rectangle of small size

We use canny edge detection method to verify the vertical line on the both rectangle and determine the centre point of each of the line, say p1(x1, y1) and p2(x2, y2). The detected line is likely to be on the iris boundaries

Calculate the distance d1 and d2 of the point p1 and p2 from the center.

The radius of the iris is obtained by taking the average of the distance d1and d2.

With Centroid and radius ,we segment the iris region.

Normalization

During normalization step,circular iris region that has been detected is converted to rectangular shape of uniform size. Hough Transform is used to perform this process.. The By using Hough transform technique we can isolate features of a particular shape with in an image. As its requirement is to isolate desired features must be in some parametric form, the classical Hough transform is mostly used for the verification of regular curves such as lines, circles, ellipses, etc. A generalized Hough transform can be employed in applications where a simple analytic description of a feature is not possible due to the computational complexity of the generalized Hough algorithm. We restrict the main focus of this discussion to the classical Hough transform due to the computational complexity of the generalized Hough algorithm .Beside its domain restrictions, the classical Hough transform retains many20 applications, as most manufactured parts (and many anatomical parts investigated in medical imagery) contain feature boundaries which can be described by regular curves. The main use of the Hough transform technique is that it abides of gaps in Iris feature boundary verification and is comparitively unaffected by image FEATURE EXTRACTION. Extracting features is one of the important stage in iris recognition system; as it is entirely relying on the features that are extracted from iris pattern. We have used local binary pattern (LBP) and Gray Level Cooccurrence matrix (GLCM).

Feature Extraction

Extracting features is one of the important stage in iris recognition system; as it is entirely relying on the features that has been extracted from iris pattern .We have used local binary pattern (LBP) and Gray Level Co occurrence matrix (GLCM) CLASSIFIER A probabilistic neural network (PNN) has 3 layers of nodes The architecture for a PNN that recognizes K = 2 classes, but it can be extended to any number K of classes. The input layer contains N nodes: one for each of the N input features of a feature vector. These are fan-out nodes that branch at each feature input node to all nodes in the hidden (or middle) layer so that each hidden node receives the complete input

feature vector x. The hidden nodes are collected into groups: one group for each of the K classes.

Classifier

A probabilistic neural network (PNN) has 3 layers of nodes.The architecture for a PNN that recognizes K = 2 classes, but it can be extended to any number K of classes. The input layer contains N nodes: one for each of the N input features of a feature vector. These are fan-out nodes that branch at each feature input node to all nodes in the hidden (or middle)

layer so that each hidden node receives the complete input feature vector x. The hidden nodes are collected into groups: one group for each of the K classes.

RESULTS

The Recognition rate, False Rejection rate was calculated from CASIA-V3 database. We used 20 images for training and 10 images for testing. We also calculated values of

features such as Contrast, Energy, Homogeneit
Contrast: 0.0017
Energy: 0.9966
Homogeneity: 0.9992

Table 1: False Recognition Rate & Recognition rate values for CASIA database

Database	Classifier	FRR	Recognition rate
CASIA	PNN	5.5%	94.6%

Table 2: Comparison of recognition rate with existing approaches

Method	Algorithm	Data base	Recognition rate
K.Gulmire	Global texture feature	CASIAvi	89.5%
Mayanak valsa	Topological features	CASIAvi	92.3%

CONCLUSION

ATM Security System Using Iris Recognition allows the genuine and authorize user to access the ATM system. Iris recognition system is highly secure as compared to any other system present. By identifying and comparing a user's face (IRIS) of his/her, our system resist suspected attackers. In this project, we build a system for ATM Security. Images were acquired by database and given to the computer system where it is processed by various MATLAB functions. Then the database iris image were compared with the output iris image and if it is matched then user has access to the account or else
it denies user's request. Finally, we got a system that has recognition rate of 94.6 % using PNN.

REFERENCES

Aru, O. E., & Gozie, I. (2013). Facial verification technology for use in ATM transactions. *American Journal of Engineering Research (AJER), 2*(5), 188-193.

Babaei, H. R., Molalapata, O., & Pandor, A. (2012). Face Recognition Application for Automatic Teller Machines (ATM). *ICIKM, 45*, 211-216.

Betab, G., & Sandhu, R. K. (2014). Fingerprints in automated teller Machine-A survey. *International Journal of Engineering and Advanced Technology (IJEAT)* ISSN, 2249, 8958.

Bhagat, S., Singh, V., Khajuria, N., & Student, B. (2017). Atm security using iris recognition technology and RFID. *International Journal of Engineering Science and Computing, 7*(5), 11486-11488.

Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2008). Image understanding for iris biometrics: A survey. *Computer vision and image understanding, 110*(2), 281-307.

Das, S., & Debbarma, J. (2011). Designing a biometric strategy (fingerprint) measure for enhancing ATM security in Indian e-banking system. *International Journal of Information and Communication Technology Research, 1*(5).

Daugman, J. G. (1993). High confidence visual recognition of persons by a test of statistical independence. *IEEE transactions on pattern analysis and machine intelligence, 15*(11), 1148-1161.

Garg, H., & Singh, S. (2014). A Review Paper on Facial Recognition. *International Journal of Enhanced Research in Science Technology & Engineering, 3*, 80-85.

Goel, S., Kaushik, A., & Goel, K. (2012). A review paper on biometrics: facial recognition. *International Journal of Scientific Research Engineering & Technology (IJSRET), 1*(5), 012-017.

Gulmire, K., & Ganorkar, S. (2012). Iris recognition using independent component analysis. *International Journal of Emerging Technology and Advanced Engineering, 2*(7), 433-437.

Gupta, N., & Sharma, A. (2013). Review of biometric technologies used for ATM security. *International Journal of Engineering and Innovative Technology, 3*(2), 460-465.

Gyamfi, N. K., Mohammed, M. A., Nuamah-Gyambra, K., Katsriku, F., & Abdulah, J.-D. (2016). Enhancing the security features of automated teller machines (ATMs): A Ghanaian perspective. *International Journal of Applied Science and Technology, 6*(1).

Harakannanavar, S. S., Prabhushetty, K., Hugar, C., Sheravi, A., Badiger, M., & Patil, P. (2018). IREMD: An Efficient Algorithm for Iris Recognition. *International Journal of Advanced Networking and Applications, 9*(5), 3580-3587.

Hu, Y., Sirlantzis, K., & Howells, G. (2016). Optimal generation of iris codes for iris recognition. *IEEE Transactions on Information Forensics and Security, 12*(1), 157-171.

Kamble, P., & Nikumbh, S. (2015). Security System in ATM using Multimodal Biometric System and Steganographic Technique. *Int. J. Innov. Res. Sci. Eng. Technol., 4*(4), 2161-2167.

Lim, S., Lee, K., Byeon, O., & Kim, T. (2001). Efficient iris recognition through improvement of feature vector and classifier. *ETRI journal, 23*(2), 61-70.

Malviya, D. (2014). Face recognition technique: Enhanced safety approach for ATM. *International Journal of Scientific and Research Publications, 4*(12), 1-6.

Mane, A., Rajeshirke, N., & Kumbhar, R. (2017). Measuring Effectiveness of ATMs as Workload Relievers: A Study With Reference to Cooperative and Private Sector Banks in Pune City. *Journal of Commerce and Management Thought, 8*(1), 151.

Parmar, D. N., & Mehta, B. B. (2014). Face recognition methods & applications. *arXiv preprint arXiv:1403.0485*.

Patil, M. A., Wanere, S. P., Maighane, R. P., & Tiwari, A. R. (2013). ATM Transaction Using Biometric

Fingerprint Technology. *International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE), 2*(6), 22.

Raghavendra, C. (2012). High protection human iris authentication in new atm terminal design using biometrics mechanism. *Journal of Global Research in Computer Science, 3*(11).

Rai, H., & Yadav, A. (2014). Iris recognition using combined support vector machine and Hamming distance approach. *Expert systems with applications, 41*(2), 588-593.

Raj, B. S. (2013). A Third Generation Automated Teller Machine Using Universal Subscriber Module with Iris Recognition. *image, 1*(3).

Rao, K. L. N., Kulkarni, V., & Reddy, C. K. (2012). Recognition Technique for ATM based on IRIS Technology. *International Journal of Engineering Research and Development, 3*(11), 39-45.

Sainis, N., & Saini, R. (2015). Biometrics: Cardless Secured Architecture for Authentication in ATM using IRIS Technology. *International Journal of Innovative Research in Computer and Communication Engineering, 3*(6), 5423-5428.

Smereka, J. M. (2010). A new method of pupil identification. *IEEE Potentials, 29*(2), 15-20.

Srivastava, H. (2013). Personal identification using iris recognition system, a review. *International Journal of Engineering Research and Applications (IJERA), 3*(3), 449-453.

Suganya, T., & Sunitha, T. N. C. (2015). Securing atm by image processing facial recognition authentication. *IJSRET-International Journal of Scientific Research Engineering & Technology, 4*(8).

Sunehra, D. (2014). Fingerprint based biometric ATM authentication system. *International journal of engineering inventions, 3*(11), 22-28.