Enhancing the Security Mechanism in ATM Transaction using Face Recognition, Pin and OTP

Soniya D, Tharunkumar G, Praveen Raj N, Vivekanandan S
Student, Assistant Professor
Department of Computer Science and Engineering,Velalar College of Engineering and Technology, Erode

Abstract-In order to provide reliable security solution to the people, the Project is focused on improving the verification strategies to improve the innovation. Proposed paper uses Three-factor authentication (3FA) and it is an effective security mechanism that adds an extra layer of protection to ATM transactions with various domain such as Web development, deep learning and Artificial intelligence Here we are using the Multitask cascaded convolutional neural network (MTCNN) algorithm for classification, bounding box coordinates, facial landmark location. This system imposes a three-tier security on the ATM transactions such as facial recognition along with OTP and PIN for verification. system uses Open CV to process the image being obtained and Haar Cascade classifier to detect the faces in the image. Face recognition helps the machine to identify each and every user uniquely thus making face as a key. The methodology comprised of three phases firstly, the PIN for the registered account is entered then after that the face image of a particular person is compared with database image if it is successful OTP is send to the registered mail ID and verification process takes place. **Keywords - Face recognition, OpenCV, Artificial Intelligence, Deep learning, PIN, OTP.**

I. INTRODUCTION

In recent years, with the increasing number of financial transactions being conducted through Automated Teller Machines (ATMs), the need for stronger security measures has become crucial. One such security measure is the use of Facial Recognition (FR) technology, which is an advanced biometric system that can identify individuals based on their unique facial features. There is a rapid development in science and technology, upcoming innovations are being built-up with strong security. But on the other hand, threats are also being posed to destroy this security level. Though enhancement in automation has made a positive impact overall, but various financial institutions like banks and applications like ATM are still subjected to thefts and frauds. Facial recognition is a technology that uses algorithms and artificial intelligence (AI) to identify and verify a person's identity based on their facial features. It involves capturing an image or video of a person's face using a camera and analysing the facial features, such as the distance between the eyes, the shape of the jawline, and the position of the nose, to create a unique biometric template. In face recognition, there are two kinds of comparisons. The first is verification, this is where the system compares the given individual with whom that individual says they are and gives a yes or no decision. The next one is identification this is where the system compares the currently recognized individual with all the other individuals who are already registered in the database.

The main motto of this project is to enhance security of the conventional ATM module. We have introduced a new concept that enhances the overall performance, usability, and convenience of the transaction at the ATM. Features like face recognition, PIN and One-Time Password (OTP) adds extra layer of security for accounts and improve the privacy of users. Face recognition technology help out the machine to recognize each and every user uniquely thus making face as a main key. This completely dispose the chances of fraud due to larceny and duplicity of the ATM cards. The combination of PIN, OTP, and face recognition ensures that only the authorized user can perform an ATM.

II.LITERATURE SURVEY

A.TITLE: Enhanced Security Feature of ATM's Through Facial Recognition
AUTHOR: Soundari D V; Aravindh R; Edwin Raj K; Abishek S
YEAR: 2021
DESCRIPTION:
ATM systems offer great convenience to the public for withdrawal of money from their bank accounts and provides pleasant advantage on losing their time in the bank for many hours The ATM machine

(Automated Teller Machine) is an electronic device that is used by the banks to perform banking tasks like withdrawal of money, transferring of money, and many to get many information about a user's bank account without the need to visit a bank. This System revolutionized the way of transactions. The number of ATM's a bank has can be a factor in considering the strength of a bank. The main motivation of this project is to increase the security feature of the use of ATM. The current method uses static key (PIN) for security. The proposed method uses Face-id as a key incorporated with current method. The core security of the system is the face-id that is unique for everybody; it cannot be authenticated by anybody other than the user. For the implementation of the face-id scan, the machine learning and image processing algorithms (Eigen face algorithm) are used.

B. TITLE: Safety Augmentation by IRIS & Biometric Recognition into ATM
AUTHOR: Ipsita; Abhishek Tragi, Sunil Kumar khatri, Rajbala Simon
YEAR: 2019
DESCRIPTION:

Security is becoming more dependent on iris recognition. If something is distinctive or well accepted, the iris pattern tends to stay steady throughout time. Iris recognition is employed in high-security places because of its great dependability and outstanding recognition rates. With introduction of ATMs, banking has grown simpler and more convenient. Product (ATM) is soaring in demand owing to a rising number of well-trained crooks. Consequently, financial services are in jeopardy and unreliable. As bio metric recognition systems such as fingerprint & iris recognition make significant development, this issue is likely to worsen. Selective article points may be used to encrypt a customer's passcode. Therefore, system that is safer & enables secure transfers as well as protection against numerous scams is required.

C.TITLE: An IOT implementation to ATM safety system
AUTHOR: Dhanabal Thirumoorthy; Umang Rastogi; B.Barani Sundaram;
YEAR: 2021
*DESCRIPTION***:**

Automated Teller Machine (ATM) cash robbery is very common in many countries including India. The cash robbery by damaging the ATM and breaking the cash vault is the prime technique to loot cash from ATM. Remote locations of the ATM, less or no security guards. Negligence and inadequate safety measures are the main reasons for ATM cash robbery in India. Our proposed ideology is based on this concept to detect the damage exerted on the ATM boxes. To report the damage, this research work utilizes the Internet of Things (IoT) technology, which has worldwide coverage. It is currently the most efficient communication technology. To report the incidence to the authorities, IoT is the best possible solution as it uses internet technology which is already present in the ATMs. The embedded system is combined with IoT to perform the task. The ESP8266 based IoT system connected with a vibration sensor and ATMEGA 328 P PU microcontroller is utilized for ATM robbery detection and alert to authorities. Our paper performs a detailed analysis of the issue and concludes the most appropriate solution. Also, this research work replicates the overall system.

III.EXISTINGSYSTEM

During an ATM transaction, PIN verification and fingerprint recognition techniques are used to verify the identity of a consumer. Using an effective technique for extracting the minutiae features, fingerprint's authenticity is confirmed. When customer uses swipe machine to perform a transaction, an authorization notification is obtained via GSM technology. GPS will be used to pinpoint the exact position in both scenarios. The system will immediately stop the card if any unauthorized individual attempts have been made to use it, and consumer will get notification detailing the incident. Apart from this an individual's specific behavioural and physical features may be measured by using bio metrics to identify or verify them. Palm, hand , geometry, retina, fingerprints traits are some of the most often used physical bio metrics. It is possible to establish a person's identification by using bio metrics. Comparisons are made between an entity's data and new measurements that pretend to belong to it. If the dimensions match, it assumes that the individual is who they claim to be is accepted as true. For biometric authentication, the current system makes use of Gaussian Mixture Models, Fuzzy Expert Systems and Support Vector Machines algorithms. (SVMs), Principal component analysis (PCA), LDA. Bio metric specialists were used for training and testingthesealgorithms.

IV.PROPOSEDSYSTEM

Multi cascaded Convolutional Neural Network is used in this effort to create a multi-modal security model for ATMs by combining the OTP, PIN with electronic face recognition. Applied artificial intelligence is specialization of machine learning and deep learning. Whenever it concerns into facial identification, deep learning technique assist in attaining more accuracy than typical machine learning approaches. Advanced FR system with a face detection can be used for performing alignment and calibration. The camera is initially used to identify the faces. Then the captured image is stored in the database. Finally, the FR module has been included. Facial anti-spoofing is used in the FR unit. Facial anti-spoofing is a biometric security technology used to prevent unauthorized access to systems or facilities by detecting and preventing spoofing attempts. Spoofing refers to the act of using a fake or fraudulent representation of an individual's biometric data, such as a photo, video, or 3D mask, to gain access to a secured system or location. For training and testing, either live or pre-processed faces are used. Once the deep features of the test data set have been extracted, various topologies and loss functions may be used to extract discriminative deep features, while training and face matching approaches can be used for performing feature classification.

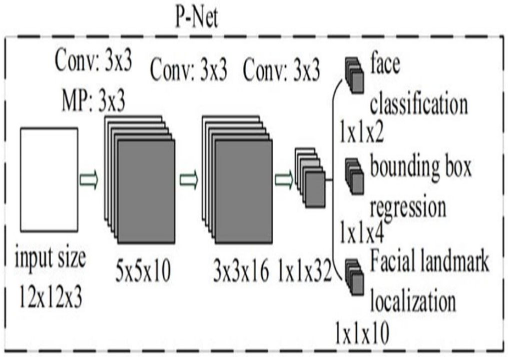
MULTI-TASKCASCADED CONVOLUTIONAL NEURAL NETWORK

MTCNN (Multi-Task Cascaded Convolutional Neural Network) is a deep learning algorithm that is widely used in face detection and facial recognition applications. MTCNN is a multi-stage algorithm that consists of three stages, each with a separate neural network, to detect faces at different scales and refine the results.

The three stages of the MTCNN algorithm are:

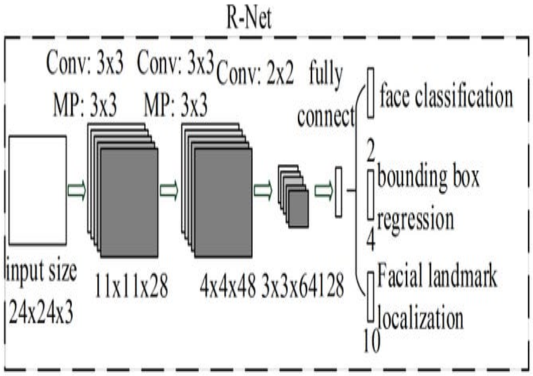
Stage 1: Proposal Network (P-Net)

P-Net takes an image as input and applies a set of convolutional filters to detect potential faces. The output of P-Net is a set of bounding boxes, each representing a potential face region in the image.
These bounding boxes are then passed through to the next stage of the algorithm, the R-Net. The R-Net further refines the bounding boxes by eliminating false positives and improving the accuracy of the face detection.



2.Refinement Network (R-Net):

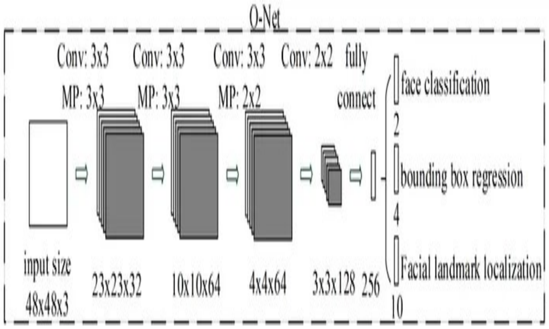
R-Net takes the bounding boxes generated by P-Net as input and applies a more complex neural network to further filter and refine the face detections. Specifically, R-Net takes a cropped image of the candidate face region and outputs a refined bounding box with higher accuracy. IN addition to refining the bounding boxes, R-Net also provides facial landmark detection. It predicts the locations of various facial landmarks, such as the corners of the eyes and the mouth.



3. Output Network (O-Net):

The O-Net is a more complex neural network than the previous stages, designed to perform facial feature point detection and face classification. It takes the refined bounding boxes generated by the R-Net as input and produces the final face detection results, including the location of the face and the facial landmarks.

The O-Net is trained to detect various facial features, such as the eyes, nose, mouth, and ears. It can also classify faces as either male or female, and estimate the age of the individual.

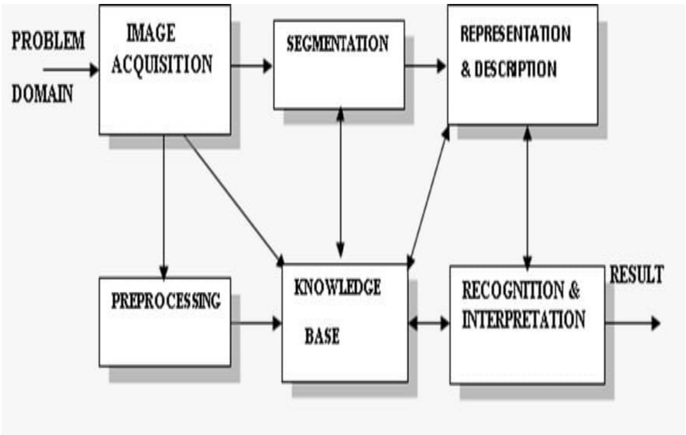


TECHNIQUES:

FACE RECOGNITION MODULE

Image acquisition module:

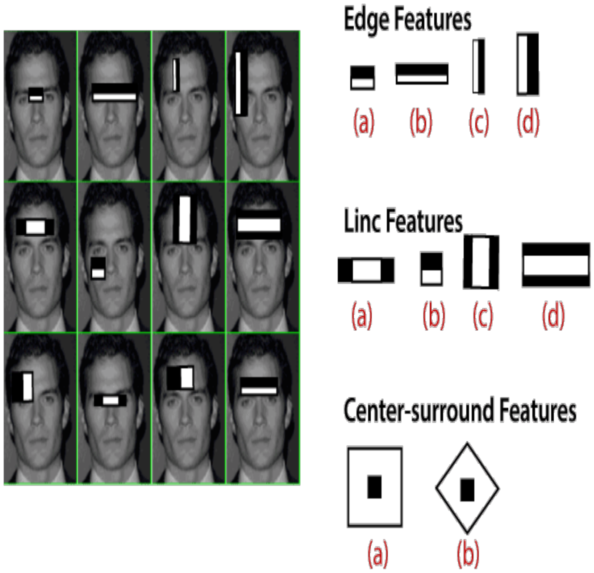
Inorder to collect the meaningful footage, ATMs should be outfitted with cameras. A webcam is used in conjunction with a computer to capture images. It is used for, storage, pre-processing, segmentation, representation, recognition and interpretation of the obtained images.



As shown in the diagram, the first step in the face recognition process is image acquisition from the camera. The next step is the pre-processing which involves transforming the raw input face images into a format that is suitable for analysis by a machine learning algorithm. The pre-processing step helps to enhance the quality of the input images, reduce noise, and remove unwanted variations that can affect the performance of the face recognition system.Segmentation is a technique used in face recognition to separate the different regions of a face, such as the eyes, nose, mouth, and cheeks, and extract more specific features. This can help to improve the accuracy of the face recognition system.Representation in face recognition refers to the way in which facial features and characteristics are represented and analysed by a face recognition system. In face recognition, a face image is typically represented as a mathematical vector or a set of features that capture important facial attributes such as the distance between the eyes, the shape of the nose, the contour of the face, and the texture of the skin. Interpretation refers to obtaining a meaningful insight of an image. It is also used to obtain unique pattern, features from the captured image.

Image processing module:

In pre-processing section, the input image may be in different size, contains noise and it may be in different colour combination. These parameters need to be altered with respect to the requirement of the process. Image noise is considered to be most apparent in image regions with low signal level such as shadow regions or under exposed images. There are so many kinds of noise like salt and pepper noise, film grains etc., All these noise are removed by using filtering algorithmsInpre-processing module image acquired will be processed for obtaining correct output.



Feature extraction module:
In order to extract the important characteristics that will be utilized for classification, the face picture is passed via the classification algorithm after being used to identify faces. The facial information, including the eyes, nose, and mouth, is automatically collected from each position and utilized to determine the consequences of change utilizing its link to the front facial template.
The main purpose of feature extraction is to reduce the amount of data in an image while retaining the most important information. This can make it easier to process the image, reduce computational requirements, and improve the accuracy of subsequent image analysis techniques.
Image classification module:
During the enrolling process, DCNN algorithms were developed to automatically identify and reject incorrect face photos. This will guarantee that all students are properly enrolled, which will lead to greatest potential results.
Pre-processing module: This module performs image processing tasks such as face detection, face alignment, and normalization to prepare the input images for feature extraction.

Face database module: This module stores the extracted features of known individuals in a database for later comparison with new faces.
Recognition module: This module compares the features of new faces with the stored features in the face database to determine if there is a match.
Decision module: This module makes a decision based on the recognition results and sends a signal to control access or trigger an alert if there is a match or no match.
User interface module: This module provides a graphical user interface (GUI) for users to interact with the system and perform tasks such as adding new faces to the database, deleting faces, or adjusting the system settings.

V EXPERIMENTS

1. Collect and training of data set: Collect a data set of images frames of individuals using the camera. The data set includes a variety of lighting conditions, poses, and facial expressions to ensure the face recognition system can work under different scenarios. Training of the data set is done with a large set of labelled images to teach a machine learning model to identify different individuals in a given image the goal of training is to help the machine learning algorithm learn the visual patterns that distinguish one individual from another and to
Use this knowledge to recognize new individuals in previously unseen images
2. Analysis: This section presents the data collected during the experiment, such as the number of images or video frames used for training and testing, the number of faces recognized correctly, and the number of false positives and false negatives.
3. Evaluation Metrics: This section includes the evaluation metrics used to measure the performance of the face recognition system. Common metrics include accuracy, precision, recall, and F1 score.
4. Refine the system: Refine the face recognition system by adjusting the algorithms, models, or parameters based on the results of the evaluation. This step helps to improve the accuracy and reliability of the system.
5. Results: This section presents the results of the experiment, including tables, graphs, and charts to visualize the data and evaluation metrics. It includes a comparison of the performance of different face recognition algorithms and models.

The upcoming table includes columns for the algorithm used, the training and testing datasets, and the evaluation metrics such as accuracy, precision, recall, and F1 score. The table compares the performance of three different algorithms (MTCNN, HAAR, and PCA)on the Labelled Faces data sets.

Algorithm	**Training Dataset**	**Testing Dataset**	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1 Score**
PCA	LFW	LFW	75.3	82.1	68.2	0.748
HAAR	LFW	LFW	87.2	91.8	83.7	0.874
MTCNN	LFW	LFW	94.8	96.2	93.6	0.945
MTCNN	LFW	YTF	89.6	92.1	87.2	0.892

The results show that the CNN algorithm achieved the highest accuracy and F1 score on both datasets, while the HAAR algorithm performed better than PCA. The precision and recall metrics show how well the algorithms can correctly identify positive and negative samples, respectively. Overall, the results suggest that MTCNN is the most effective algorithm for face recognition, and using a larger and more diverse dataset can improve the performance of the system.

VI CONCLUSION

In this project we will implement, ATM model which enhances security by using Facial verification software adding up facial recognition systems to the identity confirmation process used in ATMs can reduce forced transactions to a great extent and provide hard-secure authentication. Biometrics at Automated Teller

Machines (ATM) will be able to identify and authenticate account holders to eliminate the illegal transactions. Biometric traits may be used to not only identify the persons but also to authenticate them. As a part of the current ATM safety systems, the security design provides the possibility of proxy utilization in the existing security tools and information (besides an ATM Card). The bank account holder is also involved in all of widely accessible information available in real time. The aim of our work is to use embedded ATM camera to perform face detection with the help new computer vision framework. Authentication of customers at computerized teller machines (ATMs) is normally dependent on PIN-based totally verification. Several elements had been studied so far in enhancing the security for authentication of customers at ATM.

REFERENCES

[1] Raj M, Anitaz Julian, 2015. "Design and implementation of anti-theft ATM machine using embedded systems", IEEE, DOI 10.1109/ICCPCT.2015.7159316

[2] W.A. Shier, S.N. Yanushkevich. "Biometrics in human-machine interaction", the international conference on information and digital technology 2015.

[3] Nagarajan C., Neelakrishnan G., Akila P., Fathima U., Sneha S. "Performance Analysis

[4] and Implementation of 89C51 Controller Based Solar Tracking System with Boost

[5] Converter" Journal of VLSI Design Tools &amp; Technology. 2022; 12(2): 34–41p.

[6] 2. C. Nagarajan, G.Neelakrishnan, R. Janani, Maithili, G. Ramya "Investigation on Fault

[7] Analysis for Power Transformers Using Adaptive Differential Relay" Asian Journal of

[8] Electrical Science, Vol.11 No.1, pp: 1-8, 2022.

[9] Kande Archana, Dr A. Govardhan. "To enhance the security for ATM with help of sensor and controllers", IEEE. DOI 10.1109/ICECDS.2017.8389590 .

[10] V. Gokula Krishnan., G.N. Kirran, K.P. Deepkarasan, J. Kishore Kumar, 2020." Face Detection Based Atm Safety System In lot Using Secure Transaction", International Research Journal of Engineering and Technology.

[11] Joyce Soares, A.N. Gaikwad. 2016 "A Self banking biometric m/c with fake detection applied to fingerprint and iris along with GSM test for OTP",IEEE DOI 10.1109/ICCSP.2016.7754189.

[12] Albert Ali Salah. 2013 "short term face recognition for ATM users" IEEE. DOI 10.1109/ICECCO.2013.671824.

[13] Claudio Porretti. 2016 "A New Vision Fpr ATM Security Management", IEEE. DOI 10.1109/ARES.2016.50.

[14] C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T

[15] Series Parallel Resonant Converter' - Journal of ELECTRICAL ENGINEERING, Vol.63 (6), pp.365-372,

[16] Dec.2012.

[17] C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID

[18] Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011.

[19] C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy

[20] Logic Controller Using State Space Techniques'- Taylor &amp; Francis, Electric Power Components and

[21] Systems, Vol.39 (8), pp.780-793, May 2011.

[22] Nagarajan and M.Madheswaran - 'Experimental Study and steady state stability analysis of CLL-T Series

[23] Parallel Resonant Converter with Fuzzy controller using State Space Analysis'- Iranian Journal of

[24] Electrical &amp; Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

[25] Apurva Taralekar.2017 "One touch multibanking transaction on atm system using biometric and gsm authentication", IEEE. DOI 10.1109/BID.2017.8336574.

[26] V.Prasanan, R.Sandeep Kumar, C.Deepak, R.DeepakKummar, S.Navin Kumar, 2019. "IOT Based Atm Maintenance and Security System", International Journal of Applied Engineering Research.

[27] Rasanayagam, K., Kumarasiri, S.D.D.C., Tharuka, W.A.D.D., Samaranayake, N.T., Samarasinghe, P. and Siriwardana, S.E., 2018, December. CIS: An Automated Criminal Identification System. In 2018 IEEE International Conference on Information and Automation for Sustainability (ICIAfS) (pp. 1-6). IEEE.

[28] Tokuno, K. and Yamada, S., 2011. Codesign-oriented performability modeling for hardware-software systems. IEEE Transactions on Reliability, 60(1), pp.171-179.

[29] Beazley, D.M., 1996, June. Using SWIG to control, prototype, and debug C programs with Python. In Proc. 4th Int. Python Conf.

[30] Balwir, S.P., Katole, K.R., Thakare, R.D., Panchbudhe, N.S. and Balwir, P.K., 2014. Secured ATM Transaction System Using MicroController. International Journal o f Advanced Research in computer science and software engineering, 4(4).

[31] Ajaykumar, M. and Kumar, N.B., 2013. Anti-theft ATM machine using vibration detection sensor. International journal o f advanced research in computer science and software engineering, 5(12).

[32] Maiti, S., Vaishnav, M., Ingale, L. and Suryawanshi, P., 2016. ATM robbery prevention using advance security. Int Res J Eng Technol (IRJET), 5(02), pp.2395-0056.