



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.524

Design and Implementation of Artificial Intelligence Based ATM Theft Detection and Secure Cardless Transaction System Using Facial Recognition Technology

J. Priyadharshini¹, S. Shanmugam², L. Prakasam³

PG Scholar, Department of Embedded System Technologies, PSV College of Engineering and Technology, Krishnagiri,
Tamil Nadu, India¹

Assistant Professor, Department of ECE, PSV College of Engineering and Technology, Krishnagiri,
Tamil Nadu, India^{2,3}

ABSTRACT: Many financial transactions are conducted using automated teller machines (ATMs). However, ATM fraud such as card and PIN theft continues to be a major concern for consumers and financial institutions. The main goal of this project is to create a secure ATM that uses identity verification. ATM usage is increasing, but so is fraud. ATMs play an important role in the banking industry, but people are afraid to use the ATM system due to fraud. This new system eliminates the need for a physical card and increases security through facial recognition technology. The user initiates the transaction by entering a password, activating the camera to recognize the face, and the face is captured and stored in the database. If the person is authorized to use the facial recognition algorithm, the transfer will go smoothly. For older users, relationships such as male or female can be registered and their faces can be stored in a secure location. This not only adds a layer of personal security, but also meets the needs of older people who may find traditional ATM transactions difficult. The system also uses alert devices to enhance security. The system has various hardware devices to ensure security against unauthorized access, which means that the system captures images and sends them to an email address via the SMTP protocol for instant notification and action alert. Nano microcontrollers are used to monitor and control various hardware devices, including LCD screens. If the system detects that an unknown person is trying to use the ATM machine, the door is automatically closed by a gear drive. At the same time, a pump is used to release chloroform gas, knocking the person unconscious and preventing further crimes. The integration of hardware with facial recognition technology provides high security, protecting users and financial assets from fraud and theft.

I. INTRODUCTION

Automated Teller Machines (ATMs) have become an integral part of daily life, allowing users to easily perform a variety of financial transactions. However, the rise of ATM fraud, including card and PIN theft, has raised serious concerns about the security of these systems. As the reliance on ATMs increases, there is an urgent need to improve ATM security to protect consumers and financial institutions. The project aims to address these issues by creating a secure ATM that integrates advanced authentication methods. The program uses facial recognition technology to eliminate the need for a physical card, providing a safer and more convenient user experience. In this system, users initiate a transaction by entering their PIN, and then a camera records their face to instantly verify their identity. The captured images are stored in a secure file, ensuring that only authorized users can access the ATM. This new approach reduces the risk of fraud and increases the overall security of ATM transactions.

II. OBJECTIVE

Enable secure authentication that replaces traditional ATM cards and PINs with facial recognition and OTP technology to reduce security threats such as theft, burglary, and card skimming. Facial recognition and account security for accessing ATM services.

III.LITERATURE SURVEY

The main goal of this challenge is to support the development of algorithms that can recognize facial expressions captured outside of a studio-style photo collection. Our classification in the GBU challenge problem demonstrates the many advantages that can arise when comparing faces captured under these conditions.[1] This model allows researchers to focus on the complexity of the problem without sacrificing the performance of simpler problems. Learn to overcome the shortcomings and limitations of previous systems. The ability to demonstrate significant improvements in face recognition suggests that this connection has the potential to be important in other visual domains.[2] Define the problem. Unlike most current work, we take into account the knowledge that there are occlusions in both the gallery and the probe. We propose a new method called Dynamic Image-to-Category Warping (DICW) that determines the order of faces to recognize non-existent faces. [3] We first represent face images as ordered sequences and then treat the image matching problem as a process of finding similarities between the search sequence and the standard gallery. Comparison - a nice way. [4] The SFCA test uses the same data used to test other state-of-the-art methods to make it robust and show that SFCA improves the accuracy of face recognition as an alternative trade-off for illumination, exposure, expression, face size, occlusion, and distance to the camera. The results show that SFCA can satisfy these conditions when the data size is small or medium (e.g., when the number of points does not exceed the face).[5]

IV. EXISTING & PROPOSED SYSTEM

1. EXISTING SYSTEM

- Current systems designed to enhance ATM security are integrating biometric authentication and networking technology to create security solutions. The user interface is designed using HTML, CSS, and JavaScript to provide users with a great and visually pleasing experience.
- The authentication process begins with the user entering their username and password through a web-based interface. Biometric verification is then performed via a fingerprint scanner.
- A fingerprint recognition algorithm is then used to match the captured fingerprint with the stored pattern. To further enhance security, the system uses a live detection device to verify that the fingerprint is from a live person, not a static or printed image.
- Once the authentication process is complete, users can perform transactions such as withdrawing or depositing money. The technology includes PHP for external processing, which supports security and efficiency, making the ATM both reliable and fraud-proof.

1.1 DISADVANTAGES

Biometric data can be vulnerable to leakage and misuse, which can lead to privacy issues. Vulnerabilities or flaws in biometrics can lead to security risks and inefficiencies.

2. PROPOSED SYSTEM

- The system aims to enhance ATM security by combining technology to prevent fraud. Instead of relying on a physical card, the system uses facial recognition in conjunction with a PIN code entry system.
- Users initiate transactions by entering a PIN number, which enables the camera to recognize the face. Facial images are stored in a secure location and analyzed using facial recognition algorithms. For adult users, the system allows trusted individuals, such as family members, to be registered, with facial images also stored for easy access.
- To further enhance security, the system includes a screen capture feature that sends images of unauthorized users to email addresses via the SMTP protocol for instant notification.
- The system is controlled by a Nano microcontroller that controls various hardware components, including the LCD display. When an unauthorized access attempt is made, the system uses a glass motor to close the ATM door and a pump that releases chloroform gas to deter intruders and prevent further crime.
- This comprehensive approach combines advanced facial recognition with powerful hardware to provide secure and efficient ATM access.

2.1 ADVANTAGES

Use facial recognition and secure PIN access to reduce card and PIN theft. Block and prevent unauthorized access.

V.BLOCK DIAGRAM

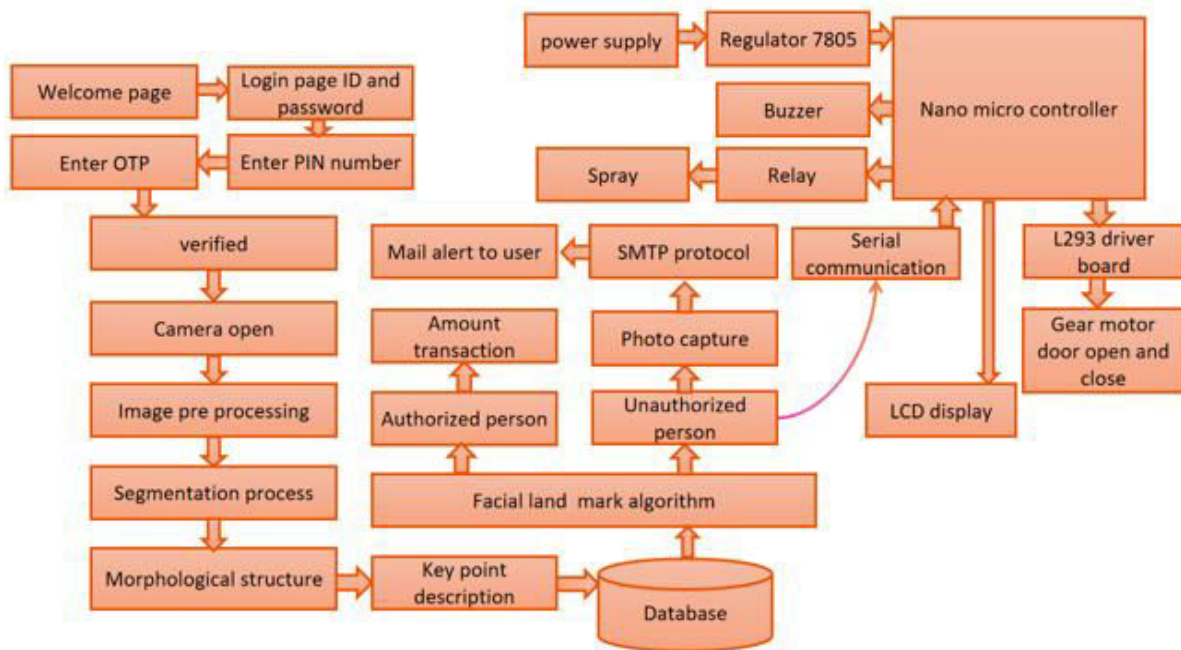


Fig No:1 Block Diagram

VI.HARDWARE REQUIREMENTS

1.Nano Micro Controller

Nanocontroller refers to a small, compact microcontroller designed to work in embedded systems and IoT (Internet of Things). These controllers are usually characterized by their small size, low power consumption, and high performance, making them ideal for systems that require less space and energy. Nanocontrollers are usually built around architectures such as ARM Cortex-M or AVR and have various input/output interfaces (such as GPIO, PWM, ADC) and communication protocols (such as I2C, SPI, and UART). Their main role is to control and manage various devices, sensors, and actuators in various applications, including robotics, home automation, wearables, and industrial controls. Widely used in hobbyist and professional applications due to their low cost and versatility, nanocontrollers offer simple solutions for creating smart devices and connectivity.

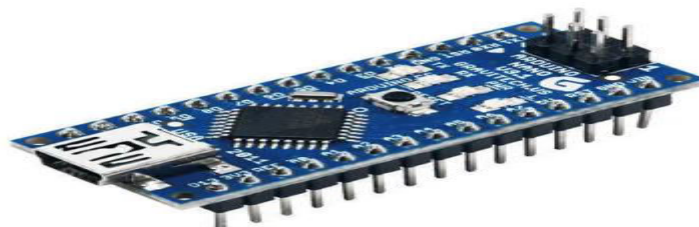


Fig No:2 Nano MicroController

2.Buzzer

A bell or chime is an electronic device, usually electrical, used in cars. It usually has switches or sensors connected to the control panel that determine if a button has been pressed or if a preset time has passed, and usually sets an LED or light control and causes a continuous noise or beep. At first, the device works like an electric machine, such as an electric machine without a metal gong (which makes the sound). These devices are usually fixed to the wall or ceiling and use the ceiling or wall as the sound source.



Fig no:2 Buzzer

3. Driver Board

A driver board is a critical electronic circuit that acts as the interface between a controller (such as a microcontroller or microprocessor) and the components it controls (such as motors, sensors, or other devices that require higher power). Drivers are often used to control and propagate signals from low voltage systems to meet the high power requirements of actuators or loads. For example, in a motor control application, a driver board takes a low signal from the microcontroller and converts it to a higher current and voltage requirement to drive a DC motor, stepper motor, or servo motor. Most drivers include features such as power management, current measurement, and power protection (overload, overcurrent, and thermal shutdown) to ensure safe and efficient operation. These boards can also control the direction and speed of the motor, provide PWM (Pulse Width Modulation) signals for motor control, and even control multiple devices simultaneously. Control panels are widely used in robotics, automation, automotive systems and other applications that require precise control of electronic components.

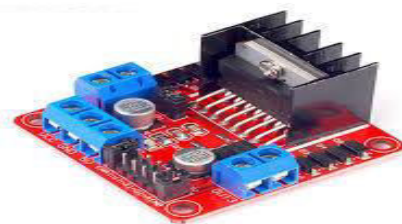


Fig no:3 Driver motor

4. LCD Display

LCD (liquid crystal display) is a flat panel used for displaying information in various electronic devices. It consists of a thin layer of liquid crystal sandwiched between two layers of polarizing material. When electricity is passed through the liquid crystal, its behavior changes, allowing or blocking light to pass through, creating an image or text on the screen. LCDs are widely used because they provide good visual results, are low-power, and come in many sizes, from small displays found in digital watches or smartphones to displays too large to be used on a TV or computer monitor. LCDs come in different types, such as monochrome or color displays, and can support different resolutions and brightness levels. Small LCDs (such as 16x2 or 20x4 displays or LCDs) are often used in electrical and electronic devices to display information about time, status, and words. These instructions are usually controlled by microcontrollers via protocols such as I2C or SPI, and are widely used in electronics, home appliances, measurement, and commercial products due to their benefits, affordability, and variety.



Fig. no:4 LCD Display

5. Pump Motor

The R385 6-12V DC Diaphragm Mini Aquarium Pump is an ideal pump for a variety of liquid movement applications. It has sufficient pressure and can be used with nozzles to create a spray. The pump can handle hot liquids up to 80°C and when used correctly, it can pump water up to 2m through pipes and discharge water up to 3m. Small water pumps, automatic water plants, water fountains or music to make people dance, etc. The pump is quiet when pumping liquid. The pump can also suck air but is very popular in comparison. The pump can pump hot water up to 80C and, when used correctly, it can pump water up to 2m through pipes and up to 3m vertically.



Fig no: 5 Centrifugal pump motor

VII. RESULT

A secure ATM increases security by eliminating the need for traditional cards and using advanced facial recognition technology. The integration of facial landmark algorithms allows users to enter the ATM only, ensuring accurate identification. In the first stage, facial images are collected, trained and stored in a database. Detect faces using the facial landmark algorithm. In the second stage, the new development is designed to meet the needs of elderly users by allowing family members to register, thus adding a personal security system. Real-time email alerts provide immediate notification of suspicious activity. Integrated facial recognition, integrated hardware, and security features such as automatic door locks and fuel drains have successfully reduced intrusions and fraud.

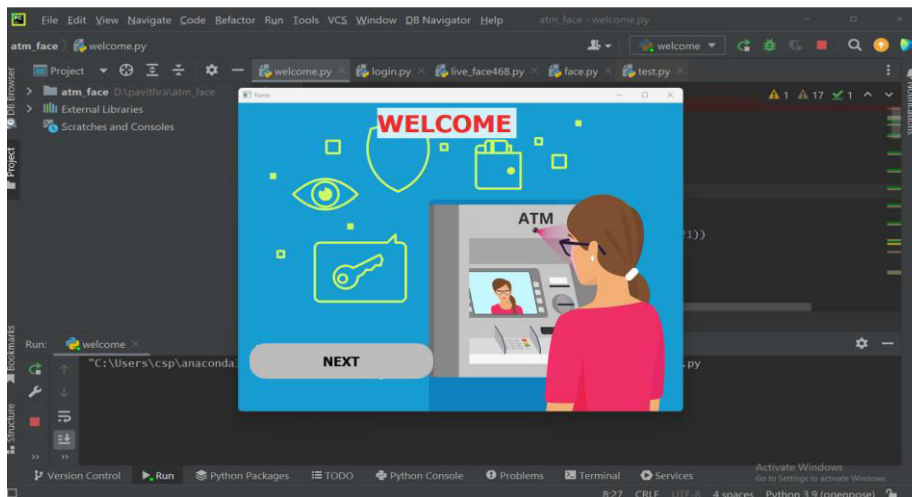


Fig no: 8.1 Welcome page

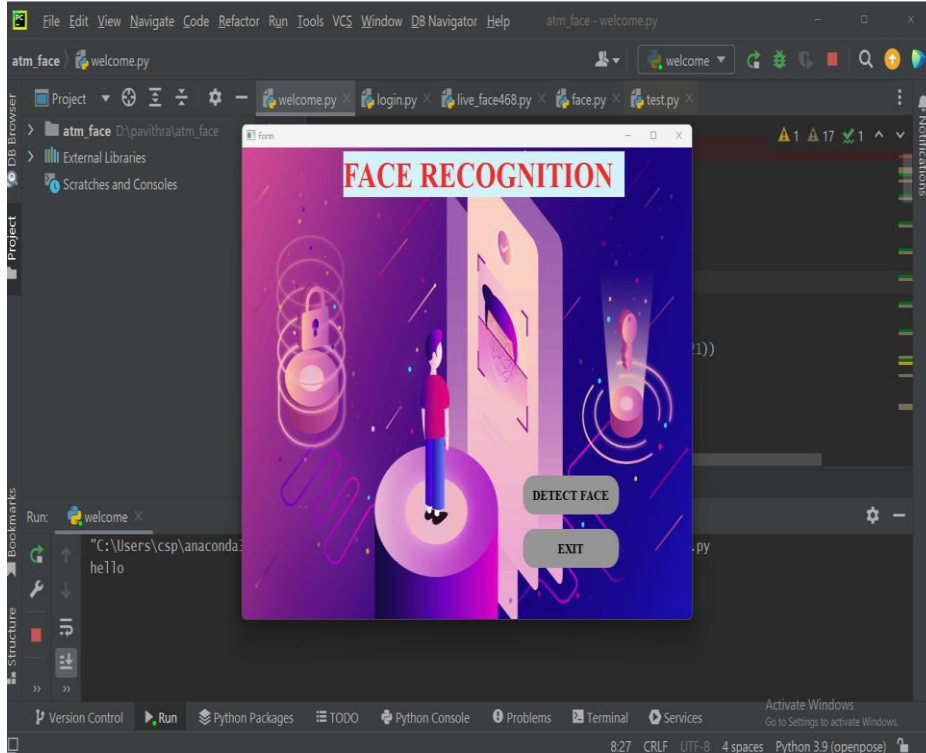


Fig no: 8.2 Face detected page

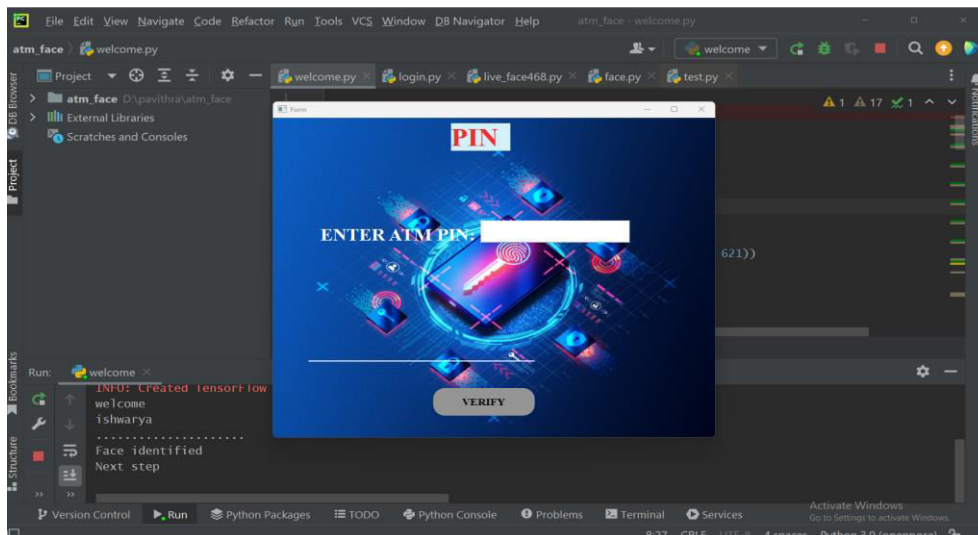


Fig no: 8.3 Enter Pin number

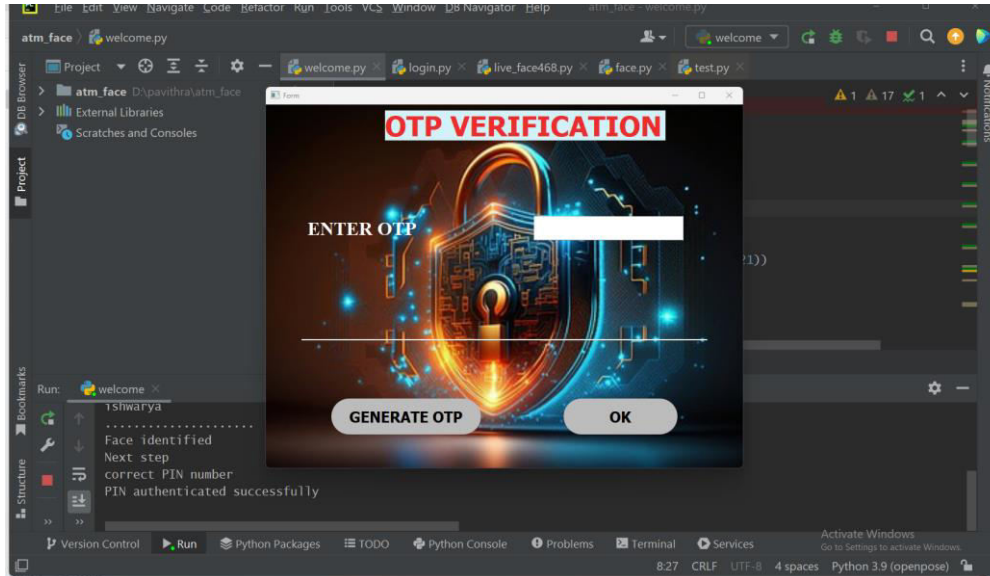


Fig no: 8.4 OTP verification

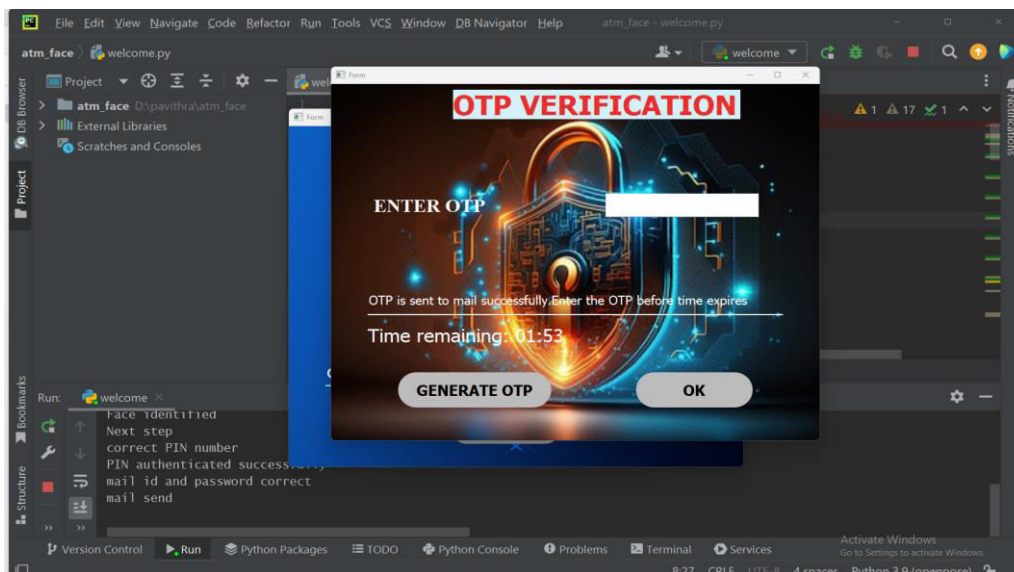


Fig no: 8.5 OPT Generator

VIII. CONCLUSION

Today's approach includes facial recognition with PIN verification and addresses key vulnerabilities associated with traditional ATMs, such as card theft, fraud, etc. Using deep learning algorithms for face-to-face interactions, the system reduces the risk of unauthorized access by ensuring that only authorized users can access accounts. The addition of features such as one-time passwords (OTP) strengthens security protections to ensure user privacy and account security in the event of an unauthorized person being found. This includes taking photos of intruders, sending notifications to legitimate users, locking ATM doors in rooms, and using chloroform-based sprinkler systems to neutralize intruders.

REFERENCES

- [1] A. Mohite, S. Gamare, K. More and N. Patil, "IRJET - Deep learning based ATM cardless using fingerprint and face recognition technology" "Deep learning based ATM cardless using fingerprint and face recognition technology" information technology", International Journal of Research in Engineering and Technology, vol. 3504, 2022, [Online].
- [2] "Face recognition based ATM security system using Raspberry Pi", N. V. Kalyankar, S. B. Patil and S.S. Lokhand.
- [3] Vimal.p, Priyanka.V, Rajyasree.M, Santhiya Devi.P.T, Jagadeeshraja. M, Suthanthira Vanitha.N, "Novel methods for automatic irrigation and sprinkler irrigation using embedded systems", International Journal of VLSI and Embedded Systems - IjvesVol05, Article 03257 March 2021;
- [4] Sathiyabama P, Lakshmi Priya C, Ramesh Sm, PreethiB, Mohanaarasi M, — Designing an embedded system to irrigate fields with different crops using soil moisture sensor, International Journal of Innovative Research in Computers and Communications Engineering Vol. 2, 8 March 2020.
- [5] Cindy Vijaya; Andreas Noel Ronard; Desai - Face detection based ATM security system using embedded Linux platform -. King and T. Aravindan, "ATM security using facial recognition", International Journal of Contemporary Engineering and Scientific Research (ijcesr), vol. 5, 4 March 2021. [online].
- [6] A. Bangia and S. Prabu, "ATM PIN Authentication using Facial Recognition," 2019. [Online].
- [7] A. Mohite, S. Gamare, K. More, and N. Patil, "IRJET-Deep Learning Based Card-Less ATM Using Fingerprint And Face Recognition Techniques Deep Learning based Card-Less At using Fingerprint and Face Recognition Techniques," International Research Journal of Engineering and Technology, Vol. 3504, 2008, [Online].
- [8] "Facial Recognition-Based ATM Security System Using Raspberry Pi" by N. V. Kalyankar, S. B. Patil, and S. S. Lokhande.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details