Development of Facial Detection System for Security Purpose Using Machine Learning

M Srinivasa Sesha Sai [1], *Ranjith Kumar Gatla*[2*], Ch Vijaya Lakshmi[3], Addagatla Prashanth[4], D S Naga Malleswara Rao[5] and *Anitha Gatla*[6]

[1]Department of Information Technology, KKR & KSR Institute of Technology and Sciences, Adhara Pradesh, India
[2]Department of Computer Science and Engineering (Data Science), Institute of Aeronautical Engineering, Telangana, India
[3]Department of Electrical and Electronics Engineering, PSCMR College of Engineering and Technology, Andhra Pradesh, India
[4]Department of Computer Science and Engineering (AI & ML), Institute of Aeronautical Engineering, Telangana, India
[5]Department of Electrical and Electronics Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, India
[6]Department of Information Technology, Institute of Aeronautical Engineering, Telangana, India

Abstract. Face recognition is a technique for recognizing or authenticating someone's identification based on a quick glance at their face. After that, this application can employ computer vision to discover a potential face inside its stream. Facial recognition is been used in a various routine operation, from mobile phone unlocking to ATMs. Individuals and businesses use automated teller machines (ATMs) to conduct a spectrum of financial activities, includes banking, for both individuals and organizations. There seem to be ATMs everywhere, such as in restaurants, supermarkets, convenience stores, malls, schools, gas stations, hotels, workplaces, banking facilities, airports, entertainment venues, transportation facilities, and numerous other locations. Consumers often have access to ATMs on a continuous basis, allowing them to conduct financial transactions at any time of day or week. In this project, face recognition and a tiered security mechanism are used. Machine learning, OpenCV, and Python are used to implement face recognition. In this situation, Face embeddings are used to extract characteristics from the face. A neural network uses a picture of a person's face as input and generates vectors representing the most important face attributes. This vector is called an We refer to it as face embedding since it occurs in machine learning. The project aims to reduce the risks associated with remote ATMs and the problems associated with fraudulent transactions, such as misusing someone else's card to withdraw money. Therefore, to overcome this problem, we developed a solution using ML to limit card use to just authorized individuals who can be recognized using face recognition software.

1 Introduction

Face recognition is a technique which recognizes and validates a person's face in digital pictures or video frame. Without any effort, a human can recognize the face. For us, it is a simple task, but for a computer, it is a challenging one. Low resolution, occlusion, lighting variances, and other issues add to the complexity. These parameters have a significant impact on the computer's ability to detect faces more accurately. Face recognition is a technique that identifies or authenticates a person by using an image, video, or other audio-visual aspect of his face. Typically, this identification is used to get access to an application, system, or service.

Body measurements are used in this sort of biometric identification. In this instance, we use a person's head and face to confirm their identification by using their facial biometric pattern and data. In order to identify a person, the approach captures a variety of distinct biometric data related to their face and facial expression. identify, verify, and/or authenticate them. Many individuals are already familiar of face recognition technology thanks to Biometric Authentication, which is used to unlock smartphones. Face recognition typically does not require a huge number of photos to identify a person; instead, it only recognizes one person as the device's sole owner and denies access to everyone else. [2].

Face detection encompasses much more than facial recognition. The ability of a technology to recognize a person's face in a picture or video is referred to as face detection. Facial recognition is an example of a face detection application. Autofocus cameras are capable of face detection. Face recognition, on the other hand, is an essential face detection application. A type of biometric technology called face recognition goes beyond merely recognizing a person's face. It truly wants to know who it is. A digital image of a person's face is taken by a computer programmer (typically from a video frame), and it is compared to images that have been recorded in a database of historical data. Despite its limitations, facial recognition technology can identify whether a person's face has a good chance of matching one in the database.

There are many uses for face recognition. Phones and particular apps can already be opened and unlocked using face recognition. Face recognition is also a part of biometrics. The way individuals conduct business is fast

evolving in the information era. More and more jobs are being done online instead of on paper or in person. The requirement for prompt and accurate user identification and verification increases along with the volume of electronic transactions. In computers, bank accounts, and buildings, PINs are used for identification and security purposes. If the PIN is entered correctly, transactions can be completed successfully, but the PIN user is not verified. [3]

2 Literature Survey

Using the Haar rectangle as a feature and the AdaBoost learning technique, the system chooses appropriate classifiers for face detection. When it extracts facial data from a movie, it labels the face data with the system time and stores it to a database. The outcomes show that this system can successfully identify human faces in a range of circumstances and save the detection data into a database after adding a time label. It simplifies video surveillance search and retrieval. [1] According to the authors, a fingerprint shield ATM is an idea that integrates biometric authentication by using fingerprints with a smart card along with database server. Because of the unique properties of each of the minutiae, fingerprint technology is a valuable identification tool. Despite the fact that users must add 1.5 seconds to their authentication time for fingerprint verification, security is significantly improved and assured. [2], With fingerprint authentication, it will no longer be possible to steal someone else's PIN or skim an ATM card to access their bank account. Additionally, the public is not often aware of the technologies used to steal someone else's fingerprint. [2]
The system can move on to the next stage of the transaction after the primary security check, the iris scanner. A fingerprint sensor included inside the ATM card serves as the supplementary security check for the system. The transaction operation is only successful if the input data from the cardholder matches the database. It is appropriate for usage since it also consumes less energy. The suggested updated method is practical and economical when compared to other current ATM categorization and validation methods. The RFID card has a fingerprint sensor from the FIM3030 series connected, along with small power source. This serves as our first line of defense.
We propose using horizontal and vertical IPC to precisely pinpoint the facial area (Integral Projection Curves). This study looks into the role of essential facial features including the nose and eyes. The distinctive features are developed using a time-saving technique based on PCA and EFM (Event-Driven Modelling) (Enhanced Fisher Model), and then sent to the classification stage using SVM and Distance Measurements as two different techniques (Support Vector Machine). [8]
Both posture estimation and face alignment are required for the FRS pre-processing stage. Face alignment seeks to automatically locate the human face in the proper spot-on a given face picture. We use a number of processing techniques, such as fusion (Mean, Max), classification, and regression to determine the role and impact of the patch nose + eyes in our system (SVM, distance measurement). Face detection is accomplished using IPC. To choose the patches of interest regions, we used face image subdivision. The results revealed that expression alterations have little effect on the nose and eyes patch. Combining the Mean and Max methods allows for the merging of 2D and 3D data. [8].
you should check your figure captions carefully and remove any reference to colour in the illustration and text. In addition, some colour figures will degrade or suffer loss of information when converted to black and white, and this should be taken into account when preparing them.

3 Proposed Method

Face recognition is an algorithm for identifying individuals from their photographs that have been collected in a metadata collection. Face recognition has long been a major priority, despite the fact that alternative methods of identifying are more exact of research due to its non-intrusive nature and the ease with which people can identify themselves.
Facial recognition works by comparing photographs of people on a watch list to those passing via specific cameras. The images on the watch lists might be of anyone, including persons who have not been suspected of crime, and could have originated from anywhere, including our social media accounts. Facial technology systems operate in a number of ways, but they all provide the same function:
When a facial recognition system first sees a face, it registers it and associates it with an identity so that it can be stored in the system. The variant in which the user is authorized before being registered, the incoming data from the camera is compared to the data already present in the database in this process, which is also known as digital onboarding with facial recognition. The system uses the user's credentials to enable access if his face matches a previously captured identification.

Facial technology systems operate in a number of ways, but they all follow the same basic principles:

Step 1: Face recognition

The camera is used to recognize or locate a face, either in an alone or in a crowd. The subject of the shot may be looking directly ahead or in profile.

Step 2: Examine your face

The face is photographed and assessed after that. The majority of facial recognition technology uses 2D photographs rather than 3D images since it is simpler to match a 2D image with available images or those in a database. The software examines your face. Basic factors include the depth of your eye sockets, the separation between your eye brows, the curvature of your cheekbones, and the shape of your lips, ears, and chin. The goal is to determine which face features help you recognize yourself.

Step 3: Extracting info from the image

The face seize technique transforms analogue facts (a face) into a hard and fast of virtual facts primarily based totally on a person's facial characteristics (facts). A mathematical formula is used to examine your face. Face print refers to the numerical code. Face prints are similar to thumbprints in that everyone has a unique set.

Step 4: Find a mate.

Then your face print is compared to a database of people's faces. Your face print is in comparison to a photograph in a facial popularity database to look in the event that they match.

3.1 Face recognition in ATM

The method of withdrawing cash from an ATM is well-known and appears to be straightforward. This procedure, on the other hand, is a hybrid of computer operations, technology, and research that has been tweaked and enhanced through time to provide clients with a flawless experience. You must first identify yourself at the ATM before withdrawing money. Previously, this process involved inserting the card and inputting the pin connected with it; however, as we'll see later, emerging methods like as face biometrics are replacing this way of identification at ATMs. With the advancements in banking industry's financial infrastructure, most clients prefer to conduct their banking activities through Automated Teller Machines and Internet portals. Our principal goal is to create a pc imaginative and prescient gadget that makes use of the embedded ATM digital cam to understand faces. The ATM card is swiped first. A webcam established at the ATM records a stay photograph, this is as compared to photograph saved inside the database.

The transaction can move forward if it matches.

In a handful of seconds after recognition, the following processes occur:

- The availability of funds is checked, and if it is, authorization is granted.
- Money trays are placed in strategic locations and are linked to the ATM system.
- The required invoices are chosen one by one by an intelligent gadget.
- An optical sensor is used to test the quantity and legitimacy of the invoices.
- A slot opens, and the buyer is given the specified amount of cash.
- Before the procedure is complete and the user is logged out, he is asked if he wants an operation receipt.

But without the first, none of these stages would have been possible: right identity of the purchaser asking for a withdrawal from his account. Face biometric identification has revolutionized and optimized this technique.

Face biometrics era is without problems included, into normal ATM software, permitting for identification and get right of entry to verification. At ATMs, facial biometrics identification is used.

- The customer approaches the cash machine.
- Then face the camera present near the machine.
- The system verifies and validates the client's identification.
- The client's system, accounts, and credit cards are all given access.
- The customer can withdraw cash or do duties linked to the ATM's numerous services.

Face biometrics may be readily integrated into standard ATM software to verify identification and access. With the use of Machine Learning, we attempted to strengthen security by incorporating face recognition into the system. ATM machines, which are utilized debit and credit cards to withdraw money have been introduced, installed, and widely used in modern society. However, numerous unauthorized ATM access attempts are made using the cardholder's password and withdrawing money without the cardholder's knowledge, cardholder in addition to the financial institution must be concerned. To address this issue, we've created this project to give an ATM safety mechanism. Unauthorized access is discovered only after the transaction has been completed or the sum has been deducted from the authorized user's account. As a result, this project focuses on a strategy for preventing ATM security threats posed by unauthorized users by providing access only after a camera attached on the ATM machine has confirmed the user's identification. When consumers try to withdraw money from an ATM, the machine uses face detection and recognition to compare their image to the image of the bank's account holder.

People currently utilize Automated Teller Machines extensively. However, carrying their ATM card everywhere is difficult; clients can also additionally misplace their Passcode or ATM card. The ATM card can be damaged, preventing consumers from accessing their funds. Biometric authentication is preferred over PIN and ATM card authentication in our opinion. Face ID is given top priority because the combination of these biometrics has shown to be the most effective identifying and verification method. When ATM machines are installed, there is a risk that they will be accessed by unauthorized individuals who have a valid authentication code. The new photograph is used to train the model for even greater precision if the user is sincere. Using OpenCV to analyses the picture, this system searches for faces using the Haar Cascade Classifier. GLCM characteristics are used to recognize faces.

The work in this paper, proposed facial recognition ATM and is described with the following steps:

(i) Block Diagram of Proposed Method
(ii)Process of Face Recognition
(iii)Algorithms and Process in Proposed Method

3.2 Block diagram of proposed method

From the survey, it is understandable that theft and replication of ATM cards are possible, leading in fraud. A user can undertake a number of banking transactions, which includes cash withdrawal and transfer of money, with an ATM. An unauthorized individual can simply access the account if the bank card is stolen and the number is known. To prevent this problem, we use face recognition system in ATM and to overcome fraudulent transaction like misusing others card to withdraw money and etc. This reduces the possibility of ATM card theft and duplication resulting in fraud and also sends alert through Gmail. We use a Haar cascade, GLCM feature, and a neural network to perform this face recognition. The block diagram of the proposed method is shown in Fig. 1

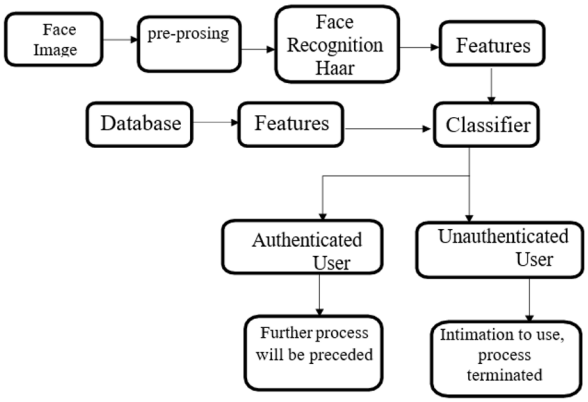

Fig 1. Block Diagram of proposed method

3.3 UML diagram of proposed method

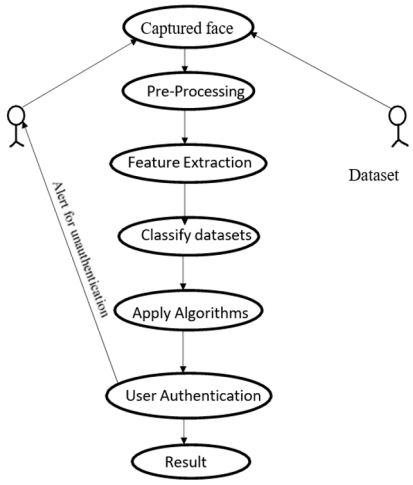

Fig 2. UML diagram for proposed method

To better understand, maintain, or document information about a system, a UML diagram shown in Fig.2 is a visual depiction of the system's major participants, roles, activities, artefacts, or classes. A system's architecture is graphically represented using UML. architectural blueprints that include actors, business processes, and reusable software components.

3.4 Activity diagram

A behavioural diagram that shows the behaviour of a system is called an activity diagram which is shown Fig.3 An activity diagram shows the control flow from beginning to end while emphasizing the many decision-making pathways that are available over the course of the activity. As a series of actions, an activity diagram depicts business and software processes

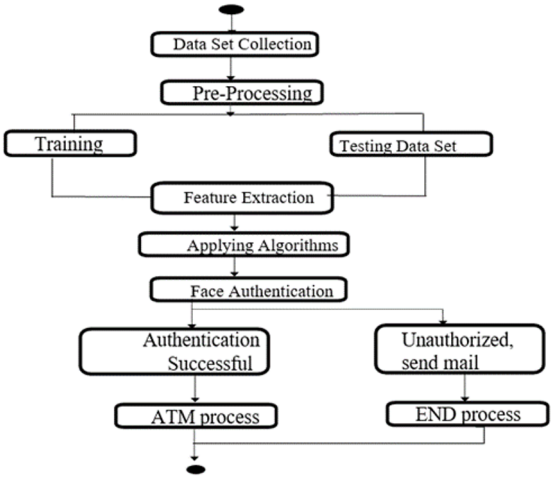

Fig 3 Activity diagram for proposed method

3.5 Algorithms and processes

- Pre-Processing
- Haar Cascade Classifier
- GLCM Feature Extraction
- Face Detection

The simulation is run using OpenCV in the Python IDE. Here datasets are created for each person and then the person face is recognized if the facial features match with any dataset otherwise, the mail has been dispatched, and no more transactions are possible.

- To begin with, we need to create data consisting of different persons face. Each person face is stored in separate dataset.
- We need to create a cascade classifier which will eventually give us the features of the face.
- Utilize OpenCV to work with features file and picture.
- Data of the person can be taken based on number of times the loop runs.
- For face recognition, we need to call the data sets so that, when the person face is given as input then, two cases are possible.
- The person's face is recognized, if it is present in the dataset.
- Sends mail when the person is not present in dataset
- If the persons face is recognized then the further transaction is possible otherwise, no transaction is possible.

The simulation first creates the data of the person in the dataset and then, the face is recognized based on the person's facial traits in the dataset and the person's face image as input

Fig 4 Dataset of first person


Fig 5 Dataset of second person

Fig 6 Dataset of all the records

Dataset is created for the person who is registered, and the number of snapshots depends on the loop that runs of create data. The data set of the first and second persons is shown in Fig.4 and Fig.5 respectively. Fig.6 shows the dataset of all records

The GLCM is built using the Gray-co-matrix function. The frequency with which a pixel with the intensity (Gray-level) value I appears in a given spatial connection to a pixel with the value j is determined by the gray-co-matrix function (GLCM). The pixel immediately to its right (horizontally adjacent) is the default spatial relationship between the two pixels, but you can define different relationships. The overall frequency with which a pixel with the value I appeared in the specified spatial relationship. The output GLCM element is a pixel with the value j in the input picture (i, j). Gray-co-matrix scales the input image since it would take too much processing to create a GLCM for a picture's whole dynamic range. By default, gray-co-matrix decreases the amount.

Prediction models called neural networks are created by modelling the actions of biological neurons. The coining of the term "neural network" was one of the great PR victories of the 20th century. According to the technical description, it surely seems more exciting than "a network of weighted, additive values with nonlinear transfer functions." Contrary to popular belief, neural networks are neither "thinking machines" or "artificial brains." 100 neurons make up a typical artificial neural network.

4 Results and discussion

The system calculates the face embedding of each new face we provide it with and compares it to the ones we currently have. If the face embedding closely resembles any other face embedding in the database. Here as, we already have the face in our dataset the face is matched by showing a green box around face and the name with the person and then the further transaction is possible. When the persons face is passed to the system then if the facial features of the person do not match the facial features in the database, we receive an email warning saying 'There are security breaches and the operation is suspended

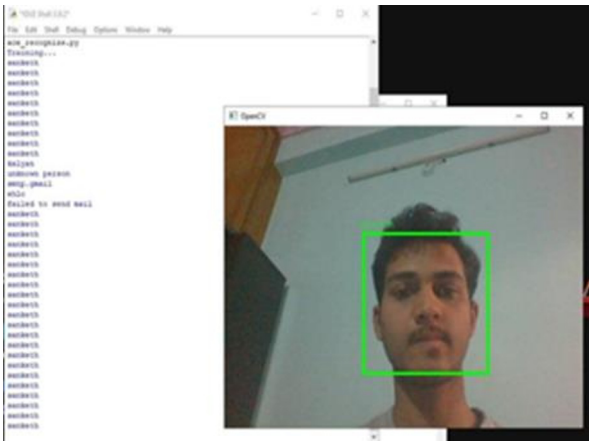
Fig 7 Face Recognition of the person


Fig 8 Mail is sent for unauthorized transaction

5 Conclusion

Face recognition is precise, which takes less time and less storage space. ATM model that provides security by combining facial verification software with Hard-secure authentication is made possible by the identity validation mechanism employed in ATMs, which can dramatically lower forced transactions, reduces the risk involved in ATM machines that were installed in remote area, also the issue related to fraudulent transaction like misusing others card to withdraw money and etc. Therefore, in order to address these issues, we have created a solution that will use ML & AI to limit transaction access to just those people who are permitted and who can be identified by a facial recognition algorithm

References

1. Banerjee, S. Mookherjee, S. Saha, S. Ganguli, S. Kundu and D. Chakravarti, "Advanced ATM System Using Iris Scanner," p.p 1-3 Doi: 10.1109/OPTRONIX.2019.8862388
2. Christiawan, Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar, "Finger Shield ATM – ATM Security System using Fingerprint Authentication" Doi: 10.1109/ISESD.2018.8605473
3. Indranil Banerjee, Sjivangam Mookherjee, Sayantan Saha, Souradeep Ganguli, Debduhita Chakravarti," Advanced ATM System Using Iris Scanner" 2019 International Conference on Opto-Electronics and Applied Optics (Optronix), Kolkata, India. Doi: 10.1109/OPTRONIX.2019.8862388
4. Y. Cheng, W. Shang, L. Zhu and D. Zhang, "Design and implementation of ATM alarm data analysis system," p.p 1-3 Doi: 10.1109/ICIS.2016.7550948
5. C. Porretti, R. Lahaije and D. Kolev, "A New Vision for ATM Security Management: The Security Management Platform," p.p 493-498 Doi: 10.1109/ARES.2016.50
6. H. R. Babaei, O. Molalapata and A. A. Pandor, Face Recognition Application for Automatic Teller Machines (ATM), in ICIKM, 3rd ed. vol.45, pp.211-216, 2012.
7. Chin-Seng Chua, Feng Han, Yeong-Khing Ho," 3D Human Face Recognition Using Point Signature", Doi: 10.1109/AFGR.2000.840640
8. Mebarka Belahcene, Ammar Chouchane, Nadia Mokhtari, "2D and 3D Face Recognition Based on IPC Detection and Patch Of Interest Regions" Doi: 10.1109/ICCVE.2014.7297624
9. Xizhi Hu, Bingyu Huang," Face Detection based on SSD and Cam Shift" Doi: 10.1109/ITAIC49862.2020.9339094
10. Karen Simonyan & Andrew Zisserman + Visual Geometry Group," Very Deep Convolutional Networks for Large-Scale Image Recognition" Department of Engineering Science, University of Oxford, Published as a conference paper at ICLR 2015.
11. Y. Kale, N. Sakhare, M. Varghese, U. Dafe, P. Sawarkar and A. Bagade, "Deploying a Sliding Gate by Utilizing Computer Vision and Machine Learning Techniques," *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, Uttarakhand, India, 2023, pp. 22-26, doi: 10.1109/ICIDCA56705.2023.10099906.
12. F. Romero-Moreno, "AI facial recognition and biometric detection: balancing consumer rights and corporate interests," *2021 International Carnahan Conference on Security Technology (ICCST)*, Hatfield, United Kingdom, 2021, pp. 1-5, doi: 10.1109/ICCST49569.2021.9717403.
13. I. Aydin and N. A. Othman, "A new IoT combined face detection of people by using computer vision for security application," *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, Malatya, Turkey, 2017, pp. 1-6, doi: 10.1109/IDAP.2017.8090171.
14. A. Dali, A. Mane, H. Challawala and J. Damani, "Implementation of Security System Using Computer Vision and Temperature Detection," *2022 International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP)*, Hyderabad, India, 2022, pp. 1-5, doi: 10.1109/ICICCSP53532.2022.9862487
15. L. Kalapala, H. Yadav, H. Kharwar and S. Susan, "Facial Expression Recognition from 3D Facial Landmarks Reconstructed from Images," *2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, Gunupur Odisha, India, 2020, pp. 1-5, doi: 10.1109/iSSSC50941.2020.9358815.
16. N. Sabri *et al*., "A Comparison of Face Detection Classifier using Facial Geometry Distance Measure," *2018 9th IEEE Control and System Graduate Research Colloquium (ICSGRC)*, Shah Alam, Malaysia, 2018, pp. 116-120, doi: 10.1109/ICSGRC.2018.8657592.