Section: Research Paper

SECURED ATM SYSTEM USING IRIS RECOGNITION TECHNIQUE

Parika Jain, Palak Garg, Shreya Asthana, Shristi, Meharban Ali

parika.jain.cs.2019@miet.ac.in, palak.garg.cs.2019@miet.ac.in,
Shreya.asthana.cs.2019@miet.ac.in, shristi.mukesh.cs.2019@miet.ac.in
meharban.ali@miet.ac.in

Department of Computer Science

Meerut Institute of Engineering and Technology, Meerut

Abstract

This research study describes the ATM with a feature of Iris Recognition for making the ATM more secure. For performing financial transactions, generally, ATM cards are used for authentication but there is a risk of cards getting misplaced or stolen or if the ATM PIN (4- digit Personal Identification Number) is accessed by some unauthorized person, it will enhance the chances of fraud. Hence, biometrics like fingerprint, face recognition, and iris recognition, are used for enhanced security along with ATM PIN. Out of these biometrics, iris recognition is the most effective way as it is more suitable with ages and because of the uniqueness and correctness of different people's iris. This method is more reliable and has a high recognition rate. The False Accept Rate & False Reject Rate are used to assess the effectiveness of ATM system. Keywords: ATM System, Biometric, and Iris Recognition.

Introduction

Automated teller machines, or ATMs, are specialized computers that make managing money for people with bank accounts straightforward. The user is given the option to keep an eye on account balances, make withdrawals or deposits, and print a statement of account activity or transactions. Currently, most ATM systems are based on ATM cards and PINs, which is not much secure because of increasing fraud and stealing of cards. The criminals can tamper with ATM system & can steal the user credit card details and ATM PIN. Hence, Biometrics, the process of relating to or involving the application of statistical analysis to biological data, is used along with ATM PIN for more safe, secure, and improved transactions. Biometric ATMs are self-service cash machines that identify customers using biometric measures and allow them to withdraw cash. Biometrics can be in form of fingerprint, face recognition, and iris recognition. Out of which, Iris recognition is an automated biometric identification method that analyses images of a person's distinctive and stable complex patterns in one or both eyes to identify the person. The Iris recognition method has more accuracy in authenticating and verifying the

individual's identity as every individual has a different iris and the complex pattern of the iris is unique [1][2][3].

Figure 1-View of human eye

The following four components can be divided into this way to identify a individual's iris:

Image acquisition, Segmentation, Encoding, Matching [4].

This ATM system's iris recognition feature will first identify the user's iris before comparing it to a database image. Once the image is verified, then the system will require the ATM PIN without inserting the ATM card. Then that PIN will be verified as per the corresponding account details of the user in the database. The user will be allowed to make transactions only when his iris and PIN will match the database of the information the user has. Iris Recognition is more reliable as it remains stable with age and also, the correctness and uniqueness of every individual's iris reduces the fault acceptance rate [5].

Iris recognition is a type of biometric technology that belongs to the same class as face and fingerprint recognition. The two essential processes in the identification of the iris picture are the extraction of attributes from the images acquired and labelling of the iris images. Therefore , it’s decided to employ Iris Recognition for the reasons listed below [6][7].

1.Reliable: All biometric authentication methods most frequently employ the iris since it is more trustworthy because each person's unique iris exhibits slight variances in its tiny architecture. 2.Provides more security: As compared to other biometrics iris recognition provides more security. 3.Accuracy: The accuracy of iris recognition is 90-99%, according to the NIST. A study by ScienceDirect also demonstrated the iris recognition technique's complete efficacy. 4.Difficult to spoof: Iris recognition is difficult to spoof by Cybercriminals because of its features and characteristics. 5. Perpetual: The cornea protects the iris. Hence, it doesn't vary as individuals become older.As other biometrics like fingerprint changes with time [8][9].

Everyone utilizes ATMs because they are widespread and banks employ innovative technology. The customer has access to their account at all times and from any location. By inserting the ATM card with the scratched side facing the reader and entering the PIN, a customer can access their bank account, complete a transaction, transfer money, etc. after receiving a PIN or password in confidence from the bank. Yet, the convenience, memorability, and security of using PINs without extra security may provide a risk and barrier for customers. The account holder may suffer as a result because it is easily invaded and hacked. Anything you keep for security may be misplaced, and things you know, such as passwords or PINs, may be forgotten. An alternative to these techniques is biometrics, which can also be used in conjunction (multimodal). There are substantial disadvantages to using biometrics such retinal blood vessel patterns, DNA, fingerprints, voiceprints, and signatures. Identification of a fingerprint or handprint requires physical contact, and both can be faked or distorted by objects [10][11].

Even identical twins have different irises because identical twins' DNA is not distinctive from one another. Comparatively speaking to the other biometric identifiers, the majority of the commercial iris recognition algorithms now in use have relatively low false acceptance rates. Replay attacks can be problematic for some biometric identifiers, such as fingerprints. The liveness of the eye can be used to check replay attacks using the iris biometric. The procedure used to take the iris image is non-intrusive. Iris recognition is acknowledged to be more accurate than all other biometric techniques, and iris scans can be computer matched more precisely than a facial image. [12][13].

Literature Review

The first practical approach for iris recognition was proposed by (Daugman, 1993), and it serves as the foundation for the majority of current research and development efforts in iris biometrics. Using a video camera, he was able to capture and identify a human eye. Daugman use an integro differential operator to find circular region of the pupil & iris as well as the lower and upper eyelids' arcs. By adjusting circular contour radius & centre x and y positions, operator looks for circular path with highest change in pixel values. To acquire exact localization, the operator is used until the degree of Smoothing is gradually reduce. The location of eyelids is parallel [1]. (Wilde, 1997) described an innovative method in which a regular video camera and an LED point source were used to capture the subject's eye image. The outside and inside iris boundaries are calculated using a gradient based binary edge map & circular Hough transform. In constructing a template for an iris signature, Wilde's approach uses isotropic band pass decomposition attain from the Laplacian of gaussian at various scales. The normalised correlation for the goodness of match was approximated using these templates to determine resemblance. In his experiment, Wilde used around 60 irises from 40 different people [2]. (Kong and Zhang, 2001) created a system that focused primarily on noise problems, eyelash occlusion, and specular reflections involved in iris picture segmentation. After using the Hough transform to isolate the iris, 1-d Gabor filters were applied in the spatial domain, and a threshold function was used to identify the presence of the eyelid and the specular reflection, respectively. The use of the variance of intensity measurements allowed the detection of several eyelashes. After extracting the features, a binary feature vector was created using 2-d Gabor filters. In order to determine the differences between any two irises, a score that matches them is obtained. This

method offers a noise detecting model throughout the segmentation process, improving performance rates [3]. (Abikoye et al., 2014) used the Fast Wavelet Transform (FWT) to extract the iris' characteristics. In order to create the iris feature codes, the crucial iris characteristics were encoded, compared to templates, and employed. The algorithm offers a low level of complexity and runs quickly[4]. Utilising MATLAB 2016a, (Khanam et al., 2019) constructed a machine learning technique for iris recognition utilising a neural network and discriminant analysis. The recommended approach outperforms SVM in terms of recognition rate and has a lower computational complexity. Discriminant and neural network techniques are used to match and gauge recognition accuracy. The accuracy obtained using the discriminant analysis is 99.99%, as opposed to the neural network's accuracy of 94.44%. [5].

Proposed Methodology

Image capture, localization, normalization, enhancement, & matching are the stages of Iris Recognition. The iris images are obtained during the data acquisition stage. Infrared illumination is typically employed in iris acquisition equipment. During the Iris Segmentation procedure, the iris region is located in the ocular picture. In most algorithms, the iris boundaries are frequently depicted as two circles, assuming that the pupil is displayed almost frontally. Between the pupil and the iris is the inner ring known as the papillary border. The Outer circle contains the Limbic barrier (between the iris & sclera). The segmentation procedure frequently incorporates noise processing. During the encoding process, the iris picture texture is transformed into a vector code bit. Most algorithms collect information on the texture of the iris using filters. The filters' outputs are afterward converted into a bit vector code. The proper level of pairing determines whether a pairing is authorized or unlawful by calculating the distance between iris codes [14][15][16].

Image acquisition-The process of image acquisition, sometimes referred to as data capture, records the Iris Image. The Iris picture can be extracted from a number of free datasets on the internet. A well-known database called the CASIAIris-V1 Image Database exists. There are other databases, like the LEI and the UPOL, UBRIS [17].

Figure 3- Image Acquisition

Localization and segmentation -The process of localization involves locating an object within an image and pinpointing its location using a bounding box [18].

For use in Digital Image Processing & computer vision, image segmentation is the division of digital image into various image segments. Segmentation is used to simplify & change how an image is represented so that it is more meaningful and clear. The approach of image segmentation entails giving each pixel in a picture a label such that pixels with the same label

have particular qualities. The results of image segmentation are either a set of segments that collectively cover entire image or set of contours extracted from the image (see edge detection). All of the pixels in a region are comparable for any characteristic or computed feature, such as color, intensity, or texture.

Normalization- The mapping of the annular iris region to dimensionless pseudo polar coordinate system is one of the key steps in normalization, which is one of the key stages in iris recognition. This procedure results in the rectangular shape that is used to account for variations in pupil size as well as scale differences.

Feature Extraction- Usually, the color photographs of the iris are converted to grayscale photos. In order to extract the features, which are often a numerical characterization of the underlying biometrics, the feature extraction method first finds the IRIS Effective Region (IER). By comparing the data acquired from this algorithm with the pre - stored features and creating a similarity score, this aids in identifying a certain person. The similarity between the two sets of biometric data that were compared is indicated by this score. The person can be recognised based on how similar they are. The iris has distinctive characteristics like stripes, freckles, coronas, and more. The texture of the iris refers to all of these characteristics as a whole.

The SIFT method is used to identify and label local characteristics on images of irises.

SIFT Algorithm:

SIFT refers to Scale Invariant Feature Transform. It locates image's important points and calculates its descriptions. Using cv2.SIFT create, we first create a SIFT object (). Sift is then used to find the keypoints. Where sift is the newly formed SIFT object, use detect (). We employ cv2.drawKeypoints to draw keypoints ().

Steps-

Following are the instructions below to use the SIFT method to find and draw keypoints in the supplied image.

Import the necessary NumPy and OpenCV libraries. Make that they are already installed. Use the cv2.imread() function to read the input picture. Provide the image's whole path. Use the cv2.cvtColor() technique to convert the source image to a grayscale version.SIFT object creation using sift=cv2.SIFT create with default settings () and then find the focal spots in the grayscale picture. Employ sift.detect (). Keypoints are returned. Draw the found keypoint on the image using the function cv2.drawKeypoints(). By passing flags=cv2, rich keypoints can be drawn. As a parameter, use DRAW MATCHES FLAGS DRAW RICH KEYPOINTS.

Matching- The Iris template must compared to the template that was recorded in the database during enrollment after the iris code was generated to check if a match exists. With the aid of various thresholding approaches, such as Hamming Distance, Weight Vector, Winner Selection, Dissimilarity Function, etc., the feature vectors are categorized. The sum of matching elements that differ between two vectors is discovered using the Hamming Distance. In real life, the two vectors diverge more the bigger the Hamming Distance. Conversely, the closer the two vectors

are, the smaller the Hamming Distance. The following mathematical formula represents the Hamming Distance:

$$\mathbf{d(x,y) = 1/n \, \Sigma \, |x_i - y_i| \;\; , (\Sigma = 1 \text{ to } n)}$$

The scipy, cv2 library are used for calculating hamming distance by using function hamming (). This function is part of spatial distance library which includes other helpful functions used to calculate distances. The advantages are:
No touching is made while scanning, accurate performance in matching, less False Accept Ratio as compared to other biometrics, because the cornea shields the iris, it is unaffected by ageing, eliminate delays and inconvenience and facilitate Self-Service.

Flowchart:

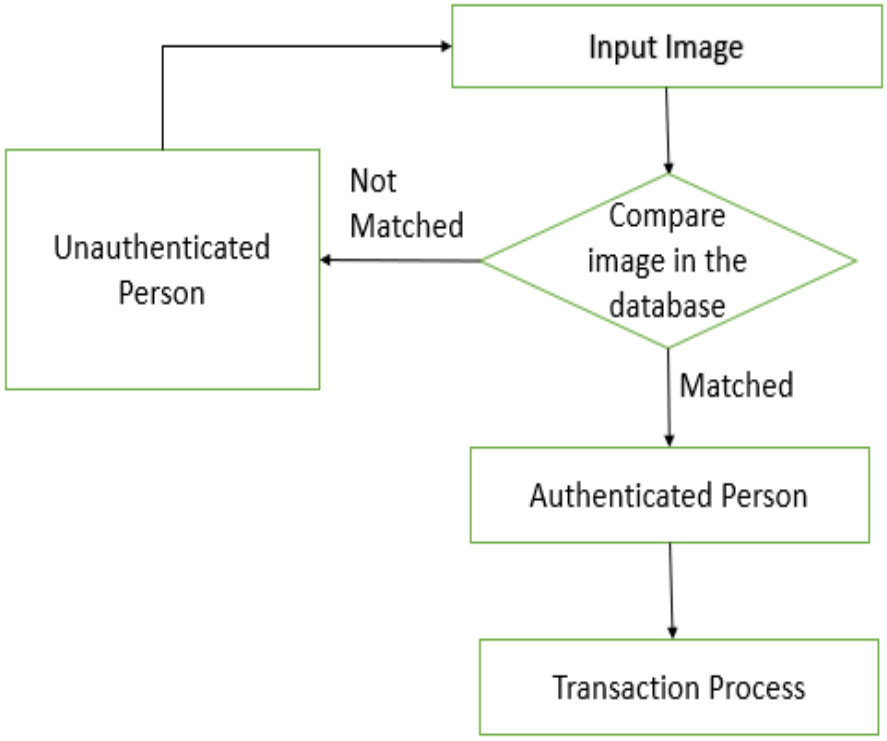

Fig. 1- Flowchart of proposed ATM system

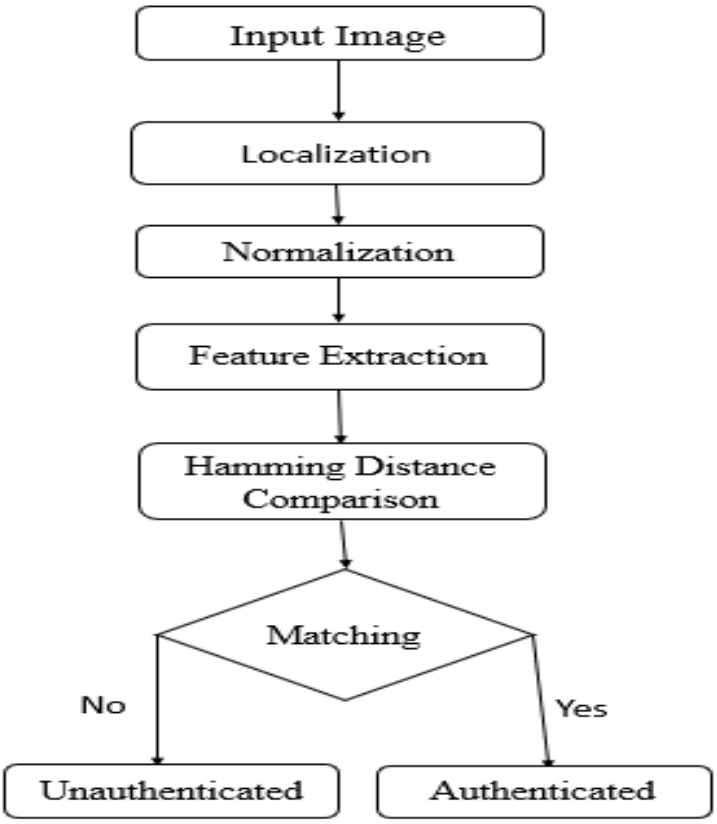

Fig. 2- Flowchart for Iris Recognition Technique

Steps-

1. **Train and Test of Image**-

   Over 756 eye pictures can be found in the CASIA-irisV1 iris image database. These photos come from 108 different people, each having 4 images. By this technique, we test 756 samples.

2. **Localization of iris**-

   It locates and recognizes the iris region in both eye pictures at first. Then, it encrypts crucial iris features for each user.Next, use OpenCV to construct SIFT method to relate features.

3. **Extraction of features-** Use the SIFT method to identify and label local characteristics on images of irises.

4. **Classification-** The same person's iris is recognized when the matching score meets the threshold.

Conclusion:

A new technology based on image enhancement algorithms is used in the design of ATM systems based on iris recognition, taking advantage of the security, accuracy, stability, reliability of iris characteristics. The systems also include original method of verifying, which involved entering the owner's pin. The stability and dependability of the owner recognition were greatly improved by the security components. Since embedded system technology underpins the entire system, it has higher levels of security, reliability, and usability. Due to its individualized identification and verification based on the physiological and behavioral features of the subject, biometrics became popular in security applications. The most promising biometric technology now available is iris recognition, which make use of the visible pattern of the human iris. Therefore, iris biometrics is one of the most efficient ways to increase the security of ATM transactions.

Results Discussion:

False Accept Rate (FAR)- how frequently does the system accept an invalid user?

FAR = Total no. of false acceptance / Total no. of identification attempts

False rejection rate (FRR)- The percentage of validation transactions with genuine identity claims that are wrongly denied.

FRR =Total no. of false rejection / Total no. of identification attempts.

Performance evaluation-

- A false accept rate is 0 when there is no match between the images.
- A false reject rate is 5% when a 95% match is discovered.

References

1. Daugman J., (1993). High confidence visual recognition of persons by a test of statistical independence. IEEE transaction, Pattern analysis and machine intelligence, vol. 15: 1148-1161.
2. Wildes, R.P., (1997). Iris recognition: an emerging biometric technology, Proceedings of the IEEE. Vol. 85, pp. 1348-1363.
3. W. K. Kong, D. Zhang, B. T. Centre, and H. Kong, "Accurate Iris Segmentation Based on Novel Reflection and Eyelash Detection Model," pp. 3–6.
4. Abikoye, Oluwakemi & S., Sadiku & S., Adewole & Gbenga, Jimoh. (2014). Iris Feature Extraction for Personal Identification using Fast Wavelet Transform (FWT). International Journal of Applied Information Systems (IJAIS). 6. 1-6
5. Ruqaiya Khanam, Zohreen Haseen, Nighat Rahman and Jugendra Singh (2019) Performance Analysis of Iris Recognition System.

6. Narayan, V., & Daniel, A. K. (2022). FBCHS: Fuzzy Based Cluster Head Selection Protocol to Enhance Network Lifetime of WSN. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 11(3), 285-307.

7. Narayan, V., & Daniel, A. K. (2019). Novel protocol for detection and optimization of overlapping coverage in wireless sensor networks. Int. J. Eng. Adv. Technol, 8.

8. Awasthi, S., Srivastava, A. P., Srivastava, S., & Narayan, V. (2019, April). A Comparative Study of Various CAPTCHA Methods for Securing Web Pages. In 2019 International Conference on Automation, Computational and Technology Management (ICACTM) (pp. 217-223). IEEE.

9. Narayan, V., & Daniel, A. K. (2022). Energy Efficient Protocol for Lifetime Prediction of Wireless Sensor Network using Multivariate Polynomial Regression Model. Journal of Scientific & Industrial Research, 81(12), 1297-1309.

10. Choudhary, S., Narayan, V., Faiz, M., & Pramanik, S. (2022). Fuzzy approach-based stable energy-efficient AODV routing protocol in mobile ad hoc networks. In Software Defined Networking for Ad Hoc Networks (pp. 125-139). Cham: Springer International Publishing.

11. Srivastava, S., & Sharma, S. (2019, January). Analysis of cyber related issues by implementing data mining Algorithm. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 606-610). IEEE.

12. Srivastava, S., Yadav, R. K., Narayan, V., & Mall, P. K. (2022). An Ensemble Learning Approach For Chronic Kidney Disease Classification. Journal of Pharmaceutical Negative Results, 2401-2409.

13. Srivastava, S., & Singh, P. K. (2022). Proof of Optimality based on Greedy Algorithm for Offline Cache Replacement Algorithm. International Journal of Next-Generation Computing, 13(3).

14. Salagrama, S., Kumar, H. H., Nikitha, R., Prasanna, G., Sharma, K., & Awasthi, S. (2022, May). Real time social distance detection using Deep Learning. In 2022 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES) (pp. 541-544). IEEE.

15. Mahadani, A. K., Awasthi, S., Sanyal, G., Bhattacharjee, P., & Pippal, S. (2022). Indel-K2P: a modified Kimura 2 Parameters (K2P) model to incorporate insertion and deletion (Indel) information in phylogenetic analysis. Cyber-Physical Systems, 8(1), 32-4

16. Tyagi, N., Rana, A., Awasthi, S., & Tyagi, L. K. (2022). Data Science: Concern for Credit Card Scam with Artificial Intelligence. In Cyber Security in Intelligent Computing and Communications (pp. 115-128). Singapore: Springer Singapore.

17. Awasthi, S., Kumar, N., & Srivastava, P. K. (2021). An epidemic model to analyze the dynamics of malware propagation in rechargeable wireless sensor network. Journal of Discrete Mathematical Sciences and Cryptography, 24(5), 1529-1543.

18. Singh, M. K., Rishi, O. P., Awasthi, S., Srivastava, A. P., & Wadhwa, S. (2020, January). Classification and Comparison of Web Recommendation Systems used in Online Business. In 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM) (pp. 471-480). IEEE.