Atm Security System Using Face Recognition In OpenCV

Mrs.Jerrin Simla A, Deepika S,Divya A,Nandhana S S
Mrs.Jerrin Simla A,AP/CSE Anna University, Panimalar Institute ofTechnology
Deepika S, Anna University, Panimalar Institute of Technology Divya A,Anna University, Panimalar Institute of Technology Nandhana SS, Anna University, Panimalar Institute of Technology

Abstract:
Automated Teller Machine (ATM) is an electronic device installed by the bank that allowscustomers to perform financial transactions with the bank from any location and at any time. ATM is used by the banks to perform banking tasks like withdrawal of money, transferring of money, to get information about a user's bank account without the need to visit the bank. ATM's are widely used in our daily lives due to their convenience, wide spread availability and time independent facilities. The account holder can access the ATM through ATM card which is unique for each customer and carries his identity. As there is increase in the number of ATM's, there is also increase in the fraudulent activities happening in the ATM. The main objective of this project is to increase the security of the ATM. The current method uses PIN for security. The proposed method uses face as a key incorporated with current method. The advantages can be found as that the face-id is unique for everybody and it cannot be used by anybody other than the exact user. Face recognition technology helps the machine to identify each and every user uniquely which uses face as a key. This completely reduces the chances of fraud due to theft and duplicity of the ATM cards. For the implementation of the face-id scan, the machine learning algorithm (Haar Cacade algorithm) is used.

Keywords- ATM, Face-id, Haar Cascade algorithm, Machine Learning, face recognition, face detection

1.INTRODUCTION

Face recognition has been used as an authentication processespecially in computer security related activities, such as building access security, criminal identification, as well as user identification in mobile devices. However, this concept of authentication also have some drawbacks. It's known that the user face is not a unique identifier and it is ahuge vulnerability for any access control system based on face recognition. We have made our project to improve the security by including face recognition with the help ofMachine Learning Algorithm. The ATM machines used to withdraw money are introduced. But there are many unauthorized access was attempted in the ATM by knowing the password of user and withdrawing money without the knowledge of them. This leads to a serious problem, to rectify this problem we have introduced this project to provide a safetymechanism for ATM. The unauthorized access could be found only after the transaction is completely done or whenthe amount gets debited from the account of the authorized user. So this project deals with the method to prevent the ATM security threat related to unauthorized users by allowing access to the user only after the confirmation of the user identity by using camera that is inbuilt on the ATMMachine. . When the people try to take money from the ATM, ATM's will use face detection and face recognition to check it with the account holder image in the bank database. If the image matches the user, the system will permit to continue the transaction of money.

BIOMETRIC AUTHENTICATION:

An authentication system usually works by comparing the input data given with the user information stored in the database. In current trend they are referred as passwords. For example, in a facial recognition system, different facial features are processed and converted into numerical data. These data are stored in a database. When a persontries to log in to a system it first tries to collect the user's face and compare with the numerical data accumulated in the database.

Face Authentication:

It is a biometric that uses the body feature. In this type, face and head of a person are considered as facial biometric pattern**.** It gathers a set of required unique biometric data of each person related to their face to identify, verify and authenticate a person into the system.

Fingerprint Authentication:

Fingerprints are a unique feature that everyone has. Fingerprint is used as a biometrics to both authenticate and identify the user. Fingerprint is widely distributed, which is cost-effective, easy to use, and are hard to fake making them a secure and useful tool for authentication process.

Iris Authentication:

Iris Recognition is biometric method of identifying people based on iris pattern surrounding the pupil of the eyewhich is unique to every individual, making it an ideal form of biometric verification or identification.

EXISTING SYSTEM:

Transactions are validated by the card and PIN-based system for the existing ATM system. After that, the bank customers are given access to cash withdrawals and deposits, account transfers, balance inquiries, etc. Every ATM user's entered PIN is compared to the authorization PIN that is stored in the database of the system. The system verifies the user and grants access to all ATM services in the event that there is a match. On the other hand, if there is a mismatch, the user authentication process fails, and the user is given two more chances to enter the correct PIN. The card is blocked if an incorrect PIN is entered for the third time. However, the current system is somewhat degrading because it requires an ATM card for the Recognition and Identification process as well as a PIN. The user may forget their PIN number in certain circumstances.

DEMERITS OF EXISTING SYSTEM:

Anybody who knows the PIN can easily use the other user's card for the transaction purpose without the user's knowledge. Since the PIN is static and standard which is easy to prone for many crime activities, through hacking. Scanning the magnetic strip of the ATM card will lead to the exposure of the complete details of the card. Therefore, this causes the duplication of the user's cards.

PROPOSED SYSTEM:

Facial recognition as an authentication method is used in our proposed system to improve the ATM's security system.

- The facial acknowledgment process utilizes Haar Cascade Algorithm to identify and perceive the face.
- Using a webcam, the Haar Cascade facial recognition process can be carried out successfully from

more than 200centimeters away.

- The type of detection can still detect the face when it is oriented to the side up to about 15 degrees, despite the fact that it only works on straight faces (frontal faces). As a result, it can get around the problem with the current system.

SYSTEM ARCHITECTURE:

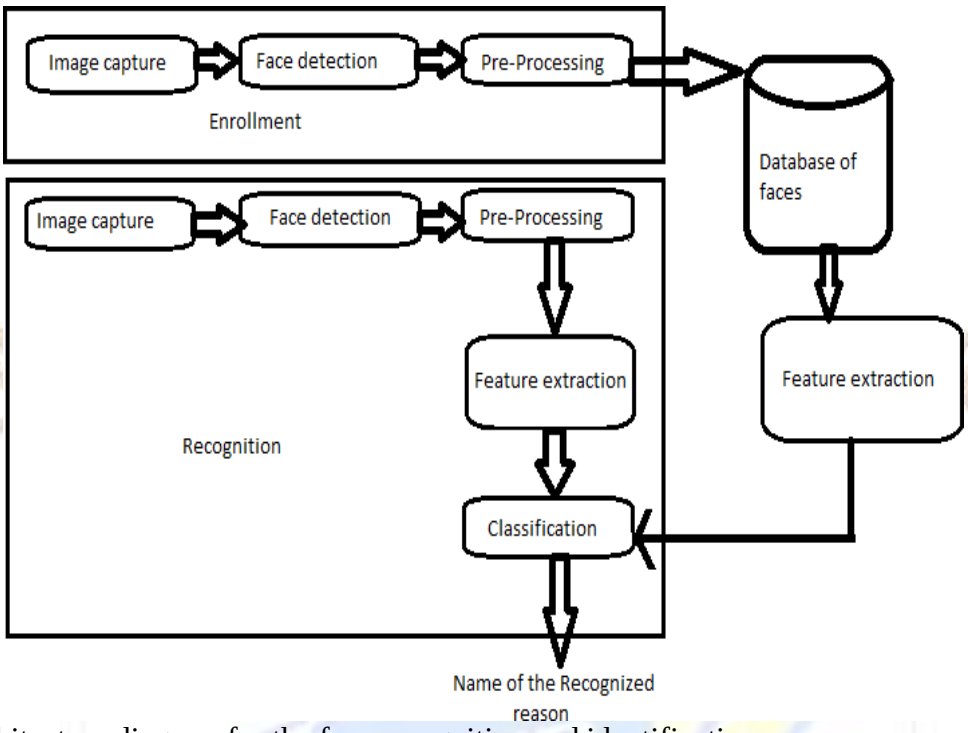

FIGURE 1. Architecture diagram for the face recognition and identification

Face recognition commonly undergoes through four phases; they are: face detection, face alignment, feature extraction,and finally face recognition.
Facial Detection: Find one or more faces in the image and mark with a bounding box. Face Alignment: Normalize faces to database like geometry and photometry.
Feature Extraction: Takes features from the face that can be used in the recognition task.
Facial Recognition: Perform face matching with one or more known faces in a ready-made database. HAAR CASCADE ALGORITHM:
The method begins with the Haar feature phase where face recognition is performed by utilizing a higher differentiator between 'face' and 'not face'. On some parts of the image, asdepicted in Figure, there are two types of rectangular features: white (bright) and black (dark). Based on these rectangles, the Haar-like feature can be calculated. The following formula shows how the difference between the sum of the pixels in the dark area and the sum of the pixels in the bright area resultsin the Haar-like feature:

$$F(Haar)= \sum F_{White}- \sum F_{Black} \quad (1)$$

where,

$\sum F_{Black}$= summation of the pixels of the dark area

$\sum F_{White}$= summation of the pixels of the bright areaF(Haar)= the Haar-like features

When the Haar-like feature is higher than a certain threshold, it can be said that a face or faces are within the area. Anintegral image technique is used to effectively to filter many faces in the image.

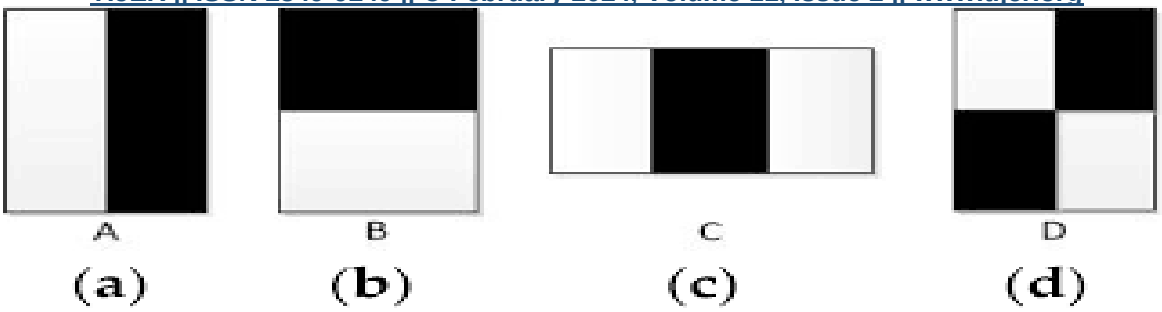

FIGURE 2**.** Four Haar-like feature operators. (**a**) Two-rectangle feature where rectangular regions are horizontally adjacent,(**b**) Two-rectangle feature where rectangular regions are vertically adjacent, (**c**) Three-rectangle feature, (**d**) Four-rectangle feature.

Definition:

The machine learning technique known as Haar Cascading involves drilling a classifier out of a large number of positive and negative photos. Paul Viola and Michael Jones forwarded the algorithm. For object detection, Haar feature-based cascade classifiers are utilized. This classifier pursues AI technique in which an outpouring activity is taught from the photographs to find things in extra photographs. The exercise is finished by showing the classifier both positive and negative images. The characteristics are then extracted from the image. Every characteristic is an individual value, which is acquired by subtracting sum of pixels in white rectangle from the summation of pixels in black rectangle where it recognizes the faces of various people in various settings. Integralimages make it possible to calculate the Haar-like feature of any size in constant time.

FIGURE 3**.** Application of haar cascades

PERFORMANCE ANALYSIS:

TABLE 1. Face Recognition rate for various algorithms

ALGORITHM	LDA	PCA	SVM with binary	CAMSHIFT	HAAR-CASCADE
OGNITIONRATE	85%	88%	91.2%	93%	95%

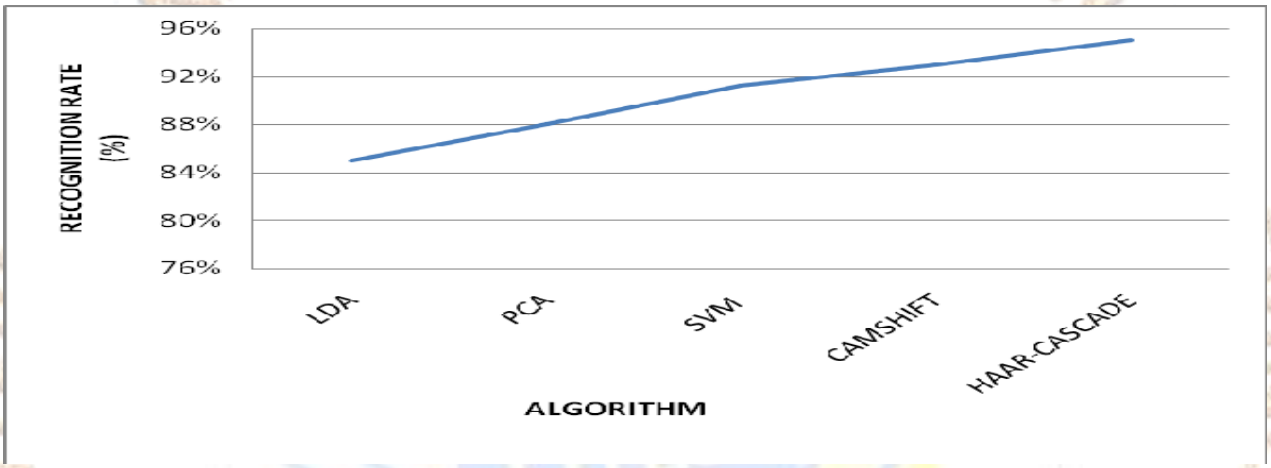

FIGURE 4. Performance Rate for different algorithms

CONCLUSION:

We thus have developed an ATM model that is more reliable in providing security by using facial recognition software. ATM model which provides security by using Facial verification software adding up facial recognition systems to the identity confirmation process used in ATMs can be used to reduce forced transactions. As facial recognition technique seems more challenging as comparedto other biometrics system, thus more efficient algorithm should be involved .On summing up, the method what we proposed is better in increasing the security feature of the ATM system. The main goal of our paper is to incorporate the facial recognition feature along with the existing method for the betterment of the user. The Haar Cascade algorithm used here is used for comparing the face of the user with the face stored in the database. Machine learning is used to train the face recognizer. The Adaboost face recognition algorithm has the success rate of 75% but the algorithm produces the success rate of 95%. The future scopes of this method are that to use the high-quality durable cameras.

REFERENCES

1. J. Lei, Q. Pei, Y. Wang, W. Sun and X. Liu, "PrivFace: Fast Privacy-Preserving Face Authentication With Revocable and Reusable Biometric Credentials," in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3101-3112, 1 Sept.-Oct. 2022, doi: 10.1109/TDSC.2021.3083970.
2. S. Shavetov and V. Sivtsov, "Access Control System Based on Face Recognition," 2020 7th International Conference on Control, Decision and Information Technologies (CoDIT), Prague, Czech Republic, 2020, pp. 952-956, doi: 10.1109/CoDIT49905.2020.9263894.
3. D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2017, pp. 342-347, doi: 10.1109/ICITISEE.2017.8285524.
4. G. -S. Hsu and C. -H. Tang, "Dual-View Normalization for Face Recognition," in IEEE Access, vol. 8, pp. 147765- 147775, 2020, doi: 10.1109/ACCESS.2020.3014877.
5. M. Mei, J. Huang and W. Xiong, "A Discriminant Subspace Learning Based Face Recognition Method," in IEEE Access, vol. 6, pp. 13050-13056, 2018, doi:10.1109/ACCESS.2017.2773653.
6. B. Knyazev, R. Shvetsov, N. Efremova and A. Kuharenko, "Leveraging Large Face Recognition Data for Emotion Classification," 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, China, 2018, pp. 692-696, doi: 10.1109/FG.2018.00109.
7. Y. Lin and H. Xie, "Face Gender Recognition based on Face Recognition Feature Vectors," 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE), Dalian, China, 2020, pp. 162-166, doi:10.1109/ICISCAE51034.2020.9236905.
8. W. -Y. Chen, M. -M. Li, J. -S. Lin and S. -C. Ni, "Massive Face Recognition Algorithm Based on the Hadoop Technique," 2016 International Symposium on Computer, Consumer and Control (IS3C), Xi'an, China, 2016, pp. 789- 792, doi: 10.1109/IS3C.2016.201.
9. L. Fu and X. Shao, "Reseach and Implementation of Face Detection, Tracking and Recognition Based on Video," 2020 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS),Vientiane, Laos, 2020, pp. 914-917, doi:10.1109/ICITBS49701.2020.00202.
10. G. George, R. Boben, B. Radhakrishnan and L. P. Suresh, "Face recognition on surgically altered faces using principal component analysis," 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT), Kollam, India, 2017, pp. 1-6, doi: 10.1109/ICCPCT.2017.8074324.
11. M. Kumar, R. Gupta, D. Kumar and K. S. Raju, "UMLBP-A Novel Approach for Face Recognition System using OPENCV," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2018, pp. 448-452, doi: 10.1109/ICRITO.2018.8748765.
12. K. R. Sreelakshmi, R. Anitha and K. R. Rebitha, "Multiple media based face recognition in unconstrained environments using eigenfaces," 2016 International Conference on Next Generation Intelligent Systems (ICNGIS), Kottayam, India, 2016, pp. 1-6, doi: 10.1109/ICNGIS.2016.7854053.
13. J. Li and D. Zhang, "Face gesture recognition based on clustering algorithm," 2019 Chinese Control And Decision Conference (CCDC), Nanchang, China, 2019, pp. 2008- 2012, doi: 10.1109/CCDC.2019.8833105.
14. J. J. Patoliya and M. M. Desai, "Face detection based ATM security system using embedded Linux platform," 2017 2nd International Conference for Convergence in Technology (I2CT), Mumbai, India, 2017, pp. 74-78, doi: 10.1109/I2CT.2017.8226097.
15. S. R. Dubey and S. Mukherjee, "A Multi-Face Challenging Dataset for Robust Face Recognition," 2018 15th International Conference on Control, Automation, Robotics and Vision (ICARCV), Singapore, 2018, pp. 168- 173, doi: 10.1109/ICARCV.2018.8581283.