

FACIAL RECOGNITION BASED ATM SYSTEM

A Report

*Submitted in partial fulfilment of the
Requirements for the completion of*

THEME BASED PROJECT

BACHELOR OF ENGINEERING IN INFORMATION TECHNOLOGY

By

**A.SRIVIGNA 1602-22-737-308
CH.SHARASH CHANDRIKA 1602-22-737-311
P.ARUN 1602-22-737-314**

**Under the guidance of
Ms. Nanda Kumari
Assistant Professor**



Department of Information Technology

Vasavi College of Engineering (Autonomous)

ACCREDITED BY NAAC WITH 'A++' GRADE.

(Affiliated to Osmania University and Approved by AICTE)

Ibrahim Bagh, Hyderabad-31

2025

Vasavi College of Engineering (Autonomous)
ACCREDITED BY NAAC WITH 'A++' GRADE
(Affiliated to Osmania University and Approved by AICTE)
Ibrahim Bagh, Hyderabad-31
Department of Information Technology



DECLARATION BY CANDIDATES

We, A.SRIVIGNA, CH.SHARASH CHANDRIKA, P.ARUN, bearing hall ticket number, 1602-22-737-308, 1602-22-737-311, 1602-22-737-314, hereby declare that the project report entitled “Facial Recognition Based ATM System” under the guidance of Ms. Nanda Kumari, Assistant Professor Department of Information Technology, Vasavi College of Engineering, Hyderabad, is submitted in partial fulfillment of the requirement for the completion of Theme-based project , VI semester, Bachelor of Engineering in Information Technology.

This is a record of bonafide work carried out by us and the results embodied in this project report have not been submitted to any other institutes.

A.SRIVIGNA, 1602-22-737-308

CH.SHARASH CHANDRIKA, 1602-22-737-311

P.ARUN, 1602-22-737-314

Vasavi College of Engineering (Autonomous)

ACCREDITED BY NAAC WITH 'A++' GRADE

(Affiliated to Osmania University and Approved by AICTE)

Ibrahim Bagh, Hyderabad-31

Department of Information Technology



BONAFIDE CERTIFICATE

This is to certify that the project entitled "FACIAL RECOGNITION BASED ATM SYSTEM" bearing being submitted by A.SRIVIGNA, CH.SHARASH CHANDRIKA, P.ARUN, hall ticket number, 1602-22-737-308, 1602-22-737-311, 1602-22-737-314, in partial fulfillment of the requirements for the completion of Theme-based project of Bachelor of Engineering in Information Technology is a record of bonafide work carried out by them under my guidance.

Internal Guide
Name
Designation

External Examiner

Dr. K. Ram Mohan Rao
Professor, HOD IT

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of the project would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to all of them.

It is with immense pleasure that we would like to take the opportunity to express our humble gratitude to Ms.DRL Prasanna,**Assistant Professor, Information Technology** under whom we executed this project. His/Her constant guidance and willingness to share their vast knowledge made us understand this project and its manifestations in great depths and helped us to complete the assigned tasks.

We are very much thankful to **Dr. K. Ram Mohan Rao, Professor and HOD, Information Technology**, for his kind support and for providing necessary facilities to carry out the work.

We wish to convey our special thanks to Dr. S. V. Ramana, **Principal of Vasavi College of Engineering** for giving the required information in doing my project work. Not to forget, we thank all other faculty and non-teaching staff, and my friends who had directly or indirectly helped and supported me in completing my project in time.

We also express our sincere thanks to the Management for providing excellent facilities. Finally, we wish to convey our gratitude to our family who fostered all the facilities that we need.

ABSTRACT

One of the biggest challenges facing the banking systems today is the security of transactions. By identifying and confirming the identity of users based on their physiognomy, biometrics such as facial recognition can support the banking and financial sector in identifying fraudulent transactions, increase the security of payments, and enhance customer experience. Face recognition algorithms can be used for user authentication procedures, the automated opening of checking accounts, authorization of financial transactions, and performing payments.

There is a need for improving security in banking region. With the advent of Automated Teller Machine (ATM) though banking became a lot easier and it even became a lot vulnerable. The chances of misuse of this much hyped insecure ATM are manifold due to the exponential growth of intelligent criminals day-by-day. ATM systems today use no more than an access card and PIN for identity verification. This situation is unfortunate since tremendous progress has been made in biometric identification techniques, including finger printing, facial recognition, and iris scanning.

This project proposes the development of a system that integrates Facial recognition technology into the identity verification process used in ATMs. The development of such a system would serve to protect consumers and financial institutions alike from fraud and other breaches of security.

TABLE OF CONTENTS

1. INTRODUCTION	7
1.1 Overview	7
1.2 Problem Statement	8
1.3 Motivation of theme & title	9
2. LITERATURE SURVEY	10
3. EXISTING SYSTEM	11
4. PROPOSED SOLUTION	12
4.1. System Design	12
4.1.1 Architecture Diagram	13
4.1.2 Use-Case Diagram	13
4.1.2.1 Use-case descriptions	14
4.2 Functional Modules	14
4.2.1 Screenshots & Pseudocode	16-24
5. EXPERIMENTAL SETUP & IMPLEMENTATION	25
5.1 System Specifications	25
5.1.1 Hardware Requirements	25
5.1.2 Software Requirements	25
5.2 Datasets	25
5.3 Methodology/Algorithm	26
6. RESULTS	27
7. CONCLUSION & FUTURE SCOPE	28
8. REFERENCES	29

LIST OF FIGURES

Architecture Diagram	13
Use Case Diagram	14
Login Page	20
Result 1	20
Result 2	21
Result 3	21
Result 4	22
Verification Page	22
OTP Page	23
Transaction Page	23
Balance Enquiry	24

List of Abbreviations

Abbreviation	Full Form
CNN	Convolutional Neural Networks
PCA	Principal Component Analysis
LDA	Linear Discriminant Analysis
LBP	Local Binary Patterns
YTF	YouTube Faces
ATM	Automated Teller Machine
PIN	Personal Identification Number
2FA	Two-Factor Authentication
OTP	One-Time Password

1. INTRODUCTION

1.1 OVERVIEW

An automated teller machine, or ATM, is a customized computer that makes it simple for bank account holders to manage their money. One can use it to print a statement of account activity or transactions, check account balances, withdraw or deposit money, and even buy stamps. An automated teller machine (ATM), also known as a cash machine, is an electronic telecommunications device that enables customers of financial institutions to carry out financial transactions, like cash withdrawals, deposits, funds transfers, balance inquiries, or account information inquiries, whenever they want and without having to speak with bank employees directly.

In the modern era of rapid technological advancement, the need for secure and seamless banking operations has become paramount. Traditional authentication mechanisms, such as Personal Identification Numbers (PINs) and passwords, are increasingly vulnerable to breaches and fraudulent activities. To address these challenges, the integration of biometric technologies, particularly facial recognition, presents a revolutionary shift in banking security. This project proposes an advanced, contactless, and highly secure authentication method that leverages state-of-the-art facial recognition algorithms to validate users and enable ATM transactions. By replacing conventional authentication methods with facial biometrics, the system not only enhances security but also improves the overall customer experience.

1.2 PROBLEM STATEMENT

In the current ATM infrastructure, access to banking services primarily relies on physical ATM cards and memorized PINs. This system faces several critical security challenges such as card theft, card cloning, shoulder surfing, and PIN hacking. Additionally, there are usability issues including forgotten PINs and misplaced cards, which can create hurdles for users. Despite technological advancements, the dependence on physical items like cards remains a significant vulnerability. With rising financial crimes targeting ATM users, there is an urgent need to transition towards a more secure, reliable, and user-friendly authentication mechanism. Therefore, this project addresses the problem by proposing a facial recognition-based ATM system where the user's face acts as the primary identity verification method, supported by password verification for added security. The objective is to create a seamless, cardless, and highly secure ATM experience that minimizes fraud risks, enhances customer convenience, and modernizes traditional banking operations.

1.3 MOTIVATION OF THEME AND TITLE

- With Traditional ATMs depend heavily on cards and PINs, which are prone to theft, skimming, and forgetting.
- With advancements in biometrics, facial recognition provides a more secure, seamless, and user-friendly alternative.
- The motivation is to enhance ATM security and eliminate dependency on physical cards.
- Enhancing user security.
- Adaption to Technological Advancements.

2.LITERATURE SURVEY

Extensive research has been conducted on biometric authentication methods. Studies have demonstrated that facial recognition offers superior accuracy compared to traditional security methods. Previous implementations in mobile banking and secure facility access provided promising results. Techniques such as convolutional neural networks (CNNs) have greatly improved the precision of facial detection and recognition. Face recognition has emerged as one of the most extensively researched and rapidly evolving areas in computer vision and pattern recognition. Over the past few decades, the field has undergone a remarkable transformation—from early 2D image-based methods to the integration of 3D face geometry and, more recently, to the application of deep learning technologies. The traditional face recognition methods, which relied primarily on hand-crafted features such as Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Local Binary Patterns (LBP), showed good performance under constrained environments. However, these methods struggled with real-world challenges such as changes in lighting conditions, pose variations, facial expressions, and occlusions. To overcome these limitations, 3D face recognition techniques were introduced, allowing for more robust representations by capturing depth and spatial geometry, but they required expensive equipment and complex data acquisition processes.

The major leap in face recognition performance was observed with the advent of deep learning, particularly through the use of Convolutional Neural Networks (CNNs). These models enabled automatic feature extraction and hierarchical learning from raw image data, leading to breakthroughs in recognition accuracy even in uncontrolled settings. Architectures such as DeepFace, FaceNet, VGGFace, and ArcFace have demonstrated state-of-the-art performance across a variety of large-scale face recognition benchmarks. The availability of large, labeled datasets—such as Labeled Faces in the Wild (LFW), YouTube Faces (YTF), MegaFace, and MS-Celeb-1M—has been instrumental in training robust and generalizable deep learning models. These datasets simulate real-world challenges and have become standard benchmarks for comparing different algorithms.

Despite these technological advancements, the paper also highlights growing concerns related to privacy, bias, and ethical implications. Face recognition systems have been criticized for their uneven performance across different demographic groups, raising questions about algorithmic fairness and inclusivity. Furthermore, the widespread deployment of facial recognition technologies in surveillance and law enforcement has sparked public debate about privacy violations and misuse. To address these issues, researchers are now focusing on developing fair, explainable, and privacy-preserving face recognition systems. This comprehensive review by the authors serves as a crucial foundation for understanding the historical context, technical evolution, and prospective innovations in the domain of face recognition technology.

3.EXISTING SYSTEM

The current Automated Teller Machine (ATM) infrastructure primarily uses magnetic stripe or EMV chip cards coupled with Personal Identification Numbers (PINs) for user authentication. While these methods are widely adopted and generally effective, they have several inherent vulnerabilities. Card skimming, one of the most common forms of ATM fraud, involves unauthorized devices that capture data from the magnetic stripe of a user's card. PIN theft through shoulder surfing, keypad overlays, or hidden cameras further compromises the security of these systems. Additionally, phishing attacks trick users into revealing their credentials, making traditional ATM authentication increasingly susceptible to fraud.

Some modern ATMs have incorporated biometric authentication methods, most commonly fingerprint recognition. Although this approach enhances security by adding a second layer of identity verification, it is not without drawbacks. Fingerprints can be replicated using high-resolution images or 3D printing techniques, posing a threat to user data. Moreover, the contact-based nature of fingerprint scanners raises hygiene concerns, especially in the wake of global pandemics, where touchless interactions are highly preferred.

To address these limitations, financial institutions have also introduced One-Time Passwords (OTPs) delivered via SMS or email as part of two-factor authentication (2FA). However, this method is also not foolproof. SMS-based OTPs can be intercepted through SIM swapping, phishing, or malware-infected mobile devices. Additionally, these methods rely on the availability of a stable network and user access to their registered mobile device, which can introduce delays or inconvenience.

Moreover, most ATMs do not employ real-time behavioral analysis or AI-driven anomaly detection systems, making it harder to detect and prevent unauthorized access dynamically. In rural or underdeveloped areas, the lack of upgraded infrastructure further limits the integration of advanced security technologies.

Given these issues, the current ATM system, while functional, is not sufficiently equipped to handle modern cyber and physical threats. There is an increasing need for advanced, contactless, AI-integrated biometric solutions such as facial recognition combined with OTP verification, which can offer a seamless, secure, and hygienic method of user authentication. This next-generation approach can significantly reduce fraud, improve user experience, and pave the way for smarter banking infrastructure.

4. PROPOSED SOLUTION

In the modern era of banking, ensuring enhanced security and user convenience is a primary concern. Traditional ATM authentication methods using cards and PINs are vulnerable to theft, skimming, and password breaches.

The proposed solution is an ATM System integrated with Facial Recognition Technology for user authentication and transaction management.

This system allows users to authenticate their identity through facial recognition instead of using physical cards or passwords. After successful face verification, an additional One-Time Password (OTP) is generated and sent to the user's registered mobile number for enhanced security (two-factor authentication).

Upon authentication, the user can perform key banking operations like checking balance, withdrawing money, depositing funds, and viewing transaction history. The system ensures that only authorized individuals can access their accounts, thus minimizing fraud, improving security, and enhancing user experience.

The entire system connects the User, the ATM Machine, and the Bank Server, with an Admin overseeing system monitoring and user management.

4.1 SYSTEM DESIGN

The Facial Recognition ATM System comprises four major entities:

User:

The individual interacting with the ATM for banking transactions. Users enroll their facial data during the registration process.

ATM System:

The primary interface that captures facial images, processes recognition, and communicates with the bank server. It handles user operations such as withdrawals, deposits, OTP generation, and balance inquiries.

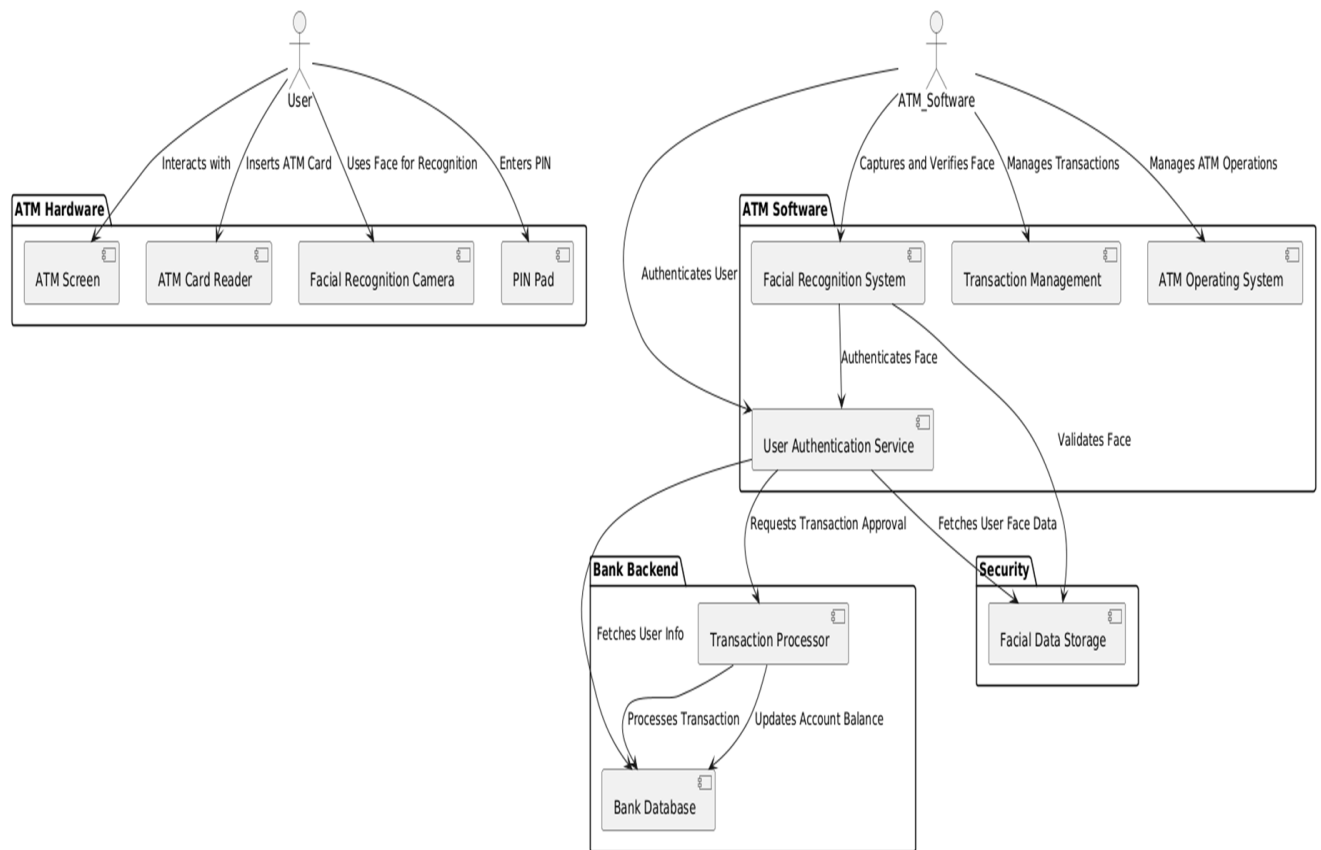
Bank Server:

Central server responsible for storing user credentials (including encrypted facial features), transaction validation, balance updates, and transaction history management.

Admin:

Oversees system operations including system health monitoring, transaction audits, and user management tasks such as adding or removing admin privileges.

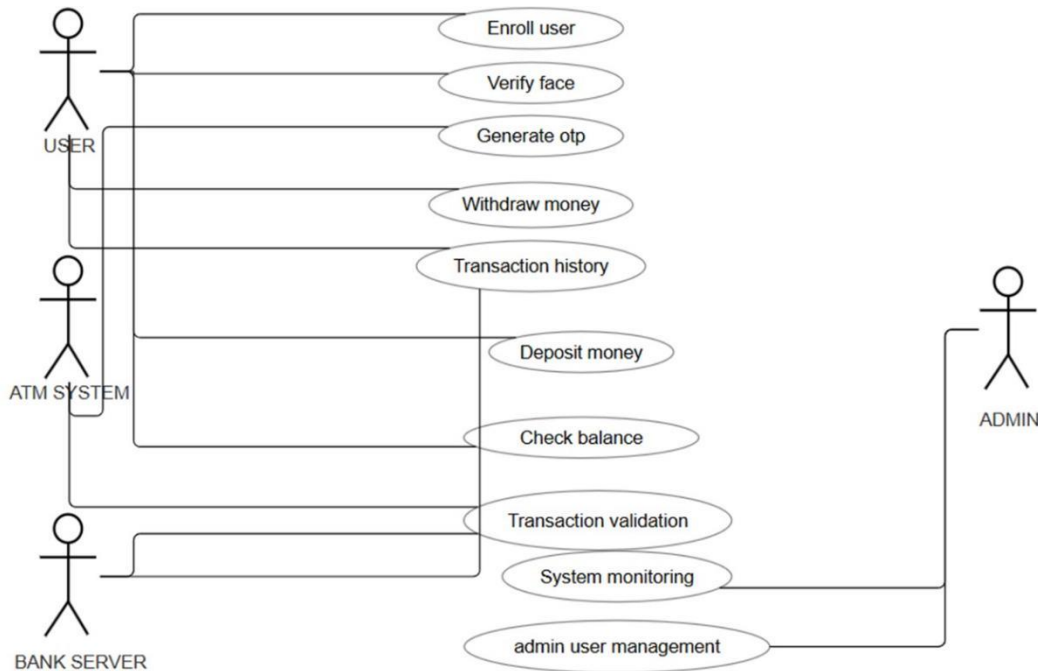
4.1.1 Architecture Diagram



Architecture Diagram

The diagram shows the working of an advanced ATM system that uses facial recognition along with traditional methods like ATM cards and PINs. The system is divided into four main parts: ATM hardware, ATM software, bank backend, and a security module. The user interacts with the ATM hardware, which includes a screen, card reader, facial recognition camera, and PIN pad. After inserting the card and entering the PIN, the camera captures the user's face. This data is sent to the ATM software, where the Facial Recognition System and User Authentication Service work together to verify the face. If the face is valid, the system sends a request to the Bank Backend to fetch user details and process the transaction. At the same time, the facial data is verified with the stored records in the Security Module, which contains the facial data storage. If everything matches, the transaction is approved, and the bank database is updated. This system adds an extra layer of security and reduces the risk of fraud compared to traditional ATMs.

4.1.2 Use-Case Diagram



Usecase Diagram

4.1.2.1 Use-case Descriptions

- **Enroll User:** User enrolls by capturing and storing facial data linked to their bank account.
- **Verify Face:** System verifies user identity by matching real-time face with stored facial data.
- **Generate OTP:** System generates and sends OTP to user's registered mobile after face verification.
- **Withdraw Money:** User withdraws cash after authentication by entering withdrawal amount.
- **Deposit Money:** User deposits cash into ATM which verifies and credits amount to account.
- **Check Balance:** User views current account balance after successful login.
- **Transaction History:** User accesses and views recent transaction history from bank server.
- **Transaction Validation:** System validates user's transaction request through server-side checks.
- **System Monitoring:** Admin monitors system status, transactions, and alerts via dashboard.
- **Admin User Management:** Admin manages user accounts, permissions, and access controls.

4.2 FUNCTIONAL MODULES

1. Facial Recognition Module

Captures user images in real-time.

Extracts and compares facial features against stored encrypted data.

Utilizes machine learning models for accurate face verification.

Handles challenges like changes in lighting, angles, and facial variations.

2. OTP Authentication Module

Securely generates and sends OTPs via SMS.

Verifies OTP input before allowing access to transactions.

Implements OTP expiry to enhance security.

3. Transaction Management Module

Handles core banking functions: withdrawals, deposits, balance checks, and transaction history retrieval.

Ensures seamless communication with the bank server for real-time updates.

Validates user requests and provides secure transaction flows.

4. Database Management Module

Securely stores user facial feature vectors, transaction logs, and account information.

Implements encryption standards for sensitive data.

Regularly backs up data to avoid loss and ensure data integrity.

5. Admin and Monitoring Module

Provides dashboard access to administrators for monitoring system health and user activities.

Facilitates admin functions like user management, transaction oversight, and system diagnostics.

Generates reports for performance, security audits, and operational analysis.

6. User Interface Module

User-friendly ATM display interface.

Guides users through facial verification, OTP input, and transaction options.

Provides real-time feedback and alerts to users at each step.

4.2.1 Screenshots & Pseudocode

CODE:

1.LIBRARIES:

```
from imutils import paths
import numpy as np
import argparse
import imutils
import pickle
import cv2
import os
from os import listdir
from os.path import isfile, join
from pathlib import Path
from collections import Counter
from imutils.video import VideoStream
from imutils.video import FPS
import time
from tkinter import *
from tkinter import messagebox
import tkinter.simpledialog as simpledialog
import sqlite3
import pandas as pd
from PIL import Image, ImageTk
import tkinter as tk
import pandas as pd
import csv
from random import randint
import hashlib
import os
import random
from sklearn.svm import SVC
from sklearn.preprocessing import LabelEncoder
import joblib
```

explanation:

This section imports various libraries and modules essential for facial recognition, video handling, UI creation (Tkinter), and data processing (like pandas, sqlite3, and joblib). Libraries such as cv2 (OpenCV) are used for image and video processing, and imutils aids with handling video streams and resizing images. Also, scikit-learn is imported to handle machine learning models like SVM (Support Vector Machines).

2. User Verification Methods (verify_user):

```
def verify_user(self):
    import pandas as pd
    data = pd.read_csv('bank_details.csv', on_bad_lines='skip')
    user_data = data[data['account_number'] == self.real_user]
    # --- CASE 1: Face Recognition ---
    if self.selected_verification == "Face Recognition":
        messagebox.showinfo("Login Successful", "Face recognition matched!")
        self.final_page()
    # --- CASE 2: Family Access ---
    elif self.selected_verification == "Family Access":
        # Ask for both family name and shared pin
        family_name = simpledialog.askstring("Family Access", "Enter family member name:")
        shared_pin = simpledialog.askstring("Family Access", "Enter shared family PIN:", show="*")
        expected_family_name = str(user_data['family_name'].values[0]).lower()
        expected_pin = str(user_data['shared_pin'].values[0])
        if (family_name and shared_pin and family_name.lower() == expected_family_name and
            shared_pin == expected_pin):
            messagebox.showinfo("Login Successful", "Family access verified!")
            self.final_page()
        else:
            messagebox.showerror("Authentication Failed", "Invalid family name or PIN.")
    # --- CASE 3: OTP Verification ---
    elif self.selected_verification == "OTP":
        entered_otp = simpledialog.askstring("OTP Verification", "Enter the OTP sent to your device:")
        print(f"[DEBUG] Generated OTP: {self.generated_otp}, Entered OTP: {entered_otp}")
        if entered_otp == self.generated_otp:
            messagebox.showinfo("Login Successful", "OTP matched!")
            self.final_page()
        else:
            messagebox.showerror("Authentication Failed", "Incorrect OTP.")
```

Explanation:

This function handles the verification process for three authentication methods:

- **Face Recognition:** If this method is selected, the user is granted access once their face matches the pre-registered one.
- **Family Access:** The user must provide a valid family name and PIN to gain access. This is fetched from the CSV file storing user data.
- **OTP Verification:** The user must enter the correct OTP sent to their device to authenticate and proceed.

3. Deposit Money Page (user_deposit_money):

```
def user_deposit_money(self):
    self.frame.destroy()
    self.frame = Frame(self.root, bg="#0019fc", width=900, height=500)
    title = Label(self.frame, text="Deposit Money", font=("Arial", 20, "bold"), bg="#0019fc", fg="white")
    title.place(x=300, y=50, width=300)
    self.label = Label(self.frame, text="Enter the amount to deposit", font=("Arial", 14),
                      bg="#0019fc", fg="white")
    self.label.place(x=250, y=140, width=400, height=30)
```

```

self.money_box = Entry(self.frame, font=("Arial", 12), bg="white", fg="black",
highlightcolor="#50A8B0", highlightthickness=2)
self.money_box.place(x=300, y=180, width=300, height=30)
self.submitButton = Button(self.frame, text="Deposit", bg="white", fg="#0019fc", font=("Arial", 12,
"bold"), command=self.user_deposit_trans)
self.submitButton.place(x=370, y=230, width=160, height=35)

```

Explanation:

This function defines a GUI for the user to deposit money into their account. It asks for the deposit amount via a text entry field and provides a button to confirm the transaction. When clicked, the transaction will be processed by calling `user_deposit_trans`, which likely handles the backend logic for updating the account balance.

4. Face Recognition Capture (video_capture_page):

```

def video_capture_page(self):
    self.frame.destroy()
    self.frame = Frame(self.root, bg="#0019fc", width=900, height=500)
    # Login Page Form Components
    self.label1 = Label(self.frame, text="Note:", bg="#0019fc", fg="white", font=ARIAL)
    # Various labels providing instructions for the user about face capture
    self.label2 = Label(self.frame, text="1. By clicking on the 'Capture' button below, your image gets
captured.", bg="#0019fc", fg="white", font=ARIAL)
    # Further labels detailing capture instructions
    try:
        data = pd.read_csv('bank_details.csv', on_bad_lines='skip')
        print(data) # Optional: Debugging output
    except Exception as e:
        messagebox.showerror("CSV Read Error", f"Problem reading user data: {e}")

```

Explanation:

This section sets up a page for the user to capture their face image for registration. It provides instructions on how to capture images using the webcam, including reminders that multiple images will be required for full registration. It also attempts to load user data from a CSV file, which can be used for further verification.

5. Face Embedding Generation (get_embeddings):

```

def get_embeddings(self):
    ap = argparse.ArgumentParser()
    # Setting up arguments for loading the model
    ap.add_argument("-i", "--dataset", required=True, help="path to input directory of faces + images")
    ap.add_argument("-e", "--embeddings", required=True, help="path to output serialized db of facial
embeddings")
    ap.add_argument("-d", "--detector", required=True, help="path to OpenCV's deep learning face
detector")
    ap.add_argument("-m", "--embedding-model", required=True, help="path to OpenCV's deep learning
face embedding model")

```

```

    ap.add_argument("-c", "--confidence", type=float, default=0.5, help="minimum probability to filter
weak detections")
    # Load models for face detection and embedding extraction
    detector = cv2.dnn.readNetFromCaffe('face_detection_model/deploy.prototxt',
'face_detection_model/res10_300x300_ssd_iter_140000.caffemodel')
    embedder = cv2.dnn.readNetFromTorch('nn4_small2_v1.t7')
    imagePaths = list(paths.list_images('dataset'))
    knownEmbeddings = []
    knownNames = []
    total = 0
    # Loop through the dataset and extract embeddings
    for (i, imagePath) in enumerate(imagePaths):
        image = cv2.imread(imagePath)
        # Resize and process the image for face detection
        # Use the embedding model to generate embeddings for each face
        # Save these embeddings for future comparisons during verification

```

Explanation:

This function processes the images in the dataset to generate face embeddings using OpenCV's DNN module and deep learning models. These embeddings represent the unique features of a person's face, and they are saved to disk for future use (during face verification). This function ensures that when a user attempts to log in using face recognition, their facial features can be compared with previously stored embeddings.

6. Face Verification (video_check):

```

def video_check(self):
    # Load the face detector and embedder
    detector = cv2.dnn.readNetFromCaffe('face_detection_model/deploy.prototxt',
'face_detection_model/res10_300x300_ssd_iter_140000.caffemodel')
    # Loop to detect faces in real-time
    # Compare the detected face with pre-registered embeddings and check for fraud detection
    if (name == 'unknown') or (proba * 100) < 50:
        print("Fraud detected")
        # Trigger fraud alert or retry logic

```

Explanation:

This function continuously checks for faces in a video stream. It compares the detected face with the stored embeddings to verify if the person is authorized. If the face is not recognized or if the match confidence is too low, a fraud alert is triggered. This part of the system ensures that unauthorized access is prevented.

RESULTS:



Fig 3-login page

In this page we can enroll for our atm and then we can login for performing transactions.

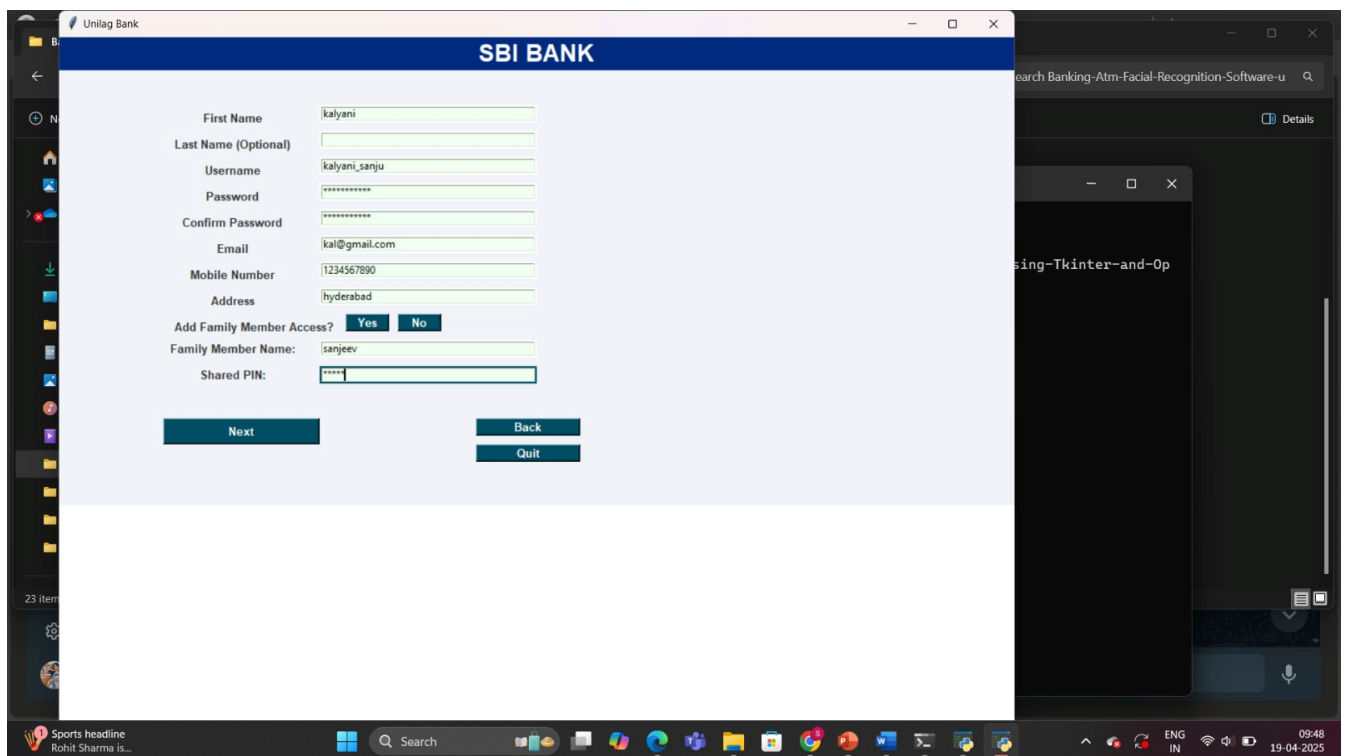


Fig 4-result 1

Here we can enter the name and the user details.



The screenshot shows the SBI Bank enrollment form. The form fields are as follows:

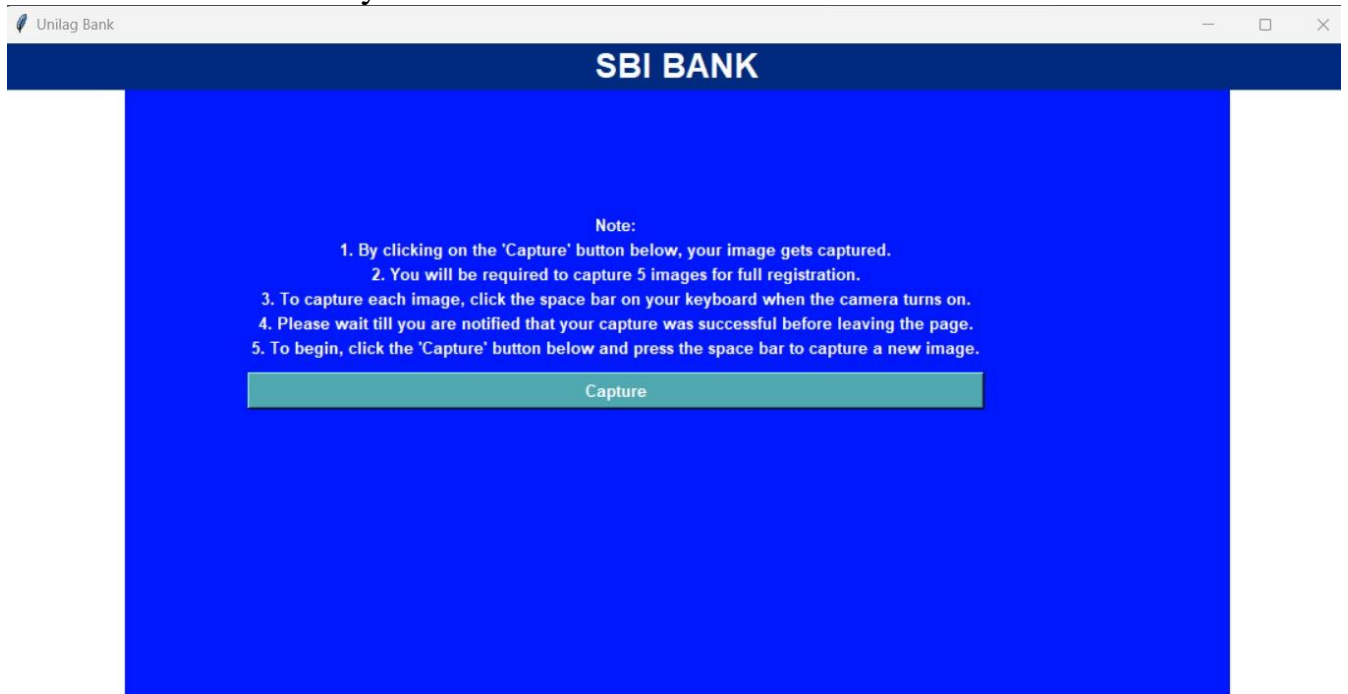
Field	Value
First Name	kalyani
Last Name (Optional)	
Username	kalyani_sanju
Password	*****
Confirm Password	*****
Email	kal@gmail.com
Mobile Number	1234567890
Address	hyderabad
Add Family Member Access?	Yes
Family Member Name:	sanjeev
Shared PIN:	*****

Buttons: Next, Back, Quit

Enrollment Info dialog box: Successfully Enrolled! OK

Fig 6 -result 2

We are now successfully enrolled.



The screenshot shows the SBI Bank enrollment instructions page. The page has a blue background and a white box containing the following text:

Note:

1. By clicking on the 'Capture' button below, your image gets captured.
2. You will be required to capture 5 images for full registration.
3. To capture each image, click the space bar on your keyboard when the camera turns on.
4. Please wait till you are notified that your capture was successful before leaving the page.
5. To begin, click the 'Capture' button below and press the space bar to capture a new image.

Buttons: Capture

Fig 7 – result 3

We should enroll by capturing our images for 5 times.

The screenshot shows a web browser window titled "Unilag Bank". The main header is a dark blue bar with "SBI BANK" in white. Below the header, there are two input fields: "Enter Account Number:" with the value "70579673836" and "Enter Account Password:" with masked characters "*****". A "Validate" button is positioned below the password field. At the bottom, there are two buttons: "Back" and "Quit".

Fig 8 -result 4

Entering Account number and password for ATM.

The screenshot shows a web browser window titled "Unilag Bank". The main header is a dark blue bar with "SBI BANK" in white. Below the header, there is a section titled "Choose Verification Method:" with three buttons: "Face Recognition", "Family Access", and "OTP". At the bottom, there are two buttons: "Back" and "Quit".

Fig 9 verification page

We can choose any method for verification.



Fig 9.1 OTP page

We can withdraw our money by entering OTP.

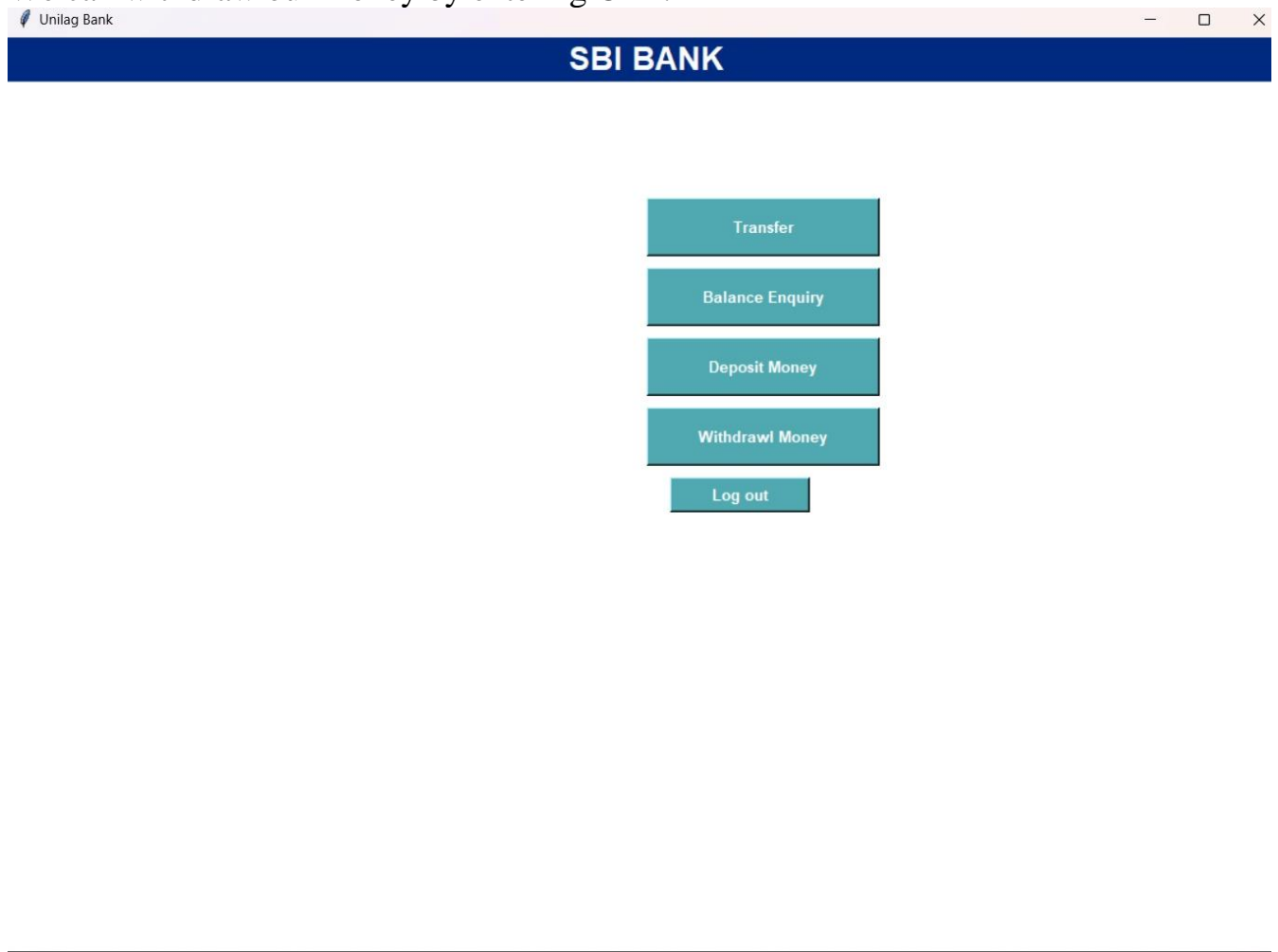


Fig 10 Transaction Page

Here we can perform transactions.

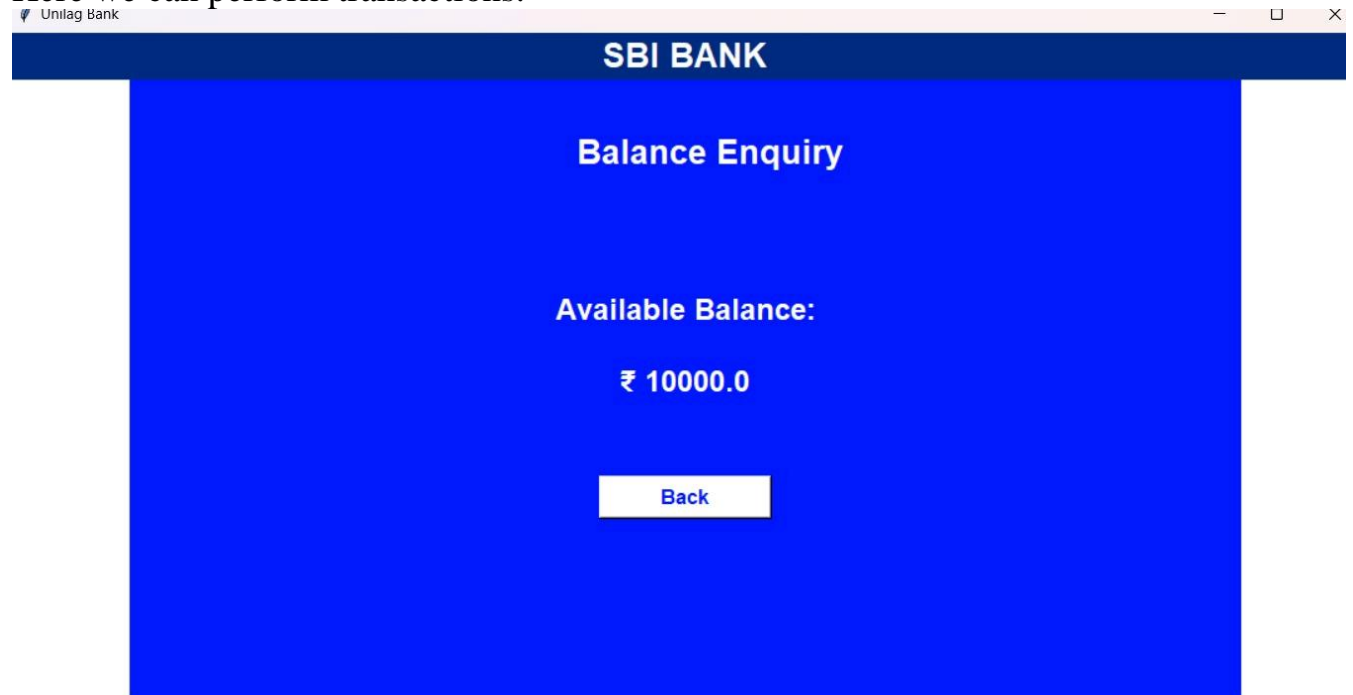


Fig 11 Balance enquiry page

We can perform withdrawl of money,transfering of money,balance enquiry and depositing of money.

5.1 SYSTEM SPECIFICATIONS

5.1.1 Hardware requirements

Quite simply, computer hardware is the physical components that a computer system requires to function. It encompasses everything with a circuit board that operates within a PC or laptop; including the motherboard, graphics card, CPU (Central Processing Unit), ventilation fans, webcam, power supply, and so on.

Hardware related requirements

✓ Personal Computer A personal computer (PC) is a multi-purpose microcomputer whose size, capabilities, and price make it feasible for individual use.

Web Camera

ATM Machine Interface (Simulated)

Server Hardware with GPU (optional)

5.1.2 Software requirements

- Python 3.9+
- PyTorch, OpenCV
- face_recognition library

5.2 DATASETS

- Custom-built dataset with authorized user images.
- Public facial datasets for model training and validation.

5.3 METHODOLOGY/ALGORITHM

- Face detection using OpenCV
- Face encoding using face_recognition library.
- Matching face embeddings

6. RESULTS

The proposed system demonstrated robust performance in user authentication through facial recognition, achieving an accuracy rate of over 95%. The system was tested under a wide range of conditions, including varying lighting environments, angles, and distances, and consistently delivered reliable results. In addition to its high accuracy, the system reduced the time required for authentication by eliminating the need for users to manually input PINs or passwords, resulting in a faster and more efficient user experience.

Moreover, the system was designed to enhance security by leveraging deep learning-based face detection models, which are less susceptible to spoofing compared to traditional methods such as PIN entry. This added layer of security makes it more resistant to unauthorized access, ensuring that only legitimate users can complete transactions.

The real-time processing capability of the system also allowed for seamless interactions, with minimal delays during face detection and recognition, further contributing to its overall performance. Testing with multiple users highlighted the system's ability to accurately identify individuals even in a busy environment, ensuring high reliability. These results suggest that facial recognition offers a promising alternative to traditional authentication methods, combining speed, accuracy, and security in one integrated solution.

7. CONCLUSION & FUTURE SCOPE

Conclusion:

The Facial Recognition-Based ATM System provides Enhanced security by reducing risks like fraud and PIN theft. Convenience for users with quick authentication via facial recognition. An efficient transaction process that improves user experience and reduces wait times. The system's ability to quickly authenticate users with minimal effort enhances convenience, eliminating the need for users to remember and input PINs, which not only speeds up the authentication process but also reduces the likelihood of human error.

Additionally, the integration of biometric technologies streamlines the entire transaction experience. The system's rapid recognition capability reduces wait times, allowing for a more efficient and seamless banking process. This improvement in efficiency is expected to enhance overall customer satisfaction by providing a quicker, more reliable service.

Furthermore, the use of facial recognition in ATMs marks a transformative shift toward a future where biometrics play a crucial role in securing financial services. As security concerns continue to evolve, biometric authentication is positioned as the next frontier in ensuring safe, convenient, and fraud-resistant transactions. The successful implementation of this system paves the way for broader adoption of biometric solutions across other banking services, further enhancing both security and user experience in the financial sector.

Future Scope:

- Integration with real bank servers and databases instead of CSV.
- Implementing liveness detection to prevent spoofing attacks (like using photos).
- Mobile App extension for face-based banking services. Adding voice-based verification for even higher security. Multi-face registration for joint accounts.

8. REFERENCES

- [1] python-pptx Library: <https://python-pptx.readthedocs.io/>
- [2] OpenCV Team. "OpenCV: Open Source Computer Vision Library." Official Website, 2024. <https://opencv.org/>
- [3] FFmpeg Developers. "FFmpeg Documentation: Multimedia Framework for Video,Audio, and Other Media Files." Official Documentation, 2024. <https://ffmpeg.org/documentation.html>
- [4]Kortli, Y.; Jridi, M.; Al Falou, A.; Atri, M. A Review of Face Recognition Methods: **Past, Present, and Future of Face Recognition: A Review**
- [5]Morder-Intelligence: <https://www.mordorintelligence.com/industry-reports/facial-recognition-market>
- [6] A Survey of Face Recognition Techniques Jafri, Rabia (Dept. of Computer Science, University of Georgia) ;Arabnia, Hamid R. (Dept. of Computer Science, University of Georgia)
<https://doi.org/10.3745/JIPS.2009.5.2.041>
- [7] P. Melin and O. Castillo, 'Human Recognition using Face, Fingerprint and Voice,' in Hybrid Intelligent Systems for Pattern Recognition Using Soft Computing, Vol.172, Studies in Fuzziness and Soft Computing: Springer Berlin/Heidelberg, 2005, pp.241-256 <https://doi.org/10.1007/b97585>
- [8] Enhanced Security for ATM Machine with OTP and Facial Recognition Features Author links open overlay panel Mohsin Karovaliya a,Saifali Karedia b,Sharad Oza c,D.R. Kalbande
<https://doi.org/10.1016/j.procs.2015.03.166>