A

FINAL PROJECT REPORT

ON

ENHANCED ATM SECURITY USING FACIAL RECOGNITION

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE OF

BACHELOR OF ENGINEERING
INFORMATION TECHNOLOGY

BY

Trupti Khade	B190058597
Prashant Patil	B190058676
Manish Raut	B190058683
Shashank Satghare	B190058693

Under the guidance of
Mr. Abhinay G. Dhamankar

Department Of Information Technology
Pune Institute of Computer Technology
Pune - 411 043.

2023-2024

SCTR's PUNE INSTITUTE OF COMPUTER TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY

C E R T I F I C A T E

This is to certify that the final project report entitled
ENHANCED ATM SECURITY USING FACIAL RECOGNITION
submitted by

Trupti Khade	B190058597
Prashant Patil	B190058676
Manish Raut	B190058683
Shashank Satghare	B190058693

is a bonafide work carried out by them under the supervision of **Mr. Abhinay G. Dhamankar** and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University for the award of the Degree of Bachelor of Engineering (Information Technology).

This project report has not been earlier submitted to any other Institute or University for the award of any degree or diploma.

Mr. Abhinay G. Dhamankar
Project Guide

Dr. A. S. Ghotkar
HOD IT

SPPU External Guide

Dr. S. T. Gandhe
Principal

Date: 19/04/2024
Place: Pune

Acknowledgement

We, the members of the group, wish to specify our true appreciation to all those who have played an imperative part within the effective completion of our Bachelor of Engineering (BE) group project. This try has been a critical portion of our scholarly travel, and we are thankful for the bolster and commitments from taking after people and organizations. To begin with and preeminent, we amplify our ardent much appreciated to our extent direct, Mr. A. G. Dhamankar Sir, for their persistent direction, skill, and faithful back. Their mentorship and feedback were instrumental in forming our venture and guaranteeing its quality. We moreover wish to recognize the HOD Dr. Archana Ghotkar Ma'am for her direction for the venture.Additionally, we extend our heartfelt gratitude to our principal, Dr. S. T. Gandhe, for his continuous support and encouragement throughout our project journey. His leadership and vision have been inspiring and invaluable to us.We also wish to express our gratitude to the director, Dr. P. T. Kulkarni, for his guidance and support, which have been instrumental in shaping the direction of our project. We moreover wish to recognize the staff of the Information Technology Department at PICT for giving us a conducive scholarly environment and for conferring the information and aptitudes that were fundamental for the fruitful execution of our venture. To our individual understudies and companions who have given bits of knowledge, proposals, and collaborative endeavors, we offer our appreciation. Your collective endeavors enormously enhanced our venture and its results.

Trupti Khade	B190058597
Prashant Patil	B190058676
Manish Raut	B190058683
Shashank Satghare	B190058693

Abstract

This project explores the integration of facial recognition technology into Automated Teller Machines (ATMs) to reinforce security measures and improve user experiences. Centering on anticipating unauthorized get to and decreasing card extortion, the think about evaluates facial recognition's viability as a strong confirmation strategy. By dispensing with the require for conventional PINs or physical cards, facial recognition not as it were improves security but moreover streamlines ATM transactions, advertising more noteworthy comfort to clients. In addition, the technology advances inclusivity by giving an elective verification strategy reasonable for people with incapacities or challenges utilizing conventional strategies.

In expansion to its security benefits, facial recognition ingrains believe among ATM users, guaranteeing them of the security of their monetary exchanges. The usage of progressed security measures not as it were discourages fraudsters but too fortifies client certainty in ATM services.

Moreover, the research examines the integration of a comprehensive extortion discovery and notice framework nearby facial recognition. This instrument ceaselessly screens ATM transactions for suspicious exercises, instantly recognizing unauthorized get to endeavors or false activities. By combining facial recognition with vigorous extortion location, ATM security gets to be more strong against rising dangers. By synthesizing industry improvements and observational discoveries, this paper offers bits of knowledge and direction for policymakers, money related educate, and analysts in advancing ATM security. Highlighting the multifaceted benefits of facial acknowledgment innovation, this think about contributes to invigorating money related frameworks against extortion and unauthorized get to, cultivating believe and certainty among ATM users.

Keywords: Artificial Intelligence, Facial Recognition, Deep Neural Networks, OpenCV, Convolutional Neural Networks (CNN), Machine Learning, ATM Security, ATM Fraud Detection, Biometric Authentication, Fraud Detection, Automatic Alert System, Real-time Monitoring, Multi-factor Authentication, Risk Management, Fraud Prevention.

Contents

List of Figures

List of Tables

Abbreviations

ATM	:	Automated Teller Machine
DNN	:	Deep Neural Network
PCA	:	Principal Component Analysis
API	:	Application programming interface
SMS	:	Short message service

1. Introduction

1.1 Introduction

Automated Teller Machines (ATMs) play an urgent part in giving helpful get to to banking administrations, however they confront diligent security challenges, especially concerning extortion and unauthorized get to. Conventional verification strategies like PINs and attractive stripe cards are defenseless to misuse, inciting a requirement for more progressed security measures.Facial recognition technology rises as a promising arrangement to sup- port ATM security. By analyzing interesting facial biometrics, this technology offers vigorous confirmation, moderating dangers related with unauthorized get to and card- related extortion. This project explores the integration of facial recognition into ATM systems, utilizing machine learning algorithms and deep neural networks for accurate user identification. Past improving security, facial recognition too improves user comfort by eliminating the requirement for PINs or physical cards. In addition, it cultivates inclusivity by giving an elective confirmation strategy appropriate for people with disabilities or those confronting troubles with conventional strategies.

The venture moreover considers the obstacle impact of facial recognition on fraudsters, strengthening belief among ATM clients. Coupled with a comprehensive extortion discovery and notice framework, facial recognition reinforces the ATM security framework against developing dangers.

In essence, this project aims to contribute to the headway of ATM security, advertising bits of knowledge for policymakers, financial institutions, and researchers. By combining experimental inquiry with technological innovation, it looks to progress the security, comfort, and openness of ATM services universally.

1.2 Motivation

The inspiration for setting out on this venture stems from the pressing need to address the rising security challenges confronting Automated Teller Machines (ATMs) around the world. In spite of their comfort, ATMs are progressively focused on by fraudsters, coming about in security breaches and budgetary misfortunes for clients. Conventional security measures like Personal Identification Numbers (PINs) and verification cards have demonstrated inadequately against advanced assaults such as ATM skimming and card

cloning.

Subsequently, there's a critical imperative for progressed security solutions to protect ATM exchanges and ensure users' financial assets. This venture points to address this require by investigating the integration of imaginative advances, counting facial recognition and an alert system, into ATM systems. By leveraging biometric verification and a comprehensive alert system, we look to brace ATM security, streamline confirmation forms, and guarantee convenient notice of any suspicious action to bank account holders. In addition, past relieving security dangers, this venture moreover points to advance budgetary inclusivity. By executing open and user-friendly security measures, we point to guarantee that all people, counting those with differing needs, can safely get to managing an account administrations. Eventually, the inspiration behind this venture lies in our commitment to reinforcing ATM security, cultivating belief in banking services, and advancing financial incorporation for all. Through our endeavors, we aim to form significant commitments to the astuteness and availability of ATM transactions around the world.

1.3 Objectives

1. Explore and assess the current scene of profound learning procedures, with a particular center on facial recognition technology inside deep neural networks (DNNs), within the setting of enhancing ATM security infrastructure.

2. Explore a range of techniques and structures utilized in Deep Neural Networks (DNNs) for facial recognition, especially within the domain of ATM security, to find out their viability, exactness, and versatility in tending to real-world security challenges and scenarios. Besides, Investigate techniques to upgrade the effectiveness of DNN models.

3. Conduct a comprehensive execution assessment and comparative analysis of distinctive models utilized for facial recognition within the setting of ATM security. This evaluation will consider different measurements such as exactness, execution consistency, and flexibility over differing operational situations and user socioeconomics.

4. Explore the integration of an automated alert system into the ATM security infrastructure, pointing to expeditiously inform bank account holders of any recognized suspicious

5. Exercises, subsequently improving security measures and guaranteeing opportune reaction to potential dangers.

6. Conduct user-centric research to survey client discernments, acceptance, and convenience of facial recognition technology in ATM security, pointing to recognize potential ease of use challenges and illuminate the development of user-friendly security arrangements.

7. Explore administrative and security contemplations encompassing the execution of facial recognition technology in ATM security, guaranteeing compliance with information assurance laws and tending to potential security concerns associated with biometric information utilization.

1.4 Scope

The research presents energizing openings for enhancing the integration of facial recognition over different sectors. A key zone for encouraging examination includes joining different biometric systems such as fingerprint and voice recognition to invigorate security measures. Utilizing multi-factor verification in this way can support the security of ATM transactions, rendering them more versatile to false exercises. The objective here expands past simple exactness enhancement; it moreover includes invigorating the capacity to preempt prompt dangers. Given the advancing scene of cyber dangers, there's a requirement for novel models able to quickly adjust to developing dangers. Moreover, prioritizing user involvement enhancement remains fundamental. This involves actualizing instinctive plan standards to streamline ATM intuitive and guarantee comfort for users. Furthermore, consistent integration of facial recognition technology into versatile banking applications holds monstrous potential, empowering users to consistently and safely execute over assorted stages. Strong security shields are crucial, and future research endeavors ought to concentrate on leveraging cutting-edge protection technologies to unequivocally protect individual data. Usage of automated security responses, such as enacting alerts or locking ATM cabins, within the event of suspicious exercises such as robbery or endeavored burglary. Explore advances like IoT-enabled sensors and automated door locks to improve physical security measures.

2. Literature Survey

Title	Authors	Technique used	Evaluation methods and findings
Secure ATM transactions Using face recognition and OTP(Pub. 2022) [1]	Pooja Surwase,Sonam Bhange, Shreya Taru, Samruddhi Khot, Prof. Jayashree Mundada	OTP using face verification	Different types of users can have different types of security
Recent advances in Deep Learning Techniques for face recognition(Pub. 2021) [2]	Md.Tahmid hasan faud,awal ahmad fime, deolwar sikder, md. Akil raihan iftee, jakaria rabbi, mabrook s. Alrakhmi ,abdu gumae, ovishaken sen, mohtasim faud	Image processing and face recognition in deep Neural network in face recognition pipeline	Recent trends in face recognition using different deep learning architectures.
GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations [3]	MOHAMAD ALANSARI (Member, IEEE), OUSSAMA ABDUL HAY SAJID JAVED , ABDULHADI SHOUFAN YAHYA ZWEIRI (Member, IEEE), AND NAOUFEL WERGHI(Senior Member, IEEE)	GhostNetV1,GhostNetV2	Reducing the amount of computation is must and to do this Ghost net can be used which uses all series of linear transformation which are inexpensive to extract features

Towards Accurate and Lightweight Masked Face Recognition: An Experimental Evaluation [4]	YOANNA MARTÍNEZ-DÍAZ1, HEYDI MÉNDEZ-VÁZQUEZ 1, LUIS S. LUEVANO 2, (Member, IEEE), MIGUEL NICOLÁS-DÍAZ1, LEONARDO CHANG 2, AND MIGUEL GONZÁLEZ-MENDOZA2	Periocular recognition	Various models of CNN are used
Biometrically Secured ATM Vigilance System [5]	Navin Kumar.M, Raghul.S, Nirmal Prasad. K, Naveen Kumar. P	Biometric authentication; microcontroller; face recognition; fingerprint sensor; OTP (One Time Password	ATMs require physical safety features such as a strong door, secure machines, a security guard along with the ATM software being used.
Biometric Based Smart ATM Using RFID [6]	Gokul. S, Kukan. S, Meenakshi.K, Vishnu Priyan S, Rolant Gini J, M.E. Harikumar	Microcontroller; fingerprint sensor; embedded system; signal processing	For extra security, some features can be implemented such as RFID number, Fingerprint scanners.This information can be verified in a database.
ENHANCED SECURITY FEATURE OF ATM'S THROUGH FACIAL RECOGNITION [7]	Ms. SOUNDARI D V, ARAVINDH R, EDWIN RAJ K, ABISHEK S	ATM, Face-id, Eigenface algorithm, Machine Learning	Face-ID can be used as key along with other authentication methods

Biometric And IOT Technology Based Safety Transactions In ATM [8]	C. Bhuvaneswar, C. Bhuvaneswar, Anupriya Giri, Sushmita Mahato	ATM Transactions; Face Recognition System; Internet of Things; Machine to Machine Communication	In contemporary society, incidents of ATM fraud have become increasingly commonplace.This is due to various machines designed to deceive people.
AN EFFICIENT DEEP NEURAL NETWORKS TRAINING FRAMEWORK FOR ROBUST FACE RECOGNITION [9]	Canping Su, Yan Yan , Si Chen, Hanzi Wang	Face recognition, deep neural networks, triplet loss function	A new framework for training the DNN model was proposed. It has an accuracy of 97.3
Face Detection and Recognition Based on General Purpose DNN Object Detector [10]	Veta Ghenescu, Roxana Elena Mihaescu, Marian Traian Ghenescu, Eduard Barnoviciu, Serban-Vasile Carata, Mihai Chindea	Face recognition, Deep Neural Network, YOLO- You Only Look Once, Darknet	The model was trained on a proprietary database. The method is based on the YOLO (You Only Look Once) model,The database has over 120,000 samples.
Face Recognition using Deep Neural Network with "LivenessNet" [11]	Samana Jafri, Satish Chawan, Afifa Khan	Face recognition, Artificial intelligence, Deep Neural Networks, Computer Vision, OpenCV, and LivenessNet	A DNN framework LivenessNet was discussed,

Pixel-Level Face Image Quality Assessment for Explainable Face Recognition [12]	Philipp Terhörst, Marco Huber, Naser Damer, Member, IEEE, Florian Kirchbuchner, Member, IEEE, Kiran Raja, Senior Member, IEEE, and Arjan Kuijper, Member, IEEE	Authentication via biometrics, advanced analytics, transparent facial recognition,intuitive facial recognition.	A new concept of pixellevel face image was introduced. It is a training free approach which can adapt to various other networks.
DeepWTPCA-L1: A New Deep Face Recognition Model Based on WTPCA-L1 Norm Features [13]	AYYAD MAAFIRI, OMAR EL-HARROUSS, (Member, IEEE), SAAD RFIFI, SOMAYA AL-MAADEED , (Senior Member, IEEE), AND KHALID CHOUGDALI	Face recognition, WTPCA-L1 algorithm, CNN-LSTM architecture.	A new face recognition model was proposed called DeepWTPCA-L1 using WTPCA-L1 features and a CNN-LSTM architecture.
Multi-View Face Recognition Via Well-Advised Pose Normalization Network [14]	XIAOHU SHAO, XIANGDONG ZHOU , ZHENGHAO LI, AND YU SHI	Facial recognition from multiple viewpoints, GANs, transforming faces to a frontal view, and evaluating the quality of facial data	In facial recognition having different poses causes problems. To tackle this problem a new approach was proposed.

A Review of Face Recognition Technology [15]	LIXIANG LI,XIAOHUI MU, SIYING LI, AND HAIPENG PENG	Facial recognition, image processing, neural network, artificial intelligence	The paper introduces the related research of face recognition from different perspectives. The article describes the development stages of facial recognition and other technologies.
A Real-Time CNN-Based Lightweight Mobile Masked Face Recognition System [16]	BUSRA KOCACINAR, BILAL TAS, FATMA PATLAR AKBULUT, (Member, IEEE), CAGATAY CATAL, AND DEEPTI MISHRA, (Senior Member, IEEE)	Convolutional neural networks, deep learning, ne tuning, masked face recognition, TinyML, transfer learning.	A new approach for facial recognition was proposed for people wearing masks. The approach is based on fine-tuned lightweight deep Convolutional Neural Networks (CNN).The proposed model achieves 90.40% validation accuracy using 12 individuals' 1849 face samples.
A New Deep Neural Architecture Search Pipeline for Face Recognition [17]	NING ZHU, ZEKUAN YU, AND CAIXIA KOU	Neural architecture search, trainable architecture, reinforcement learning, face recognition, large-scale face dataset.	A new deep neural architecture search pipeline combined with neural architecture search(NAS) technology and reinforcement learning strategy into face recognition.The network architectures has achieved good accuracy in the large-scale face dataset, which achieved 98.77% top-1 in the MS-Celeb-1M dataset and 99.89% in LFW dataset.

A Study on the Performance of Unconstrained Very Low Resolution Face Recognition: Analyzing Current Trends and New Research Directions [18]	LUIS S. LUEVANO, (Member, IEEE), LEONARDO CHANG, HEYDI MÉNDEZ-VÁZQUEZ, YOANNA MARTÍNEZ-DÍAZ, MIGUEL GONZÁLEZ-MENDOZA	Improving face recognition in low resolution and unconstrained settings through innovative coupled mappings, super resolution, and lightweight neural networks.	The study discussed the advances and challenges in facial recognition. It also proposes a new method to tackle the very low resolution face recognition problem and provide an in-depth analysis of their design, effectiveness, and efficiency for a real-time surveillance application.
512KiB RAM Is Enough! Live Camera Face Recognition DNN on MCU [19]	Maxim Zemlyanikin Alexander Smorkalov Tatiana Khanova Anna Petrovicheva Grigory Serebryakov	RISC-V MCU porting, DNN model optimization	The paper discusses how small devices can manage huge computational work such as facial recognition. It covers the full development and deployment pipeline of Face Recognition with a live camera.
Color Face Recognition by Using Quaternion and Deep Neural Networks [20]	Abdelmajid EL ALAMI, Zouhir LAKHILI, Aissam BERRAHOU ,Hassan QJIDAA, Abderrahim MESBAH	Quaternion, color face recognition, complexity, deep neural networks	This paper proposes a new model for color face recognition based on quaternion number and deep neural networks (DNN), to enhance the classification accuracy of color face recognition.

Face Recognition In Low Lighting Conditions Using Fisherface Method And CLAHE Techniques [21]	Muhammad Fauzan Rahman, Febryanti Sthevanie and Kurniawan Nur Ramadhani	Face recognition, fisherface, face detection, image enhancement, contrast limited adaptive histogram equalization	This paper proposes a new system with facial images in low light conditions, by adding image enhancement with contrast adaptive histogram equalization (CLAHE) contrast techniques to create good quality lighting images.
LOCAL BINARY PATTERNS AND ITS VARIANTS FOR FACE RECOGNITION [22]	K.Meena, Dr.A.Suruliandi	Face recognition techniques such as Local Binary Pattern (LBP), Differential LBP (MLBP), CS-LBP, and LBPV exhibit distinct patterns.	This study compares various face recognition patterns such as Local Binary Pattern (LBP),Multivariate Local Binary Pattern (MLBP), Center Symmetric Local Binary Pattern (CS-LBP) and Local Binary Pattern Variance (LBPV)
Two Dimensional Principal Component Analysis Based Independent Component Analysis for Face Recognition [23]	Xingfu Zhang, Xingfu Zhang, Xiangmin Ren	Principal Component Analysis; Two Dimensional Principal Component Analysis; Independent Component Analysis; face recognition	This study proposes Two Dimensional Principal Component Analysis based Independent Component Analysis algorithm, which processed the two dimensional images directly in preprocessing procedure. This algorithm is more effective than classical PCA, 2dPCA and ICA algorithms.

Table 2.1: Literature Survey

2.1 Existing Methodologies

The article titled "Enhanced Security Feature of ATMs Through Facial Recognition" introduces a facial recognition approach utilizing eigenfaces. This method assesses algorithms utilized in previous systems, emphasizing the reliability, speed, and storage efficiency of PCA-based algorithms. However, a notable drawback of this method is its susceptibility to manipulation using the user's image. It is suggested that employing 3D masks could enhance security, albeit with associated high production costs. In "Face Recognition in Low Lighting Conditions Using Fisherface Method and CLAHE Techniques" [21], the author demonstrates Fisherface's ability to recognize faces with a success rate of 77.69%. In "Two-Dimensional Principal Component Analysis-Based Independent Component Analysis for Face Recognition" [23], the author proposes an ICA algorithm based on 2DPCA, outperforming traditional PCA, 2DPCA, and ICA methods. Nevertheless, limitations of 2DPCA encompass sensitivity to image variations, high computational demands, restricted pattern distinction capability, and reliance on preprocessed data. In "Local Binary Patterns and Its Variants for Face Recognition" [22], by K. Meena and Dr. A. Suruliandi, the authors introduce a facial recognition method rooted in Local Binary Patterns and modified variants, achieving a notable recognition rate of up to 87%. In "An Efficient Deep Neural Networks Training Framework for Robust Face Recognition" [9], a novel DNN training framework employing softmax loss and triple loss functions is proposed to accurately capture human facial features. A specialized DNN architecture initialized with softmax loss is devised, with the addition of triple regression to enhance the DNN's capability in discerning features amidst evolving functions.In the paper "ATM SAFETY AND SECURITY ALERT" [25], the authors proposed The concept of creating and implementing an ATM safety and security warning helps to deter ATM thieves from robbing ATMs. The sensors will activate and transmit a signal to the controller if someone tries to open or raise the ATM. Following then, the GSM module sends an alarm message to the registered cellphone number. This aids in the police apprehending the thief. In the paper "ATM PLUS WITH FACE RECOGNITION AND OTP MECHANISM" [26], the authors examine a facial recognition method coupled with an OTP mechanism for authenticating users during transactions. The face recognition software is created using MATLAB, wherein the algorithm evaluates facial features by extracting the relative positions, sizes, and shapes of facial components such as the eyes, nose, cheekbones, and jaw. MATLAB is employed to calculate the Eigenvalues. The OTP mechanism is implemented using the Amazon Simple Notification Service.

2.2 Research Gap Analysis

Existing Authentication Methods: The reliance on physical cards and PINs for ATM authentication presents a notable security loophole, leaving systems vulnerable to theft, skimming, and various forms of fraud. Identity Verification: Facial recognition emerges as a promising solution to the current deficiency in biometric identification, providing a robust method for authenticating individuals. Card Cloning: The susceptibility of the current system to card cloning attacks underscores the need for enhanced security measures, such as the integration of facial recognition technology. Unauthorized Access: Instances of unauthorized access to ATMs, whether through physical tampering or cyber intrusion, persist as significant vulnerabilities. Facial recognition offers a viable means to mitigate such risks by preventing unauthorized individuals from accessing ATM functionalities. Fraud Detection: Traditional security measures may fall short in detecting sophisticated fraudulent activities. Facial recognition not only strengthens user authentication but also enables the identification of suspicious behavior or individuals attempting fraudulent transactions.

Additionally, the integration of an alert system further enhances the security infrastructure of ATMs. Upon detecting any suspicious activity, such as unauthorized access attempts or fraudulent transactions, the alert system promptly notifies the account holder and temporarily deactivates the ATM card, mitigating potential losses and enhancing overall security measures.

3. Requirement Specification and Analysis

3.1 Problem Definition

In light of the persistent threat of card-related fraud and unauthorized usage at ATMs, urgent action is imperative to bolster ATM security. The conventional reliance on magnetic cards and PINs has proven to be susceptible to exploitation by fraudulent actors, resulting in significant financial losses. Critical challenges include the prevalence of card cloning, vulnerabilities in PIN systems, unauthorized access, and the utilization of social engineering tactics. To address these issues effectively, a robust multi-factor authentication system is paramount, encompassing features such as instant authentication, encryption, and biometrics. Additionally, user education initiatives and regular software updates are crucial components of this comprehensive security strategy. By implementing these measures, the risk associated with card-related fraud and unauthorized ATM usage can be mitigated, thereby reducing financial losses and ensuring the integrity of transactions.
Furthermore, the integration of an alert system serves as an additional layer of security enhancement. Upon detecting any suspicious activity, such as unauthorized access attempts or potential fraudulent transactions, the alert system promptly notifies the account holder and initiates temporary deactivation of the ATM card. This proactive approach not only mitigates potential financial losses but also strengthens overall transaction security.

3.2 Scope

Given the escalating concerns surrounding ATM security, there is a pressing need to expand the scope of the project to address emerging threats and vulnerabilities. The traditional reliance on conventional security measures, such as magnetic cards and PINs, has proven inadequate in thwarting sophisticated fraud attempts and unauthorized access. Key areas of concern include the prevalence of card cloning, vulnerabilities in PIN systems, and the susceptibility to social engineering tactics.
To effectively address these challenges, the project scope will encompass the implementation of a comprehensive security framework. This framework will include robust multi-factor authentication mechanisms and the integration of cutting-edge biometric technologies. Additionally, the scope will extend to incorporate proactive measures such as real-time fraud detection and instant alert systems.
By broadening the project scope to encompass these critical aspects, we aim to fortify

ATM security and enhance overall transaction integrity. The project will not only reduce the risk of financial losses associated with fraudulent activities but also bolster user confidence in the security of ATM transactions. Moreover, the implementation of advanced security measures will contribute to the establishment of a resilient ATM infrastructure capable of mitigating evolving security threats.

3.3 Objectives

The objectives of the project encompass a comprehensive review and analysis of current advancements in deep learning, particularly focusing on deep neural networks (DNNs), within the realm of facial recognition technology. This paper will specifically explore their relevance and application in fortifying automated teller machine (ATM) security infrastructure.

Furthermore, the project aims to investigate various methodologies and architectures of DNNs for facial recognition, with a specific emphasis on their efficacy, precision, and resilience in addressing real-world security challenges encountered in ATM environments.

Additionally, the project seeks to evaluate and compare the performance of different DNN models tailored for facial recognition within the ATM security context. This evaluation will take into account critical factors such as performance metrics, versatility, and adaptability across diverse environments and user scenarios.

Moreover, the project will integrate an alert system to enhance security measures. This system will enable real-time detection of suspicious activities, triggering immediate notifications to account holders and temporary deactivation of ATM cards if necessary. Through this integration, the project aims to not only enhance ATM security through advanced facial recognition technology but also proactively address emerging security threats.

3.4 Proposed Methodology

Our proposed methodology aims to leverage deep neural networks (DNN) to enhance ATM security, particularly through the implementation of facial recognition technology. DNN facial recognition is a cutting-edge approach that utilizes advanced deep learning techniques to accurately identify individuals based on their facial features. This method offers superior accuracy and adaptability across various applications, including ATM security.

The process begins with the collection of diverse facial data, which is then utilized to

train the DNN facial recognition model. Initially, convolutional neural networks (CNN) are employed to preprocess the facial data, extracting relevant features and removing noise. During the training phase, the DNN learns to encode specific facial characteristics, generating digital representations known as face embeddings. These embeddings enable the system to distinguish between different individuals accurately.

In the authentication phase, the system utilizes the trained DNN model to compare input facial images with stored embeddings in the database. By analyzing facial placements and similarities, the system can effectively authenticate users and grant access to ATM functionalities.

Additionally, we propose integrating an alert system into the ATM software to enhance security further. This alert system will continuously monitor ATM transactions for any suspicious activities or unauthorized access attempts. In the event of such occurrences, immediate notifications will be sent to account holders, alerting them to potential security threats.

The effectiveness of our proposed methodology relies on the architecture of the DNN model and the quality of the training data. By optimizing these factors and implementing robust security measures such as the alert system, we aim to achieve high levels of accuracy and reliability in identifying individuals and safeguarding ATM transactions against fraudulent activities.

3.5 Project Requirements

3.5.1 Datasets

The datasets used in our project comprise both pre-trained models and a custom training dataset tailored to our specific requirements. These pre-trained models, obtained from the Torch and Caffe frameworks, have undergone training on extensive datasets, including ImageNet, which contains millions of labeled images across various categories. Leveraging these pre-trained models provides our system with a foundation of generalized features and patterns learned from vast amounts of data. Additionally, we incorporate a custom training dataset that continuously evolves as new users register. This dataset encompasses facial images captured from diverse angles, expressions, and lighting conditions, ensuring the robustness and accuracy of our facial recognition model. To further enrich our training dataset, we employ data augmentation techniques such as rotation, flipping, scaling, and noise addition, augmenting the variability of facial images. This approach helps prevent overfitting and enhances the model's capability to accurately recognize faces in real-world scenarios. By combining the knowledge distilled from large-scale pre-trained datasets

with our tailored training data, our facial recognition system achieves a refined balance between leveraging existing knowledge and adapting to specific user needs, ultimately enhancing its accuracy, reliability, and usability.

3.5.2 Functional Requirements

Facial Recognition System: The system must possess the capability to capture and process facial images promptly and accurately in real-time. It should be equipped with robust algorithms to detect and recognize registered users' faces with precision.

User Authentication: Authentication of users should rely on facial recognition technology, utilizing a comprehensive database containing authorized users' facial data for verification purposes.

Security Alerts: The system should be designed to promptly alert security personnel upon detecting an unrecognized face or any suspicious activity. It should have the capability to generate real-time alerts to mitigate potential security breaches effectively.

Integration with ATM: Seamless integration with ATM software is imperative for user verification prior to conducting transactions. The system should seamlessly interface with the ATM interface to ensure a smooth authentication process.

Accuracy and Performance: The facial recognition system must exhibit exceptional accuracy in identifying users, adhering to stringent performance standards. It should deliver consistent performance within acceptable response times to facilitate swift user authentication processes.

Alert System Integration: Additionally, the system should include an alert mechanism to notify account holders in real-time in case of any detected suspicious activity or security breaches. This feature enhances the system's ability to promptly address security concerns and ensure the safety of ATM transactions.

3.5.3 Non Functional Requirements

The system must meet stringent security standards to prevent unauthorized access, including robust defenses against hacking and spoofing attempts. Ensuring high reliability is crucial, with minimal downtime and errors even during periods of heavy usage. Both customers and bank staff should find the system intuitive and user-friendly, with clear instructions and feedback throughout the facial recognition process. Scalability features are necessary to accommodate a growing user base and increasing transaction volumes while maintaining optimal performance. Compliance with privacy and data protection regulations, as well as adherence to banking industry standards, is imperative to safe-

guard sensitive information. The system should also facilitate easy maintenance, allowing for regular updates and enhancements, with a well-documented codebase to streamline troubleshooting and debugging processes. Additionally, integrating an alert mechanism will promptly notify users and security personnel of any detected suspicious activity or security breaches, enhancing the system's overall security posture and ensuring swift response to potential threats.

3.5.4 Hardware Requirements

The system necessitates compatible ATM hardware capable of integrating facial recognition technology, potentially requiring modifications or upgrades to accommodate requisite cameras and processing capabilities. High-quality cameras with facial recognition functionality are indispensable for capturing and analyzing user facial data accurately. Adequate processor and memory resources are essential to facilitate efficient operation of facial recognition algorithms. Secure storage solutions are imperative for safeguarding biometric data against unauthorized access. Reliable network connectivity is indispensable for enabling real-time communication with central systems for authentication and monitoring purposes. Additionally, power backup solutions are essential to ensure uninterrupted system operation, particularly during power outages. Integrating hardware components to support the alert system, such as sensors for detecting suspicious activity or breaches, and communication devices for transmitting alerts to users and security personnel, is also imperative to enhance overall system security and responsiveness.

3.5.5 Software Requirements

The software and modules utilized in the project, along with some recommendations, are as follows:

Facial Recognition: Utilizing the DNN (Deep Neural Network) framework for facial recognition purposes. Operating System (OS): The project can run on either the Linux or Windows operating systems, providing flexibility and compatibility with various environments.

Database Management System (DBMS): SQL (Structured Query Language) for managing and storing user data, including biometric information and authentication records.

Alert System: Integration with Twilio for implementing real-time alerts and notifications, ensuring prompt communication in case of suspicious activities or security breaches.

User Interface (UI): Tkinter, a Python library, can be employed to develop a user-

friendly interface for interacting with the facial recognition system and accessing ATM functionalities.

Development Environment: Jupyter Notebook can be utilized for training the DNN model, facilitating interactive and collaborative development, as well as enabling seamless integration with the user registration process. By leveraging these software components and modules, the project aims to deliver a robust and user-centric solution for enhancing ATM security through facial recognition technology

3.6 Project Plan

3.6.1 Project Resources

Hardware Resources:

1. ATM Hardware: Existing or new ATM hardware compatible with facial recognition technology, potentially requiring modifications or upgrades. Robust CPUs and GPUs are essential for effectively training deep learning models, enabling the processing of extensive datasets and intricate neural network structures.

2. Cameras: High-quality cameras capable of capturing and analyzing facial images for authentication purposes. Top-tier cameras are required to capture precise and well-defined facial images to facilitate authentication. These cameras must be suitable for the ATM setting and adaptable to various lighting conditions.

3. Processor and Memory: Sufficient processing power and memory to efficiently run facial recognition algorithms.

4. Network Connectivity: Reliable network connectivity to enable real-time communication with central systems for authentication and monitoring. Power Backup: Backup power solutions to ensure continuous operation, particularly during power outages.

Software Resources:

1. Operating System (OS): Compatibility with both Linux and Windows operating systems for flexibility and adaptability. Facial Recognition Framework: Utilization of DNN (Deep Neural Network) framework for facial recognition tasks.

2. Database Management System (DBMS): Implementation of SQL (Structured Query Language) for efficient management and storage of user data, including biometric

information and authentication records. Alert System: Integration with Twilio for real-time alerts and notifications, enabling prompt communication in case of security breaches or suspicious activities.

3. User Interface (UI) Development: Use of Tkinter, a Python library, for developing a user-friendly interface to interact with the facial recognition system and access ATM functionalities.

4. Integrated Development Environment (IDE): Development environments such as PyCharm or Visual Studio Code are utilized for coding, debugging, and testing the software modules.

5. Development Environment: Utilization of Jupyter Notebook for interactive development, facilitating training of the DNN model and seamless integration with the user registration process.

By ensuring the availability and proper configuration of these hardware and software resources, the project aims to create a robust and efficient system for enhancing ATM security through facial recognition technology.

3.6.2 Module Split-up

To effectively manage the development of the Enhanced ATM Security using Facial Recognition project, we have organized it into various modules.

1. Data Collection and Preprocessing Module: This module handles the collection and preprocessing of the facial recognition dataset. It involves tasks such as data cleaning, labeling, and preparation for model training.

2. Facial Recognition Model Development Module: This segment focuses on constructing the deep neural network model for facial recognition. It includes developing and refining the model architecture.

3. Integration with ATM Software Module: This module revolves around integrating the facial recognition system with the existing ATM software. Collaboration with the ATM software development team is essential for this task.

4. User Interface Module: Responsible for designing and implementing the user interface for the facial recognition system on the ATM, ensuring a user-friendly experience.

5. Security and Compliance Module: This module emphasizes enhancing the security aspects of the facial recognition system. It involves implementing security protocols and alert systems to address any suspicious activity.

6. Testing and Quality Assurance Module: This segment is accountable for testing the facial recognition system for accuracy, reliability, and security, encompassing both functional and non-functional testing.

7. Documentation and Reporting Module: In charge of creating comprehensive documentation for the project, including technical specifications, user manuals, and reports.

3.6.3 Functional Decomposition

The entire system can be decomposed into more manageable subparts as follows:

1. Facial Recognition System:
   - Capture and Process Facial Images
   - Detect and Recognize Registered User's Face
   - Compare Facial Data with Database Records

2. User Authentication:
   - Authenticate Users Based on Facial Recognition
   - Store and Retrieve Authorized Users' Facial Data
   - Handle User Authentication Errors and Edge Cases

3. Security Alerts and Monitoring:
   - Monitor ATM Area for Suspicious Activities
   - Generate Real-time Alerts for Security Breaches
   - Implement Security Protocols for Potential Threats
   - Integrate Alert System for Instant Notifications

4. Integration with ATM Software:
   - Integrate Facial Recognition System with ATM Software
   - Coordinate Communication Between ATM and Facial Recognition System
   - Ensure Smooth Transaction Flow with User Authentication

5. Accuracy and Performance Optimization:
   - Ensure High Accuracy in User Identification
   - Optimize Facial Recognition Algorithm for Speed and Efficiency
   - Enhance Performance in Various Lighting Conditions

6. User Interface Design:
   - Design Intuitive and User-friendly Interface for Facial Recognition
   - Provide Clear Instructions and Feedback to ATM Users
   - Create a Seamless User Experience during Authentication

7. Documentation and Reporting:
   - Prepare Technical Documentation for the Facial Recognition System
   - Develop User Manuals and Guidelines for ATM Staff and Users
   - Incorporate Reporting Mechanisms for System Performance and Security Alerts

3.6.4 Project Team Role and Responsibilities

Project Manager:

Role: Oversees project progress, ensures coordination among team members, and resolves any conflicts or issues that arise.

Responsibilities: Plans project milestones, facilitates team meetings, tracks progress, and communicates updates to the team.

Facial Recognition Specialist & Data Scientist:

Role: Leads the development of the facial recognition system, focusing on its accuracy and effectiveness. Manages the facial recognition dataset and ensures its quality for training the model.

Responsibilities: Designs and fine-tunes the deep neural network model, conducts research on facial recognition techniques, preprocesses the data, performs data analysis, and optimizes the dataset for effective model training. Collaborates with team members to integrate the system with the ATM software.

Software Developer:

Role: Implements the integration of the facial recognition system with the ATM software, focusing on seamless functionality.

Responsibilities: Writes code, tests software components, troubleshoots integration issues, and ensures compatibility with existing ATM software.

Database Administrator:

Role: Manages the database for storing and retrieving facial recognition data securely.

Responsibilities: Ensures data integrity, implements backup and recovery procedures, and optimizes database performance. Works closely with the software developer to ensure seamless integration with the ATM software.

Documentation Specialist:

Role: Manages project documentation and reporting, ensuring clarity and completeness.

Responsibilities: Prepares technical specifications, user manuals, and project reports. Maintains records and communicates project updates to team members.

Front-End Developer:

Role: Develops the user interface of the ATM software, focusing on user experience and interaction design.

Responsibilities: Implements visual elements and user interactions, integrates the user interface with the back-end, and optimizes the user experience for different devices.

Back-End Developer:

Role: Manages server-side application logic and database integration to support the facial recognition system.

Responsibilities: Develops the server architecture, creates APIs for communication between the front-end and the database, and ensures data security and integrity. Collaborates with the software developer to ensure smooth integration with the ATM software.

3.6.5 Project Plan 3.0

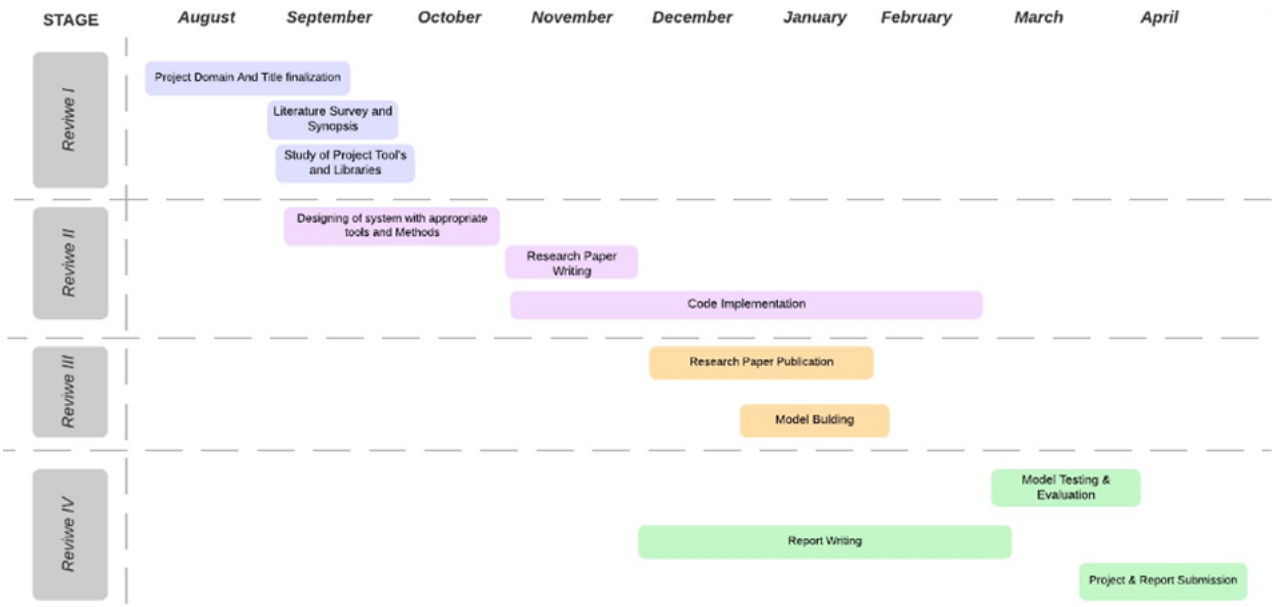

Figure 3.1: Project Plan 3.0

3.6.6 PERT Table

Task	Duration
Defining project scope and objective	week 1
Requirement analysis and system architecture	week 2-week 6
Data collection and preprocessing	week 3 - week 6
Environment building	week 5- week 9
Evaluation metrics and criteria	week 8- week 10
Model Building	week 9- week 16
Model evaluation	week 13- week 17
Testing and debugging	week 16- week 19
Project termination	week 19- week 22

3.6.7 PERT Diagram

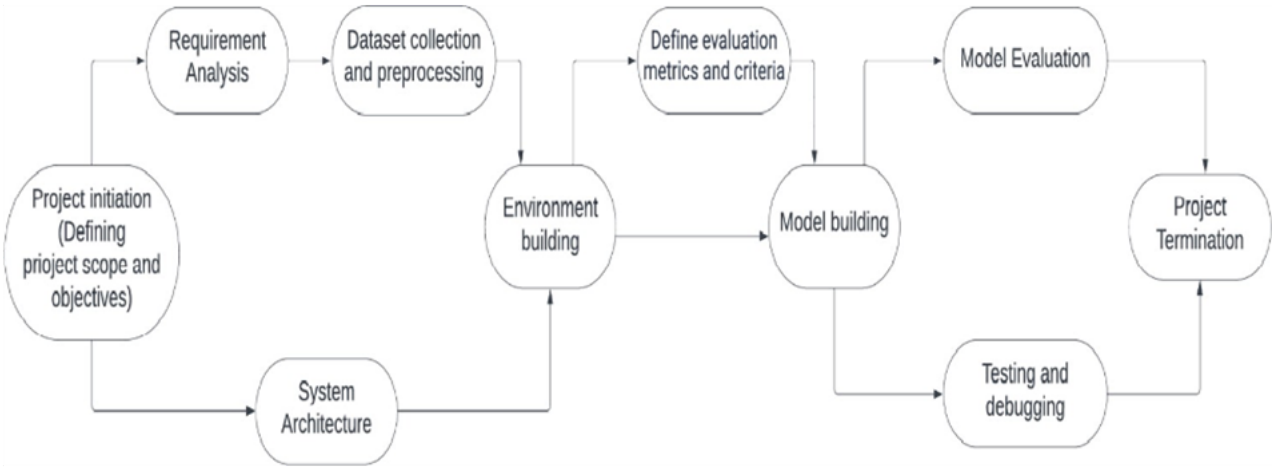

Figure 3.2: PERT

4. System Analysis and Design

4.1 System Architecture

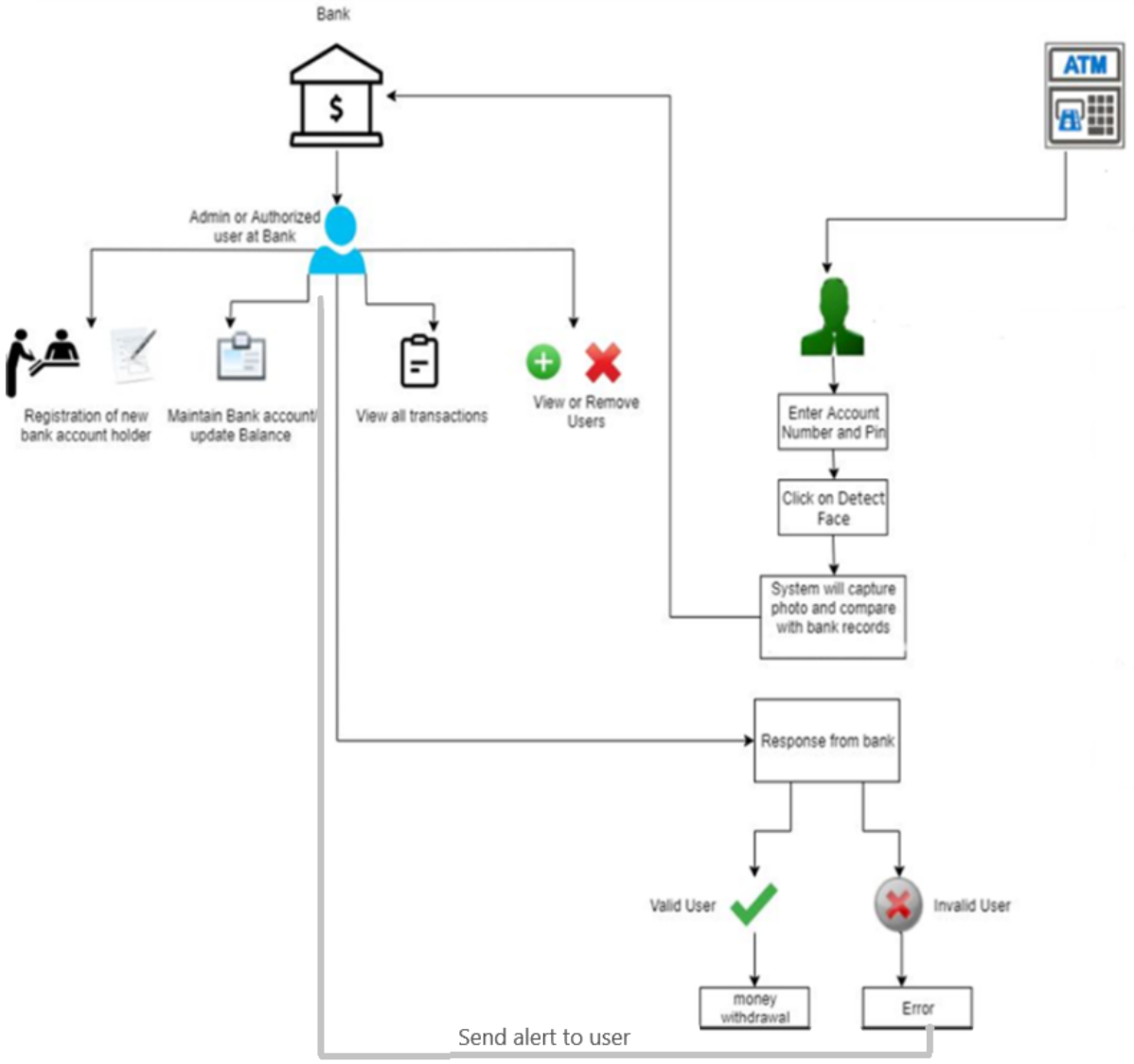

Figure 4.1: Architecture Diagram

4.2 Necessary UML Diagrams

4.2.1 Use Case Diagram

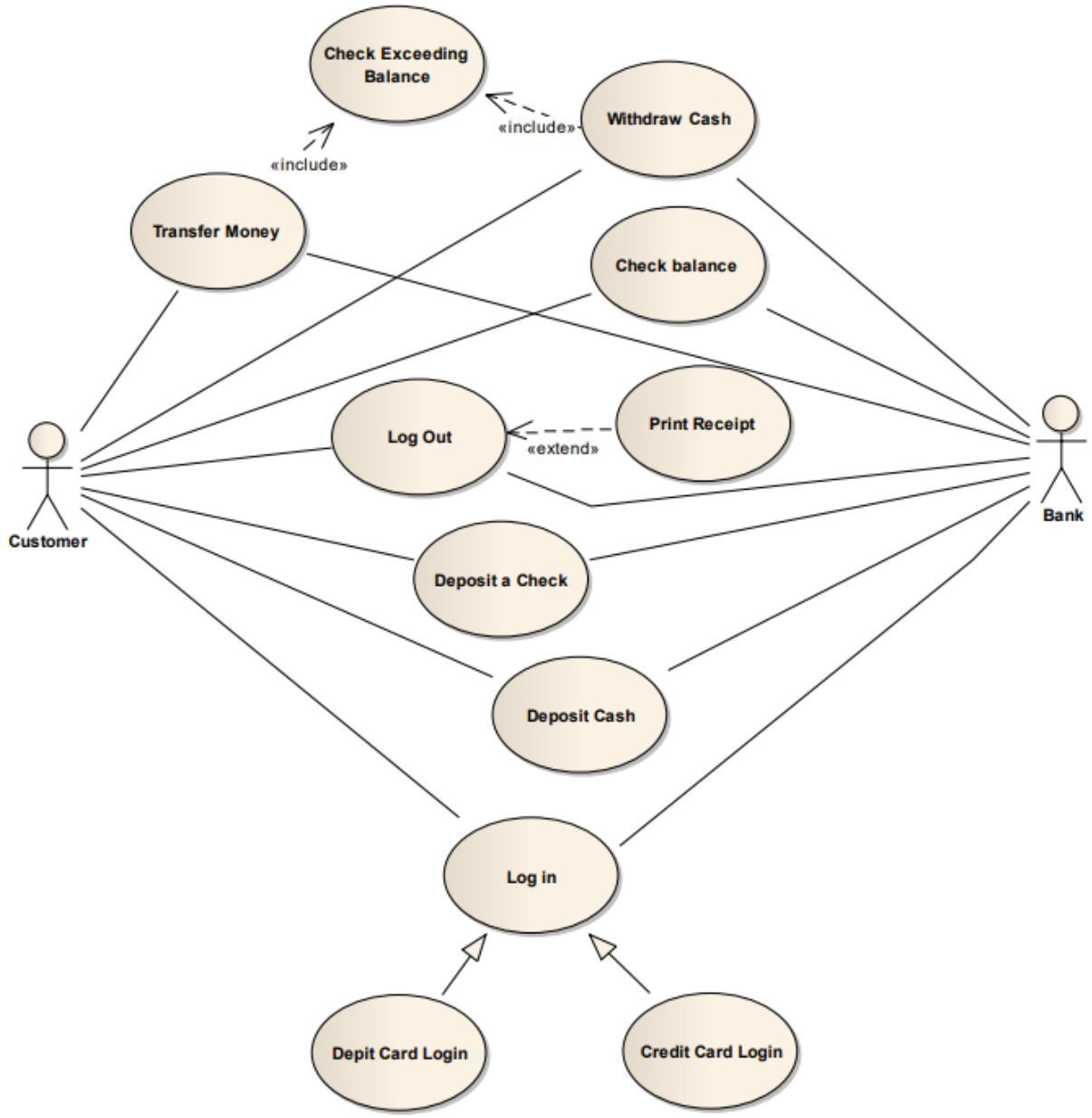

Figure 4.2: Use Case Diagram

4.2.2 DFD

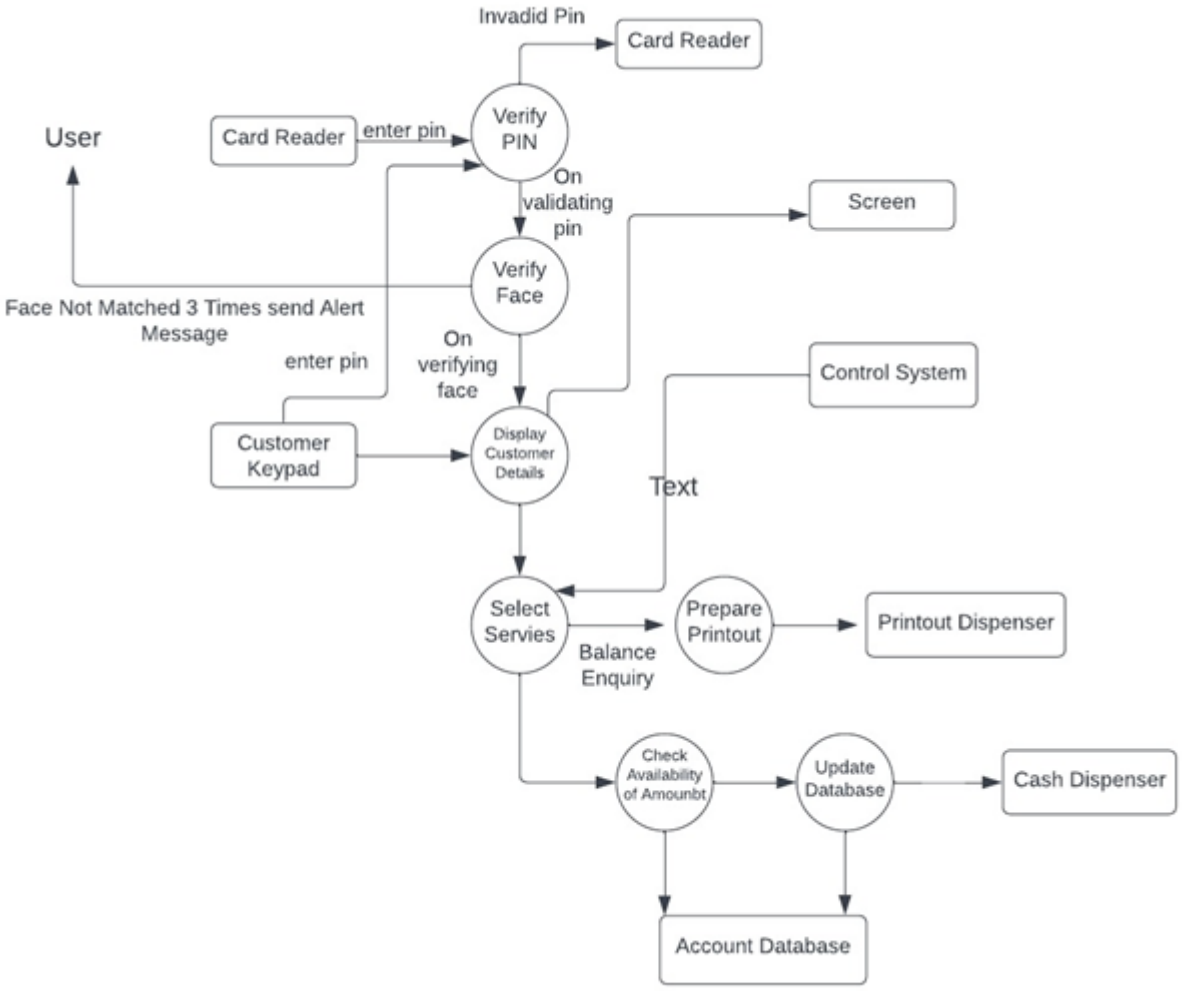

Figure 4.3: Data Flow Diagram

4.2.3 Activity Diagram

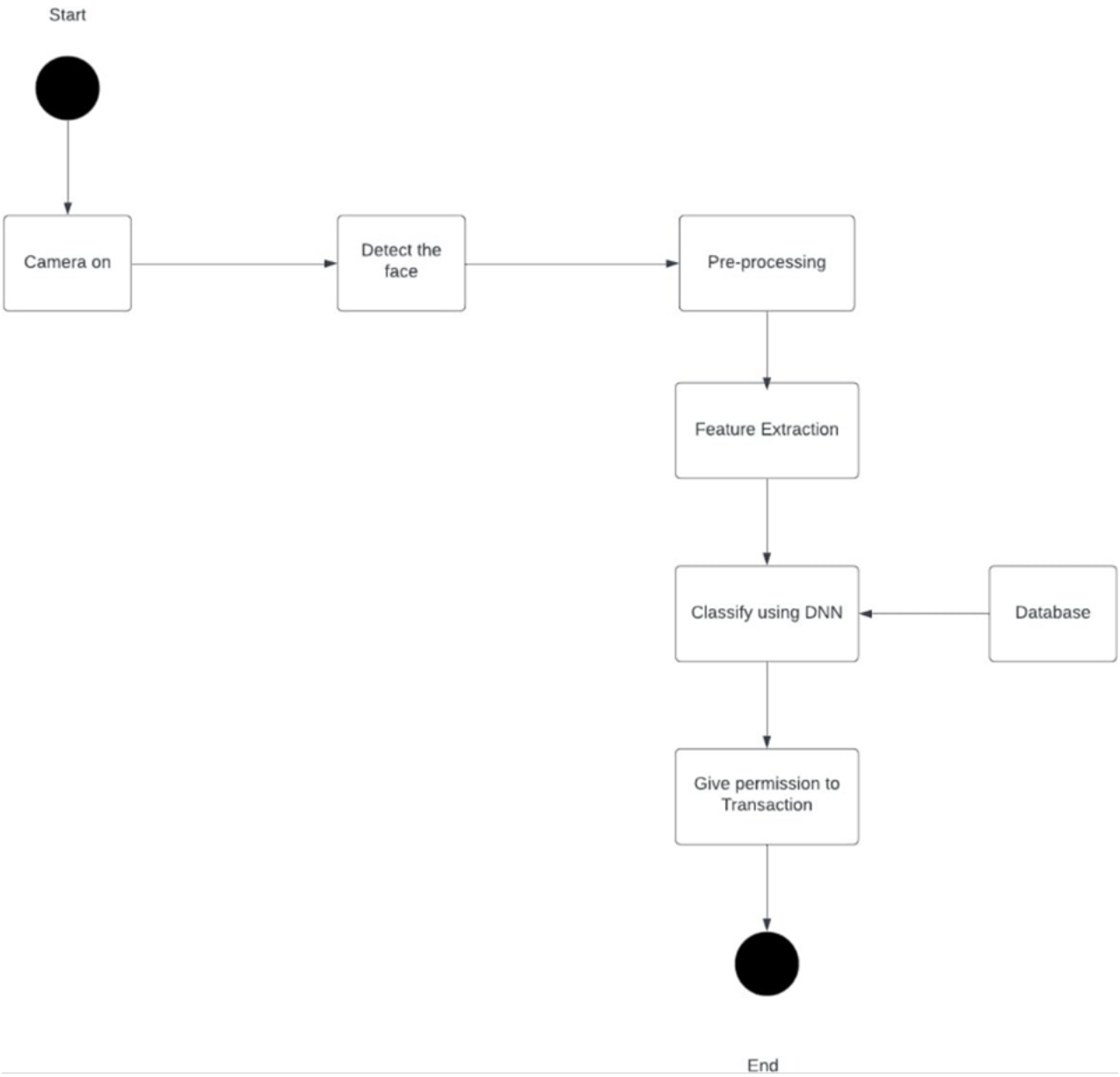

Figure 4.4: Activity Diagram

4.2.4 Sequence Diagram

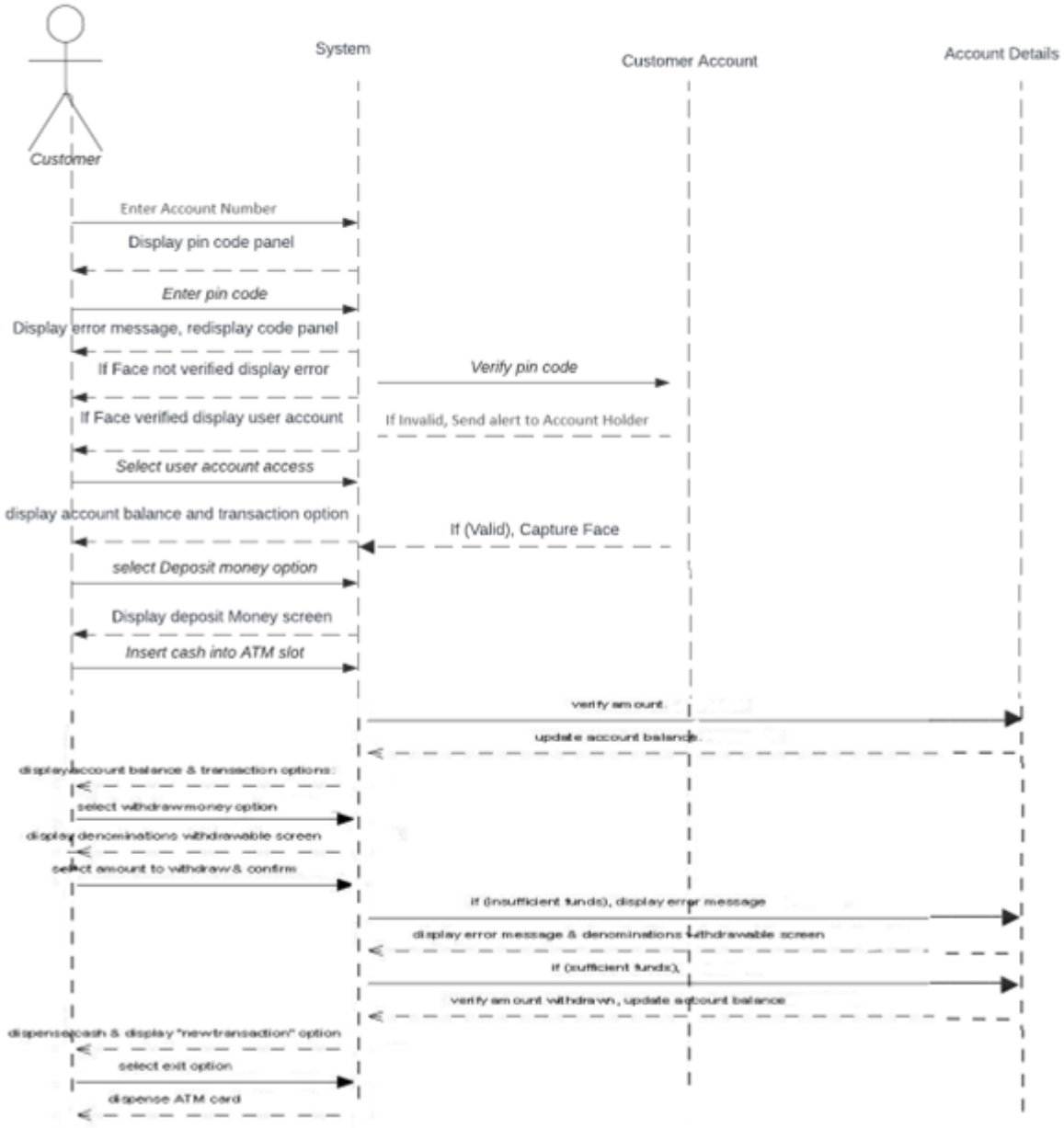

Figure 4.5: Sequence Diagram

4.3 Algorithm and Methodologies

1. Data Collection and Preprocessing: Effective face-to-face data collecting, data management, and prioritizing strategies are critical to obtaining high-quality, consistent, and reliable data.

2. Facial Recognition Methods: Investigate and assess the current landscape of deep learning techniques, with a specific focus on facial recognition technology within deep neural networks (DNNs), in the context of enhancing ATM security infrastructure.

3. Facial Recognition Algorithms: Compare and contrast different approaches, such as the use of various DNN models for face detection in images and extracting facial embeddings, to provide a comprehensive understanding of the field.

4. Model Training and Evaluation: Proficiency in training models, validation, and assessment processes to gauge the performance of facial recognition models is essential. Familiarity with metrics like accuracy, precision, recall, and F1 score is imperative for evaluating the quality of the model.

5. Software Development and Integration: Proficiency in programming languages like Python and frameworks such as TensorFlow or PyTorch for implementing DNNs is indispensable. Understanding software development methodologies and version control is also beneficial.

6. Accessibility: Conduct user-centric research to assess user perceptions, acceptance, and usability of facial recognition technology in ATM security, aiming to identify potential usability challenges and inform the development of user-friendly security solutions.

7. Fraud Detection and Notification System: In addition to facial recognition technology, the system incorporates a robust fraud detection and notification mechanism. This feature enhances account security by continuously monitoring for suspicious activities, such as unauthorized access attempts where the facial features do not match those of the original account holder.

5. Implementation

5.1 Stages of Implementation

5.1.1 Implementation of Modules

The implementation of the project involves the development and integration of several modules to achieve the objectives of enhancing ATM security through facial recognition technology. Each module is responsible for specific functionalities, and their successful implementation ensures the overall effectiveness of the system. Here is a breakdown of the implementation of each module:

1. **Data Collection and Preprocessing Module:**

   - The data collection module is implemented to gather a diverse dataset of facial images for model training.

   - Preprocessing techniques such as cleaning, labeling, and standardizing the collected data are applied to prepare it for training.

   - Data augmentation methods may also be employed to increase the diversity and robustness of the dataset.

2. **Facial Recognition Model Development Module:**

   - This module focuses on developing the deep neural network (DNN) model for facial recognition.

   - The model architecture is designed, taking into account factors such as network depth, layer configurations, and activation functions.

   - Training of the DNN model is conducted using the preprocessed dataset, with adjustments made to optimize performance and accuracy.

3. **Integration with ATM Software Module:**

   - The integration module involves incorporating the facial recognition system into the existing ATM software infrastructure.

   - Communication protocols and APIs are established to facilitate data exchange between the facial recognition system and the ATM software.

   - Compatibility testing is conducted to ensure seamless integration and functionality within the ATM environment.

4. **User Interface Module:**

   - The user interface module is responsible for designing and implementing the graphical interface for the facial recognition system on the ATM.

   - User-friendly features such as clear instructions, feedback messages, and intuitive navigation are incorporated to enhance user experience.

   - Iterative testing and refinement are performed to optimize the usability and effectiveness of the interface.

5. **Alert System Module:**

   - The alert system module is responsible for implementing real-time monitoring and response mechanisms to detect and respond to security incidents or suspicious activities.

   - Upon detecting a security threat, the alert system generates immediate notifications to designated security personnel or authorities, enabling timely response and intervention.

   - The alert system is designed to be highly responsive and configurable, allowing for customization of alert triggers, notification methods, and escalation procedures based on predefined security policies and requirements.

6. **Testing and Quality Assurance Module:**

   - The testing module involves comprehensive testing of the entire system to verify its functionality, performance, and security.

   - Functional testing is conducted to validate each module's individual functionalities, while integration testing evaluates the system as a whole.

   - Non-functional testing, including performance testing and usability testing is performed to assess the system's reliability and effectiveness under various conditions.

By successfully implementing these modules, the project aims to achieve its objectives of enhancing ATM security through facial recognition technology, providing users with a secure and seamless banking experience.

5.2 Experimentation Setup

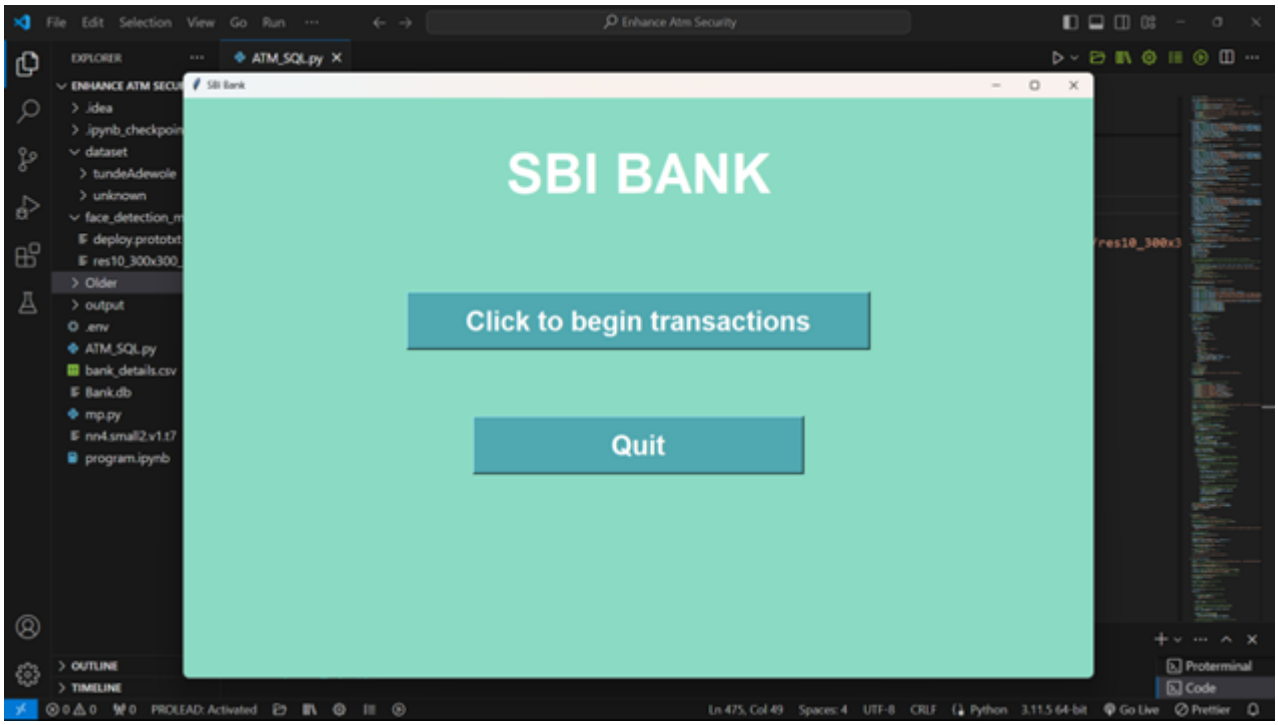

Figure 5.1: Welcome Page

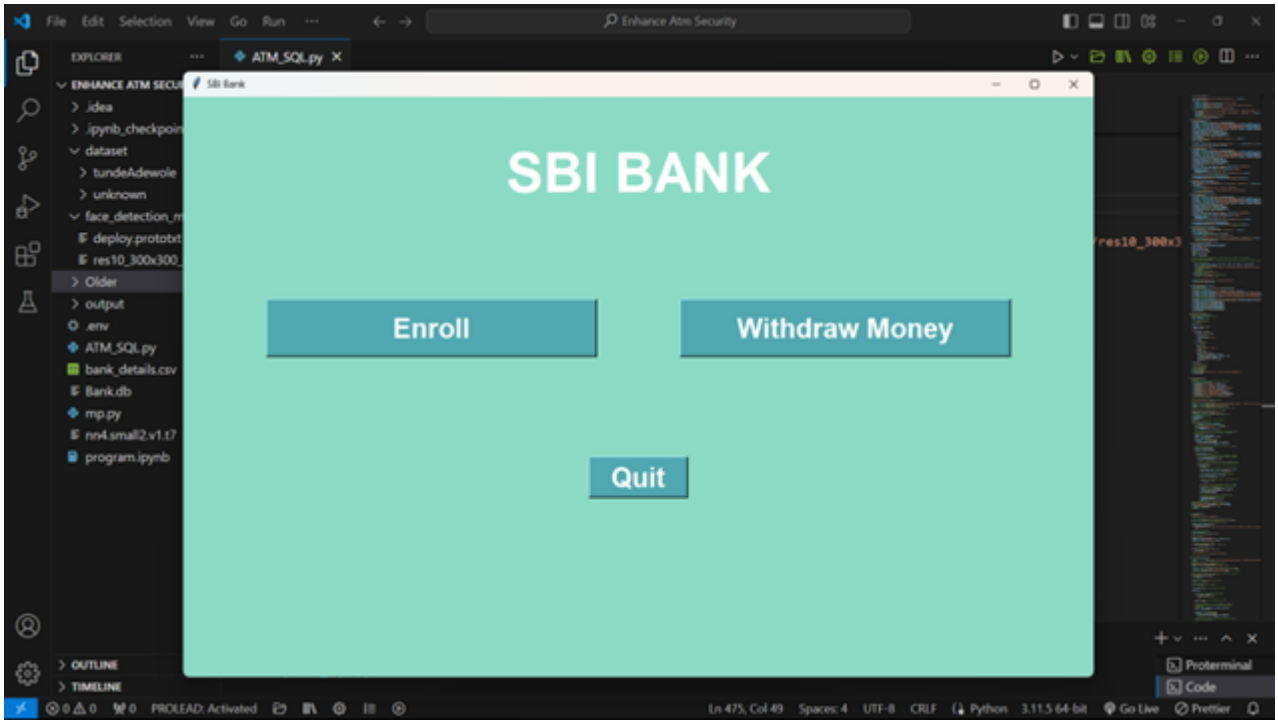

Figure 5.2: Registration/Login Selection Page

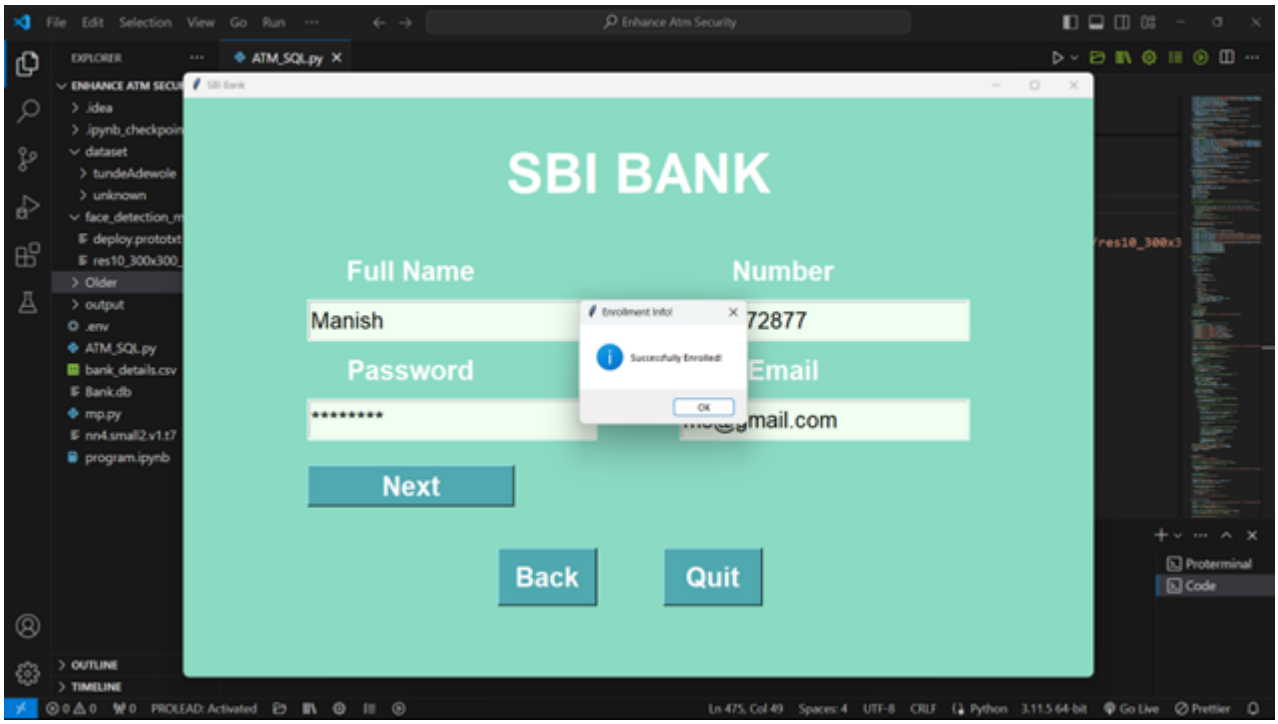

Figure 5.3: User Enrollment Page

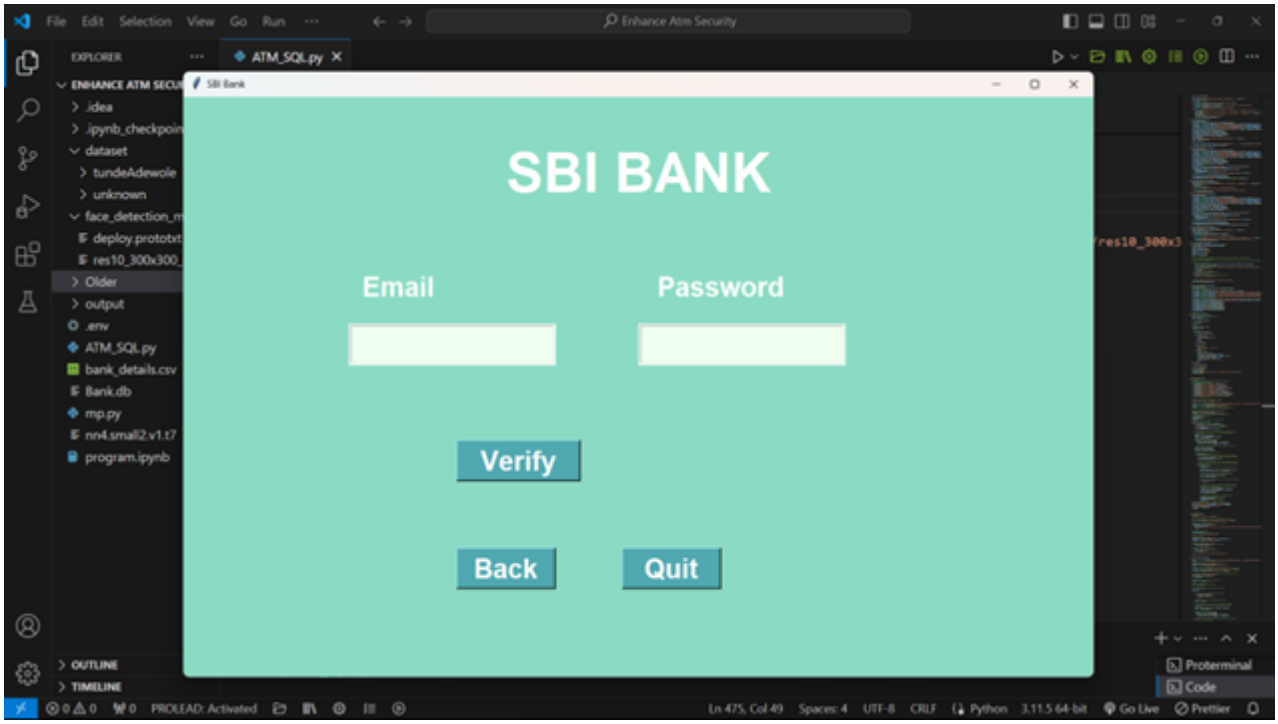

Figure 5.4: Login Page

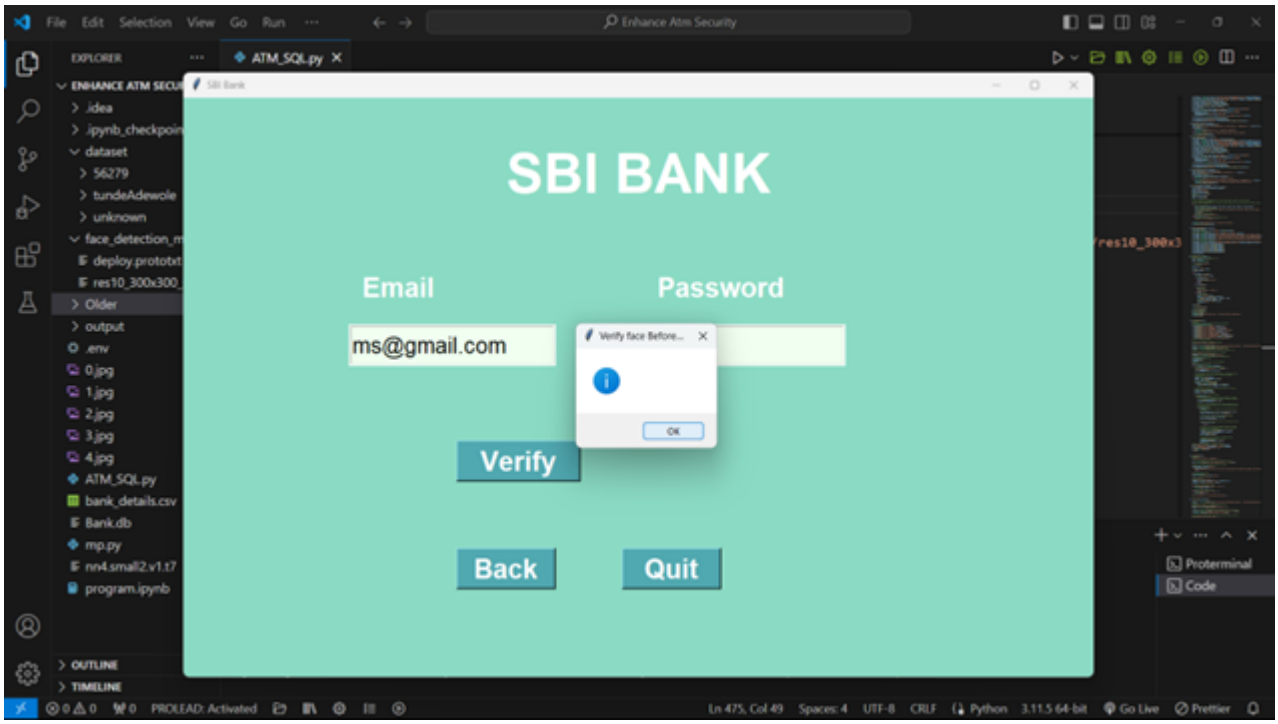

Figure 5.5: Login Success

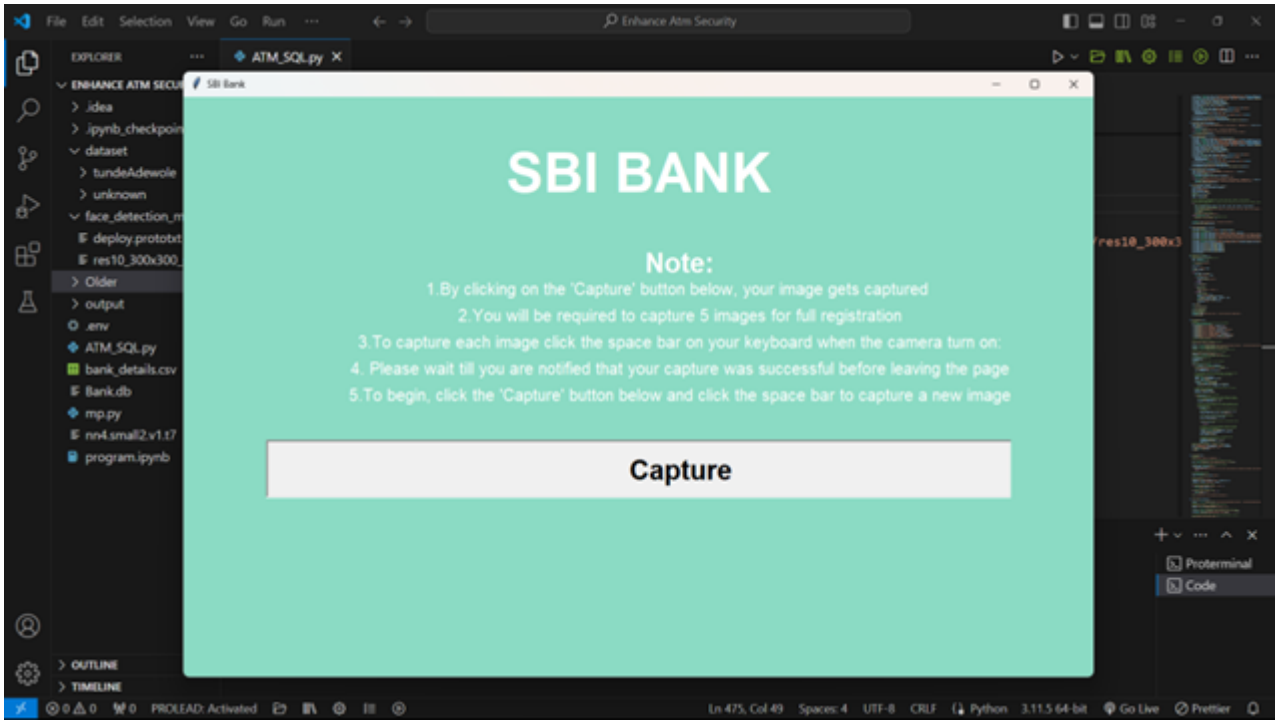

Figure 5.6: Capture Face for Database Page

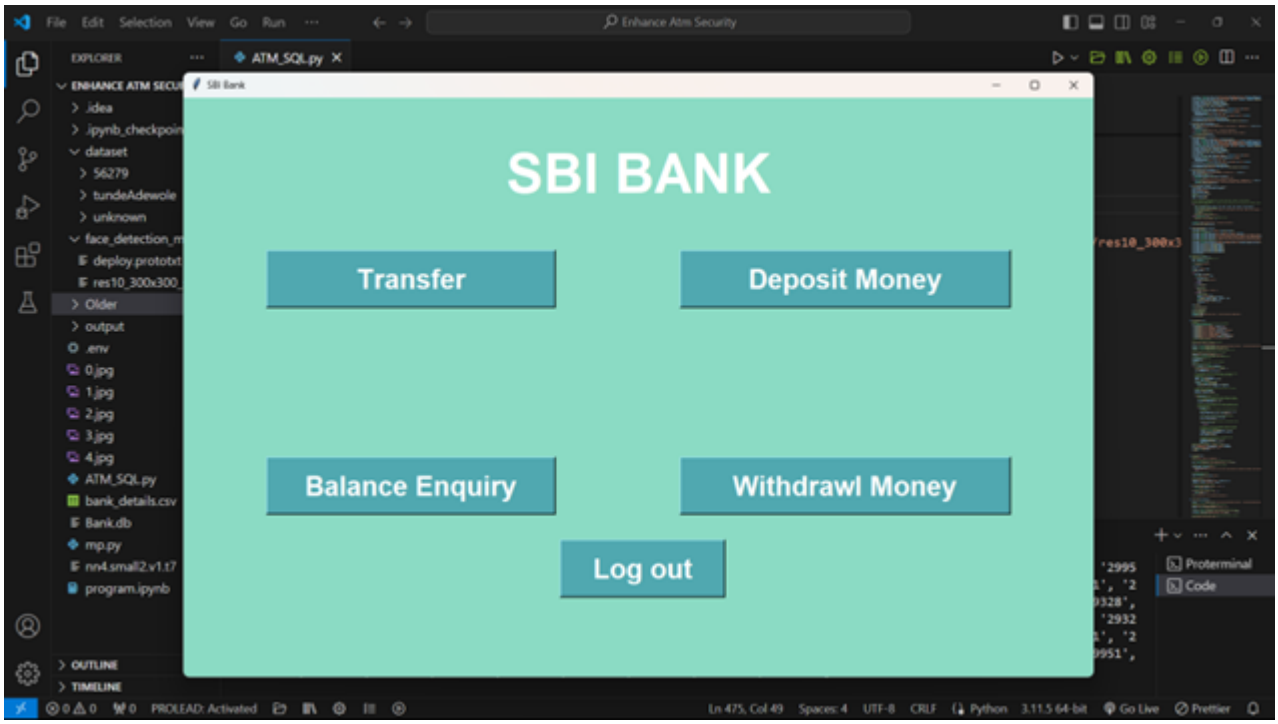

Figure 5.7: Home Page

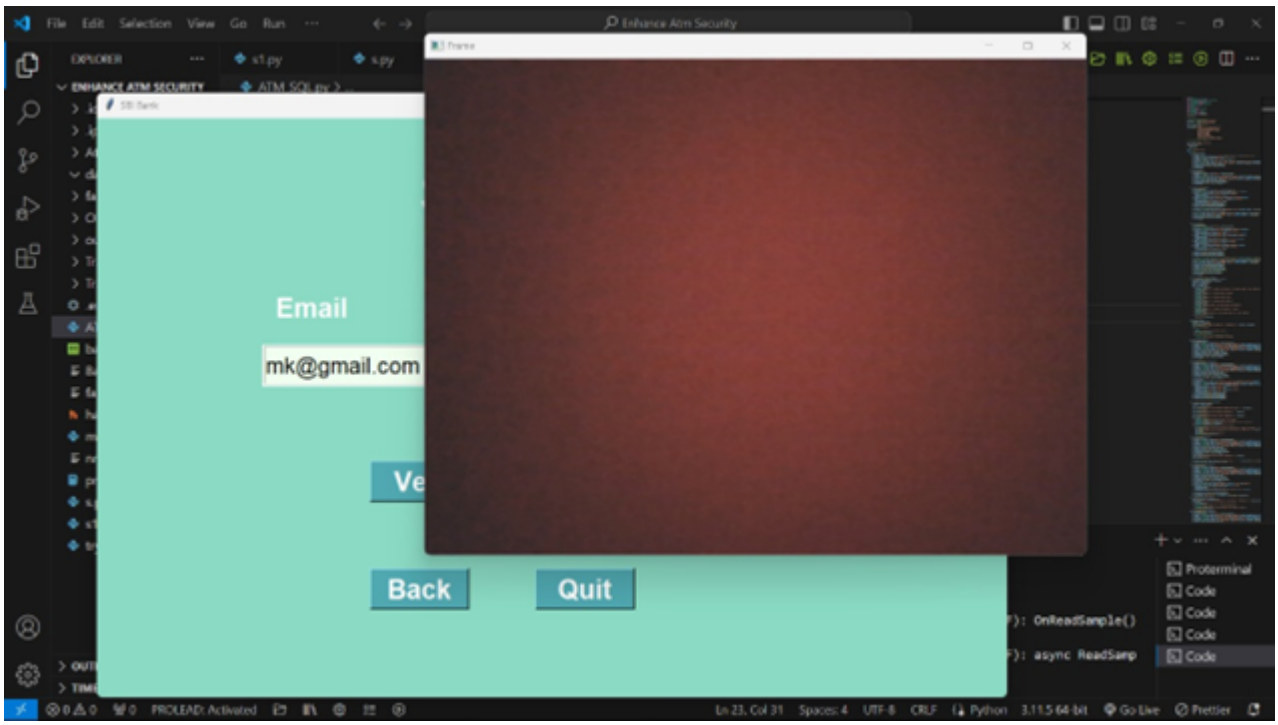

Figure 5.8: Face Verification Page

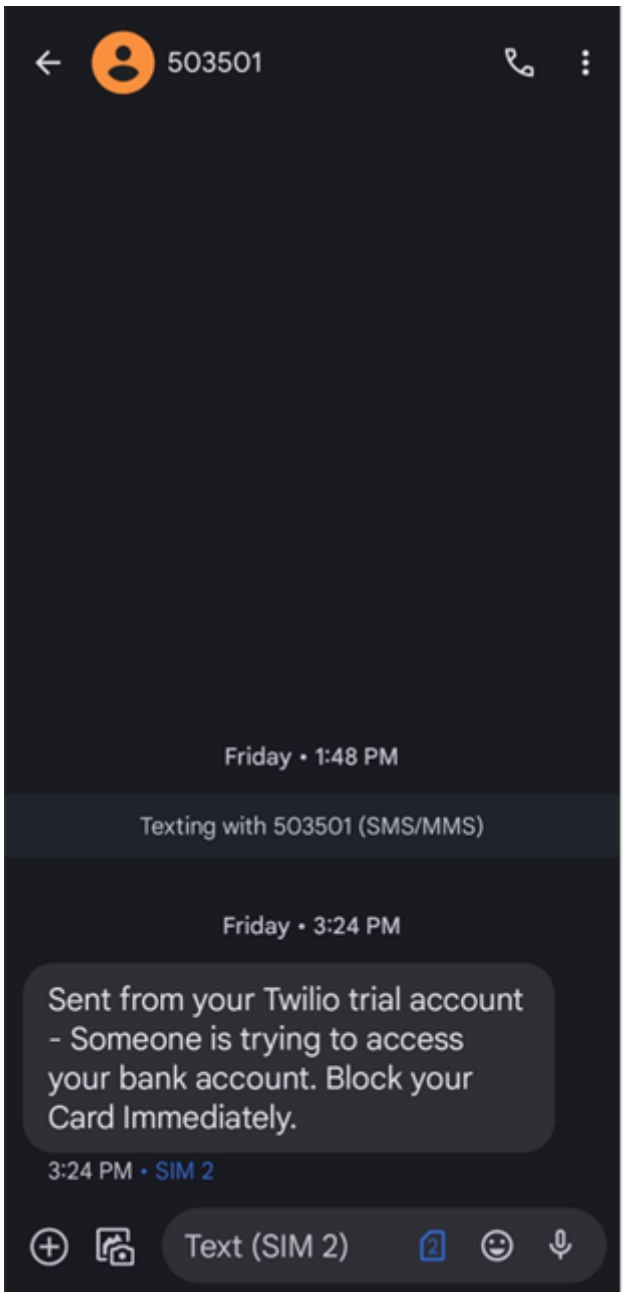

Figure 5.9: Alert Message on the Phone

6. Results

6.1 Results of Experiments

6.2 Result Analysis

The project has been successfully implemented with all the necessary features to enhance ATM security through facial recognition technology. Key components of the system, including data collection and preprocessing, facial recognition model development, integration with ATM software, user interface design, security alerts and monitoring, and testing and quality assurance, have been effectively developed and integrated.

The facial recognition system is capable of capturing and processing facial images in real-time, accurately detecting and recognizing registered users' faces. Through the integration with ATM software, the system seamlessly authenticates users before transactions, ensuring secure interactions.

Moreover, the user interface has been designed to be intuitive and user-friendly, providing clear instructions and feedback during the facial recognition process. Security alerts and monitoring mechanisms have been implemented to detect and notify security personnel in real-time in the event of any suspicious activities, thereby enhancing the overall security posture of the ATM system.

Testing and quality assurance efforts have been conducted to ensure the accuracy, reliability, and security of the facial recognition system. Functional and non-functional testing have been performed to validate the system's performance under various conditions, meeting the specified requirements.

Overall, the implementation of the project has demonstrated its effectiveness in enhancing ATM security through facial recognition technology, providing users with a secure and seamless banking experience. Further details on the performance metrics and outcomes of the testing phase are presented in the subsequent sections.

6.3 Testing

White Box

Following is the white box testing in our project:

1. **Pin Verification Testing:**

   - Verify that the pin entered by the user during login matches the original pin stored in the database.

   - Test various scenarios such as correct pin, incorrect pin, empty pin, and invalid pin format to ensure robust pin verification.

2. **Data Storage Testing:**

   - Validate the functionality of data storage mechanisms to ensure that user data entered after registration is accurately saved into the database.

   - Test scenarios involving different types of user data such as username, password, contact information, and transaction details to verify data integrity and consistency.

3. **Database Interaction Testing:**

   - Verify the interaction between the application and the database to ensure seamless data retrieval and manipulation.

   - Test CRUD (Create, Read, Update, Delete) operations to ensure that data can be properly added, retrieved, updated, and deleted from the database.

4. **Error Handling Testing:**

   - Test error handling mechanisms to ensure that appropriate error messages are displayed when unexpected events or invalid inputs occur.

   - Validate error scenarios such as network errors, database connection failures, and input validation errors to ensure graceful handling of exceptions.

Unit Testing

Integration Testing

Following is the black box integration testing in our project:

1. **Authentication Integration Testing:**

   - Test the integration between the authentication module and other modules to ensure seamless user authentication functionality.

   - Verify that the user authentication process, including login and registration, integrates correctly with the user interface, database, and other system components.

2. **Alert System Integration Testing**

   - Validate the integration of the alert system module with other system components to ensure timely detection and notification of suspicious activities.

   - Test the interaction between the alert system and user authentication, database, and security modules to verify the generation and delivery of alerts as per system requirements.

3. **Transaction Processing Integration Testing**

   - Verify the integration between the transaction processing module and other system components to ensure accurate and secure handling of financial transactions.

   - Test scenarios involving deposit, withdrawal, balance inquiry, and fund transfer to validate the interaction between transaction processing, authentication, and database modules.

4. **User Interface Integration Testing**

   - Validate the integration of the user interface with backend functionality to ensure a seamless and intuitive user experience.

   - Test user interface elements such as buttons, forms, menus, and navigation paths to verify their interaction with backend services and data retrieval mechanisms.

5. **Database Interaction Integration Testing** - Test the integration between the application and the database to ensure proper data storage, retrieval, and manipulation. - Verify the interaction between different modules and the database, including CRUD operations, data consistency, and transaction management.

6. **I**nput Validation Integration Testing

   - Validate user mobile number. the mobile number should contain 10 digits.

7. **Error Handling Integration Testing**

   - Test the integration of error handling mechanisms with system components to ensure graceful recovery from unexpected events or errors.

   - Verify the interaction between error handling modules and user interface, transaction processing, and database modules to ensure consistent error reporting and recovery strategies.

Black Box

Test Cases

The test cases for our project encompass various critical functionalities to ensure the system's reliability and security. User authentication tests focus on validating registration, login, and password policies, while the alert system tests ensure timely and accurate notifications for suspicious activities. Transaction processing tests validate deposit, withdrawal, balance inquiry, and fund transfer functionalities to ensure accurate and secure transactions. User interface tests aim to guarantee smooth navigation and usability across different devices, while database interaction tests ensure data integrity, concurrency handling, and backup procedures. Input validation tests the acceptance of valid data. Lastly, error handling tests verify the system's ability to handle various errors gracefully, display meaningful error messages, and maintain system integrity. Through comprehensive testing, we aim to deliver a robust and reliable system to our users.

Summary of Black Box Testing

The black box testing conducted on our project involved comprehensive evaluations of various functional aspects to ensure the system's effectiveness and user satisfaction. Tests were conducted on user authentication processes, including registration, login, and password management, to validate their accuracy and security. Additionally, the alert system's functionality was thoroughly tested to ensure timely and precise notifications for any suspicious activities detected within the system. Transaction processing tests were conducted to verify the accuracy and reliability of deposit, withdrawal, balance inquiry, and fund transfer functionalities, ensuring seamless financial transactions for users. User

interface tests focused on assessing the system's usability and accessibility across different devices, ensuring a smooth and intuitive user experience. Database interaction tests validated data integrity and backup procedures, ensuring the reliability and consistency of stored information. Throughout the black box testing phase, various scenarios were simulated to identify and address any potential issues, ultimately ensuring the robustness and reliability of our system.

7. Conclusion and Future Scope

7.1 Conclusion

In conclusion, this project has explored the integration of facial recognition technology into Automated Teller Machines (ATMs) to enhance security measures and elevate user experiences. Through comprehensive examination of deep learning techniques, facial recognition algorithms, and training methodologies, we have illustrated the potential of facial recognition technology in strengthening ATM security infrastructure.

The project has emphasized the significance of multi-factor authentication, integrating facial recognition to reinforce ATM transaction security and combat fraudulent activities effectively. Moreover, advancements in Deep Neural Network (DNN) development offer promise for enhancing the adaptability and responsiveness of security systems to evolving cyber threats.

Additionally, our research underscores the importance of prioritizing user experience enhancement in ATM interactions. Seamless integration of facial recognition technology into mobile banking applications presents an opportunity to enhance the convenience and security of financial transactions across various platforms.

While pursuing these advancements, we remain steadfast in upholding robust privacy protections and adhering to ethical considerations. Future research endeavors should continue exploring innovative solutions for safeguarding personal data and ensuring compliance with regulatory guidelines.

In essence, the outcomes of this research project contribute to ongoing initiatives aimed at strengthening ATM security, enhancing user experiences, and fostering financial inclusivity. By harnessing the potential of facial recognition technology and embracing continuous improvement, we strive to create a safer and more seamless banking experience for users worldwide.

Furthermore, the incorporation of an alert system introduces an additional layer of security to the ATM environment. Designed to detect and notify security personnel in real-time of any suspicious activities, such as unauthorized access attempts or tampering with ATM components, this proactive approach enhances the overall security posture of the ATM system and helps mitigate potential security breaches before they escalate.

7.2 Limitations of the Project

While the project on Enhanced ATM Security using Facial Recognition offers numerous advantages, it is also accompanied by several limitations and challenges that necessitate careful consideration. Some of the primary limitations of this project include:

1. Privacy Concerns: The adoption of facial recognition technology raises concerns regarding the privacy and security of individuals' biometric data, presenting potential regulatory and ethical hurdles. Technical Challenges: Facial recognition systems may encounter technical hurdles such as accuracy issues in diverse lighting conditions, occlusions, and the potential for false positives or false negatives.

2. Adversarial Attacks: Facial recognition systems are vulnerable to adversarial attacks, wherein malicious actors can manipulate the system by presenting altered facial images or employing other tactics to deceive the authentication process.

3. Integration Complexity: Integrating the facial recognition system with existing ATM software and infrastructure may prove complex and require substantial modifications to the current setup, potentially resulting in compatibility issues and system disruptions.

4. Cost and Resource Intensiveness: Implementing and sustaining a robust facial recognition system demands significant financial investment, specialized hardware, and a proficient technical team, posing notable resource challenges for certain organizations.

5. Additionally, the incorporation of an alert system may introduce its own set of limitations, such as the possibility of false alerts or delays in detecting suspicious activities, which could impact the overall effectiveness of the security measures.

7.3 Future Scope

The study uncovers promising avenues for advancing the integration of facial recognition technology across diverse sectors. One prominent area for further exploration involves integrating various biometric systems, such as fingerprint and voice recognition, to strengthen security measures. This multi-factor authentication approach can significantly enhance the security of ATM transactions, making them more resilient against fraudulent activities.

Continued advancements in Deep Neural Network (DNN) development are essential, aiming not only to enhance accuracy but also to fortify the system's ability to anticipate and respond to immediate threats. With the evolving landscape of cyber threats, there is a pressing need for novel models capable of rapid adaptation to emerging risks. Moreover, prioritizing the enhancement of user experience remains crucial. Implementing intuitive design principles can streamline ATM interactions, ensuring convenience for users. Additionally, the seamless integration of facial recognition technology into mobile banking applications holds immense potential, enabling users to securely transact across various platforms.

Robust privacy safeguards are indispensable, and future research should focus on leveraging state-of-the-art privacy technologies to safeguard personal information effectively. Furthermore, implementing automated security responses, such as activating alarms or locking ATM cabins in response to suspicious activities like theft or attempted robbery, can enhance physical security measures. Exploring technologies like IoT-enabled sensors and automated gate locks can further bolster security protocols.

Bibliography

[1] Surawse, P., Bhange, Taru, S., Khot, S., Mundada, Prof. J. (2022, February). Secure ATM Transactions Using Face Recognition OTP, 2022 JETIR February 2022, Volume 9, ISSN-2349-5162

[2] M. T. H. Fuad et al.,"Recent Advances in Deep Learning Techniques for Face Recognition," in IEEE Access, vol. 9, pp. 99112-99142, 2021, doi: 10.1109/ACCESS.2021.3096136.

[3] M. Alansari, O. A. Hay, S. Javed, A. Shoufan, Y. Zweiri and N. Werghi, "GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations," in IEEE Access, vol. 11, pp. 35429-35446, 2023, doi: 10.1109/ACCESS.2023.3266068.

[4] Y. Mart´ınez-D´ıaz, H. M´endez-V´azquez, L. S. Luevano, M. Nicol´as-D´ıaz, L. Chang and M. Gonz´alez-Mendoza, "Towards Accurate and Lightweight Masked Face Recog- nition: An Experimental Evaluation," in IEEE Access, vol. 10, pp. 7341-7353, 2022, doi: 10.1109/ACCESS.2021.3135255.

[5] M. Navin Kumar, S. Raghul, K. Nirmal Prasad and P. Naveen Kumar, "Biometrically Secured ATM Vigilance System," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 919-922, doi: 10.1109/ICACCS51430.2021.9441975.

[6] S. Gokul, S. Kukan, K. Meenakshi, S. S. V. Priyan, J. R. Gini and M. E. Harikumar, "Biometric Based Smart ATM Using RFID," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 406-411, doi: 10.1109/ICSSIT48917.2020.9214287.

[7] S. D V, A. R, E. R. K and A. S, "Enhanced Security Feature of ATM's Through Facial Recognition," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 1252-1256, doi: 10.1109/ICICCS51141.2021.9432327.

[8] C. Bhuvaneswari, T. Malini, A. Giri and S. Mahato, "Biometric And IOT Technology Based Safety Transactions In ATM," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 949-952, doi: 10.1109/ICACCS51430.2021.9442051.

[9] C. Su, Y. Yan, S. Chen and H. Wang, "An efficient deep neural networks training framework for robust face recognition," 2017 IEEE International Conference on Image Processing (ICIP), Beijing, China, 2017, pp. 3800-3804, doi: 10.1109/ICIP.2017.8296993.

[10] V. Ghenescu, R. E. Mihaescu, S. -V. Carata, M. T. Ghenescu, E. Barnoviciu and M. Chindea, "Face Detection and Recognition Based on General Purpose DNN Object Detector," 2018 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 2018, pp. 1-4, doi: 10.1109/ISETC.2018.8583861.

[11] S. Jafri, S. Chawan and A. Khan, "Face Recognition using Deep Neural Net- work with "LivenessNet"," 2020 International Conference on Inventive Com- putation Technologies (ICICT), Coimbatore, India, 2020, pp. 145-148, doi: 10.1109/ICICT48043.2020.9112543.

[12] P. Terh¨orst, M. Huber, N. Damer, F. Kirchbuchner, K. Raja and A. Kuijper, "Pixel-Level Face Image Quality Assessment for Explainable Face Recognition," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 2, pp. 288-297, April 2023, doi: 10.1109/TBIOM.2023.3263186.

[13] A. Maafiri, O. Elharrouss, S. Rfifi, S. A. Al-Maadeed and K. Chougdali, "DeepWTPCA-L1: A New Deep Face Recognition Model Based on WTPCA-L1 Norm Features," in IEEE Access, vol. 9, pp. 65091-65100, 2021, doi: 10.1109/ACCESS.2021.3076359.

[14] X. Shao, X. Zhou, Z. Li and Y. Shi, "Multi-View Face Recognition Via Well-Advised Pose Normalization Network," in IEEE Access, vol. 8, pp. 66400-66410, 2020, doi: 10.1109/ACCESS.2020.2983459.

[15] L. Li, X. Mu, S. Li and H. Peng, "A Review of Face Recognition Technology," in IEEE Access, vol. 8, pp. 139110-139120, 2020, doi: 10.1109/ACCESS.2020.3011028.

[16] B. Kocacinar, B. Tas, F. P. Akbulut, C. Catal and D. Mishra, "A Real-Time CNN-Based Lightweight Mobile Masked Face Recognition System," in IEEE Access, vol. 10, pp. 63496-63507, 2022, doi: 10.1109/ACCESS.2022.3182055.

[17] N. Zhu, Z. Yu and C. Kou, "A New Deep Neural Architecture Search Pipeline for Face Recognition," in IEEE Access, vol. 8, pp. 91303-91310, 2020, doi: 10.1109/ACCESS.2020.2994207.

[18] L. S. Luevano, L. Chang, H. M´endez-V´azquez, Y. Mart´ınez-D´ıaz and M. Gonz´alez- Mendoza, "A Study on the Performance of Unconstrained Very Low Resolution Face Recognition: Analyzing Current Trends and New Research Directions," in IEEE Ac- cess, vol. 9, pp. 75470-75493, 2021, doi: 10.1109/ACCESS.2021.3080712.

[19] M. Zemlyanikin, A. Smorkalov, T. Khanova, A. Petrovicheva and G. Serebryakov, "512KiB RAM Is Enough! Live Camera Face Recognition DNN on MCU," 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW), Seoul, Korea (South), 2019, pp. 2493-2500, doi: 10.1109/ICCVW.2019.00305.

[20] A. E. Alami, Z. Lakhili, A. Mesbah, A. Berrahou and H. Qjidaa, "Color Face Recognition by Using Quaternion and Deep Neural Networks," 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, Morocco, 2019, pp. 1-5, doi: 10.1109/WITS.2019.8723788.

[21] M. F. Rahman, F. Sthevanie and K. N. Ramadhani, "Face Recognition In Low Lighting Conditions Using Fisherface Method And CLAHE Techniques," 2020 8th International Conference on Information and Communication Technology (ICoICT), Yogyakarta, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICoICT49345.2020.9166317.

[22] K. Meena and A. Suruliandi, "Local binary patterns and its variants for face recognition," 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 2011, pp. 782-786, doi: 10.1109/ICRTIT.2011.5972286.

[23] Xingfu Zhang and Xiangmin Ren, "Two Dimensional Principal Component Analysis based Independent Component Analysis for face recognition," 2011 International Conference on Multimedia Technology, Hangzhou, China, 2011, pp. 934-936, doi: 10.1109/ICMT.2011.6002199.

[24] Aman Jain, Mallika Goel, Shamyak Jain, Shubhjay Kumar, Anshul Agarwal, Vinay Kumar Jadoun,Microcontroller based ATM monitoring system for security purpose,Materials Today: Proceedings,Volume 51, Part 1,2022,Pages 894-899,ISSN 2214-7853.

[25] Chattar, Narsikar, Uphale, Bera, Khade. (2021). "ATM Safety and Security Alert" International Journal for Research Trends and Innovation, 6(5), ISSN: 2456-3315.

[26] Singh, P., Shahin, S., Chauhan, Dr. U. (2024). "ATM Plus with Face Recognition and OTP Mechanism" International Research Journal of Modernization in Engineering Technology and Science, 06(01), ISSN: 2582-5208.

Document Information

Analyzed document	GID_30_Project_Report_PH2.pdf (D190403156)
Submitted	2024-04-19 08:25:00 UTC+02:00
Submitted by	Abhinay Gulabrao Dhamankar
Submitter email	agdhamankar@pict.edu
Similarity	1%
Analysis address	agdhamankar.pict@analysis.urkund.com

Sources included in the report

SA **Pune Institute of Computer Technology / BE_Preliminary_gr9.pdf**
Document BE_Preliminary_gr9.pdf (D177667653)
Submitted by: ameya.a.dhake@gmail.com
Receiver: sbdeshmukh.pict@analysis.urkund.com

1

Entire Document

A FINAL PROJECT
REPORT ON ENHANCED ATM SECURITY USING FACIAL RECOGNITION
SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF ENGINEERING
INFORMATION TECHNOLOGY BY
Trupti Khade (B190058597) Prashant Patil (B190058676) Manish Raut (B190058683) Shashank Satghare (B190058693)
Under
the guidance of Mr. Abhinay G. Dhamankar Department Of Information Technology Pune Institute of Computer Technology Pune - 411 043. 2023-2024
SCTR's PUNE INSTITUTE OF COMPUTER TECHNOLOGY DEPARTMENT OF
INFORMATION TECHNOLOGY C E R T I F I C A T E This is to certify that the final project report entitled
ENHANCED ATM SECURITY USING FACIAL RECOGNITION submitted by
Trupti Khade (B190058597) Prashant Patil (B190058676) Manish Raut (B190058683) Shashank Satghare (B190058693)
is a bonafide work
carried out
by them under the supervision of
Name of the project supervisor
and it is approved for the
partial fulfillment of the requirement of Savitribai Phule Pune University for the award of the Degree of Bachelor of Engineering (
Information Technology).
This project report has not been earlier submitted to any other Institute or
University for the award of any degree or diploma. Mr. Abhinay G. Dhamankar Dr. A. S. Ghotkar Project Guide
HOD IT Dr. S. T. Gandhe SPPU External Guide Principal Date: Place:
i
Acknowledgement
We,
the
members of the group, wish to specify our true appreciation to all those who
have played
an imperative part within the e↵ective
completion of our

IMPROVING ATM SECURITY VIA FACE RECOGNITION

K John Peter,
Asst Prof,Dept of Information Technology ,
VINS Christian College of Engineering,
Nagercoil,Tamil Nadu ,India
Email:kjohnpeter@gmail.com.

G.Gimini Sahaya Glory,
IV year, Information Technology,
Vins Christian College of Engineering,
Nagercoil, India,
Email:gimini.g27@gmail.com.

Dr S.Arguman,
Chief Exec utiveOfficer
Nandha Engineering College,
Erode,Tamil Nadu ,India
Email:armugan@gmail.com.

G.Nagarajan,
PG Scholar,Dept of CSE ,
VINS Christian College of Engineering,
Nagercoil,Tamil Nadu ,India,
Email:info.nagarajan@gmail.com.

Sanjana Devi.V.V ,
IV year, Information Technology,
Vins Christian College of Engineering,
Nagercoil, India,
Email:sanjanadevi555@yahoo.co.in.

Dr. K Sentamarai Kannan
Professor,Department of Statitics
Manonmaniam Sundarnar University,
Tirunelveli,Tamil Nadu ,India,
Email:sentamaraikannan@gmail.com.

***Abstract*—A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. Proposed paper uses face recognition technique for verification in ATM system. For face recognition, there are two types of comparisons. The first is verification, this is where the system compares the given individual with who that individual says they are and gives a yes or no decision. The next one is identification this is where the system compares the given individual to all the other individuals in the database and gives a ranked list of matches. Face recognition technology analyzes the unique shape, pattern and positioning of the facial features. Face recognition is very complex technology and is largely software based. This Biometric Methodology establishes the analysis framework with PCA algorithms for each type of biometric device. Face recognition starts with a picture, attempting to find a person in the image. This can be accomplished using several methods including movement, skin tones, or blurred human shapes.**

Keywords: Biometric, Face recognition, ranked list, PCA-Principal Component Analysis.

I. INTRODUCTION

The information age is quickly revolutionizing the way transactions are completed. Everyday actions are increasingly being handled electronically, instead of with pencil and paper or face to face. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearences. Using the proper PIN gains access, the successful transactions can occur, but the user of the PIN is not verified. When ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. This paper describes how face recognition technology can help to the real world ATM machines.

978-1-4244-8679-3/11/$26.00 ©2011 IEEE

II. GETTING A DIGITAL FACE: THE FACIAL RECOGNITION SYSYTEM

Figure 1 below shows the typical way that a facial recognition system can be made operational.

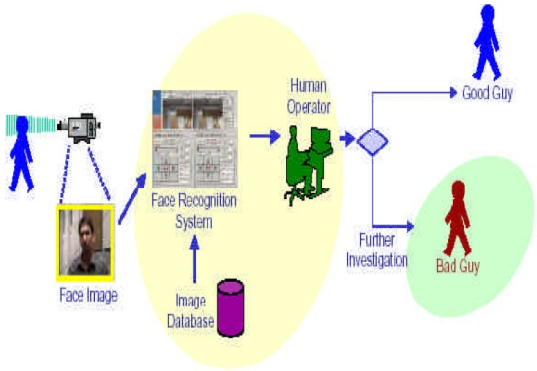

Figure 1: Overview of FRS

The first step is the capturing of a face image. This would normally be done using a still or video camera. The face image is passed to the recognition software for recognition (identification or verification). This would normally involve a number of steps such as normalizing the face image and then creating a 'template' of 'print' to be compared to those in the database. The match can either be a true match which would lead to investigative action or it might be a 'false positive' which means the recognition algorithm made a mistake and the alarm would be cancelled. Each element of the system can be located at different locations within a network, making it easy for a single operator to respond to a variety of systems.

III. PRINCIPAL COMPONENT ANALYSIS

Principal component analysis (PCA) involves a mathematical procedure which extracts facial features for

recognition, this approach transforms face images into a small set of characteristic feature images called eigenfaces.The first principal component accounts for as much of the variability in the data as possible, and each succeeding component accounts for as much of the remaining variability as possible.

These methods capture the local facial features and their geometric relationships. They often locate anchor points at key facial features (eyes, nose, mouth, etc), connect these points to form a net and then measure the distances and angles of the net to create a unique face 'print'.

IV. FACE RECOGNITION VENDOR TEST

The medium size database consisted of number outdoor and video images from various sources. *Figure 2* below gives an indication of the images in the database. The top row shows nodal position (red dots) for the images and bottom row shows the various poses of images.

Figure 2: *Various poses images from the medium data base.*

With the very good images from the large database (37,437 images) the identification performance of the best system at rank one is 96% at a false accept rate of 1%.

A. The size of the database

The Face Recognition Vendor Test (FRVT) has recognized the face recognition in four technical areas. They are high resolution still imagery, 3D facial scans, multi sample still facial imagery and preprocessing algorithm (PCA) that compensate pose and illumination.

B. Individual's face

The method of defining the matrix varies according to the algorithm (the mathematical process used by the computer to perform the comparison).

Here the part inside the oval is chosen and the other parts are rejected, artificial intelligence is used to simulate human interpretation of faces.

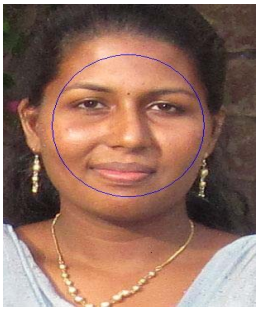

Figure3: Analytical oval face.

In order to increase the accuracy and adaptability, some kind of machine learning of 3D face tracking, 3D face reconstruction has to be implemented.

V. WORKING OF FACE RECOGNITION SYSTEMS

The face recognition system locates the head and finally the eyes of the individual, a matrix is then developed based on the characteristics of the Individual's face. There are 80 nodal points on a human face, and also few nodal points (red dots) that are measured by the software.

Figure 4 :working of face recognition technology

The method of defining the matrix varies according to the algorithm (the mathematical process used by the computer to perform the comparison). This matrix is then compared to matrices that are in a database and a similarity score is generated for each comparison. There are approximately two methods of capture. One is video imaging and the other is thermal imaging. Video imaging is more common as standard, video cameras can be used. The precise position and the angle of the head and the surrounding lighting conditions may affect the system performance. The complete facial image is usually captured and a number of points on the face can then be mapped, position of the eyes, mouth and the nostrils as an example. More advanced technologies make 3-D map of the face which multiplies the possible measurements that can be made.

Thermal imaging has better accuracy as it uses facial temperature variations caused by vein structure as the distinguishing traits. As the heat pattern is emitted from the face itself without source of external radiation these systems can capture images despite the lighting condition, even in the dark. The drawback is high cost, also they are more expensive than standard video cameras. The facial verification process involves computing the distance between the stored pattern and the live sample. The decision to accept or reject is dependent on a predetermined threshold. (Decision threshold).

VI. AUTOMATIC ACQUISITION OF FACE IMAGE SETS REJECTION OF FALSE POSITIVES

The face detector achieves high true positive rates for our database. A larger problem is caused by false alarms, even a small number of which can affect the density estimates. We use a coarse skin color classifier to reject many of the false detections. The classifier is based on 3-dimensional color histograms built for two classes: skin and non skin pixels. A pixel can then be classified by applying the likelihood ratio test. We apply this classifier and reject detections in which too few (< 60%) or too many (> 99%) pixels are labeled as skin. This step removes the vast majority of nonfaces as well as faces with grossly incorrect scales.

VII.POSE INVARIANCE

Pose variations are typically less problematic than illumination as the corresponding manifold is of lower dimensionality *(figure 2)*. It shows a typical face manifold due to pose changes (pitch and yaw) in an un-changing illumination setup. This manifold, that appears to be 2-dimensional, is accurately reconstructed by our method from components of a Gaussian Mixture Model (GMM).

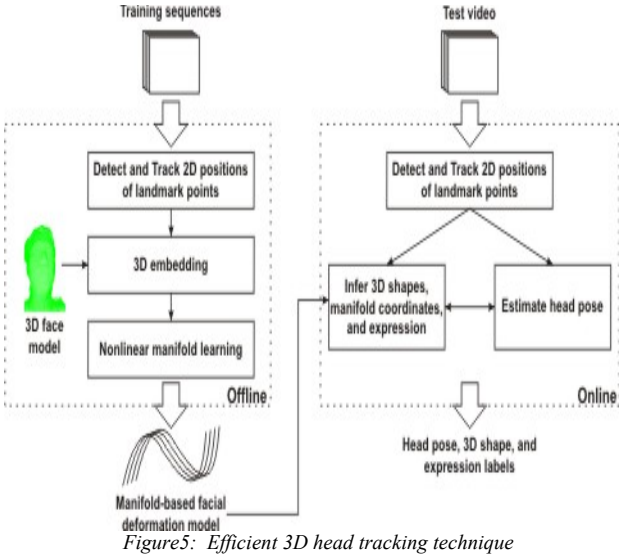

Figure5: Efficient 3D head tracking technique

We propose a person-dependent, manifold-based approach for modeling and tracking rigid and nonrigid 3D facial deformations from monocular video sequences. We analyse new framework to model the deformable shape using nonlinear manifolds. The main contribution is two-fold. First, instead of using a linear sub-space analysis, we argue the 3D facial deformations are better modeled as a combination of several 1D manifolds. Each 1D manifold represents a mode of deformation or expression, such as smile, surprise, blinking, etc. By learning these manifolds, a 3D shape instance, usually represented by a very high dimensional vector, can be mapped into a low-dimensional manifold. The coordinate on the manifold corresponds to the magnitude of facial deformation along that mode. Second, we analyse a novel framework of nonlinear manifold learning based on N-D Tensor Voting . Tensor Voting estimates the local normal and tangent spaces of the manifold at each point. The estimated tangent vectors enable us to directly navigate on the manifold.

Tensor Voting is a computational framework to estimate geometric information. It was originally developed in 2D for perceptual grouping and figure completion, and later to 3D and ND for other problems, such as stereo matching and motion processing. Since the focus of this paper is not the Tensor Voting framework,let us explain how to work with multiple manifolds with our implementation of codes.Consider a point X and recovered low dimensional embedding L for manifold κ,we define the joint probability of X and L using mixture modeling:

$P(X, L|\kappa)=w_m P_m(X|L,\kappa)P_m(L|\kappa) \sim w_m \kappa P_G(X|f_{TV}(L;\kappa), \Sigma^{\kappa}_m)P_G(L|\mu^{\kappa}_m, \sigma_m^{\kappa})$ where $f_{TV}(.; k)$ is the mapping using manifold k.$P_G(X|f_{TV}(L; k), \Sigma^{\kappa}_m)$ is the Gaussian pdf,with mean $f_{TV}(L; k)$ and covariance matrix Σ_m.

For simplicity, we assume Σ^{κ}_m is $_k$ diagonal. $P_G(L|\mu^{\kappa}_m, \sigma_m^{\kappa})_{\kappa}$ is the Gaussian pdf with mean μ_m and standard deviation σ_m.

VIII. PERFORMANCE

A. False acceptance rate (FAR)

The probability that a system will incorrectly identify an individual or will fail to reject an imposter. It is also called as type 2 error rate**.**

FAR= NFA/NIIA

NFA= number of false acceptance

NIIA= number of imposter identification attempts.

B.False rejection rates (FRR)

The probability that a system will fail to identify an enrollee. It is also called type 1 error rate.

FRR= NFR/NEIA

Where FRR= false rejection

NFR= number of false rejection rates

NEIA= number of enrollee identification attempt.

C.Response time

The time period required by a biometric system to return a decision on identification of a sample.

D.Threshold/ decision Threshold

The acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the system can be made more or less strict depending on the requirements of any given application.

E.Enrollment time

The time period a person must spend to have his/her facial reference template successfully created.

F.Equal error rate

When the decision threshold of a system is set so that the proportion of false rejection will be approximately equal to the proportion of false acceptance.

IX. CONCLUSION

Face recognition technologies have been associated generally with very costly top secure applications. In the Face recognition technology of ATM, pose variance, false positives are still a problem. Our paper has proposed a method of efficient 3D head tracking technique to overcome the consequence. Certain applications of face recognition technology are now cost effective, reliable and highly accurate. Face recognition technology can be used worldwide to access buildings, however it can be used in ATMs, which would help address potential security threats in near future.

ACKNOWLEDGMENT

First and foremost we would like to thank Head of department Mr.K.John Peter M.Tech, who gave moral support to do this paper, I would like extend my gratitude to Mr.G.Nagarajan M.E who gave an idea to do this paper ,have expressed enthusiasm and dedicated help throughout this paper. We have had support from many people including family, Lectures, and friends.

REFERENCES

[1] Faune Hughes, Daniel Lichter,Richard Oswald, and Michael Whitfield ,Face Biometrics:A Longitudinal Study, Seidenberg School of CSIS,Pace University, White Plains,NY 10606,USA.

[2] GaryG.Yen, Nethrie Nithianandan, Facial Feature Extraction Using Genetic Algorithm, Intelligent Systems and Control Laboratory School of Electrical and Computer Engineering. Oklahoma State University, Stillwater, OK 74074-5032, USA.

[3] D.L. Jiang, Y.X. Hu, S.C. Yan, H.J. Zhang, "*Efficient 3D Reconstruction for Face Recognition*", 0031_3203/2004 Pattern recognitionsociety:doi:10.1016/j.patcog.2004.11.004

[4] Animetrics offers FaceR™ CredentialME service on Sprint 3G and 4G networksAugust 12th, 2010

[5] Zigelman, G., Kimmel, R., Kiryati, N. Texture mapping using surface flatten-ing via multi-dimensional scaling, IEEE Trans. Visualization and Comp. Graphics, 8, pp. 198-207 (2002).

[6] T. F. Cootes, C. J. Taylor, D. Cooper, and J. Graham. Ac-tive shape models - their training and application. CVIU, 61(1):38–59, Jan. 1995.

[7] C. Vogler, Z. Li, A. Kanaujia, S. Goldenstein, and D. Metaxas. The best of both worlds: Combining 3d de-formable models with active shape models. ICCV 2007.

[8] P. Mordohai and G. Medioni. Tensor Voting: A Perceptual Organization Approach to Computer Vision and Machine Learning. Morgan and Claypool Publishers, 2007.

[9] X. Pennec. Intrinsic statistics on riemannian manifolds: Ba-sic tools for geometric measurements. Journal of Mathemat-ical Imaging and Vision, 25(1):127–154, July 2006.

[10] L. Gu and T. Kanade. 3d alignment of face in a single image. CVPR 2006, pp. 1305–1312.

[11] C. Huang, H. Ai, B. Wu, and S. Lao. Boosting nested cascade detectors for multi-view face detection. ICPR 2004, pp. 415– 418.

[12] C. Vogler, Z. Li, A. Kanaujia, S. Goldenstein, and D. Metaxas. The best of both worlds: Combining 3d de-formable models with active shape models. ICCV 2010.

[13] 3D Face Tracking and Expression Interference from a 2D sequence Using Manifold Learning: Wei kaiLiao and Gerard Medioni,

[14] A. Elgammal. Learning to track: Conceptual manifold map for closed-form tracking. CVPR 2005, pp. 724–730. 1

[15] A. Elgammal and C.-S. Lee. Inferring 3d body pose from silhouettes using activity manifold learning. CVPR 2004, pp. 681–688.

[16] L. Gu and T. Kanade. 3d alignment of face in a single image. CVPR 2006, pp. 1305–1312.

[17] C. Huang, H. Ai, B. Wu, and S. Lao. Boosting nested cascade detectors for multi-view face detection. ICPR 2004, pp. 415– 418.

[18] J. Xiao, S. Baker, I. Matthews, and T. Kanade. Real-time combined 2d+3d active appearance models. CVPR 2004, pp. 535–542.

[19] Z. Zhu and Q. Ji. Robust real-time face pose and facial ex-pression recovery. CVPR 2006, pp. 681–688.

[20] X. Pennec. Intrinsic statistics on riemannian manifolds: Ba-sic tools for geometric measurements. Journal of Mathemat-ical Imaging and Vision, 25(1):127–154, July 2006.

[21] S. T. Roweis and L. K. Saul. Nonlinear dimensionality reduc-tion by locally linear embedding. Science, 290(5500):2323– 2326, Dec. 2000.

[22] Y. Bengio, M. Monperrus, and H. Larochelle. Nonlo-cal estimation of manifold structure. Neural Computation, 18(10):2509–2528, Oct. 2006. S

[23] V. Blanz and T. Vetter. Face recognition based on fitting a 3d morphable model. PAMI, 25(9):1063–1074, Sept. 2003

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023-2024

PROJECT REVIEW – 1

STUDENT PERFORMANCE EVALUATION

Students' Contribution and Performance					
Particulars		Marks (25 M)			
		Group Members			
		1	2	3	4
1.	Background and Topic (3 M)	3	3	3	3
2.	Project Scope and Objectives (3M)	3	3	3	3
3.	Literature Survey (4 M)	2	2	2	2
4.	Project Planning (2 M)	1	1	1	1
5.	Presentation Skills (3 M)	1	1	1	1
6.	Teamwork(2 M)	2	2	2	2
7.	Regular interaction with the guide and timely submission (4M)	2	2	2	2
8.	Question and Answer (4 M)	3	3	3	3
	Total Marks	17	17	17	17
Comments (if any): - Latest Papers should be included. - Algorithmn identification required. - Soft. specification required in detailed study					

To be filled by internal guide & reviewer(s) only.

Project Review – I: Deliverables

✓ Problem Statement / Title ✓ Purpose, Scope, Objectives ✓ Abstract (System Overview) ✓ H/W, S/W & other requirement. Test Environment/Tools	✓ Introduction (System Overview Architecture and High-Level Design) ✓ Literature Survey ✓ References ✓ Project Plan 1.0 **(Gantt Chart)**

Name & Sign of evaluation committee –

MRS. AMRUTA A. PATIL
Name of Reviewer 1

MRS. DEEPALI P. SALAPURKAR
Name of Reviewer 2

MR. ABHINAY G. DHAMANKAR
Name of Internal Guide

Savitribai Phule Pune University | Faculty of Information Technology

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023 -20 24

RESEARCH PUBLICATION REVIEW – 1

STUDENT PERFORMANCE EVALUATION

Students' Contribution and Performance					
Particulars		Marks (25 M)			
		Group Members			
		1	2	3	4
1.	System Architecture & Literature Survey (Review-1)	Y/N	Y/N	Y/N	Y/N
2.	Precise Title, Abstract and Keywords (2 M)	2	2	2	2
3.	Motivation and scope of research work (2 M)	2	2	2	2
4.	Literature Survey and identification of research gap (2 M)	2	2	2	2
5.	Proposed Methodology /Algorithm/System Architecture (3M)	3	3	3	3
6.	Effective Conclusion and Future Scope (2 M)	2	2	2	2
7.	Relevant References (2 M)	2	2	2	2
8.	Effective Technical Writing and Presentation Skills (4 M)	3	3	3	3
9.	Originality (Plagiarism <10%) (2M)	2	2	2	2
10.	Teamwork(2M)	2	2	2	2
11.	Regular interaction with the guide and timely submission (4M)	2	2	2	2
12.	Identification of quality journals/international conferences	Y/N	Y/N	Y/N	Y/N
	Total Marks	22	22	22	22
Comments (if any):					

To be filled by internal guide & reviewer(s) only.

Research Publication Review – I: Deliverables

• Paper Title, Abstract and keywords • Introduction • Literature Survey • Proposed Methodology/ Algorithm • System Architecture/ Workflow Diagram	• Conclusion and Future Scope • References • Identified WoS (SCI/SCIE) /Scopus indexed international journals and/or Scopus indexed international conferences.

Name & Sign of evaluation committee –

Name of Reviewer 1: Mrs. AMRUTA A. PATIL

Name of Reviewer 2: MRS. DEEPALI P. SALAPURKAR

Name of Internal Guide: MR. A. G. DHAMANDHAR

Savitribai Phule Pune University | Faculty of Information Technology

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023-2024

PROJECT REVIEW – 2

STUDENT PERFORMANCE EVALUATION

Students' Contribution and Performance					
Particulars		Marks (25 M) Group Members			
		1	2	3	4
1.	System Architecture & Literature Survey (Review-I)	4	4	4	4
2.	Project Design (4 M)	4	4	4	4
3.	Methodology /Algorithms and Project Features (3 M)	3	3	3	3
4.	Project Planning (2 M)	2	2	2	2
5.	Basic details of Implementation (3 M)	3	3	3	3
6.	Presentation Skills (3 M)	2	2	2	2
7.	Teamwork (2M)	2	2	2	2
8.	Regular interaction with the guide and timely submission (4M)	3	3	3	3
9.	Question and Answer (4 M)	3	3	3	3
10.	Summarization of ultimate findings of the Project	~~22~~			
	Total Marks	22	22	22	22
Comments (if any):					

To be filled by internal guide & reviewer(s) only.

Project Review – 2: Deliverables

• Problem Statement / Title • Abstract • Introduction • Literature Survey (comparison with existing system) • Proposed Methodology • Design / algorithms / techniques used	• Modules Split-up • Proposed System • Software Tools / Technologies to be used • Proposed Outcomes • Partial Report (Semester – I) • Project Plan 2.0 (Gantt Chart)

Name & Sign of evaluation committee –

Name of Reviewer 1
MRS. AMRUTA A. PATIL

Name of Reviewer 2
MRS. DEEPALI P. SALAPURKAR

Name of Internal Guide
MR. A. G. DHAMANKAR

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023-2024

PROJECT REVIEW – 3

STUDENT PERFORMANCE EVALUATION

Students' Contribution and Performance					
Particulars		Marks (25 M)			
		Group Members			
		1	2	3	4
1.	Architecture / System Design -(if any modification)	4	4	4	4
2.	60 % Implementation (7 M)	7	7	7	7
3.	Partial results obtained (5 M)	5	5	5	5
4.	Presentation skills (3 M)	3	3	3	3
5.	Teamwork (2M)	2	2	2	2
6.	Regular interaction with the guide and timely submission (4M)	3	3	3	3
7.	Question and Answer (4 M)	3	3	3	3
8.	Summarization of the methodologies / Algorithms implemented / to be implemented	4	4	4	4
	Total Marks	23	23	23	23

Comments (if any):
- Try to make frontend nice -
- write paper for ~~Review~~ publication & their review-2

To be filled by internal guide & reviewer(s) only.

Project Review – 3: Deliverables

- Detailed Design (if any deviation)
- 60% of code implementation
- Some Experimental Results
- Project Plan 3.0

Name & Sign of evaluation committee –

MRS. AMRUTA A. PATIL
Name of Reviewer 1

MRS. DEEPALI P. SALAPURKAR
Name of Reviewer 2

17/1/2024
MR. ABHINAY G. DHAMANKAR
Name of Internal Guide

Savitribai Phule Pune University | Faculty of Information Technology

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023-2024

RESEARCH PUBLICATION REVIEW – 2

STUDENT PERFORMANCE EVALUATION

Students' Contribution and Performance					
Particulars		Marks (25 M)			
		Group Members			
		1	2	3	4
1.	Implementation (Review-III)	✓	✓	✓	✓
2.	Title, Abstract, Keywords, Introduction, Literature Survey, Proposed Methodology (4M) (Research Publication Review-I Outcome)	3	3	3	3
3.	Experimentation Results and Empirical Analysis (5M)	5	5	5	5
4.	Effective Conclusion and Future Scope (2 M)	2	2	2	2
5.	Relevant References (2 M)	2	2	2	2
6.	Effective Technical Writing and Presentation Skills (4 M)	4	4	4	4
7.	Originality (Plagiarism <10%) (2M)	2	2	2	2
8.	Teamwork (2M)	2	2	2	2
9.	Regular interaction with the guide and timely submission (4M)	4	4	4	4
10.	Identification of quality journals/international conferences				
	Total Marks	24	24	24	24
Comments (if any): – Pl. Identify best journal.					

To be filled by internal guide & reviewer(s) only.

Research Publication Review – 2: Deliverables

• Paper Title, Abstract and keywords • Introduction • Literature Survey • Proposed Methodology/ Algorithm • System Architecture/ Workflow Diagram	• Experimentation Results and Empirical Analysis • Conclusion and Future Scope • References • Identified WoS (SCI/SCIE) /Scopus indexed international journals and/or Scopus indexed international conferences.

Name & Sign of evaluation committee –

Name of Reviewer 1
MRS. AMRUTA A. PATIL

Name of Reviewer 2
MRS. DEEPALI P. SALAPURKAR

Name of Internal Guide
MR. ABHINAY G. DHAMANKAR

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023-2024

PROJECT REVIEW – 4

STUDENT PERFORMANCE EVALUATION

Students' Contribution and Performance					
Particulars		Marks (25 M)			
		Group Members			
		1	2	3	4
1.	Implementation (100%) (3 M)	3	3	3	3
2.	Testing, Results and Performance Evaluation (3 M)	3	3	3	3
3.	Final Project Report (4 M)	3	3	3	3
4.	Publications (2 M)	2	2	2	2
5.	Presentation skills (3 M)	3	3	3	3
6.	Teamwork (2 M)	2	2	2	2
7.	Regular interaction with the guide and timely submission (4 M)	4	4	4	4
8.	Question and Answer (4 M)	3	3	3	3
	Total Marks	23	23	23	23
Comments (if any):					

To be filled by internal guide & reviewer(s) only.

Project Review – 4: Deliverables

• Detailed Design • 100% of code implementation • Experimental Results • Performance Evaluation	• Test Cases • Result Analysis and Conclusion • Final Thesis • Project Plan 4.0.

Name & Signature of evaluation committee -

Name of Reviewer 1	Name of Reviewer 2	Name of Internal Guide
MRS. AMRUTA A. PATIL	MRS. DEEPALI P. SALAPURKAR	MR. ABHINAG G. DHAMANKAR

Savitribai Phule Pune University — Faculty of Information Technology

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023 -2024

SUMMARY OF PROJECT WORK EVALUATION SHEETS

Sr. No.	Roll No.	Exam Seat No.	Name of the Student	Project Reviews Marks (Each out of 25 Marks)				Research Publication Reviews Marks (Each out of 25 Marks)		Total (Out of 150 Marks)	Student's Sign
				1	2	3	4	1	2		
1	43140	B190058597	TRUPTI T. KHADE	17	22	23	23	22	24	131	Khade
2	43265	B190058676	PRASHANT C. PATIL	17	22	23	23	22	24	131	Patil.
3	43267	B190058683	MANISH S. RAUT	17	22	23	23	22	24	131	Raut
4	43270	B190058693	SHASHANK C. SATGHARE	17	22	23	23	22	24	131	Satghare

Overall Remarks or Comments (if any):

Name & Sign of evaluation committee -

Name of Reviewer 1	Name of Reviewer 2	Name of Internal Guide
19/4/24		
MRS. ANKUTA A. PATIL	MRS. DEEPALI P. SALAPURKAR	MR. ABHINAY G. DHAMANKAR

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023 -20 24

Monthly Planning Sheet

Semester: 1

Week No.	Activity Planned	Activity Completed Status	Student's Sign	Internal Guide's Sign
Week 1	Domain & Topic selection	Done	Rhade	
Week 2	Defining Project scope and Objective		Pati.	
Week 3	Literature Survey		Mault	
Week 4	Requirement Analysis		~~Sudy~~	
Week 5	System Analysis		Rhade.	
Week 6	Designing System Architecture		Pati.	
Week 7	Environment Setup		Mault	
Week 8	Data preprocessing		~~Sudy~~.	
Week 9	Model selection		Rhade.	
Week 10	Model Building		Pati.	
Week 11	Model Evaluation		Mault	
Week 12	UI Design		~~Sudy~~	

Ms. Abhinay Dhamankar
Name & Sign of Internal Guide

Name & Sign of Industry Mentor (if applicable)

PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE.

Department of Information Technology

A.Y. 2023-2024

Monthly Planning Sheet

Semester: 2

Week No.	Activity Planned	Activity Completed Status	Student's Sign	Internal Guide's Sign
Week 1	Integration of facial recognition to software	Done	Bhade	
Week 2	Backend Development		Patil.	
Week 3	User data storage in SQL		Maul	
Week 4	Face data storage in MongoDB		Sing	
Week 5	Transaction Management		Bhade	
Week 6	SMS alert system integration		Patil.	
Week 7	Email alert system integration		Maul	
Week 8	Finalizing Research paper		Sing	
Week 9	Adding necessary user prompts		Bhade	
Week 10	Testing the software		Patil.	
Week 11	Take user feedbacks & make improvements		Maul	
Week 12	Documentation		Sing	

MR. ABHINAY G. DHAMANKAR

Name & Sign of Internal Guide

Name & Sign of Industry Mentor (if applicable)

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

ENHANCED ATM SECURITY USING FACIAL RECOGNITION

Mr. Abhinay G. Dhamankar*1, Trupti Khade*2, Prashant Patil*3, Manish Raut*4, Shashank Satghare*5

*1Professor, Department Of Information Technology, SCTR'S Pune Institute Of Computer Technology Pune, India.

*2,3,4,5Student, Department Of Information Technology, SCTR'S Pune Institute Of Computer Technology Pune, India.

ABSTRACT

This survey explores progress in "ATM security using facial recognition" by examining the application of facial recognition technology in supporting ATM security infrastructure. The research provides a comprehensive evaluation of various methods, algorithms and systems used to integrate facial recognition into existing ATM security systems. It also provides an in-depth analysisof the benefits and limitations of using facial recognition in ATM security, including factors such as users' authenticity, trust, and familiarity. Combining current research, industry development, and regulatory recommendations, this survey aims to better understand the use of instant facial care to improve ATM security. The findings and insights presented in this survey not only contribute to knowledge but also provide important guidance to policymakers, financial institutions, and researchers interested in the development of ATM security technologies.

Keywords: Artificial Intelligence, Facial Recognition, Deep Neural Networks, Opencv, Convolutional Neural Networks (CNN), Machine Learning, ATM Security.

I. INTRODUCTION

In an increasingly connected and technological world, ATM security is a top priority for financial institutions and their customers. Security methods such as PIN and card verification have limitations. To solve these issues, we propose "Using Facial Recognition to Improve ATM Security."

Facial recognition using artificial intelligence and computer vision is revolutionizing data security and user access. This approach not only increases ATM security but also improves user experience. Thanks to unique facial recognition, ATMs provide an extra layer of protection against unauthorized access, card theft and fraud. Deep neural networks will be used to recognize faces and identify each person's unique face. In this article titled "Using facial recognition to increase ATM security", we will explore its content, benefits and advantages over traditional methods. Integration of advanced technologies such as facial recognition using deep neural networks (DNN) will be an important strategy to strengthen ATM security infrastructure.

BACKGROUND

Automated teller machines (ATMs) have revolutionized the accessibility and convenience of banking services, allowing users to carry out a variety of financial transactions quickly and efficiently. However, the widespread use of ATMs has also led to security breaches and fraud, causing serious problems for financial institutions and consumers. Although the use of traditional security measures such as PINs (Personal Identification Numbers) and special authentication cards, ATM spoofing, card fraud and theft still continues, there is a need for integration of security solutions.

MOTIVATION

Facial recognition acts as strong authentication, allowing only access to the ATM and preventing unauthorized attempts. Its integration reduces card fraud, including fraud and fraudulent use of stolen or cloned cards, and creates a safe financial environment. It increases customer convenience by eliminating the need for a PIN, speeds up ATM transactions and simplifies the overall banking experience. The technology also encourages participation and provides access to a broaderpopulation by providing an alternative method of authentication that can assist people with disabilities or those who have trouble with traditional PIN codes or reader cards. Additionally, the use of effective security measures such as facial recognition can increase the trust of ATM users, ensure the security and integrity of their transactions, ensure businessfinancing, and increase confidence in banking as a whole. Integrating DNN into facial recognition technology for ATM security is expected to

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

increase the accuracy and reliability of the authentication process, thereby reducing the risks associated with illegal logins and fraudulent transactions. Thissurvey aims to provide a comprehensive overview of the role of DNN-based facial recognition technology in changing ATM security and highlight the potential of this technology toprovide instant accurate and reliable personal identification.

OBJECTIVES

1. To review and analyze the current state of deep learning in the context of facial recognition technology, particularly in deep neural networks (DNN), as well as focusing on its application in the development of automated teller machine (ATM) security infrastructure.
2. Explore various methods and designs of Deep NeuralNetworks (DNN) for facial recognition in the contextof ATM security, examining their effectiveness, accuracy, and robustness in solving real-world security problems and situations.
3. Evaluate the performance and comparison of different DNN models for facial recognition in the context of ATM security, considering factors such asperformance, flexibility of performance, and adaptability to different environments and users.

II. RELATED WORK

In the article titled "ENHANCED SECURITY FEATURE OF ATM'S THROUGH FACIAL RECOGNITION", the author introduces a facial recognition method based on eigenfaces. This system analyzes algorithms used in previous systems. PCA-based algorithms are more reliable, very fast and use less storage space. The biggest disadvantage of this method is that it can be changed using the user's image. This method can be improved by using 3D masks, but the cost of making 3D masks is very high.

In the article " Face Recognition In Low Lighting Conditions Using Fisherface Method And CLAHE Techniques", the author found that Fisherface can recognize faces with 77.69% accuracy down to -70 light level without image enhancement. However, the fisherman algorithm also has some shortcomings, such as sensitivity to outsiders, the ability to limit the use of inconsistent information, and the impact of lighting and face change.

In the article " Two Dimensional Principal Component Analysis Based Independent Component Analysis for Face Recognition", the author proposed an ICA algorithm based on 2DPCA for face recognition. Compared to traditional algorithms such as PCA, 2DPCA and ICA, this algorithm performs better. However, disadvantages of 2DPCA include sensitivity to image changes, high computational cost, limited ability to distinguish patterns, and reliance on preprocessed data.

In the article "LOCAL BINARY PATTERNS AND ITSVARIANTS FOR FACE RECOGNITION" authors K.Meena and Dr. A. Suruliandi proposed face recognition based on Local Binary Patterns and modified CS- LBP, MLBP and LBPV. It provides a high recognition rate up to 87% and takes less timein calculation. However, compared with the DNN model, the recognition rate is still lower; about 95% - 97%. It also struggles with changes in image sets and rotations.

In the article "AN EFFICIENT DEEP NEURAL NETWORKS TRAINING FRAMEWORK FOR ROBUST FACE RECOGNITION", a new DNN training framework using softmax loss and triple loss function is proposed to effectively capture a good human face. A special DNN architecture based on softmax loss is designed to initialize DNN. Based on this, we can use triple regression to improve the discrimination ability of DNN where the function changes.

III. PROPOSED WORK

Here we propose the use of deep neural networks to improve ATM security. DNN facial recognition is a technology that uses deep learning techniques to identify and recognize people based on faces. This approach has revolutionized the field of biometrics by providing high levels of accuracy and adaptability to a variety of applications. DNN facial recognition usually starts by collecting different facial data, and then first using a convolutional neural network (CNN) forthe data and removing it. During training, the DNN learns to encode specific faces by creating a digital representation of each face. Then, during authentication, the system calculates the facial placement of the input image and compares it to the placements stored in the database to identify the person.

DNN facial recognition model uses deep learning (specificallyCNN) to extract facial information from images. It

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

converts these features into small-sized vectors called face embedding's. During training, it learns to group similar facial embedding's while controlling for differences between individuals. When using input, it matches input embedding's tostored embedding's to accurately identify people. The effectiveness of this model depends on its architecture and thequality of the training data, providing high accuracy in identifying individuals.

The accuracy of DNN facial recognition models can be very high; can often be over 99% of test data with state-of-the-art architecture and prior knowledge. The accuracy of DNN face recognition models may vary depending on many factors such as the data used for training and evaluation, model parameters, and prioritization techniques. Accuracy is often measured using metrics such as true positive rate (TPR), negative rate (TNR), negative rate (FPR), and negative rate (FNR).

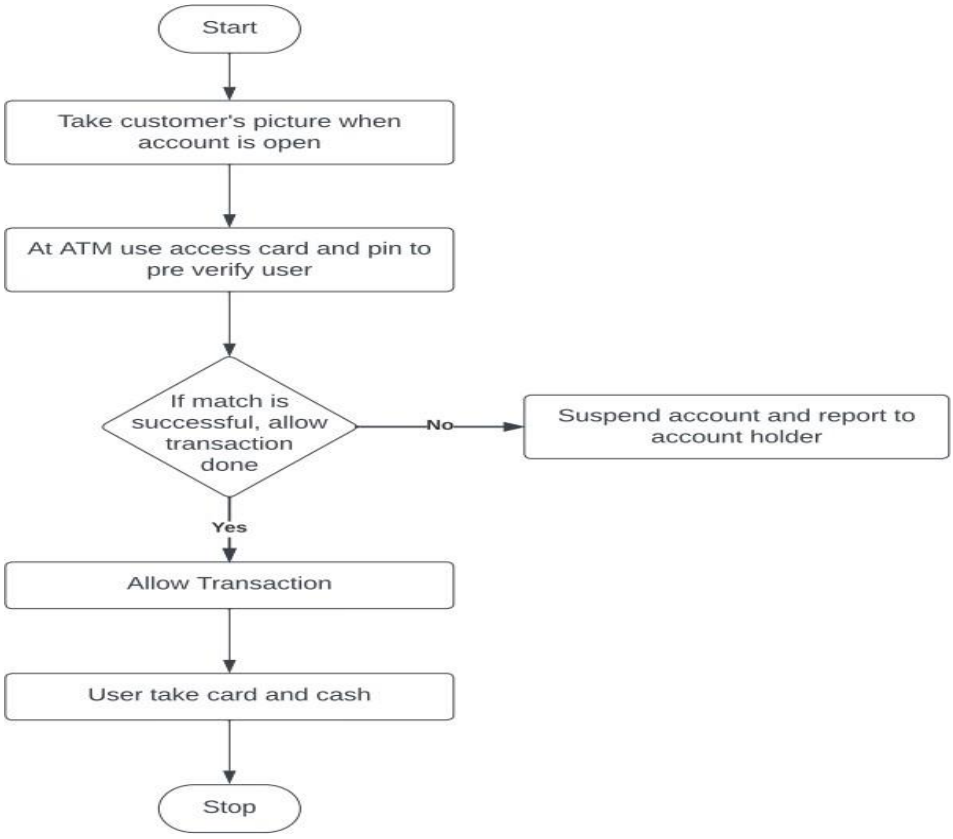

Figure 1: Data Flow diagram

Our "Enhanced ATM Security with Facial Recognition" system aims to provide a comprehensive solution that combines strong security measures with customer satisfaction. At its core, the system uses facial recognition technology to safely and easily identify ATM users. It allows only authorized individuals through unique facial recognition, thus reducing the risk of card fraud, unauthorized access and criminal tampering.

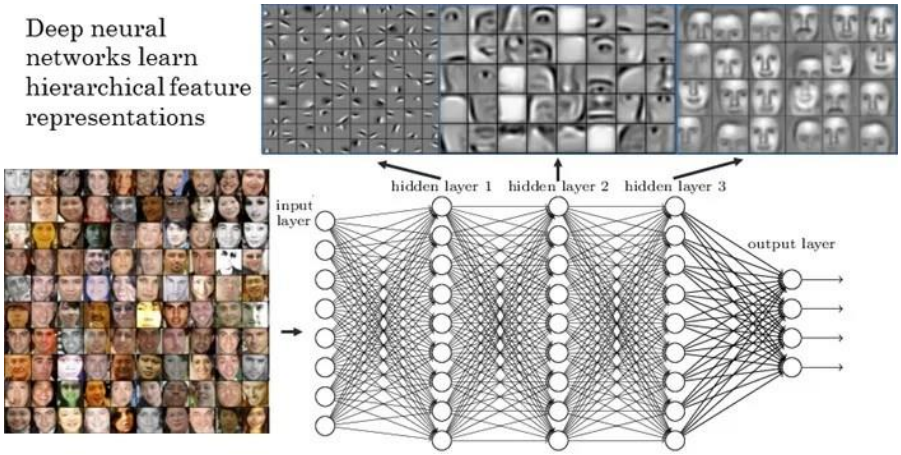

Figure 2: DNN layers

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

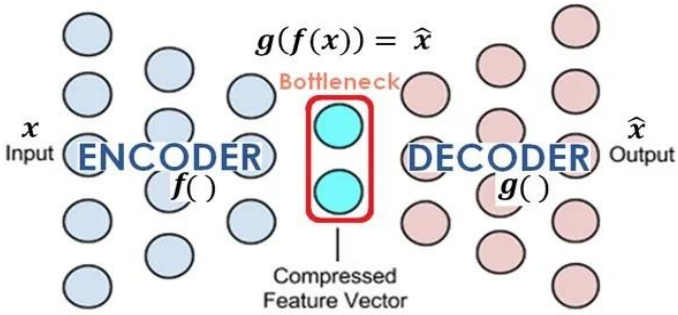

Figure 3: Feature Extraction Functions

In unsupervised learning mode, deep auto encoder networks are used to reduce dimensionality. It tries to learn a transformation that compresses the input using the f() encoderto reduce the input from the bottleneck (2 or 3 neurons) and recombines it using the g() decoder to estimate the individual availability function, thus giving an output like . f() and g() are both nonlinear neural networks (see figure below). Auto encoders reduce search time by reducing image representation to simple vectors, increasing similarity.

The integration of the DNN (deep neural network) facial recognition model with ATM software is a multi-faceted process that involves the integration of deep learning and software engineering skills. The step-by-step instructions below show you how to do this integration:

1. Identifying requirements: Start by carefully defining your goals for integrating facial recognition into ATM software. Determine whether the primary goal is to improve security, user authentication, or a combination of the two.
2. Model selection: Select the appropriate DNN facial recognition model and software based on specific requirements, including terms such as accuracy, speed, and compatibility with ATM hardware.
3. Data collection and processing: Collecting diverse and representative images of the face dataset for model training and validation. Make file progress, which may include resizing, aligning, and standardizing images to ensure consistency.
4. Model training: Train the DNN model so that it chooses to use previous data and improves its performance through optimization. This stage usuallyrequires a lot of computing resources.
5. Export model: Insert the learned DNN model into theATM software, decide whether to host it on the server or directly into the ATM hardware.
6. User interface design: Create a user interface in the ATM software to guide users through the facial recognition process. This link should include commands, capture images, and entry strategies to accomplish results.
7. Security measures: Implement effective security measures to protect the DNN model and the facial data it generates. This may include encryption, access control, and tamper-resistant hardware.
8. Testing and Quality Assurance: Strict testing of integrated components to ensure efficient and accurate performance. Successful testing should include usability, security and performance.
9. Policy Compliance: Ensure that your facial recognition system complies with all applicable laws and privacy laws, especially those related to sensitivebiometric paper processing data.
10. User registration process: If necessary, create a user registration process, including capturing facial information for facial recognition, joining number ATM, and keep this information secure.
11. Backup system: Plan for unexpected situations where facial recognition may fail, such as poor lighting or image quality. Use a trusted recovery method as authentication, such as PIN or card verification.
12. Monitor and Trace: Carefully monitor the system for problems and possible security threats. Update DNN models and ATM software regularly to ensure they remain current and secure.
13. User Training: Introduce the new facial recognition system to ATM users by explaining its functions and benefits. Address privacy and data security concerns and questions.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

IV. TECHNOLOGY AND METHODOLOGIES

A. Data Collection and Preprocessing:

Data collection techniques, data management and prioritization procedures are essential to obtainquality face-to-face data and ensure data consistency and reliability.

B. **Facial Recognition Technology**:

A deep understanding of facial recognition algorithms, technology, and best practices is important. It is especially important to understand many methods such as deep learning, including convolutional neural networks (CNN) and DNN.

C. Model Training and Evaluation:

Expertise in training models, validation, and evaluation procedures for facial recognition model performance is desired. Understanding metrics such as accuracy, precision, recall, and F1 score is crucial to assessing model quality.

D. Software Development and Integration:

Expertise in programming languages such as Python and frameworks such as TensorFlow or PyTorch for using DNN is essential. Knowledge of software development processes and version control is also useful.

V. TABLE DESCRIPTION

A table is provided with information about various research articles and their employment contract-related topics. Each entry includes details such as author, publication year, research field, location, and research focus. This information appears to be related to the development of facial recognition recommendations and their use in ATM systems.

All forms appear to contain information related to facial recognition research, including author details, research field, location and keyword.

Table 1: Summary Of Research Reviewed

Title	Authors	Techniques used	Evaluation methods and findings
Secure ATM transactions Using face recognition and OTP(Pub. 2022) [1]	Pooja Surwase, SonamBhange, Shreya Taru, Samruddhi Khot, Prof.Jayashree Mundada	OTP using face verification	Different types of users can have different types of security
Recent advances in Deep Learning Techniques for face recognition(Pub. 2021) [2]	Md. Tahmid hasan faud, awal ahmad fime, deolwar sikder, md. Akil raihan iftee, jakaria rabbi, mabrook s. Alrakhmi ,abdu gumae, ovishaken sen, mohtasim faud	Image processing and face recognition indeep Neural network in face recognitionpipeline	Recent trends in face recognition using different deep learning architectures.
GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations [3]	MOHAMAD ALANSARI (Member, IEEE), OUSSAMA ABDUL HAY SAJID JAVED , ABDULHADI SHOUFAN YAHYA ZWEIRI (Member, IEEE), AND NAOUFEL WERGHI(Senior Member, IEEE)	GhostNetV1,GhostNet V2	Reducing the amount of computation is must and to do this Ghost net can be used which uses all series of linear transformation which are inexpensive to extract features
Towards Accurate and Lightweight Masked Face Recognition: An Experimental Evaluation [4]	YOANNA MARTÍNEZ-DÍAZ1, HEYDIMÉNDEZ-VÁZQUEZ 1, LUIS S. LUEVANO 2,(Member, IEEE), MIGUELNICOLÁS-DÍAZ1, LEONARDO CHANG	Periocular recognition	Various models of CNN are used

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

	2,AND MIGUEL GONZÁLEZ-MENDOZA2		
Biometrically Secured ATM Vigilance System[5]	Navin Kumar.M, Raghul.S, Nirmal Prasad. K, Naveen Kumar. P	Biometric authentication; microcontroller; face recognition; fingerprint sensor; OTP (One Time Password	ATMs require physicalsafety features such as a strong door, secure machines, a security guard along with the ATM software being used.
Biometric Based Smart ATM Using RFID [6]	Gokul. S, Kukan. S, Meenakshi.K, Vishnu PriyanS, Rolant Gini J, M.E. Harikumar	Microcontroller; fingerprint sensor; embedded system; signal processing	For extra security, some features can be implemented such as RFID number, Fingerprint scanners. This information can be verified in a database.
ENHANCED SECURITY FEATURE OF ATM'S THROUGH FACIAL RECOGNITION [7]	Ms. SOUNDARI D V,ARAVINDH R, EDWIN RAJK, ABISHEK S	ATM, Face-id, Eigenface algorithm,Machine Learning	Face-ID can be used as key along with other authentication methods
Biometric And IOT Technology Based Safety Transactions In ATM [8]	C. Bhuvaneswar, C. Bhuvaneswar, Anupriya Giri, Sushmita Mahato	ATM Transactions;Face Recognition System; Internet ofThings; Machine toMachine Communication	In contemporary society, incidents of ATM fraud have become increasingly commonplace. This is due to various machines designed to deceive people.
AN EFFICIENT DEEP NEURAL NETWORKS TRAINING FRAMEWORK FOR ROBUST FACE RECOGNITION [9]	Canping Su, Yan Yan , SiChen, Hanzi Wang	Face recognition, deep neural networks,triplet loss function	A new framework for training the DNN modelwas proposed. It has anaccuracy of 97.3%.
Face Detection and Recognition Based on General Purpose DNN Object Detector [10]	Veta Ghenescu, Roxana Elena Mihaescu, Marian Traian Ghenescu, Eduard Barnoviciu, Serban-Vasile Carata, Mihai Chindea	Face recognition, Deep Neural Network, YOLO-YouOnly Look Once, Darknet	The model was trained on a proprietary database. The method is based on the YOLO (You Only Look Once) model, The database has over 120,000 samples.
Face Recognition using Deep Neural Network with "LivenessNet" [11]	Samana Jafri, Satish Chawan, Afifa Khan	Face recognition, Artificial intelligence, Deep Neural Networks, Computer Vision, OpenCV, and LivenessNet	A DNN framework LivenessNet was discussed,
Pixel-Level Face Image Quality Assessment for Explainable Face Recognition [12]	Philipp Terhörst, Marco Huber, Naser Damer, Member, IEEE, Florian Kirchbuchner, Member, IEEE, Kiran Raja, Senior Member, IEEE, and Arjan Kuijper, Member, IEEE	Authentication via biometrics, advanced analytics,transparent facial recognition, intuitivefacial recognition.	A new concept of pixellevel face image was introduced. It is a training free approach which can adapt to various other networks.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

DeepWTPCA-L1: A New Deep Face Recognition Model Based on WTPCA-L1 Norm Features [13]	AYYAD MAAFIRI, OMAR ELHARROUSS, (Member, IEEE), SAAD RFIFI, SOMAYA AL-MAADEED, (Senior Member, IEEE), AND KHALID CHOUGDALI	Face recognition, WTPCA-L1 algorithm, CNN-LSTM architecture.	A new face recognition model was proposed called DeepWTPCA-L1 using WTPCA-L1 features and a CNN-LSTM architecture.
Multi-View Face Recognition Via Well-Advised Pose Normalization Network[14]	XIAOHU SHAO,XIANGDONG ZHOU ,ZHENGHAO LI, AND YU SHI	Facial recognition From multiple viewpoints, GANs, transforming faces to a frontal view, and evaluating the quality of facial data	In facial recognition having different poses causes problems. To tackle this problem a new approach was proposed.
A Review of Face Recognition Technology [15]	LIXIANG LI,XIAOHUI MU, SIYING LI, AND HAIPENG PENG	Facial recognition, Image processing, Neural network, artificial intelligence	The paper introduces the related research of face recognition from different perspectives. The article describes the development stages of facial recognition and other technologies.
A Real-Time CNN-Based Lightweight MobileMasked Face Recognition System [16]	BUSRA KOCACINAR, BILAL TAS, FATMA PATLAR AKBULUT, (Member, IEEE), CAGATAYCATAL, AND DEEPTI MISHRA, (Senior Member, IEEE)	Convolutional neural networks, deep learning, ne tuning, masked face recognition, TinyML, transfer learning.	A new approach for facial recognition was proposed for people wearing masks. The approach is based on fine-tuned lightweight deep Convolutional Neural Networks (CNN).The proposed model achieves 90.40% validation accuracy using 12 individuals' 1849 face samples.
A New Deep Neural Architecture SearchPipeline for Face Recognition [17]	NING ZHU, ZEKUAN YU,AND CAIXIA KOU	Neural architecture search, trainable architecture, reinforcement learning, face recognition, large-scale facedataset.	A new deep neural architecture search pipeline combined with neural architecture search(NAS) technology and reinforcement learning strategy into face recognition. The network architectures has achieved good accuracy in the large-scale face dataset,which achieved 98.77% top-1 in the MS-Celeb-1Mdataset and 99.89% in LFW dataset.
A Study on the Performance of Unconstrained Very Low Resolution Face	LUIS S. LUEVANO, (Member, IEEE), LEONARDO CHANG,HEYDI	Improving face recognition in low resolution and unconstrained settings	The study discussed the advances and challenges in facial recognition. It also proposes a new method to

Recognition: Analyzing Current Trends and New Research Directions [18]	MÉNDEZ-VÁZQUEZ,YOANNA MARTÍNEZ-DÍAZ, MIGUEL GONZÁLEZ-MENDOZA	through innovative coupled mappings, super resolution, and lightweight neural networks.	tackle the very low resolution face recognition problem and provide an in-depth analysis of their design, effectiveness, and efficiency for a real-time surveillance application.
512KiB RAM Is Enough! Live Camera Face Recognition DNN on MCU [19]	Maxim Zemlyanikin∗ Alexander Smorkalov∗ Tatiana Khanova Anna Petrovicheva Grigory Serebryakov	RISC-V MCU porting, DNN model optimization	The paper discusses how small devices can manage huge computational work such as facial recognition. It covers the full development and deployment pipeline of Face Recognition with a live camera.
Color Face Recognition by Using Quaternion andDeep Neural Networks [20]	Abdelmajid EL ALAMI, Zouhir LAKHILI, AissamBERRAHOU ,Hassan QJIDAA, Abderrahim MESBAH	Quaternion, color face recognition, complexity, deep neural networks	This paper proposes a new model for color face recognition based on quaternion number and deepneural networks (DNN), to enhance the classification accuracy of color face recognition.
Face Recognition In Low Lighting Conditions Using Fisherface Method And CLAHE Techniques [21]	Muhammad Fauzan Rahman, Febryanti Sthevanie and Kurniawan Nur Ramadhani	Face recognition, fisherface, face detection, image enhancement, contrast limited adaptive histogram equalization	This paper proposes a new system with facial images in low light conditions, by adding image enhancement with contrast adaptive histogram equalization (CLAHE) contrasttechniques to create good quality lighting images.
LOCAL BINARY PATTERNS AND ITS VARIANTS FOR FACERECOGNITION [22]	K. Meena, Dr. A. Suruliandi	Face recognition techniques such as Local Binary Pattern (LBP), Differential LBP (MLBP), CS-LBP, and LBPV exhibit distinct patterns.	This study compares various face recognition patterns such as Local Binary Pattern (LBP),Multivariate Local Binary Pattern (MLBP), Center Symmetric Local Binary Pattern (CS-LBP) and Local Binary Pattern Variance (LBPV)
Two Dimensional Principal Component Analysis Based Independent Component Analysis for Face Recognition [23]	Xingfu Zhang, Xingfu Zhang, Xiangmin Ren	Principal Component Analysis; Two Dimensional Principal Component Analysis; Independent Component Analysis; facerecognition	This study proposes Two Dimensional Principal Component Analysis based Independent Component Analysis algorithm, which processed the two dimensional images directly

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:11/November-2023 Impact Factor- 7.868 www.irjmets.com

			in preprocessing procedure. This algorithm is more effective than classical PCA, 2dPCA and ICA algorithms.

Table 2: Advantages And Disadvantages Of Methods Used

Method	Disadvantages	Advantages
Eigenfaces	Sensitive to low-quality or noisy face images, impacting its accuracy.	It can handle variations in expressions, lighting, and pose, making it relatively robust.
Basic Template Matching	Less accurate in noisy environments or in the presenceof distortions, leading to potential false matches and reduced precision.	It is a straightforward and easy-to-understand technique for detecting patterns or objects withinan image.
PCA	It can lead to information loss as it focuses on the mostsignificant variations in the data, potentially disregarding less dominant but still relevant information.	Simplifies the complexity of high-dimensional data by transforming it into a lower-dimensionalspace while preserving the most important patterns in the data.
Local Binary Patterns	LBP can be sensitive to image noise, potentially leading to inaccuracies in feature extraction and patternrecognition.	It is computationally efficient, making it suitablefor real-time image processing and analysis tasks.
DNN	DNNs require substantial amounts of high-quality datafor effective training, and their performance can be significantly impacted by the quality, size, and representativeness of the training data	DNNs can effectively learn intricate patterns andrepresentations from complex data, making themhighly adept at recognizing and interpreting intricate relationships within the data.

VI. FUTURE SCOPE

This opens up exciting possibilities as we consider many ways to improve the integration of facial recognition into different domains. One of the main directions for further research involves the integration of various biometric systems such as fingerprint recognition and voice recognitionto create security systems. This multi-factor authentication will increase the security of ATM transactions and make them more resistant to fraud.

Continuous DNN development is another important avenue of research. The goal of this process is not only to increase accuracy, but also to improve the ability to prevent immediate threats. The changing nature of cyber threats requires the development of new models that can quickly adapt to emerging risks.

Also improving user experience is still the most important thing. This is done with a level of common sense that makes ATM interaction easier and more convenient. Seamless integration of facial recognition technology into mobile banking apps is another great possibility, allowing users to enjoy a seamless and secure transaction across multiple platforms.

Strong privacy protection is important, and future research should focus on developing the latest privacy technology to clearly ensure that personal information is protected as usual.

VII. CONCLUSION

Our survey shows together the evolution of combining facial recognition technology with deep neural networks (DNN) in the context of automated teller machines (ATMs). The projects discussed in this article represent important steps in solving critical security issues that have long plagued financial institutions, such as card fraud, Inaccessibility, and theft. Using advanced fraud detection techniques and user-friendly features, our measures not only increase ATM security but also improve the overall banking experience for customers. As we enter an era where digital transformation isvital, this project demonstrates the financial industry'sunwavering commitment to providing secure and seamless banking services. He talks about the evolution of the DNN model and emphasizes that the path to instant threat detection and user-centered modeling is a continuous process.

The field is expected to evolve in the future, and security measures will continue to improve while users' convenience and personal information are protected. In this dynamic environment, the convergence of facial recognition technology and DNN represents a ray of hope for people around the world to protect their financial transactions so they can have peace of mind when using ATMs in an increasingly digital world.

VIII. REFERENCES

[1] Surawse, P., Bhange, Taru, S., Khot, S., & Mundada, Prof. J. (2022, February). Secure ATM Transactions Using Face Recognition & OTP, 2022JETIR February 2022, Volume 9, ISSN-2349-5162

[2] M. T. H. Fuad et al., "Recent Advances in Deep Learning Techniques for Face Recognition," in IEEE Access, vol. 9, pp. 99112-99142, 2021, doi:10.1109/ACCESS.2021.3096136.

[3] M. Alansari, O. A. Hay, S. Javed, A. Shoufan, Y. Zweiri and N. Werghi, "GhostFaceNets: Lightweight Face Recognition Model From Cheap Operations," in IEEE Access, vol. 11, pp.35429-35446, 2023, doi: 10.1109/ACCESS.2023.3266068.

[4] Y. Martínez-Díaz, H. Méndez-Vázquez, L. S. Luevano, M. Nicolás-Díaz, L. Chang and M. González-Mendoza, "Towards Accurate and Lightweight Masked Face Recognition: An Experimental Evaluation," in IEEE Access, vol. 10, pp. 7341-7353, 2022, doi: 10.1109/ACCESS.2021.3135255.

[5] M. Navin Kumar, S. Raghul, K. Nirmal Prasad and P. Naveen Kumar, "Biometrically Secured ATM Vigilance System," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 919-922, doi: 10.1109/ICACCS51430.2021.9441975.

[6] S. Gokul, S. Kukan, K. Meenakshi, S. S. V. Priyan, J. R. Gini and M. E. Harikumar, "Biometric Based Smart ATM Using RFID," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India,2020, pp. 406-411, doi:10.1109/ICSSIT48917.2020.9214287.

[7] S. D V, A. R, E. R. K and A. S, "Enhanced Security Feature of ATM's Through Facial Recognition," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 1252-1256, doi: 10.1109/ICICCS51141.2021.9432327.

[8] C. Bhuvaneswari, T. Malini, A. Giri and S. Mahato, "Biometric And IOT Technology Based Safety Transactions In ATM," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2021, pp. 949-952, doi: 10.1109/ICACCS51430.2021.9442051.

[9] C. Su, Y. Yan, S. Chen and H. Wang, "An efficient deep neural networks training framework for robust face recognition," 2017 IEEE International Conference on Image Processing (ICIP), Beijing, China, 2017, pp. 3800-3804, doi: 10.1109/ICIP.2017.8296993.

[10] V. Ghenescu, R. E. Mihaescu, S. -V. Carata, M. T. Ghenescu, E. Barnoviciu and M. Chindea, "Face Detection and Recognition Based on General Purpose DNN Object Detector," 2018 International Symposium on Electronics andTelecommunications (ISETC), Timisoara, Romania, 2018, pp. 1-4, doi: 10.1109/ISETC.2018.8583861.

[11] S. Jafri, S. Chawan and A. Khan, "Face Recognition using Deep Neural Network with "LivenessNet"," 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 2020, pp. 145-148, doi: 10.1109/ICICT48043.2020.9112543.

[12] P. Terhörst, M. Huber, N. Damer, F. Kirchbuchner, K. Raja and A. Kuijper, "Pixel-Level Face Image Quality Assessment for Explainable Face Recognition," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 2, pp. 288-297, April 2023, doi:10.1109/TBIOM.2023.3263186.

[13] A. Maafiri, O. Elharrouss, S. Rfifi, S. A. Al-Maadeed and K. Chougdali, "DeepWTPCA-L1: A New Deep Face Recognition Model Based on WTPCA-L1 Norm Features," in IEEE Access, vol. 9, pp. 65091-65100, 2021, doi: 10.1109/ACCESS.2021.3076359.

[14] X. Shao, X. Zhou, Z. Li and Y. Shi, "Multi-View Face Recognition Via Well-Advised Pose Normalization Network," in IEEE Access, vol. 8, pp. 66400-66410, 2020, doi:10.1109/ACCESS.2020.2983459.

[15] L. Li, X. Mu, S. Li and H. Peng, "A Review of Face Recognition Technology," in IEEE Access, vol. 8, pp. 139110-139120, 2020, doi: 10.1109/ACCESS.2020.3011028.

[16] B. Kocacinar, B. Tas, F. P. Akbulut, C. Catal and Mishra, "A Real-Time CNN-Based Lightweight Mobile Masked Face Recognition System," in IEEE Access, vol. 10, pp. 63496-63507, 2022, doi:10.1109/ACCESS.2022.3182055.

[17] N. Zhu, Z. Yu and C. Kou, "A New Deep Neural Architecture Search Pipeline for Face Recognition," in IEEE Access, vol. 8, pp. 91303-91310, 2020, doi:10.1109/ACCESS.2020.2994207.

[18] L. S. Luevano, L. Chang, H. Méndez-Vázquez, Y. Martínez-Díaz and M. González-Mendoza, "A Study on the Performance of Unconstrained Very Low Resolution Face Recognition: Analyzing Current Trends and New Research Directions," in IEEE Access, vol. 9, pp. 75470-75493, 2021, doi: 10.1109/ACCESS.2021.3080712.

[19] M. Zemlyanikin, A. Smorkalov, T. Khanova, A. Petrovicheva and G. Serebryakov, "512KiB RAM Is Enough! Live Camera Face Recognition DNN on MCU," 2019 IEEE/CVF International Conference on Computer Vision Workshop(ICCVW), Seoul, Korea (South), 2019, pp. 2493-2500, doi: 10.1109/ICCVW.2019.00305.

[20] A. E. Alami, Z. Lakhili, A. Mesbah, A. Berrahou and H. Qjidaa, "Color Face Recognition by Using Quaternion and Deep Neural Networks," 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, Morocco, 2019, pp. 1-5, doi: 10.1109/WITS.2019.8723788.

[21] M. F. Rahman, F. Sthevanie and K. N. Ramadhani, "Face Recognition In Low Lighting Conditions Using Fisherface Method And CLAHE Techniques," 2020 8th International Conference on Information and Communication Technology(ICoICT), Yogyakarta, Indonesia, 2020, pp. 1-6, doi: 10.1109/ICoICT49345.2020.9166317.

[22] K. Meena and A. Suruliandi, "Local binary patterns and its variants for face recognition," 2011 International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, India, 2011, pp. 782-786, doi:10.1109/ICRTIT.2011.5972286.

[23] Xingfu Zhang and Xiangmin Ren, "Two Dimensional Principal Component Analysis based Independent Component Analysis for face recognition," 2011 International Conference on Multimedia Technology, Hangzhou, China, 2011, pp. 934-936, doi: 10.1109/ICMT.2011.60021

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 05/Issue 11/51100073738

Date: 22/11/2023

Certificate of Publication

*This is to certify that author "**Mr. Abhinay G. Dhamankar**" with paper ID "**IRJMETS51100073738**" has published a paper entitled "ENHANCED ATM SECURITY USING FACIAL RECOGNITION" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 05, Issue 11, November 2023***

Editor in Chief

IRJMETS Impact Factor 7.868

We Wish For Your Better Future

www.irjmets.com

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 05/Issue 11/51100073738

Date: 22/11/2023

Certificate of Publication

This is to certify that author "**Trupti Khade**" with paper ID "**IRJMETS51100073738**" has published a paper entitled "ENHANCED ATM SECURITY USING FACIAL RECOGNITION" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 05, Issue 11, November 2023**

Editor in Chief

IRJMETS Impact Factor 7.868

We Wish For Your Better Future

www.irjmets.com

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 05/Issue 11/51100073738

Date: 22/11/2023

Certificate of Publication

This is to certify that author "**Prashant Patil**" with paper ID "**IRJMETS51100073738**" has published a paper entitled "ENHANCED ATM SECURITY USING FACIAL RECOGNITION" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 05, Issue 11, November 2023**

Editor in Chief

IRJMETS Impact Factor 7.868

We Wish For Your Better Future

www.irjmets.com

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 05/Issue 11/51100073738

Date: 22/11/2023

Certificate of Publication

This is to certify that author "**Manish Raut**" with paper ID "**IRJMETS51100073738**" has published a paper entitled "ENHANCED ATM SECURITY USING FACIAL RECOGNITION" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 05, Issue 11, November 2023**

Editor in Chief

IRJMETS Impact Factor 7.868

We Wish For Your Better Future

www.irjmets.com

International Research Journal Of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

e-ISSN: 2582-5208

Ref: IRJMETS/Certificate/Volume 05/Issue 11/51100073738

Date: 22/11/2023

Certificate of Publication

This is to certify that author "**Shashank Satghare**" with paper ID "**IRJMETS51100073738**" has published a paper entitled "ENHANCED ATM SECURITY USING FACIAL RECOGNITION" **in International Research Journal Of Modernization In Engineering Technology And Science (IRJMETS), Volume 05, Issue 11, November 2023**

Editor in Chief

IRJMETS Impact Factor 7.868

We Wish For Your Better Future

www.irjmets.com