Security System Enhancement Using Iris Scan Biometric Technology for ATM Machine

Mudassir AbdullahiMayare[1], Avinash Kumar Singh[2], Owais Ahmad Shah[3]

[1,2,3]Department of Electronics and Communication Engineering, Noida International University

Abstract

Banking is currently very simple, however there are often many opportunities for cybercrime. Numerous banking transactions have been the victim of fraud. Concerns around consumer security and privacy have always revolved around authentication and verification. It is challenging to uphold the integrity and authenticity of people in theever-shiftingenvironment. On how to combat ATM fraud, many ideas and recommendations have recently been put out. We need some trustworthy security findings that we can utilize in conjunction with the current technologies to combat all of these frauds. One of the technologies that we can use in conjunction with the existing technology is biometrics. Combining related technology may help to decrease ATM fraud and hence increase the security of other financial transactions. This essay offers an overview of important iris recognition studies. An iris identification system goes through three main phases: template matching, point birth, and picture preprocessing. The most popular algorithms used in each stage are reviewed in the literature.

keywords: ATM security, fraud ; iris scanner, face recognition technology.

1. INTRODUCTION

The introduction of an iris scan biometric system for ATM machines is becoming more popular due to its security and convenience. This type of system uses a person's unique eye pattern as their personal key allowing them access to their funds without the need for cards or passwords. The increased popularity of iris scanning technology, also known as "eye-recognition" has grown exponentially in recent years with many banks offering this new service. The biometric authentication methods, such as fingerprint recognition, facial recognition, and iris scanning, have gained widespread recognition for their accuracy and difficulty to forge. Among these, iris scan biometric technology stands out as one of the most secure and reliable methods for verifying an individual's identity. The unique patterns in the iris of the human eye remain stable throughout a person's life and offer a vast number of distinctive features, making it an ideal candidate for securing sensitive transactions. Advantages include improved accuracy compared to other biometric methods (such as fingerprint recognition), heightened security features that reduces identity theft, cost saving from reduced card management fees and less time spent on authentication process. In addition, automated teller machine operators can offer customers greater privacy than other forms of identification such as fingerprints since no physical contact or records exist after the transaction is complete. Disadvantages include individuals having difficulty with iris scanning if they have vision problems, privacy related to the collection of sensitive data by financial institutions, and PIN cloning using images taken during legitimate user sessions at ATMs may require further research.

To identify an existing, it uses behavioral or physiological traits. The iris, point, face, and hand figure are the physiological features. Behavior traits include the dynamics of the voice, hands, and keystrokes. The iris has discrete phase information with a range of roughly 249 degrees of freedom among these features. This benefit makes iris recognition the most precise and trustworthy biometric identification method. [1][2]

2. LITERATURE REVIEW

There has been extensive research conducted into the use of iris scan biometrics for ATM machines. Studies have found that using such technology can result in improved security and better user experience, as well as reduced fraudulent activity. The main benefits to implementing this type of authentication system include increased accuracy, faster time-to-authentication compared with other methods, and improved customer satisfaction due to ease of use. However, there are also some potential drawbacks associated with iris scanning biometrics, such as privacy concerns and cost implications. Studies have shown that users generally respond positively when presented with an iris scanner at an ATM machine; most people report feeling safer knowing their transactions are protected by additional levels of security beyond passwords or PIN numbers. Furthermore, they tend to find it easy to use thanks to its simple yet accurate design which does not require any complicated setup procedures for end users and allows minimal personal data collection. Additionally, studies suggest that utilizing a combination of both traditional identification systems (e.g., password/PIN) alongside more modern solutions (iris scanning biometrics) will increase overall efficacy while further protecting consumers from fraudsters who may attempt access bank accounts illegally through ATMs [7]

2.1. Iris Technology.

The human iris is a thin, colored ring that surrounds the pupil, containing nitricate patterns of furrows, crypts, and filaments. These patterns are unique to each individual and remain constant over time, making them highly suitable for biometric identification purposes. Iris recognition systems utilize specialized cameras to capture high-resolution images of the iris and then extract and store its unique features in a secure database.

The Bank of United of Texas was the first financial institution in the US to introduce iris technology at ATMs for all of these security features. Without a card or word, guests can complete their ATM transactions.

Therefore, neither a card nor biometric authentication are required. Additionally, there is no client annoyance or inconvenience with this authentication process, and they can conduct banking business without carrying an ATM card. Iris surveying calculates the peculiar irascibility pattern and the many collared circles in mortal eyes. Biometry iris identification works by shining IR light on the iris to detect a distinct shape that isn't visible to the eye. The iris finally produces simply a collection of pixels. The 2 authorized persons are quickly identified using iris recognition technology, which rejects false matches.

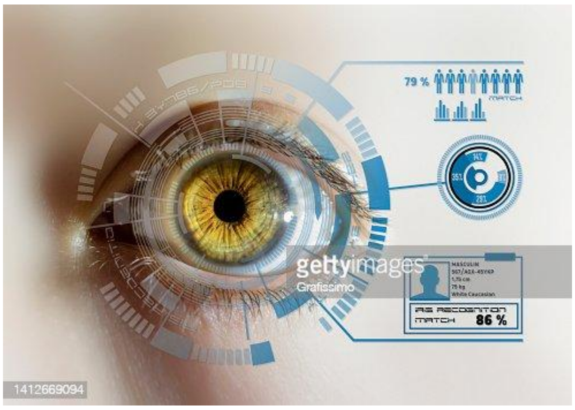
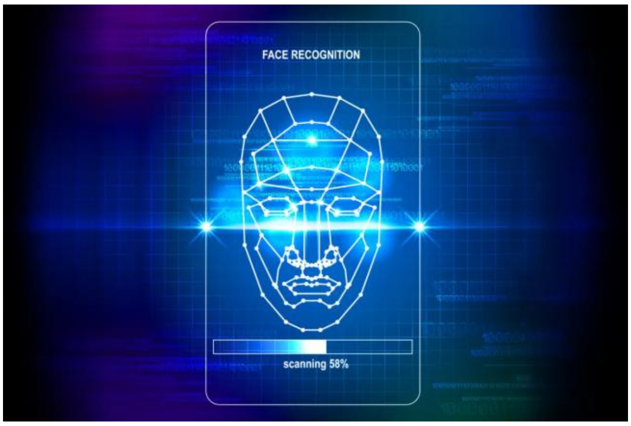


fig. (1). Iris technology.

2.2. Face Recognition Systems.

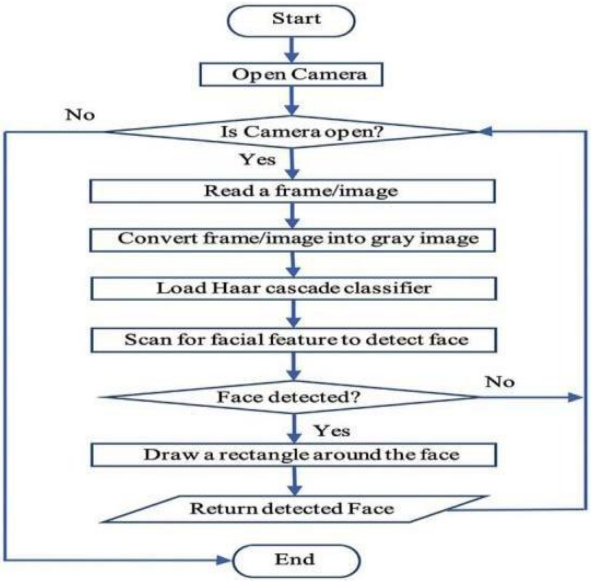
Using a digital image or videotape from a source, this technique is used to confirm the identity of a person. In this study, the ATM system uses face recognition technology for verification. There are two groups of comparisons for facial recognition. The system makes a yes or no determination after comparing the provided existing with who that existent claims to be in the initial step of verification.[3]

Identifying this system and comparing the provided image to every other image in the database's list of matches is the alternative step. A face recognition system uses technology to analyze the distinctive characteristics of the human face, such as its pattern, location, and form. The FRS technology is extremely sophisticated and heavily dependent on software. For each type of biometric in the biometric system, the analytical structure is set up using PCA methods. Face recognition thresholds are used when a photograph is used to try to identify a person in it. This can be accomplished in a variety of ways, such as through movement, skin tone, facial expressions, blurred mortal shapes, etc.



Fig(2). Face recognition system.

2.3. How Do They Work?


Start
Open Camera
Is Camera open?
No
Yes
Read a frame/image
Convert frame/image into gray image
Load Haar cascade classifier
Scan for facial feature to detect face
Face detected?
No
Yes
Draw a rectangle around the face
Return detected Face
End

Fig(3). Working of FRS in an ATM.

The FR system that checks faces maintains a database of guests' faces and iris. Face recognition comes in three different flavors.

- Face- sensor.
- Eye- localizer.
- Face- recognizer.
- The Face-sensor.

In the digital image of the customer to be honored, the face sensor recognizes the face, reduces any undesired, unrelated to the face facial area, and retires any non-facial region.

- The Eye-localizer
  This stage allows it to immediately determine the position of the face by observing the location of the eyes.
- Face Recognition
  It will review and locate the proper match in the database.

3. PROPOSE SYSTEM

The proposed system will incorporate the use of an iris scanning device to verify the identity of customers and grant access to their accounts. The system will also include a secure authentication process, utilizing advanced security measures such as encryption, to protect customer information. In addition, the system will provide customers with an improved level of convenience and security, while also providing banks with a more reliable and cost-effective security solution.

The proposed system will require customers to register their iris scans with the bank before accessing the ATM. This will be done in order to build a database of customer iris scans, which can then be used to verify the customer's identity. Once the customer has registered their iris scans, they will be able to access the ATM by simply looking into the iris scanning device. The device will then verify the customer's identity and grant access to their account.

3.1.Creating database

With the aid of MySQL's Structured Query Language (SQL), we are firstbuilding a database. The database contains information about the customers, including name, account,number,address,contact,informationetc. Additionally, there are IRIS scanning details in the form of a complex integer that contains the IRISpattern's original breadth and phase data. Furthermore, using an XLSX or CSV train, we are turning the database into a Python data set. We train and evaluate those data sets after transforming them into datasets in order to get the highest level of delicacy. Therefore, the registered customer must be present for the trade in order for the sale to take place. The system will request the IRIS for verification after the Leg (Personal Identification Number) has been validated. The smoker or customer must step in front of the scanner, and once their IRIS has been validated against the database, The sale will proceed in the following manner.

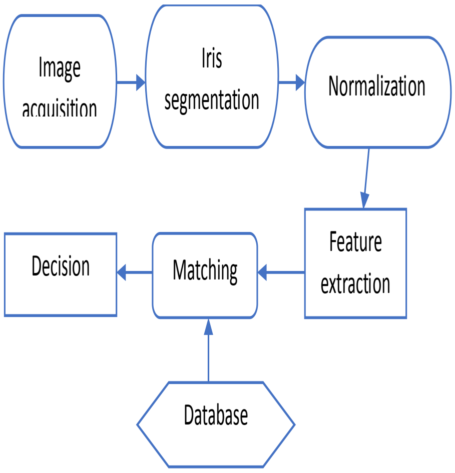


Fig (4). Data base

3.2. Iris Scan Biometric Technology

The human iris is a thin, colored ring that surrounds the pupil, containing intricate patterns of furrows, crypts, and filaments. These patterns are unique to each individual and remain constant over time, making them highly suitable for biometric identification purposes. Iris recognition systems utilize specialized cameras to capture high-resolution images of the iris and then extract and store its unique features in a secure database.

3.3. Image Acquisition

The first step in iris recognition is image acquisition. An infrared camera captures a digital image of the user's iris. Infrared light is used to illuminate the iris, making it easier to capture fine details and reducing the impact of ambient light on the image quality.

3.4.Preprocessing

The acquired iris image undergoes various preprocessing techniques to enhance its quality and eliminate noise. Preprocessing includes image normalization, segmentation, and noise reduction. Normalization ensures that the captured image is of a standard size and format, enabling consistent feature extraction.

3.5. Feature Extraction

Key features, such as ridge patterns, furrows, and crypts, are extracted from the iris image to create a unique biometric template. Feature extraction algorithms use mathematical techniques to encode the extracted patterns and create a compact representation of the iris, suitable for storage and matching.

3.6. Template Storage

The extracted template is encrypted and securely stored in a database. Since biometric data is sensitive and private It is crucial to use robust encryption and access control mechanisms to protect the data from unauthorized access and potential breaches.

3.7. Matching

During authentication, a new iris image is captured, and its features are extracted to create a template. The system then compares this template with the stored templates in the database to determine a match. Various matching algorithms, such as Hamming distance or pattern recognition methods, are employed to find the most similar templates.[3][4]

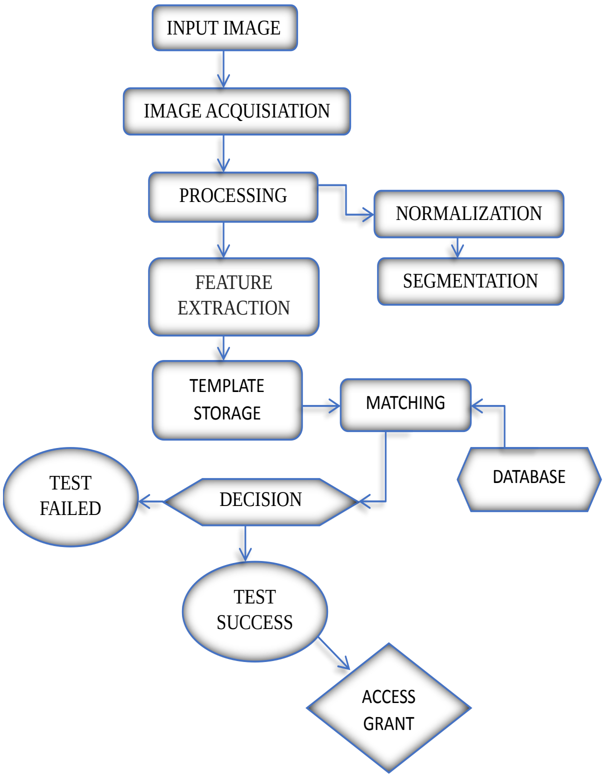


Fig (5). Flow chart of the system.

4. IMPLEMENTATION AND EVALUATION

To evaluate the effectiveness of iris scan biometrics for ATM security, a pilot program was conducted in collaboration with a leading bank. During the pilot phase, selected ATM machines were equipped with iris scanning technology, while others continued to use conventional security measures as a control group. The following metrics were analyzed:

4.1. Accuracy

The accuracy of the iris scan biometric system was measured by calculating false acceptance and false rejection rates. False acceptance occurs when the system incorrectly identifies an unauthorized user as an authorized user, while false rejection happens when the system fails to recognize an authorized user.

4.2. User Experience

User feedback and acceptance of the new authentication method were gathered through surveys and interviews. Participants were asked about their comfort level with the technology, ease of use, and overall satisfaction with the authentication process.

4.3. Security Incidents

The number of ATM-related fraud incidents, including card skimming and PIN theft, was monitored and compared between the test and control groups. Any noticeable decrease in security incidents in the test group would indicate the effectiveness of the iris scan biometric technology in preventing unauthorized access and fraudulent activities.

5. BENEFITS

The use of Iris Scan Biometrics for ATM machines offers a number of benefits, including the following:

1. Increased security – Iris scanning is much more accurate and reliable than other forms of biometric authentication. By using iris scans to verify users' identities, banks can ensure that only authorized individuals are able to access their accounts.
2. Faster transactions – With iris scan biometrics, authentication time is decreased significantly when compared with traditional methods such as entering a PIN or signing a receipt. This makes banking processes quicker and easier for customers which in turn reduces customer wait times at ATMs.
3. Reduced fraud – Due to its high accuracy and reliability, identity theft via an ATM becomes virtually impossible if the machine is equipped with an appropriate iris scanner so only genuine account holders gain access.
4. Increased convenience– Using an iris code instead of other means (PINs) provides consumers with added convenience since they do not need remember any additional information while trying to withdraw money from the ATM machine
5. The iris-id is set up as a unique identification for each person; it can only be used by the user.
6. It can be applied to lessen dishonest attempts.
7. provide a structure for a secure life
8. use the iris verification Link to prevent unauthorized access.
9. Quick and Reliable Prophecy.

6.FUTURE WORK

In order to make iris scan biometric technology more reliable and effective, there is still some work that needs to be done. Firstly, the cost of the technology needs to be reduced in order to make it more accessible to more people. Secondly, the accuracy of the technology needs to be improved in order to reduce the risk of false positives and false negatives. Thirdly, the security of the technology needs to be improved in order to reduce the risk of spoofing attacks. Finally, the technology needs to be made more user-friendly in order to make it easier to use for customers.

The IRIS Recognition and GSM modules that were built as redundant security in the ATM Terminal system's design provided identification and authentication using the information of bank account owners. The security futures were improved primarily for the stability under the obligation of the owner recognition. A new biometric technology supported by this system also includes verification styles that permit the proprietor to input the Aadhar id. The entire system is built using integrated system technology, making it safer, more dependable, and simpler to use. It's a viable strategy because it's simple to operate and maintain at a lesser cost.

7.CONCLUSION

In conclusion, iris scan biometric technology is a reliable and effective way to enhance the security of ATMs. However, there is still some work that needs to be done in order to make the technology more reliable and user-friendly. With the right improvements, the technology could become a much more secure and convenient way of authentication for ATM customers.

REFERENCES

1. Penev and Atick, Joseph J. “Local Feature Analysis: A General Statistical Theory for ject Representation.” Network: Computation in Neural Systems, Vol. 7, No. 3, pp. 477- 500,1996.
2. M. Feurer, A. Klein, K. Eggensperger, J. Springenberg, M. Blum, and F. Hutter, “Efficient and Robust Automated Machine Learning,” Advances in Neural Information Processing Systems 28, pp. 2944–2952, 2015
3. Gross, Ralph, Shi, Jianbo, and Cohn, Jeffrey F.“Quo vadis Face Recognition.” Third Workshop on Empirical Evaluation Methods in Computer Vision. Kauai:
4. December 2001
5. “Evaluating Facial Recognition Technology for Drug Control Applications.” ONDCP International Counterdrug Technology
6. FindBiometrics Global Identity Management.
7. G. Reena Jebaline, S. Gomathi, CSE department, Francis xavier engineering college, tirunelveli, Tamil Nadu,”A novel method to enhance the security of ATM by using biometrics”/International conference on circuit, power and computing technologies, 2015.
8. T. Ahonen, B. Hadid and M. Pietikainen, Face Description with Local Binary Patterns:Application to Face Recognition, in IEEE Transactions on Pattern Analysis and MachineIntelligence, vol. 28, pp. 2037-2041, Dec.2006.