ENHANCING ATM SECURITY WITH FACE AUTHETICATION USING DEEP LEARNING.

Yukeshwaran U1, Yaswin Paul R2, Subraja T3

(1) Student, Bannari Amman Institute of Technology, TAMILNADU, INDIA
(2) Student, Bannari Amman Institute of Technology, TAMILNADU, INDIA
(3) faculty, Bannari Amman Institute of Technology, TAMILNADU, INDIA

ABSTRACT

The proliferation of Automated Teller Machines (ATMs) has revolutionized banking services, providing convenient access to financial transactions. However, the traditional methods of ATM authentication, such as PINs and cards, are susceptible to various security threats, including theft and fraud. In response, biometric authentication has emerged as a promising solution to enhance ATM security. Among biometric modalities, face recognition has garnered significant attention due to its non-intrusive nature and widespread availability of camera-equipped ATMs. This paper presents a novel approach to augment ATM security by integrating a face biometric authentication system with deep learning techniques. The proposed system leverages convolutional neural networks (CNNs) for robust and efficient face recognition. Through extensive experimentation, we demonstrate the effectiveness of deep learning in accurately identifying individuals based on facial features. Moreover, we explore various pre-processing techniques to enhance the performance of the face recognition system, including image normalization, alignment, and quality assessment. Additionally, we investigate the impact of different network architectures and training strategies on the overall authentication accuracy and computational efficiency.

Keyword: ATM, biometric, GSM, Face recognition, Fingerprint Recognition, image processing, artificial intelligence.

1. INTRODUCTION

" The ever-increasing reliance on Automated Teller Machines (ATMs) for financial transactions necessitates robust security measures to safeguard user accounts. Traditional PIN based authentication systems are vulnerable to theft, loss, or social engineering attacks. Facial recognition technology presents a promising alternative, leveraging unique biometric features for secure user identification. This project proposes a Face Biometric Authentication System for ATMs utilizing Deep Learning techniques. This system aims to enhance ATM security by incorporating facial recognition alongside the traditional PIN verification process. Deep learning algorithms will be employed to analyse facial features captured by the ATM camera and authenticate users against a registered database. In an era marked by technological advancements and increasing concerns regarding security, the need for robust authentication systems in sensitive environments like Automated Teller Machines (ATMs) is paramount. Traditional authentication methods, such as Personal Identification Numbers (PINs) and magnetic stripe cards, while widely used, are susceptible to various security threats such as card skimming, shoulder surfing, and theft. To address these vulnerabilities and enhance the security posture of ATMs, this project proposes a cutting-edge Face Biometric Authentication System powered by Deep Learning technology. By leveraging facial recognition algorithms, the system aims to provide a secure and seamless authentication experience for ATM users while mitigating the risks associated with traditional authentication methods.This project offers a more secure and convenient user experience compared to conventional methods, potentially mitigating fraudulent activities and safeguarding user finances.

1.1. ORGANIZATION PROFILE: At Markdot Intellect, our content embodies the intersection of innovation, intellect, and impact. We curate and produce insightful, thought-provoking material that inspires and informs, driving meaningful conversations and fostering knowledge exchange in an ever-evolving world. Expand the company's presence in existing markets and explore opportunities to enter new markets. Drive innovation within the IT industry by creating cutting-edge products or services that address market needs and stand out from competitors.

- MISSION: Markdot Intellect is committed to pioneering intellectual exploration and fostering a culture of continuous learning. We strive to empower individuals and organizations with transformative insights, innovative solutions, and collaborative platforms, catalysing positive change and driving progress in diverse spheres of human endeavour.

- VISION: Our vision at Markdot Intellect is to be a globally recognized leader in intellectual enrichment and knowledge dissemination. We aspire to cultivate a dynamic ecosystem where creativity thrives, boundaries are pushed, and breakthrough ideas emerge, shaping the future of society, technology, and beyond.

1.2 SYSTEM SPECIFICATION

1.2.1 HARDWARE CONFIGURATION

- PROCESSOR: Intel(R) Core (TM) i5
- MOTHERBOARD: Intel chipset board
- RAM: 8GB RAM
- HARD DISK DRIVE: 932 GB
- CAMERA:1080P Resolution
- MONITOR: LCD
- KEYBOARD: Multimedia Keyboard 108 Keys
- MOUSE: Logitech Optical Mouse

1.2.2 SOFTWARE CONFIGURATION

- OPERATING SYSTEM: Windows 10
- FRONT - END: HTML
- BACK - END: Python
- FRAMEWORK: Flask Framework

2. SYSTEM STUDY

This Face Biometric Authentication System for ATMs is designed to function within the confines of a controlled environment and adheres to specific technical requirements.

Functional Requirements:

- **User Registration:** The system facilitates user enrollment, capturing facial images and associating them with a username and PIN.
- **Facial Recognition:** The system utilizes a deep learning model to identify faces captured by the ATM camera in real-time.
- **PIN Verification:** The system integrates with existing ATM infrastructure, requiring users to enter a valid PIN after successful facial recognition.
- **Access Control:** Upon successful facial recognition and PIN verification, the system grants access to standard ATM functionalities.
- **Security:** The system prioritizes user data security by storing facial encodings securely and implementing measures to prevent unauthorized access.

Non-Functional Requirements:

- **Performance:** The system should operate efficiently, with minimal processing delays during facial recognition.

- **Accuracy:** The deep learning model should achieve a high degree of accuracy in identifying registered users.
- **Reliability:** The system should function consistently and avoid unexpected errors or downtime.
- **Usability:** The ATM user interface for registration and access should be intuitive and userfriendly.
- **Scalability:** The system should be adaptable to accommodate an increasing number of registered users.
- **Security:** The system must prioritize data security, employing encryption techniques to safeguard facial encodings and user information.

2.1. EXISTING SYSTEM

In the existing system, the current landscape of ATM user authentication is dominated by a two-factor system. The first factor relies on physical access to a debit or credit card, typically equipped with a magnetic stripe or embedded chip. This card is inserted into the ATM for the machine to read the stored data. The second factor involves a Personal Identification Number (PIN) known only to the user. This PIN is entered on a keypad at the ATM and often transmitted (encrypted in some cases) to the bank's central server for validation. If both the card and PIN are verified, the user gains access to their account and can perform various transactions. While this system has served its purpose for many years, it presents several shortcomings that can be addressed. Security remains a primary concern. PINs are susceptible to social engineering tactics like shoulder surfing, where unauthorized individuals observe the user entering their PIN. Additionally, skimming devices attached to ATMs can capture card data, while stolen cards can be misused if the PIN is compromised. These vulnerabilities can lead to financial losses for users and reputational damage for banks. Furthermore, PIN entry can be a slow and cumbersome process, especially for users with physical limitations or those unfamiliar with ATM interfaces. This can negatively impact user experience and potentially lead to frustration or even abandonment of transactions. Moreover, the system itself requires ongoing maintenance and upgrades to counter evolving security threats, placing a constant burden on financial institutions.

2.1.1. DRAWBACKS

- The current PIN-based ATM authentication suffers from security weaknesses.
- PINs are vulnerable to theft through observation or skimming devices.
- Additionally, PIN entry can be slow and inconvenient, impacting user experience.
- Furthermore, maintaining and upgrading the system to address evolving security threats create an ongoing cost for banks.

2.2. PROPOSED SYSTEM

This project proposes a novel Face Biometric Authentication System for ATMs that leverages Deep Learning to enhance security and user convenience. The system aims to replace the traditional PIN-based approach with facial recognition, offering a more robust and user-friendly experience. Deep learning algorithms, specifically Convolutional Neural Networks (CNNs), will be employed to train a facial recognition model. This model will be trained on a large dataset of facial images collected from registered users. During the training process, the CNN will learn to extract and encode unique facial features, enabling it to accurately identify individuals later.The proposed system will operate within a standard ATM environment. Upon approaching the ATM, the user will be prompted to look into a built-in camera. The system will capture a real-time facial image and pre-process it to remove noise and enhance relevant features. The model will analyse the user's facial features and compare them against the encoded representations stored in a secure database. If a match is found within a predefined threshold, indicating a registered user, the system will grant access to the ATM interface. The user can then navigate the ATM menu and perform transactions without requiring a PIN.

2.2.1. FEATURES

- **Enhanced Security:** Along with vulnerable PINs system the facial recognition, a unique biometric identifier for more robust user authentication is also added.
- **Liveness Detection:** Ensures a real person is present, preventing unauthorized access through photographs or videos.
- **Scalability and Adaptability:** The deep learning model can be efficiently re-trained on an expanding user base, maintaining high accuracy.

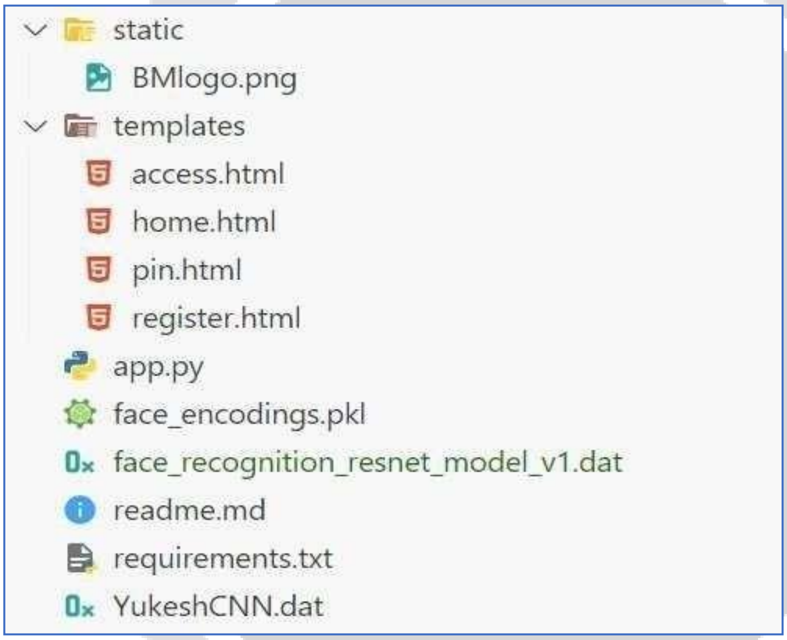
- **User-Friendly Interface:** Integrates seamlessly within the existing ATM environment, requiring minimal user interaction beyond looking into the camera.

3. SYSTEM DESIGN & DEVELOPMENT

- System design and development is a comprehensive process that involves creating, refining, and implementing systems to address specific needs or solve problems.
- involves gathering and analysing requirements from stakeholders to understandthe goals, objectives, and constraints of the system.
- the overall architecture of the system is defined, includingits components, modules, and interactions. Architects determine the structure, behaviour, and interfaces of the system, considering factors such as scalability, reliability, and maintainability.

3.1. FILE DESIGN

The Face Biometric Authentication System utilizes several files to manage data and program execution. These files can be broadly categorized into two main functions: user interface and system operation.



```
static
    BMlogo.png
templates
    access.html
    home.html
    pin.html
    register.html
app.py
face_encodings.pkl
face_recognition_resnet_model_v1.dat
readme.md
requirements.txt
YukeshCNN.dat
```

3.1.1. User Interface Files

- Home.html, register.html, access.html: These HTML templates define the visual elements and layout of the user interface.
- They are responsible for creating the web pages users interact with for registration, accessing the ATM functionalities, and navigating the system.
- These files contain HTML code, along with placeholders for dynamic content (like user names) that is populated by the Flask application during runtime.
- The Complete UI looks similar to actual ATM Machine display to replicate the flow to increase the User Experience.

3.1.2. System Operation Files

- **app.py:** This is the core Python script that drives the entire application.

- It leverages the Flask framework to define routes, handle user interactions through forms and button clicks, and orchestrate various functionalities like user registration, face recognition during access, and potentially simulated ATM operations upon successful authentication.
- This file essentially acts as the brain of the application, coordinating data flow and user requests.
- **face_encodings.pkl:** This pickle file plays a crucial role in storing user data. It holds a serialized representation of three critical data structures:
- **known_face_encodings:** This list stores the facial encodings, which are numerical representations extracted from user faces during the registration process. These encodings act as unique identifiers for each registered user's face.
- **known_face_names:** This list maintains a correspondence between the facial encodings and the usernames of the registered users. It allows the system to associate a recognized face with a specific user.
- **known_face_pins:** This list stores the user-defined PINs associated with each registered face. Upon successful face recognition, the system can prompt for the corresponding PIN for an additional layer of security.
- **face_recognition_resnet_model_v1.dat:** This file contains a trained deep learning model (CNN), specifically designed for facial recognition. Where it acts as the engine for face recognition within the system. Whenever the application captures a video frame during the access stage, this model is employed to extract facial encodings from the frame and compare them against the **known_face_encodings** stored in the pickle file.

3.2. INPUT DESIGN

- Input design is also iterative.
- It involves constant evaluation, testing, and refinement to adapt to changing user expectations and technological advancements.
- In today's fast-paced world, design plays a crucial role in differentiating your brand and staying ahead of the competition.
- Whether it's a website, an app, a product, or an experience, the design is often the first point of contact between you and your audience.
- **The Registration Form (register.html):** Username: Users provide their desired username during registration using a text input field within the registration form.
- PIN: Users create a PIN for secure authentication by entering it in a designated numeric input

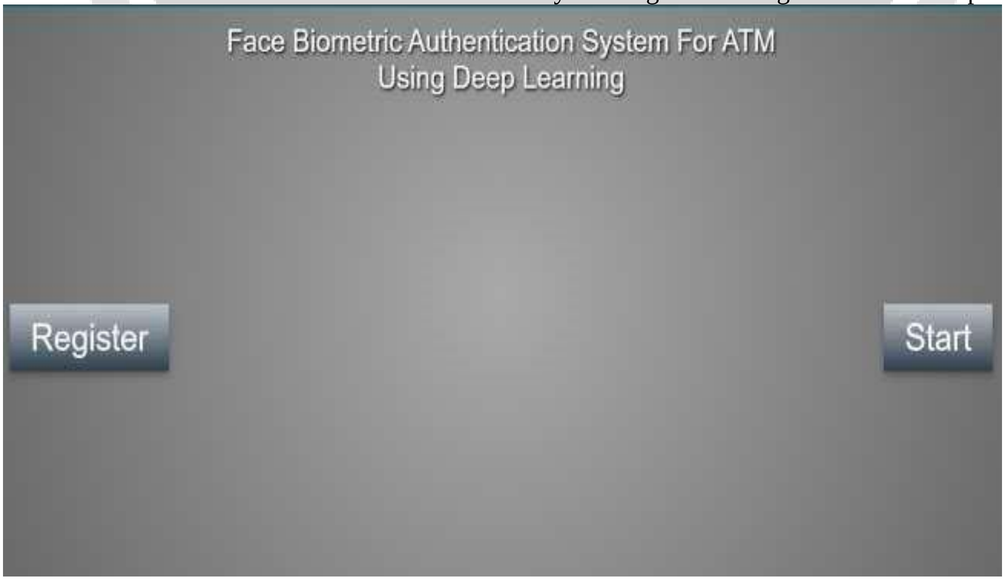
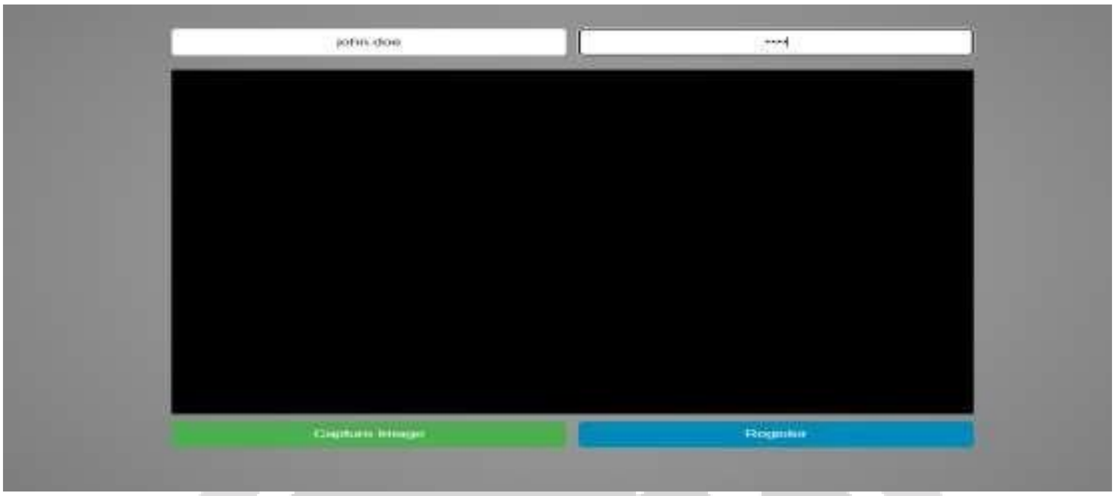


Figure: user registration

- **Access Module (access.html):**

- **Webcam Stream:** During the access stage, the system continuously captures video frames from the user's webcam. These frames serve as real-time input for face recognition.
- **PIN Verification (access.html):**
- **PIN Entry:** Upon successful face recognition, the system might prompt the user to enter their PIN through a numeric input field. This additional layer of security helps ensures authorized access.



john.doe

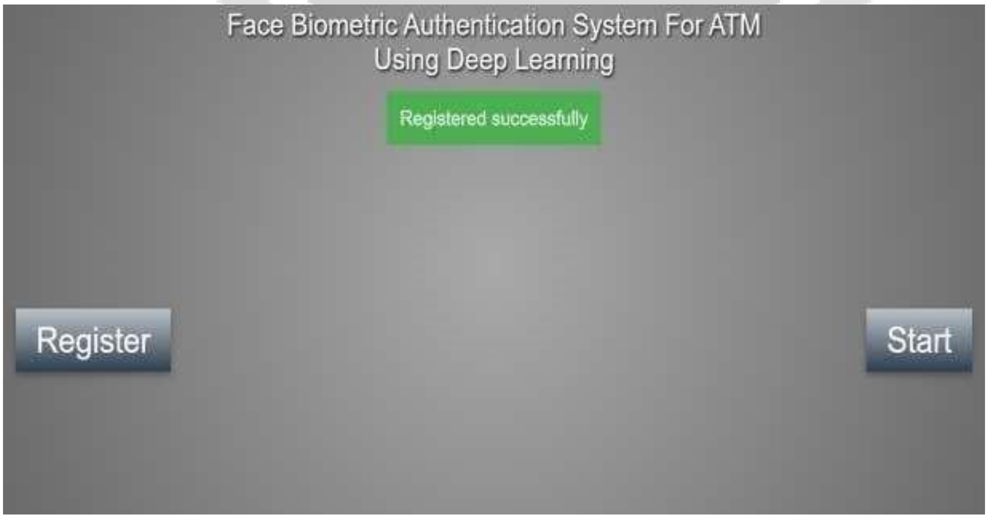
Figure: Registration Page

3.3. OUTPUT DESIGN:

- Output design is inherently collaborative.
- It involves bringing together diverse perspectives and expertise, including designers, engineers, marketers, and stakeholders, to ensure that the final product aligns with business objectives and user expectations.
- output design is about more than just aesthetics or functionality; it's about crafting experiences that inspire, delight, and make a meaningful impact on people's lives.

User Interface Feedback (HTML Templates):

- **Registration Success/Failure Messages:** The application provides feedback messages through the web interface (likely displayed on register.html) to indicate successful user registration or any errors encountered during the process.
- **Access Greetings:** Upon successful face recognition during access attempts, the system might display a personalized greeting message on the access.html page, potentially incorporating the recognized username.



Face Biometric Authentication System For ATM
Using Deep Learning

Registered successfully

Figure: registration successful

Access Denial Messages: If the system fails to recognize a face or the entered PIN doesn't match, appropriate error messages are displayed on the access.html page to inform the user. Real-time Visual Indicators:

4. TESTING

4.1. Unit Testing:

- Individual modules like user registration, data storage/retrieval, and face recognition logic within app.py can be unit tested to verify they function as intended in isolation.
- This might involve creating mock data and testing the system's response under various scenarios.

4.2. Integration Testing:

- Integration testing focuses on ensuring seamless interaction between different modules. o This could involve testing user registration followed by successful access using the registered face and PIN.
- Additionally, testing scenarios with invalid input, unregistered faces, or incorrect PINs during access attempts is important.

4.3. Performance Testing:

- Evaluating factors like processing speed and recognition accuracy across diverse lighting conditions and facial orientations is essential.
- Capturing video recordings with variations in user distance, pose, and lighting allows assessment of the system's robustness in real-world situations.

4.4. Security Testing:

- Test the system's resilience against common security threats.
- Attempt to spoof the system with fake or manipulated face images.
- Test for vulnerabilities such as input validation and authentication bypass.
- Ensure that sensitive data (such as biometric templates) is securely stored and transmitted.

4.5. Usability Testing:

- Test the system's usability from the perspective of end users.
- Evaluate the ease of use of the face authentication process.
- Gather feedback on user experience and identify any pain points.
- Ensure that error messages are clear and informative.
- Iterate on the design based on user feedback to improve usability.

5. IMPLEMENTATION

Implementing a face biometric authentication system for ATMs using deep learning involves several steps. Here's a brief overview of the implementation process:

5.1. Data Collection

- Gather a large dataset of facial images for training your deep learning model.
- Ensure diversity in terms of lighting conditions, facial expressions, poses, and demographics to make the model robust.

5.2. Data Pre-processing

- Pre-process the collected images to standardize them for training.
- This may include tasks such as resizing, normalization, and augmentation to increase the variability of the training data.

5.3. Validation and Tuning

- Validate the trained model using a separate validation dataset to assess its performance.
- Finetune hyperparameters and model architecture if necessary to improve performance.

5.4. Integration with ATM Systems

- Integrate the trained model with the ATM system's software.
- This involves developing an interface to capture live facial images from the ATM's camera, pre-processing the images, and passing them through the trained model for authentication.

5.5. Monitoring and Maintenance

- Continuously monitor the performance of the system in production and perform regular maintenance to address any issues that arise.
- Update the model periodically with new data to improve its accuracy and adapt to changes in the environment.

5.6. Compliance and Regulations

- Ensure that the implemented system complies with relevant regulations and standards for biometric authentication, such as GDPR or local data protection laws.
- Remember, implementing a face biometric authentication system for ATMs requires careful consideration of security, privacy, and usability aspects to ensure its effectiveness and acceptance by users .

6. CONCLUSION

In conclusion, the Face Biometric Authentication System for ATM demonstrates the feasibility of utilizing deep learning for secure user authentication. The project successfully integrates user registration, facial recognition, and basic access control functionalities using pretrained models. The system highlights the potential of deep learning for enhancing security and user convenience in ATM access. However, it's crucial to acknowledge limitations for real-world deployment. Further development would require incorporating liveness detection, robust encryption techniques, and integration with existing ATM infrastructure. Overall, this project serves as a valuable exploration of deep learning applications in user authentication. By building upon this foundation and addressing security considerations, future iterations can pave the way for more secure and user-friendly ATM experiences.

7. REFERENCE

- Python Tricks: A Buffet of Awesome Python Features by Dan Bader o Michael Bergman, “The deep Web: surfacing hidden value”. In the Journal of Electronic Publishing 7(1) (2001).
- "Deep Learning" by Ian Goodfellow, Yoshua Bengio, and Aaron Courville (2015).
- Goldberg D.E.: Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley Reading, MA, 1989. Google Scholar
- Daugman J.: High confidence visual recognition of persons by a test of statistical independence. IEEE Trans. Pattern Anal. Machine Intell., 15, 1148-1161, 1993.