

SECURING ATM TRANSACTIONS USING FACIAL RECOGNITION

K.VERONIKA ,S.HARSHITHA,J.KAVITHA, Dr. T. Vijaya Saradhi(Guide)
Sreenidhi Institute of Science and Technology

Abstract:

Anyone can check their balance and make cash withdrawals using an ATM. The quantity of ATMs a bank has may be taken into account when evaluating its strength. As there are more ATMs, there are also more fraudulent activities taking place inside of them. The primary goal of this initiative is to improve the security of ATM usage. The static key is used as security in the present procedure. The suggested technique incorporates Face-id as a key with the present method. The fact that each person's face ID is unique and cannot be used by anyone else except the user is one of the benefits.

The transaction is considered authorized if the cardholder is confirmed to be the user, at which point they are allowed to carry out any actions, including cash withdrawals and balance checks. We are utilizing a model and camera together with the Histogram of the Gradient method, Python modules, and a few machine-learning techniques to identify the persons. The system manipulates the image using OpenCV to recognize the faces in it. To recognize faces, one can employ the local binary pattern.

1. INTRODUCTION

Customers can do particular operations including cash withdrawals, deposits, money transfers, and account information inquiries anytime they want and independently of bank employees by using an automated teller machine (ATM). Physical security measures including CCTV surveillance of the ATM booth and security guards (human) are already in place to provide secure ATM service for consumers.

There are also other technologically based security measures in place, such as firewalls, data encryptions, network security, etc. However, scams like card theft, card fraud, card cloning, skimming, and other similar schemes have become more prevalent recently and are easily able to bypass existing security measures. It is now feasible to recognize a human face from a digital image or a video frame from a video source and to give each human face a unique identification thanks to developments in machine learning and computer vision. The goal of this project is to create an ATM that uses face recognition technology to confirm that each transaction has been approved by the account's owner.

Objective:

The primary goal of this project is to increase security, which will be different because transactions now depend not only on the right PIN but also on the person carrying out the transaction, whereas the current system just verifies the PIN and phone number (if necessary).

2. LITERATURE SURVEY

Different types of authentication used in ATMs have been explained in numerous research papers that have been published by numerous authors.

[1].For each automated teller machine (ATM), authentication is crucial. It authenticates often with an ATM card and pin. In this study, authentication was carried out using a "One Time Password" and a "Personal Identification Number" to increase security and prevent situations where a card can fall into the wrong hands and a person might carry out any transaction with the knowledge of the PIN.

[2]. A biometric system has replaced the user signature technique that was previously replaced by an ATM PIN owing to high risk. The biometric system makes use of the fingerprint, iris, retina, and veins. Cash will be distributed when it is a legitimate individual

2.1 Existing System

Entering our username and password is a straightforward authentication that we are all familiar with and follow. If we forget our password, we may also have a way to use it again and regain access to our account. A factor authentication method that covers two factors is an SMS message sent to our registered cell phone number.

The login procedure is made more secure without changing it by employing authentication, but by using the OpenCV approach, we are recognizing a picture that we put in our database.

Disadvantages

- Low security
- pin code verification is adequate.

2.2 Proposed System

To make transactions dependent on both the person making the transaction and the correct PIN on the card, this project proposes adding a new layer of security to the present ATM system. For instance, in our project, we used the Open CV Python implementation of the Local Binary Pattern Histogram technique for face recognition. **Advantages**

All industrial personnel may benefit from this proposed strategy because it is efficient in terms of security and time needs.

3. SYSTEM ANALYSIS & DESIGN

3.1 Functional Requirements:

A Software Requirements Specification (SRS) is a document that lists the requirements for software. A software system's black box specification describes how the programming will be written. It is a crucial document that bridges the communication gap between users and the developed program and helps to steer clear of fatal software project flops.

The two categories of requirements in the SRS are functional requirements and nonfunctional requirements. Functional requirements are concerned with a system's technical characteristics or the technical operations performed by each module, whereas nonfunctional requirements examine a system's operations under certain conditions.

Software Requirements Specification (SRS) objectives:

The customer will receive this as feedback.

- 1.It breaks down a system into modules and provides that information as input to the design specification.
- 2.It is used to validate and verify the product.
- 3.It supports the project management and system review processes.

Software Requirements Specification Advantages :

1. There will be open channels of communication between the client or customer and the system developers.
2. Because this area serves as a strong foundation for system design, the customer should only give all needs in this area.
3. This makes the Verification and Validation (V-Model) process easier.
4. This assists in estimating the project's cost,timeframe, and resource requirements.

3.2 Performance Requirements:

The effectiveness of a software system is described by its performance requirements. The software's performance includes response time, execution time, storage capacity, and throughput. The majority of the performance criteria for service levels were designed to support end-user tasks. Similar to other quality criteria, performance requirements are essential to the design and testing of software.

Even though gathering requirements is a crucial step in the software development process, it can be difficult. Scope, skill, and stability are the three main obstacles to collecting performance criteria. In the software development industry, project scope is usually uncertain, or different stakeholders give inconsistent or false scope assessments.

The scope of a project is frequently unknown in the software development business, or multiple stakeholders provide conflicting or deceptive scope evaluations. If one stakeholder discusses local needs while another addresses regional or national coverage, the system's design and performance may be quite different.

Establish a specified scope with stakeholders to support performance standards. Requirements are only useful if all stakeholders have a thorough understanding of the project's goals, capabilities, and restrictions. Users, clients, and other stakeholders may be completely unaware of the problems with performance. They may leave some details out.

3.3 System Architecture:

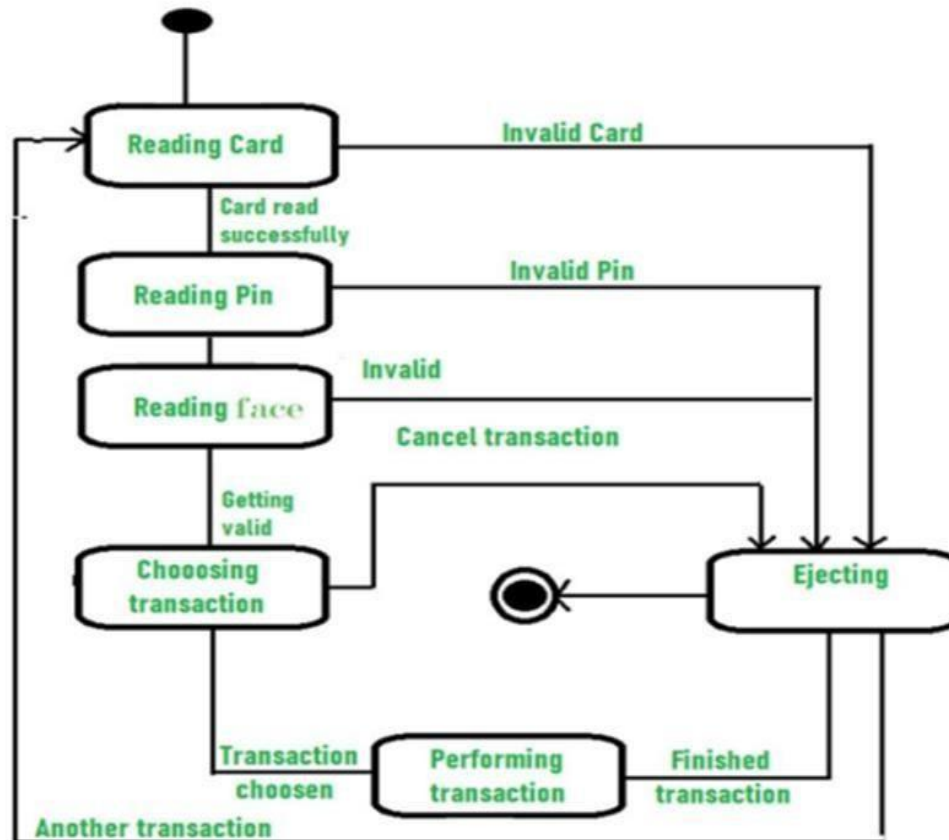


Figure 1: Architecture

INPUT DESIGN AND OUTPUT DESIGN

INPUT DESIGN

The interface between the information system and the user is provided by the input design. It entails creating standards and processes for data preparation as well as the techniques required to convert transaction data into a format that can be processed. This can be accomplished by having users directly enter the data into the system or by having them read it from a written or printed document while gazing at the computer.

Input design aims to reduce the amount of input required, manage mistakes, avoid delays, eliminate extra processes, and streamline the process. The input is made to offer ease and security while protecting privacy. Input Design kept the following things in mind:

- Which information should be supplied as input?
- How should the data be organized or coded?

- The conversation to direct the operating staff's input-giving.
- Techniques for creating input validations and procedures to take in the event of a mistake.

3.4 Data Flow Diagram :

Use case diagrams are made to show the functional requirements of a system. The components mentioned above must first be identified in order to produce a useful use case diagram.

- The name of the use case must be carefully considered. As a result, it's critical to pick a name that makes it obvious what tasks are being carried out.
- Give the performers a decent name, as well.
- The diagram should be clear in illustrating links and interdependence.
- Refrain from attempting to include all types of relationships. Because the diagram's main objective is to identify requirements.

If it's necessary to elaborate on a few key points, use a note.

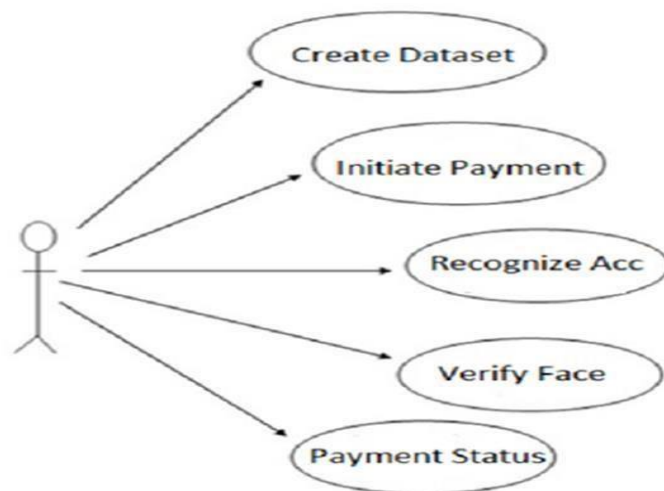


Figure 5: Use Case Diagram

4. IMPLIMENTATION AND RESUTS

The Histogram of Oriented Gradients technique is used to differentiate the human face. Making use of the dlib package, the relative modification of the face is completed. Support Vector Machine (SVM) for face classification and a Deep Convolutional Neural Network (Deep CNN) are prepared to obtain impressive estimates from the human face (128 different estimations from a single face). Here, the Local Binary Pattern (LBP) serves as the foundation for our face recognition method.

The Local Binary Pattern is successful and has been tweaked for our unique needs and improved face recognition. It is a powerful algorithm that may be modified as needed to serve our needs. An effective texturing operator for labelling picture pixels that uses the binary threshold values for each pixel's immediate neighbours.

The Face-Recognition technique known as Local Binary Pattern Histogram (LBPH) is used to detect a person's characteristics. It is renowned for its presentation and for making it possible to perceive an individual's character from both the front and side faces.

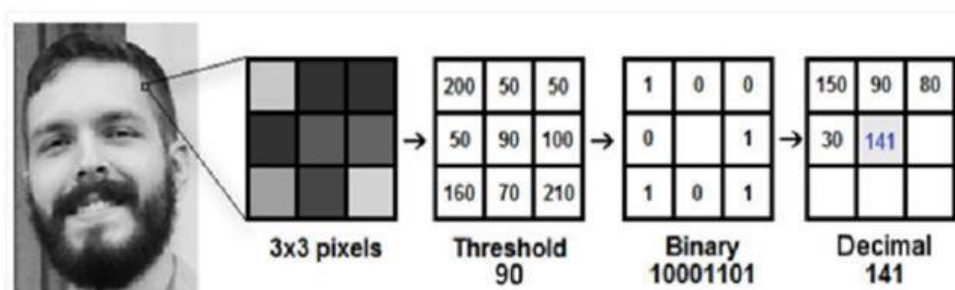


Figure 1: LBPH calculation

Before starting the logic behind the LBPH calculation, we should first understand a little bit about the specifics of Images and Pixels to understand how photos are handled before we start the content of FaceRecognition. So let's start understanding pictures and pixels.

photographs and Pixel The Matrix designs, as you can see above, which are composed of lines and parts, address all photographs. The pixel is a picture's main component. An image constitutes of many pixels.

These are all small square objects.

As previously indicated, in addition to entering card information, a pin, and our image, we added a further security measure called facial recognition.

Therefore, all information must be entered.

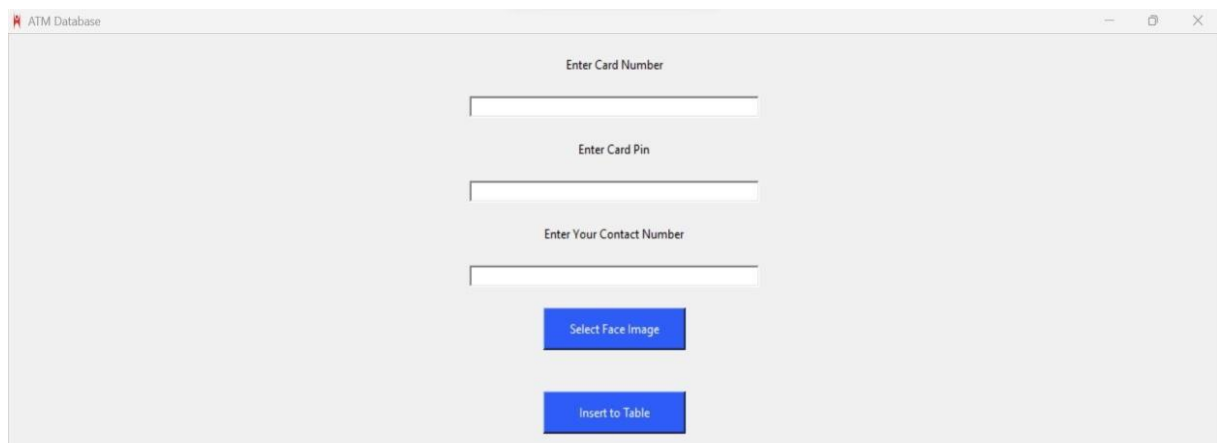


Figure 1: Database

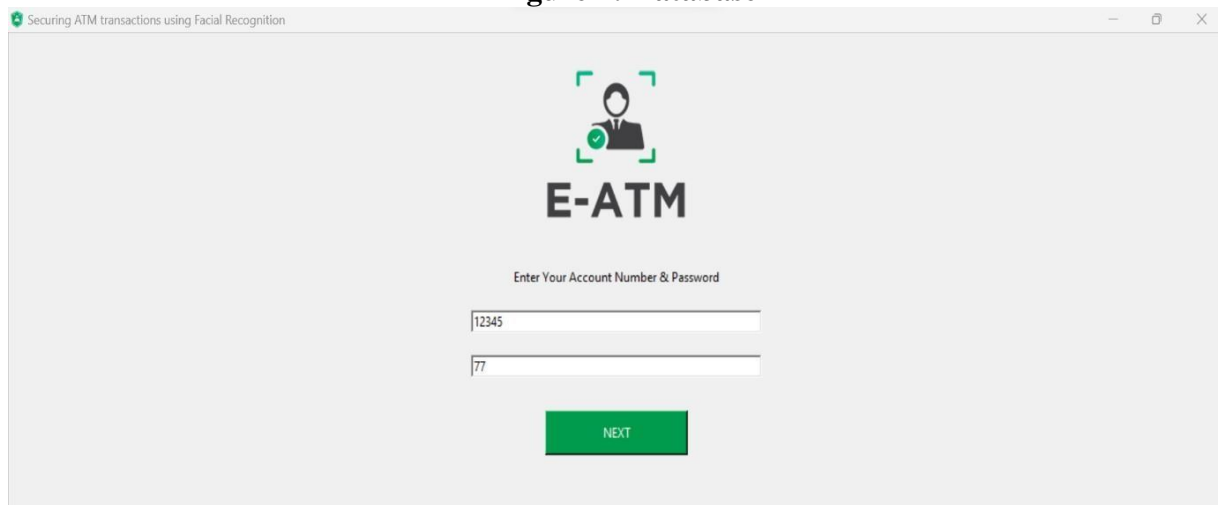


Figure 2: Input from the user

If all the information is accurate, our camera will turn on and check the image that is stored in the database, allowing the two scenarios to be observed.

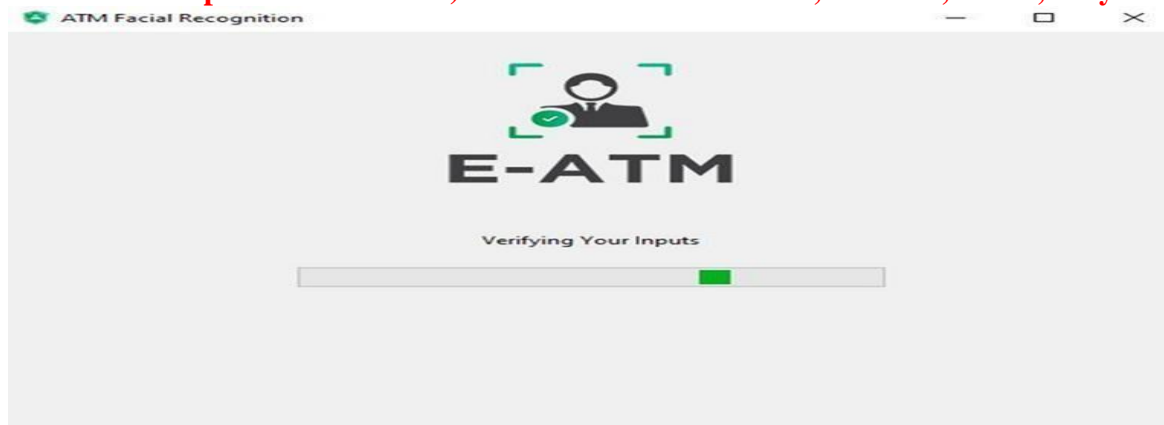


Figure 3: Face authentication

If face has no match with the image stored in database, we would get the output as If the entered pin is incorrect, then it will display as follows:

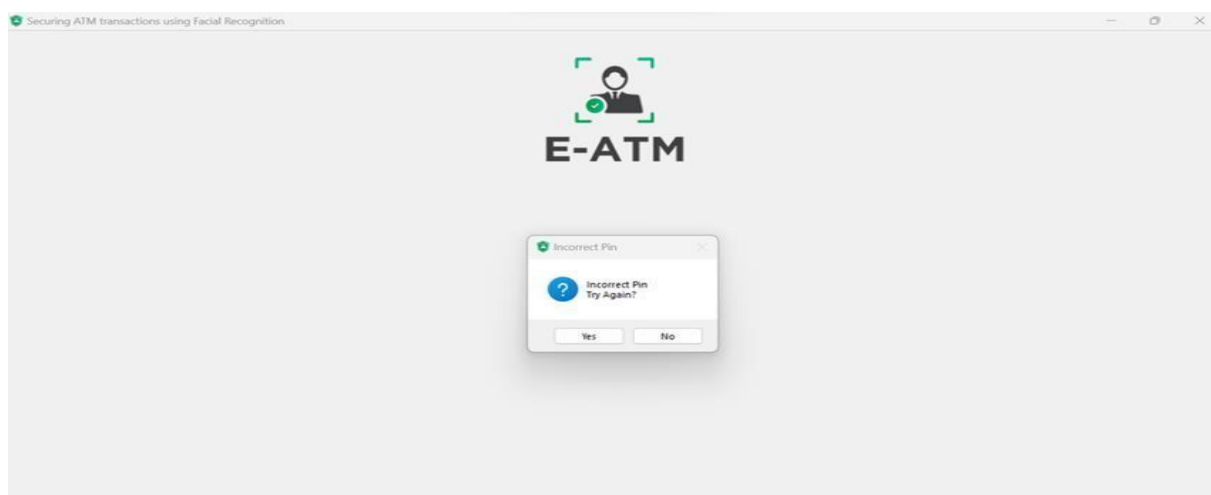


Figure 4: No face detected message

And if everything is entered correctly and the face matches with the image stored in the database:

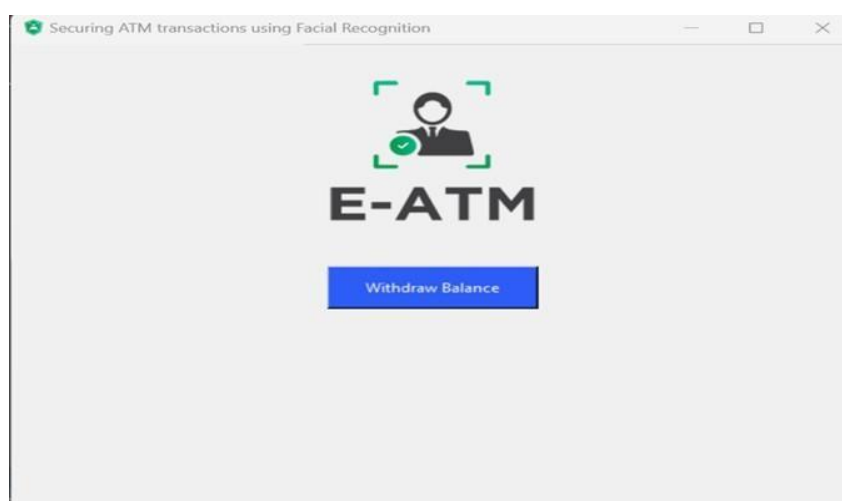


Figure 6: Withdraw option is shown

We need to input the amount in this box after clicking the Withdraw button, then click input.

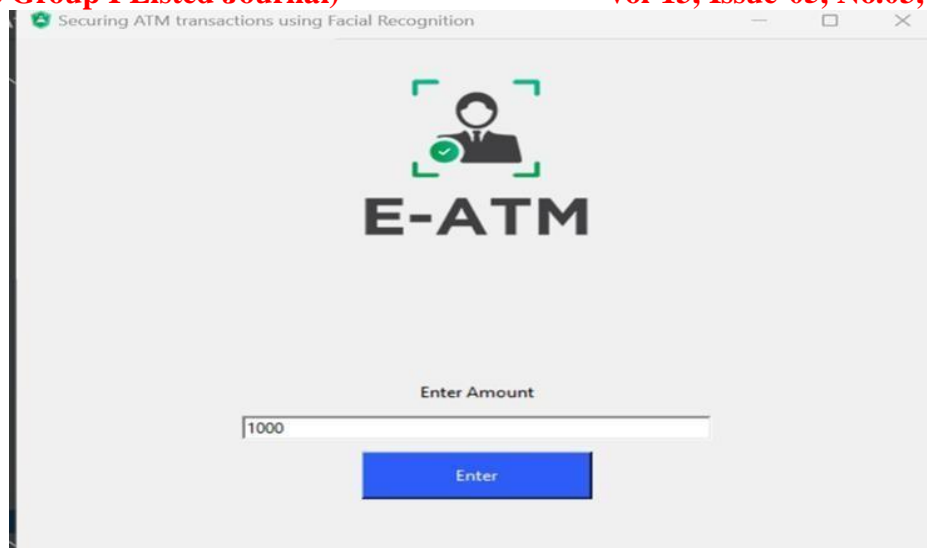


Figure 7: Entering amount to be withdrawn

If there are enough funds in our account, the sum is withheld, and we receive the message "Transaction Successful" as a result.

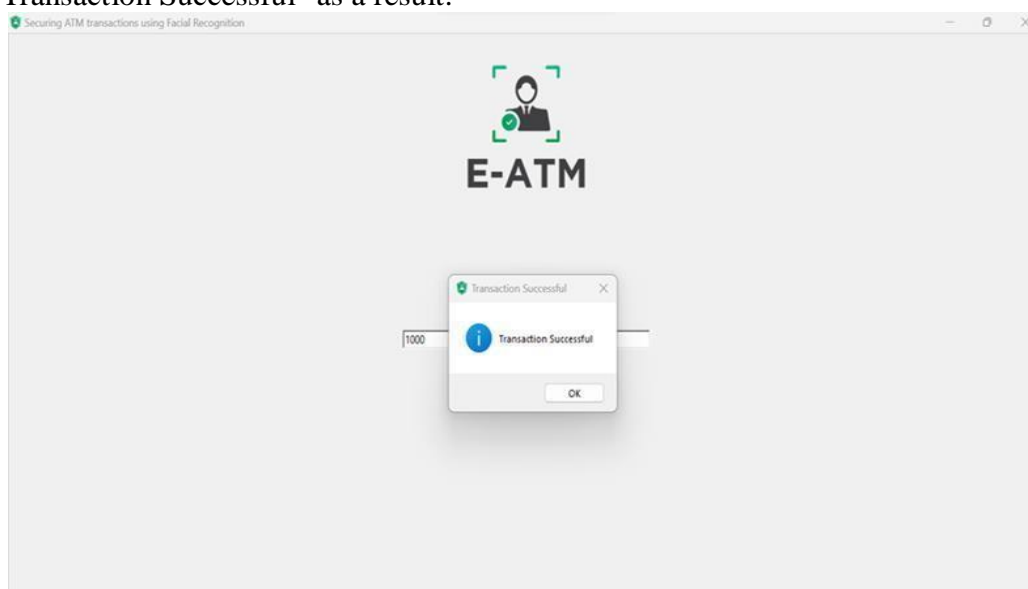


Figure 8: Final output

5. CONCLUSION

ATM transactions may be secured using several different techniques. To boost security, a new layer is added on top of the existing one. This may be developed upon and added to ATM locations and financial systems. With this implementation, ATM fraud can be stopped. This method enables two-factor authentication to verify that the transaction is being carried out by the authorised party. It prevents those with access to the PIN from using the card illegally or without permission.

This is made feasible using face recognition. The live camera is used to record the user's footage, which is then compared to the real picture stored in the bank database.

The problem of cardholder impersonation can be solved by this project. Similar to two-factor authentication, facial recognition is used to verify that the transaction was carried out by the cardholder or other individuals they have trusted. It restricts the use of cards by unauthorised individuals who know a cardholder's password. As a result, this ATM model offers protection against identity exploitation through the deployment of a verification system that uses facial recognition to check the user's identity and greatly reduce forced transactions.

The user is able to withdraw their balance after verification if both faces match, and a Transaction Successful dialogue box will display. If the faces don't match, the user won't be able to access the withdrawal. As a consequence, this verification technique verifies the permitted user and authenticates them, which greatly lowers the number of fraudulent transactions.

6. FUTURE SCOPE

The facial recognition method seems more challenging than biometrics, enabling the creation of more potent algorithms. It is possible to correct, erase, or at the very least decrease the drawbacks of facial recognition technology, such as the inability to discern between a face and a beard, ageing, glasses, or a cap. If the price drops, retinal or iris recognition could take the place of face recognition.

7. REFERENCES

- www.w3schools.com
- <https://www.jetbrains.com/pycharm/>
- <https://thinkingneuron.com/face-recognition-using-deep-learningcnn-in-python/>
- [Machine learning - Wikipedia](#)