Facial Authentication System Utilising Deep Learning with Enhanced Anti-Spoofing and Image Encryption

A Synopsis Submitted
In partial fulfilment of the Requirements
For the degree of
Bachelor Of Technology
In
Computer Science & Technology

By -
10 Bhavika Chaudhari
39 Janhavi Patil
60 Poonam Sonawane

DEPARTMENT OF COMPUTER SCIENCE & TECHNOLOGY
USHA MITTAL INSTITUTE OF TECHNOLOGY
S.N.D.T Women's University, Mumbai

ABSTRACT

The rapid advancements in biometric technologies have made facial recognition systems an integral part of modern security infrastructures. This paper presents a comprehensive facial authentication system utilizing deep learning techniques to achieve high accuracy and reliability. The system incorporates enhanced anti-spoofing measures to prevent fraudulent access and employs AES-256 encryption for secure image storage and transmission. The deep learning model is trained on a diverse dataset to ensure robustness across various environmental conditions and demographic variations. This approach not only enhances the security of authentication processes but also ensures the privacy and integrity of users' biometric data.

INTRODUCTION

Facial recognition technology has become increasingly integral in a variety of applications, ranging from unlocking personal devices to secure access control in sensitive areas. Its popularity stems from its ability to provide quick and convenient identity verification without the need for physical contact. However, the widespread adoption of facial recognition systems has also brought to light significant security concerns, particularly the vulnerability to spoofing attacks. In these attacks, an unauthorized individual can manipulate the system using images, videos, or 3D masks to impersonate legitimate users, thereby gaining unauthorized access. This challenge has driven the need for more sophisticated facial authentication systems that can reliably differentiate between genuine and spoofed inputs.

Our proposed system addresses these vulnerabilities by incorporating a Convolutional Neural Network (CNN), a deep learning algorithm known for its exceptional ability to process and analyze visual data. CNN is trained on a comprehensive dataset that includes both real and fake facial images, allowing it to learn and identify the subtle features that distinguish authentic faces from counterfeit ones. This training enables the system to perform real-time anti-spoofing checks, significantly enhancing its security. In addition to this, we employ AES-256 encryption to protect the stored facial images, ensuring that sensitive data is secure from unauthorized access or tampering.

PROBLEM STATEMENT

Facial recognition technology has emerged as a prominent method for user authentication due to its ease of use and non-intrusive nature. Despite its advantages, traditional facial authentication systems are prone to several critical issues, including vulnerability to spoofing attacks where attackers use photos, videos, or masks to deceive the system. Furthermore, the security and privacy of facial images during storage and transmission are often compromised, potentially leading to unauthorized access and misuse of sensitive biometric data. Addressing these challenges requires a solution that not only enhances the accuracy and reliability of facial recognition but also incorporates robust anti-spoofing mechanisms and secure data encryption. This Project aims to develop a facial authentication system utilizing deep learning techniques to improve recognition accuracy, integrate advanced anti-spoofing measures to prevent fraudulent access, and employ AES-256 encryption to ensure the secure handling of biometric data.

LITERATURE SURVEY

Sr. no	Title	Methodology	Observation
1.	**Login Authentication through Face Recognition using Deep Learning** By- Rajnikant Totare, Prashant Malge, Chaitanya Tate, Jayesh Minigi, Prof. Manisha Mehrotra	Integrating Multi-Task Cascaded Convolutional Networks (MTCNN) for face detection and FaceNet for facial feature extraction. MongoDB is used to store user information and facial embeddings **Algorithms Used:** 1. **MTCNN:** Utilizes a fully convolutional network to create boundary boxes around detected faces. 2. **FaceNet:** Employs a triplet loss function to minimize the distance between similar faces and maximize the distance between dissimilar ones .	Variations in facial expressions, poses, and lighting conditions can affect accuracy. Dependence on high-quality images for reliable detection and recognition .

2.	**Authentication System by Facial Recognition with Principal Component Analysis and Deep Neural Networks** By - Essam Natsheh, Howayda Said-Ahmed	The paper presents a strategy for facial recognition involving preprocessing techniques to enhance image quality and reduce noise, followed by feature extraction and classification. The approach aims to improve the efficiency and robustness of facial recognition systems **Algorithms Used:** 1. **Principal Component Analysis (PCA):** Used for dimensionality reduction and identifying significant facial features. 2. **Self-Organizing Maps (SOM):**Applied for reducing the size of input images and creating invariance to minor changes in the face. 3. **Neural Networks:**Used for feature extraction and classification .	PCA may exclude crucial data, impacting accuracy. SOM requires clear visibility of facial features. Neural Networks can be computationally intensive and require significant training data
3.	**A Survey on Authentication System using Various Facial Recognition Techniques** By - C. Prajwal, Deepika Bhat, G. B. Meghana, P. Shashank, M. Ravishankar	The paper outlines a workflow diagram for facial recognition that includes image segmentation, feature extraction, and classification strategies. The goal is to accurately identify human faces from a database by extracting and comparing facial features . **Algorithms Used:** 1. **Artificial Neural Networks -** Used for effective feature recognition. Trained on labelled datasets like the LFW dataset to handle varying lighting conditions and improve efficiency. 2. **Eigen Faces-** Used for dimensionality reduction and facial feature extraction .	1. High accuracy with ANN models. 2. Efficient handling of varying lighting conditions with ANN. 3. Effective dimensionality reduction with Eigen Faces. 4. Significant time required for training ANN. 5. Complexity in handling large-scale datasets with ANN. 6. Eigen Faces may not perform well with occlusions and varying facial expressions .

4.	**Face Anti-Spoofing Using Deep Learning Approach** By - Pawar A.H, Nikita Kadam, Yogesh Dadas, Suraj Kakade,Kajal Kamble	**Algorithms used -** 1. CNN - used to extract discriminative features from facial images to distinguish between genuine and spoofed faces. 2. RNN - RNNs analyse video sequences to capture temporal inconsistencies that may indicate spoofing. 3. Siamese Networks - compare pairs of images to identify discrepancies between genuine and spoofed faces. 4. Capsule Networks - capture multi-dimensional features and spatial relationships to improve the detection of spoofing attacks.	1. Requires large amounts of diverse data for training. 2. High computational power is necessary for training deep learning models. 3. Models may struggle to generalize to new, unseen types of spoofing attacks. 4. Needs regular updates and retraining to handle new spoofing techniques.

METHODOLOGY

Project Setup and Environment Configuration:

- **Dependencies Installation**: Install necessary libraries using pip: pip install Flask Keras TensorFlow OpenCV cryptography.
- **Environment Setup**: Configure the Flask server to handle client requests, define routes for sign-up and login, and ensure the server can process facial recognition tasks.
- **File Structure**: Organize the project into directories for the frontend (HTML, CSS, JavaScript), backend (Flask app), and models (Keras model files).

Data Collection and Preprocessing:

- **Image Capture**: Capture facial images using the client's webcam .
- **Preprocessing Steps**:
    - Convert images to grayscale if necessary.
    - Resize images to the input size required by the Facenet model (e.g., 160x160 pixels).
    - Normalize pixel values to the range [0, 1].
- **Encryption**: Encrypt the facial images using AES-256 before storing them in the database. Implement a key management system to securely handle encryption keys.

Model Implementation:

- **Facenet Model Loading**: Load the pretrained Facenet model using Keras. Utilize the model to extract 128-dimensional embeddings from facial images.
- **Feature Extraction**: For each captured image, pass it through the Facenet model to obtain the embedding vector.
- **Anti-Spoofing Mechanism**: Implement techniques such as liveness detection using eye blinking, head movements, or texture analysis to differentiate between live images and spoofed images.

Database Management:

- **User Information Storage**: Use MySQL to store user data including usernames, encrypted facial images, and their corresponding embeddings.
- **Database Design**: Design tables to store user credentials, encrypted images, embeddings, and other necessary metadata.

User Authentication Workflow:

- **Sign-up Process**:
  - Capture facial images and preprocess them.
  - Extract embeddings using the Facenet model.
  - Encrypt the images using AES-256 and store them along with the embeddings in the database.
- **Login Process**:
  - Capture facial images and preprocess them.
  - Extract embeddings and compare them with the stored embeddings using cosine similarity or another appropriate metric.
  - Decrypt the stored images when necessary for comparison.

Server-Side Processing:

- **Flask Routes**: Define routes for sign-up, login, and other functionalities. Use POST requests to handle image uploads and authentication requests.
- **Security Measures**: Implement HTTPS for encrypted communication between the client and server. Validate and sanitize inputs to prevent injection attacks.

Frontend Development:

- **Homepage Design**: Create a welcoming homepage with navigation options for sign-up and login.
- **Sign-Up Page**: Develop a page for capturing user images and inputting necessary details. Implement client-side validation to ensure proper image capture.
- **Login Page**: Develop a login interface that captures user images for authentication.
- **Dashboard**: Create a post-login dashboard that provides access to user-specific functionalities and data.

- **AJAX Integration**: Use AJAX or the fetch API to handle asynchronous communication between the frontend and backend, ensuring a smooth user experience.

EXPECTED RESULTS

User Experience: A seamless, intuitive, and secure interface that allows users to sign up and log in using facial recognition.

Accuracy: The system should achieve high accuracy in facial recognition, correctly identifying users and preventing unauthorised access.

Security: Implementation of AES-256 encryption for image storage and robust anti-spoofing mechanisms ensures the system's security.

Performance: Quick and efficient processing of authentication requests, maintaining minimal latency even under heavy load.

Scalability: The system should handle multiple concurrent users efficiently, scaling up as needed.

CONCLUSION

The Facial Authentication System Utilizing Deep Learning with Enhanced Anti-Spoofing and AES-256 Image Encryption aims to provide a secure, efficient, and user-friendly method for user authentication. By leveraging the power of the Facenet model and deep learning techniques, the system achieves high accuracy in facial recognition. Enhanced security measures, including AES-256 encryption and anti-spoofing mechanisms, ensure that user data remains protected and that only legitimate users gain access. This project not only highlights the practical application of advanced neural networks and encryption technologies but also underscores the importance of security and user experience in modern authentication systems. The developed system serves as a robust framework for future enhancements and can be integrated into various applications requiring reliable and secure user authentication .

REFERENCES

- **C. Prajwal, Deepika Bhat, G. B. Meghana, P. Shashank, M. Ravishankar.** "A Survey on Authentication System using Various Facial Recognition Techniques." *International Journal of Research in Engineering, Science and Management*, vol. 5, no. 3, March 2022.
- **Riddhi A. Vyas, S. M. Shah.** "Comparison of PCA and LDA Techniques for Face Recognition Feature Based Extraction with Accuracy Enhancement." *International Research Journal of Engineering and Technology (IRJET)*, 2018.
- **Jacky Efendi, Muhammad Zul, Wawan Yuna.** "Real-Time Face Recognition using Eigenface and Viola-Jones Face Detector." *International Journal of Computer Science and Network Security (IJCSNS)*, 2017.
- **Bhaskar Anand, Prashant K. Shah.** "Face Recognition using SURF Features and SVM Classifier." *International Journal of Computer Applications*, vol. 8, no. 1, 2016.