International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Iris Recognition For Banking And ATM Transactions

***Akash Pandey*[1], *Abhishek Dwivedi*[2]**

[1] School of Computer Applications Babu Banarasi Das University, Lucknow, India akashpandey5414@gmail.com

[2] School of Computer Applications Babu Banarasi Das University, Lucknow, India abhishekdwivedi000000@gmail.com

ABSTRACT :

Iris Recognition is one of the most advanced and sophisticated achievements in the field of biometric identification and authentication. Essentially, it also aims at providing and offering a very unique method of identifying an individual by utilizing the random patterns within the iris. By making it possible, an iris recognition system identifies individual persons captured in an image by matching against the patterns of human iris that are stored in an iris template database. Creation of the iris template database has been done in three steps. The first step is referred to as segmentation. Hough Transform is used to perform segmentation of the iris region on eye images taken from the CASIA database. So, the noise and blurring due to eyelid occlusions and reflections are removed during this stage. The third step is normalization. A method based on Hough Transform was implemented on the iris to obtain an image of the iris region that was then geometrically has been made invariant and standardized. The third and the last step is known as feature extraction. In this Local Binary Pattern and Gray level Cooccurrence Matrix are used to do the feature extraction. Finally, captured template of the new eye image will be matched with the iris template database employing Probabilistic Neural Network.

INTRODUCTION :

Every day around the world, about 25000 accounts are opened as per the Reserve Bank of India report. In the past, due to the large number of people, it was not possible to make transactions even in case of an emergency and a lot of time was consumed and hence John Shepherd came up with the ATM (Automated Teller Machine). With increased number of users the account made was to change the whole banking system.

The biometric system captures the unique characteristics of an individual in such a way that it is impossible for anyone to compromise or override the system. Due to this characteristic of Biometric, this concept was further developed in banking systems and industries. Examples of Biometric include Iris, sound, face, and thumb/finger scans recognition. Out of all the types of Biometrics being used why AMBA – iris recognition is used for ATM’s as it is easily simple, considering all the customers and users depend on the card system. But at the same time PIN or password of ATM cards can however be easily figured out and gain access to a person’s account. It becomes imperative to save the transaction reports generated by the use of. To cover these defaults. A card less system has to be developed using Red tacton. Red-tacton employs human body surface as the high speed around the world supersonic communication medium. With the new modification of the previously patented iris recognition This system has four stages: The first is Image Acquisition. In this step an image is taken with proper illumination, distance and other specifications that influence image quality and its other aspects. This step is very critical as it informs the iris Localization step.AneAnother Secondary, Image Segmentation is Recognition of the iris as The the Second ie is this. In this step of feature extraction stage, antique specifications from the segmented iris has been extracted to create an iris Performa or template.

Nonetheless from all of the biologic features the one pertaining authentication and verification is perhaps the best in terms of efficiency in regard to the protection of the bank and ATM system network. Among the most biometric methods such as fingerprint recognition, face recognition, hand and finger geometry, and iris biometry, iris uniqueness is one of the outstanding features simply because of the peculiarities of consumption pattern and its non – that is invasive enhancement of the iris pattern. From the centre of the eyeball through the white sclera isposited a number of small distinct visible features such as corneal striae, furrows and freckles which are unique to every human being (Daugman, 1993).

LITERATURE REVIEW :

The patented algorithm of iris dection relies on an advanced method of iris recognition system that John Daugman developed. He utilized an integro - differential operator in his algorithm to identify the inner and outer edges of the iris, including the upper and lower eyelids. To prepare the iris for analysis, Daugman's rubber sheet model transforms the circular iris area into a rectangular block of a fixed size. Feature extraction is conducted using 2-D Gabor transforms and Hamming distance for code matching Gabor transforms and Hamming distance. Haar wavelet transforms and contour filters were employed for image pre-processing, with Circular Hough Transform and Hysteresis thresholding used to detect iris edges. Rai and Yadav (2014) suggested a code matching method that combines two algorithms to improve accuracy and speed. They used Circular Hough Transform to extract the iris image, then identified blurring and the zigzag collarette region.

The eyelids and eyelashes were isolated and verified using parabola detection techniques and trimmed median filters. Features from the hazy and zigzag collarette regions were isolated with 1-D Log Gabor filters and Haar wavelets. To recognize the extracted features, they employed a support vector machine and Hamming distance approach.

To perform this fusion, images are converted into 3×3 patches of both the mask image and the rubber sheet model, using a sliding window technique to extract local information from individual pixels. The final features of the iris images are extracted using block-based empirical mode decomposition as a low-pass filter for analyzing iris images. Ultimately, the images from the database and the test image are compared using the Euclidean Distance classifier.

The ongoing challenge of rising fraud incidents associated with ATM transactions is addressed through the introduction of finger biometrics, which necessitates the physical presence of the account holder within the ATM enclosure. This measure effectively mitigates the occurrence of unauthorized transactions, thereby safeguarding the legitimate owner's interests (Aru & Gozie, (2013). The discourse further extends to the methodologies employed in facial recognition and their diverse applications, anticipating future developments in both two-dimensional and three-dimensional face recognition technology. Such advancement are expected to have considerable implications for large scale implementations, including passport and identification services (Parmar & Mehta,2014).

Biometric systems, which rely on quantifiable human characteristics for identification and access control, are becoming increasingly integral to various applications in computer science. These systems have been employed to identify individuals within monitored groups (Betab & Sandhu, 2014). The future integration of biometric authentication techniques in ATMs is anticipated to enhance customer identity verification processes during transactions, highlighting the heightened security associated with biometric data, particularly iris information, which is economically viable in terms of maintenance (Malviya, 2014). The established efficacy of biometric technology in achieving high accuracy and operational speed further strengthens its appeal as a verification method that is inherently linked to individual users.

In light of these developments, the necessity of identifying a robust open-source facial recognition program designed for local feature analysis becomes apparent. Such a program should be applicable across a range of operating systems, including Windows and Linux (Suganya & Sunitha, 2015). The focus of the current research is on the application of single biometric traits for recognition and authentication purposes, specifically through the enhancement of iris and palm print recognition utilizing wavelet packet transforms and WLD in conjunction with steganographic techniques (Kamble & Nikumbh, 2015).

Facial recognition algorithms capitalize on the unique characteristics of individual faces, assessing features such as the shape and spatial arrangement of the eyes, eyebrows, lips, chin, and nose (JHP00). Research in this field has proliferated, as noted by Das and Debbarma (2011). Iris recognition serves as a promising biometric solution for mitigating issues such as card theft, duplication, misplacement, and unauthorized password disclosure. This method obviates the need for physical cards, proposing a secure alternative for ATM users reliant solely on their biometric attributes (Sainis & Saini, 2015).

The implementation of biometrics within ATM systems represents a transformative shift in banking practices, fostering an environment of enhanced security while ensuring user convenience. The transaction process, contingent upon the physical characteristics of the iris, underscores the importance of biometric verification as a singular means of access (Mane, Rajeshirke, & Kumbhar, 2017). Despite the emergence of electronic identification cards and automated validation processes, biometric systems must also address potential vulnerabilities to prevent unauthorized access and misuse (Bowyer, Hollingsworth, & Flynn, 2008).

ATMs have continued to evolve in densely populated regions, providing substantial time-saving benefits to users. The proposal to modify existing ATM systems to incorporate fingerprint scanning along with blood group identification serves to delineate the advantages of such integrative systems (Gyamfi et al., 2016). Historically, ATM systems have relied on conventional methods of authentication, primarily through the use of cards and personal identification numbers (PINs). However, this traditional framework has presented numerous challenges, necessitating the adoption of biometric solutions (Lim et al., 2001).

The introduction of biometric authentication methods enhances security measures by bolstering the stability and reliability of user recognition protocols (Patil et al., 2013). The iris recognition technique, characterized by its accuracy and applicability, significantly contributes to enhanced privacy and identity protection for users (Bhagat et al., 2017). A thorough examination of biometric methodologies reveals a diverse array of techniques, including facial recognition, which is poised to play a central role in the future of banking systems (Goel et al., 2012). This exploration elucidates the multifaceted nature of biometric identification, highlighting its capacity to supplant traditional methods predicated on physical items or memorized passwords, establishing the individual as the primary locus of authentication (Gupta & S harma, 2013; Srivastava, 2013).

Despite certain limitations associated with facial recognition systems, there exists significant potential for their application in India. The implementation of such schemes could be facilitated across various sectors, including Automated Teller Machines (ATMs), the identification of duplicate voters, as well as in the verification processes for passports, visas, and driving permits. These applications extend to both governmental and private sectors (Garg & Singh, 2014).

This paper aims to enhance understanding regarding the functionality and efficacy of facial recognition technology (Gulmire & Ganorkar, 2012). By the conclusion, a thorough comprehension of facial recognition systems will be attained, laying a foundation for informed discussion on their practical applications.

METHODOLOGY :

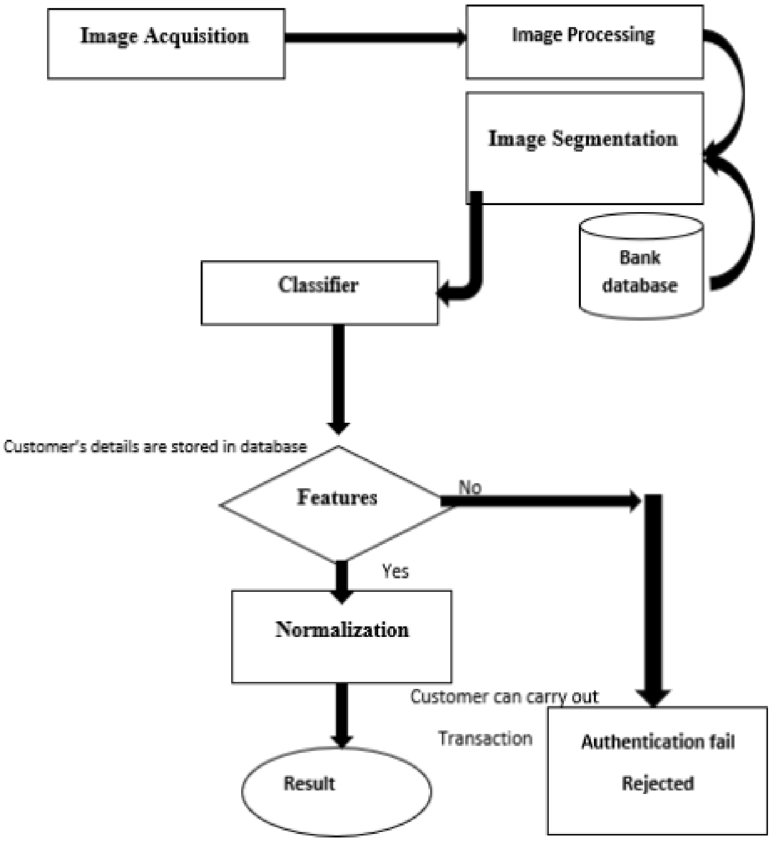

Fig. 1

Fig. 1 The operational framework of an iris recognition system can be delineated through a series of methodical steps commencing with image acquisition from a designated source. Following this initial phase, preprocessing techniques are employed to enhance the quality of the images. The objective of preprocessing encompasses the elimination of noise and blurriness, thus ensuring that the images are adequately prepared for the subsequent training process.

DATA ACQUISITION :

The dataset utilized for the training of the model was sourced from the CASIA database version 3, comprising a total of 22,035 images. To facilitate data pre-processing, several techniques were employed to address the presence of noise in the images obtained. Median filtering was implemented to mitigate the effects of noise. Furthermore, the Canny edge operator was employed as a primary method for image pre-processing. In addition, histogram equalization and a threshold function were utilized to manage eyelid occlusion and to effectively detect reflections present in the images.

SEGMENTATION

The process of segmentation involves the elimination of non-essential regions surrounding the iris. During this phase, the boundaries of both the iris and the pupil are identified. Subsequent to this identification, these defined areas are transformed into a suitable template as part of the normalization stage.

ALGORITHM

IRIS DETECTION INPUT:
EYE IMAGE OUTPUT IRIS CENTRE AND ITS RADIUS

The process of converting the input eye image into a binary format is initiated through the application of the linear thresholding method, wherein the minimum pixel value serves as the designated threshold. Subsequently, to eliminate smaller components, median filtering in conjunction with morphological operations is utilized on the binary image, thereby facilitating the extraction of a clean Iris region suitable for matching purposes.

Upon obtaining both the centroid and the radius , the segmentation of the pupil region from the eye image is performed. This segmented output can be further utilized for subsequent analysis within the algorithm.

IRIS DETECTION INPUT

An eye image, exhibiting the detected pupil region along with its center, serves as the basis for deriving the iris parameters, specifically the iris center and its radius. This procedure, documented in the International Journal of Engineering Research & Technology (IJERT), is available online at http://www.ijert.org under the ISSN: 2278-0181. The publication, titled IJERTV9IS070414, was released in Volume 9, Issue 07, in July 2020, and is licensed under a Creative Commons Attribution 4.0 International License.

In the analysis of the detected pupil, two small rectangular areas are selected from both sides of the pupil. The Canny edge detection methodology is subsequently employed to identify the vertical lines within these rectangles. The midpoint of each vertical line is determined, resulting in two critical coordinates, designated as p1(x1, y1) and p2(x2, y2). Given that these detected lines are likely aligned with the boundaries of the iris, further calculations are conducted to
establish the distances d1 and d2, representing the distances from points p1 and p2 to the center of the pupil.

The average of these distances, d1 and d2, provides an estimation of the iris radius. Utilizing the calculated centroid and the derived radius, the segmentation of the iris region is effectively achieved, thereby allowing for precise delineation of the iris within the eye image.

NORMALIZATION

In the initial phase of normalization, the circular iris region, once detected, undergoes a transformation into a uniformly sized rectangular shape. This transformation is executed with the application of the Hough Transform, a technique that facilitates the isolation of spcific shapes within an image. The traditional requirement for shape isolation necessitates that the desired features be represented in a parametric format; thus, the classical Hough Transform is predominantly utilized for the verification of regular curves, including lines, circles, and ellipses.

While the generalized Hough Transform may be applicable in scenarios where a straightforward analytic representation of a feature is unattainable, the computational demands of this generalized algorithm impose significant constraints. Consequently, the present discourse will concentrate on the classical Hough Transform, which, despite its limitations, retains a multitude of applications due to the prevalence of feature boundaries in manufactured and anatomical parts found in medical imaging. These boundaries can frequently be effectively characterized by regular curves. The process of feature extraction represents a critical component of the iris recognition system, as this system relies entirely on the
features obtained from the iris pattern. In this context, both Local Binary Pattern (LBP) and Gray Level Co-occurrence Matrix (GLCM) methodologies have been employed to facilitate effective feature extraction.

FEATURE EXTRACTION :

The extraction of features constitutes a fundamental phase in iris recognition systems, as the efficacy of such systems is contingent upon the features derived from the iris pattern. In this context, local binary pattern (LBP) and Gray Level Co-occurrence Matrix (GLCM) have been employed for feature extraction.

In terms of classification, a probabilistic neural network (PNN) is utilized, characterized by its architecture comprising three layers of nodes. The configuration of a PNN, designed to identify K = 2 classes, can be adapted to accommodate any arbitrary number of classes (K). The input layer is composed of N nodes, each corresponding to an individual feature within the feature vector. These nodes function as fan-out nodes, distributing the input across all nodes in the hidden layer, ensuring that every hidden node receives the entirety of the input feature vector, denoted as x. Furthermore, the hidden nodes are organized into distinct groups, with each group representing one of the K classes.

CLASSIFIER

A probabilistic neural network (PNN) consists of three distinct layers of nodes, designed to recognize K classes, where K can be any integer greater than or equal to two. The first layer, known as the input layer, comprises N nodes corresponding to each of the N input features of a given feature vector. These nodes function as fan-out nodes, facilitating the distribution of input data to all nodes in the subsequent hidden layer. Consequently, each hidden node is capable of receiving the complete input feature vector, denoted as x.

The architecture further organizes the hidden nodes into groups, with each group dedicated to one specific class among the K categories. This arrangement enables the PNN to process and classify the input data effectively, thereby allowing for adaptability across a variety of classification tasks. By structuring the nodes in this manner, the PNN leverages its layered design to enhance its performance in recognizing complex patterns within the input features.

CONCLUSION :

The implementation of an ATM security system utilizing iris recognition technology facilitates access exclusively for authorized users. Iris recognition is regarded as a more secure method when juxtaposed with alternative biometric systems. This system operates by capturing and analyzing the unique characteristics of an individual's iris, thus serving as a deterrent against unauthorized access attempts.

In the development of this ATM security system, a database of iris images was constructed to support the recognition process. These images were subsequently processed through various functions within MATLAB, enabling the analysis of the biometric data.
After processing, the system engages in a comparison between the iris images stored in the database and those captured in real time. Access to the account is granted only if a match is confirmed; otherwise, the system will reject the user's access request. This process highlights the effectiveness of iris recognition in enhancing the security framework of ATM transactions.

REFERENCES :

1. Aru, O. E., & Gozie, I. (2013). Facial verification technology for use in ATM transactions. American Journal of Engineering Research (AJER), 2(5), 188-193.
2. Babaei, H. R., Molalapata, O., & Pandor, A. (2012). Face Recognition Application for Automatic Teller Machines (ATM). ICIKM, 45, 211-216.
3. Betab, G., & Sandhu, R. K. (2014). Fingerprints in automated teller Machine-A survey. International Journal of Engineering and Advanced Technology (IJEAT) ISSN, 2249, 8958.
4. 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.
5. 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.
6. 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).
7. 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.
8. Garg, H., & Singh, S. (2014). A Review Paper on Facial Recognition. International Journal of Enhanced Research in Science Technology & Engineering, 3, 80-85.
9. 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.
10. Gulmire, K., & Ganorkar, S. (2012). Iris recognition using independent component analysis. International Journal of Emerging Technology and Advanced Engineering, 2(7), 433-437.
11. Gupta, N., & Sharma, A. (2013). Review of biometric technologies used for ATM security. International Journal of Engineering and Innovative Technology, 3(2), 460- 465.
12. 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).
13. 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.
14. 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.
15. 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.
16. 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.
17. Malviya, D. (2014). Face recognition technique: Enhanced safety approach for ATM. International Journal of Scientific and Research Publications, 4(12), 1-6.
18. 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.
19. Parmar, D. N., & Mehta, B. B. (2014). Face recognition methods & applications. arXiv preprint arXiv:1403.0485.
20. 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.
21. 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).
22. Rai, H., & Yadav, A. (2014). Iris recognition using combined support vector machine and Hamming distance approach. Expert systems with applications, 41(2), 588-593.
23. Raj, B. S. (2013). A Third Generation Automated Teller Machine Using Universal Subscriber Module with Iris Recognition. image, 1(3).
24. 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.

25. 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.
26. Smereka, J. M. (2010). A new method of pupil identification. IEEE Potentials, 29(2), 15-20.
27. Srivastava, H. (2013). Personal identification using iris recognition system, a review. International Journal of Engineering Research and Applications (IJERA), 3(3), 449- 453.
28. 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).
29. Sunehra, D. (2014). Fingerprint based biometric ATM authentication system. International journal of engineering inventions, 3(11), 22-28.