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

Bhavika Chaudhari[1] Janhavi Patil[2] Poonam Sonawane[3] Prof. Sumedh Pundkar[4]
[1,2,3,4]Department of Computer Science and Technology
[1,2,3,4]Usha Mittal Institute of Technology, Mumbai, India

Abstract — In this study, we propose a Facial Authentication System that uses deep leaning in order to be secure, efficient and user-friendly authentication process. Traditional ways of authentication like passwords and PINs are all prone to security threats such as hacking, phishing etc. In addition to this, we embrace biometrics in authentication by adding a feature of face recognition to overcome these challenges. The system's model should be trained using deep learning processing methods so as to rightly detect and authenticate users while putting in place measures against fraudulent access, that are using photos or videos. Further, the system contains OTP verified layers security and also uses password hashing and embedding encryption to protect sensitive biometric information. This has been developed in Flask, OpenCV and deep learning libraries with web-based easy authentication in mind. With high accuracy, real-time detection, and secure encryption techniques, this facial authentication system shows immense possibilities toward applications in banking, enterprise security, and many more industries, which require trustworthy identity verification.

Keywords: Facial Authentication, Deep Learning, Biometric Security, Anti-Spoofing, Embedding Encryption, OTP Verification, Flask, OpenCV, Secure Authentication, Real-Time Detection

I. INTRODUCTION

In the modern digital environment, security and authentication mechanisms play a vital role in protecting personal and organizational data. Conventional methods of authentication such as passwords and pin digits are still widely used, although their use has been experiencing an increasing number of security threats such as phishing attacks, brute-force hacking, leak of credentials, etc. With this in mind, there is a hassle-free user-friendly authentication system with increased levels of security that reduces any risks posed by traditional log-in mechanisms. Facial authentication, considered a cutting-edge solution, provides a seamless and efficient way of examining user identities onto certain facial features. Deep learning techniques used in efficient facial recognition systems render very high accuracy and thereby an ideal choice for modern-day authentication procedures.

This research focuses on the development of a Deep Learning Based Facial Authentication System Enhanced with Anti-Spoofing and Embedding Encryption to overcome very serious security issues in biometric authentication. One of the greatest challenges faced by facial recognition is spoofing attacks, wherein an unauthorized entrant gains access using photos, videos, or 3D masks, and thus to support the reduction of such a risk, the proposed system employs some very effective anti-spoofing procedures that is the analysis of facial depth, detection of texture, and reflection to differentiate genuine users from fake attempts. The combination of these security features along with a deep learning algorithm, makes the system enhance accuracy, privacy, and user satisfaction.

With the momentum gained from improvements in artificial intelligence, especially with the advent of convolutional neural networks and transfer learning techniques, facial recognition technology is currently going through a transformation. Indeed, these deep-learning models can accurately extract and analyze various complex features of the face. Plus, the system is designed for a multitude of devices and platforms, thus ensuring flexibility with regard to diverse real-world applications such as banking, healthcare, and secure login systems. Alternatively, deep learning coupled with anti-spoofing mechanisms and encryption techniques is what makes this facial authentication system a strong candidate for an alternative of conventional authentication systems.

This paper aims to give a comprehensive analysis of the architecture, implementation. This includes discussions regarding the face recognition deep learning model, anti-spoofing technologies incorporated, and the encryption techniques used to safeguard the facial information. In particular, targeting potential threats and challenges, the work proposes towards a more secure and intelligent facial authentication system capable of widespread adoption for applications with security concerns.

II. LITERATURE SURVEY

The application of Convolutional Neural Network and Viola-Jones detector biometrics has been explored in the study. It delivers efficiency from SqueezeNet at 98.76 percent accuracy for comparison with ResNet50, which provides comparatively higher accuracy but incurs extensive computational costs. It defines the practicality and usability of the models in these real-world biometric security systems and access controls[1].

This paper presents a hybrid model that combines MobileNet for efficiency and VGG-16 for accuracy, thereby increasing identification and security. The system implements real-time anti-spoofing measures by color-coding the truthfulness of facial inputs for ensuring greater security against fraud attempts. The study demonstrates that compare with MobileNet (0.919), the accuracy of VGG-16 (0.989) proved to be much better while ameliorating the vulnerabilities in biometric authentication through deep learning[2].

A hybrid model where MobileNet is used for efficiency and VGG-16 for better accuracy is thereby enhancing identification and security. The system operates real-time anti-spoofing measures that color-code the truthfulness of facial inputs for greater security against fraud attempts. The study proves that VGG-16 (0.989) achieved far greater accuracy as compared to MobileNet (0.919) while

ameliorating the vulnerabilities of biometric authentication using deep learning[3].

With the development of this research, anti-spoofing model will be implemented for face recognition system based on CNN pipelines which include AlexNet and VGG-16 architectures. The system is trained and tested on NUAA and CelebA datasets for detecting photograph, video, and mask-based spoofing attacks. Research model evaluation will go ahead on the bases of accuracy, precision, recall, F1 score, AUC, and ROC with pre-processing steps like Haar cascade face detection, data augmentation, and noise removal using GrabCut algorithm, demonstrating good robust anti-spoofing performance. [4].

The research aims to secure the digital images through encryption by the AES Rijndael Algorithm with a security mechanism that strengthens itself against various formats of images, including JPG, PNG, BMP, GIF, TIFF, and HEIC image files from outsiders. The possible applications of these include military, healthcare, and aviation sectors, where data is costly and sensitive. Further, it opens future possibilities for extending the techniques of encryption from videos to documents and other types of files so that one can secure all data at once[5].

The paper proposes a method that merges face detection and encryption in the future of biometric security using the Viola-Jones algorithm for face detection and PCA for feature extraction. The method also applies cryptographic encryption with a carrier image to hide facial details. The study showcases competent face detection with fewer errors and cryptic image generation to preserve confidentiality. Future development may consist of decryption procedures and the scaling of systems for real-world implementations that attempt to address certain vulnerabilities, like spoofing and tampering[6].

The proposed research presents a biometric encryption system intended for watchlist applications, enhancing security through feature extraction using PCA (Eigenfaces), AES-based cryptographic key generation, and QIM-based key binding. The secure storage of keys and the application of SHA-512 and BCH codes for error correction make our system immune to distortion. The other main objective of the system is to downsize the image dimension faster, but it remains the scalability issue for large applications, which requires further enhancement[7].

III. METHODOLOGY

The Facial Authentication System Utilizing Deep Learning with Enhanced Anti-Spoofing and Embedding Encryption seeks to enhance the accuracy, security, and efficiency of such systems with a systematic approach. Furthermore, it consists of various key phases, namely, data collection and preprocessing, face detection and feature extraction, model training and fine-tuning, and user authentication.

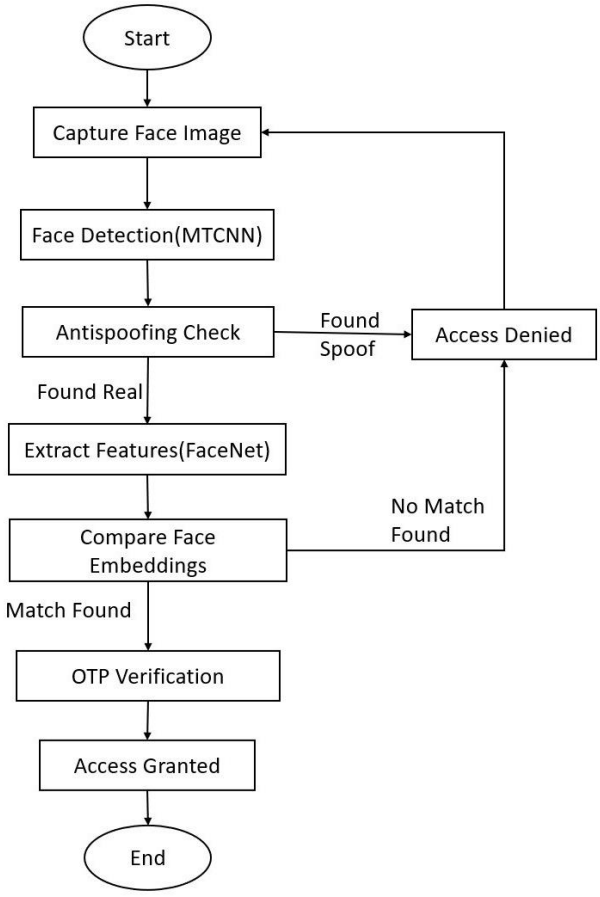

Fig. 1: Process Flowchart

While training the anti-spoofing model actual face images and fake face images are collected during the data collection and preprocessing stage. Real face images can be obtained from online recording via OpenCV, while spoofed images can be acquired from printed selfies and digital screens, as well as replaying videos. They are then stored separately in real at the /real directory and fake at the /spoof directory. Preprocessing steps include resampling the images to 128×128 pixels, normalizing the pixel values to the range [0,1], and applying augmentation techniques using Image Data Generator to improve model generalization by employing different rotations, flips, and brightness adjustments.

There are two key models employed for extracting facial features and detect faces. For detection, the Multi-Task Cascaded Convolutional Network is used, while FaceNet (pre-trained on the VGGFace2 dataset) works for extracting feature embeddings. A fine-tuned MobileNetV2 model is then incorporated for anti-spoofing classification so that it can detect dishonest entries at the face of an individual. Faces are compared to the stored embeddings in the database using the FaceNet-generated feature embeddings. Simultaneously, the antispoofing model classifies the image either as real or spoofed.

The model training and fine-tuning stage has two distinct steps. A CNN-based anti-spoofing model is first trained to discriminate between real and spoofed faces. This has a 3-layer CNN composed of Conv2D, MaxPooling2D and Dropout blocks. The model is trained using a binary classification approach: real vs. spoof, with Sigmoid

activation, optimized through Adam's optimization (learning rate = 0.0001) with Binary Crossentropy loss function. Then, to gain the model efficiency, pre-trained MobileNetV2 is fine-tuned. The last few layers along with GlobalAveragePooling2D, Dense(128, ReLU) Dropout(0.5) are replaced with new ones. At first, all the layers of MobileNetV2 are frozen so that it has all the pre-trained features, and after 25 epochs of training, the lower ones are turned from not trainable to trainable for another 5 epochs to further fine-tune. The end model is finetuned antispoofing model, which is saved in h5 format and evaluated.

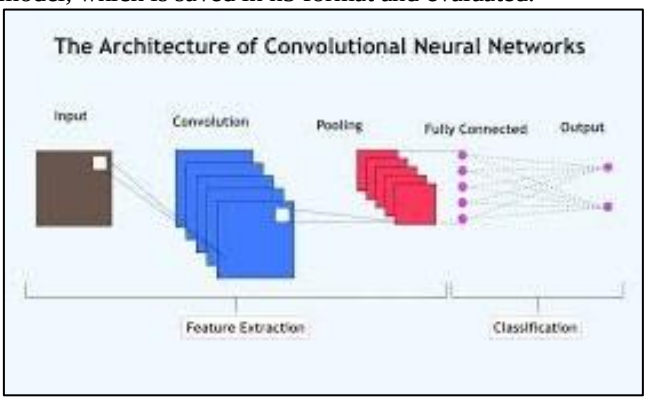

Fig. 2: CNN Architecture

The authentication procedure is composed of two blocks: user registration and user authentication. In this user registration phase, the users have to enter credentials (name, email, phone number, date of birth, and password), and the system camera captures the images of the users' faces. An anti-spoofing check is performed to check the authenticity; if the image is spoofed, the registration would be stopped; whereas, if seen as genuine, then the facial embeddings are extracted using the facenet model and saved securely in a MongoDB atlas database corresponding to the credentials provided by the registered user. After the successful completion of this process, the user is deemed to be registered and their credentials with extensions of encrypted facial embeddings will be stored for authentication purposes. If two people try to log in together (i.e., two faces are detected at the same time), login should not be allowed. If no face is detected, login should not proceed. Also if a face is already registered in the system, it should not be allowed to register again.

The user enters the authentication stage, logged in with all required credentials, and captures an image through the camera. The system then processes the photograph and carries out the anti-spoofing by the trained model to check if the image presented is fake. If it is determined to be fake, access is denied. Otherwise, the hidden face embeddings extracted from the recent image are compared to those stored in the database. In the case the two have no matching features, access is denied. Otherwise, if there's a match, the system will proceed to the final step of an OTP verification by sending onetime passwords to the user on registered emails. A user will have to feed in the OTP, and if verified, the user will gain access to the system. Such authentication systems are known to provide enhanced security, given that they are tied to a biometric system apart from the other form of registration (multi-factor).

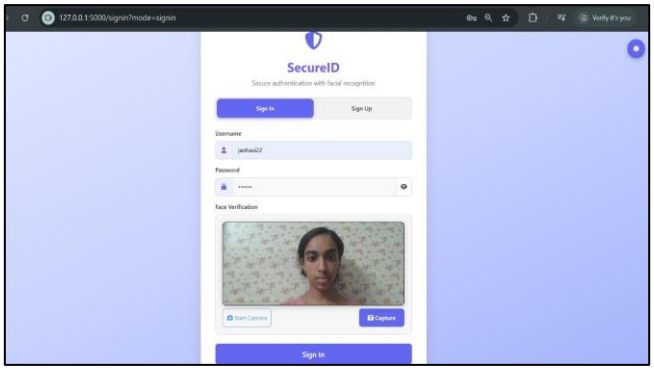

Fig. 3: User Login

In this research, the Advanced Encryption Standard (AES) with a 256-bit secret key is utilized to ensure the confidentiality of facial embeddings stored in the system. AES is a symmetric block cipher widely adopted for its high security, computational efficiency, and resilience against known cryptographic attacks. The facial embeddings, represented as NumPy arrays, are first converted into byte format and padded using PKCS7 padding to comply with the block size requirement of AES. Encryption is performed in Cipher Block Chaining (CBC) mode with a consistent 16-byte Initialization Vector (IV) derived from the secret key to maintain deterministic behavior within the controlled environment. The resulting ciphertext is encoded using Base64 encoding to facilitate secure and efficient storage in document-oriented databases such as MongoDB. This encryption approach effectively safeguards sensitive biometric data from unauthorized access, ensuring both data privacy and integrity in real-time face recognition systems.

Fig. 4: Database

IV. RESULTS AND DISCUSSIONS

The Facial Authentication System was proposed through deep learning with boosted anti-spoofing and encryption techniques and subjected to intense evaluation regarding its accuracy, efficiency, and robustness against spoofing attacks. Thus, the system combines MTCNN for face detection, FaceNet for facial embedding extraction, and fine-tuning an anti-spoofing model based on MobileNetV2. Underneath these is an assurance system that adopts Flask-based authentication, OTP verification, and a set of encryption mechanisms. Furthermore, it would provide a FaceNet-based facial recognition system that confirms collective data in recognizing people through facially embedded features.

In order to address potential spoofing threats, the fine-tuned anti-spoofing model is evaluated with various attack scenarios such as printed photo attacks, digital screen

replay attacks. Also, a second layer of security was added in the form of an OTP-based multi-factor authentication. The OTP was set up using Flask SMTP for otp email sensing to ensure that users verifiably obtained access through their email addresses.

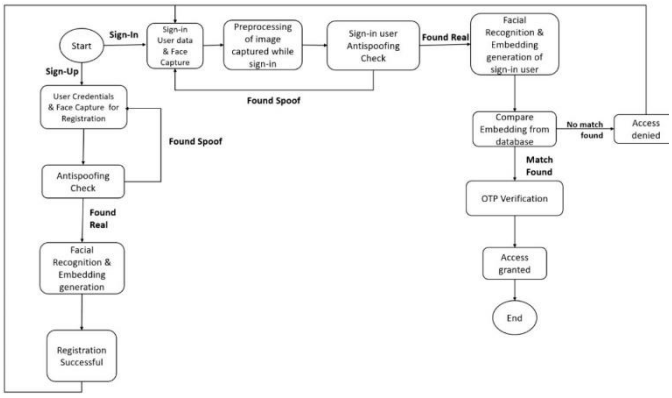

Fig. 5: System Workflow

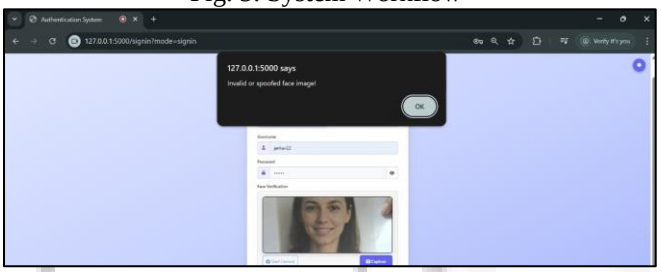

Fig. 6. System detected Spoof

With this effort, concerns regarding the security and privacy of data have been solved with respect to user credentials and facial embeddings by securely storing them in MongoDB with bcrypt hashing for password security. This process remains in compliance with data protection standards and maintains the levels of security for storage and transmission of user information. The system has been designed to be computationally efficient and would function seamlessly within resource-constrained environments since it will have the Flask-based backend with optimized deep learning models mounted for efficient handling of user authentication requests using minimal computational overhead. The choice of MobileNetV2 for anti-spoofing enables that fine trade-off between accuracy and efficiency, making it perfect for real-time applications. Lightweight architecture of the system and MongoDB atlas basis for data storage allow for seamless scalability and integration into different authentication frameworks for safe facility access control, financial transactions, and digital identity verification for e-governance.

The efficient model deployment and encryption techniques will yield a secure, scalable, and high-performance facial authentication system that can be deployed in various operating environments. However, there are still some security and ethical issues. The accuracy of the system depends on various datasets in training, and more improvements would be carried out to reduce possible biases in facial recognition and ensure fair treatment across the various races. Data privacy regulations are strictly adhered to, with biometric data being stored in an encrypted format and utilized responsibly. Emerging spoofing technologies will require further finetuning of the anti-spoofing model to recognize and detect new types of threats, such as deepfake videos or 3D mask threats. Furthermore, these developments will ensure that the system remains robust and effective in its ability for real-life applications.

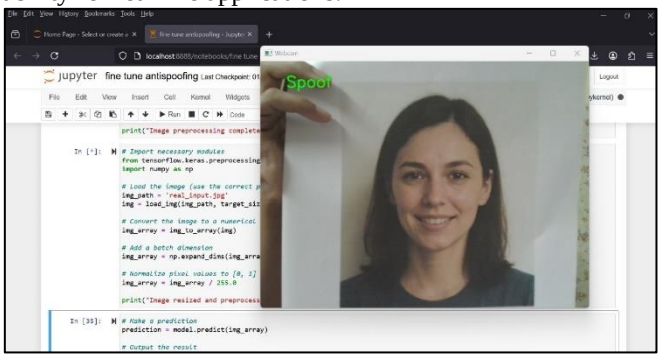

Fig. 7: Spoof Detection

V. CONCLUSION AND FUTURE SCOPE

This document puts on records an elaborate face recognition authentication system based on deep learning with better anti-spoofing measures and embedding encryption to provide security and accuracy in the highest quality possible. The overall approach is the use of FaceNet feature extraction, a classroom-tuned anti-spoofing model based on MobileNetV2, and a Flask-based backend for all authentication purposes. Hence, effective counter advanced spoofing attacks while ensuring efficiency is achieved here. Furthermore, to transform the entire system, MongoDB atlas secures the data, bcrypt hashes the password to make it secure, and OTP verification provides the third factor for authentication.

Future enhancements are expected to fine-tune these aspects even more. The incorporation of Edge AI along with these IoT devices can attain real-time facial authentication on smart cameras and mobile devices while minimizing dependence on cloud computing. Interestingly, the future developments of the system will include multi-modal biometric authentication, where the identified users will be required to verify identity through both vocal and iris identification along with facial recognition. This shall improve security against advanced spoofing attempts. Also, federated learning will be included so that there will be decentralized training to maintain privacy concerns and reduced vulnerability of data privacy. Scalability remains the most important point since the deployment could serve enterprise security, identity verification in digital transactions, and safe financial transactions. Here, ethical dimensions, including reducing potential biases in face recognition models and compliance with global privacy laws, become significant pillars of their responsible deployment.

Presenting this study, it lays a strong basis for the coming times of facial recognition authentication system, which will be an ideal mixture of precision, efficiency, and security. It will continuously improve with technology to counter the emerging legends and ensure that biometric solutions are ethical in fairness and comply with privacy requirements.

REFERENCES

[1] Yu, Z., Qin, Y., Li, X., Zhao, C., Lei, Z., Zhao, G. (2023). Deep Learning for Face Anti-Spoofing: A Survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 45(5), 5609. DOI: 10.1109/TPAMI.2022.3215850
[2] Maphisa, S., Coulter, D. (2022). Face Anti-spoofing based on Convolutional Neural Networks. 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA). IEEE
[3] Dliwati, M. A., Kumar, D. (2021). Face Recognition in the Context of Website Authentication. 2021 Asian Conference on Innovation in Technology (ASIANCON), Pune, India. IEEE
[4] Saudagar, S., Kulkarni, M., Giramkar, A., Godse, S., Gupta, S., Patil, G., Gunjal, S. (2023). Image Encryption based on Advanced Encryption Standard (AES). 2023 International Conference for Advancement in Technology (ICONAT), Goa, India. IEEE
[5] Jameera, F. B., Suresh, G., Hemalatha, S., Veronica, S. V. (2023). People Identification Through Facial Recognition and Anti-Spoofing Using Deep Learning. International Journal of Scientific Research in Science, Engineering and Technology, 10(5), 253-262
[6] Vaidya, L., Shasthrimath, V. D. (2018). Authentic Face Detection and Encryption for Security Assurance. IEEE
[7] S. Agrawal and P. Khatri, "Facial expression detection techniques: based on Viola and Jones algorithm and principal component analysis," in 2015 Fifth International Conference on Advanced Computing Communication Technologies, 2015, pp. 108-112: IEEE.
[8] FaceNet: A Unified Embedding for Face Recognition and Clustering (2015) – F. Schroff, D. Kalenichenko, J. Philbin.
[9] Kodinariya T M 2014 Hybrid Approach to Face Recognition System using Principle component and Independent component with score based fusion process
[10] Taigman, Y., Yang, M., Ranzato, M., Wolf, L. (2014).DeepFace: Closing the Gap to Human-Level Performance in Face Verification.Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 1701–1708.
[11] Parkhi, O. M., Vedaldi, A., Zisserman, A. (2015). Deep Face Recognition.British Machine Vision Conference (BMVC).
[12] Zhang, K., Zhang, Z., Li, Z., Qiao, Y. (2016). Joint Face Detection and Alignment using Multi-task Cascaded Convolutional Networks (MTCNN). IEEE Signal Processing Letters, 23(10), 1499–1503.
[13] Wang, M., Deng, W. (2021). Deep Face Recognition: A Survey. Neurocomputing, 429, 215–244.
[14] He, K., Zhang, X., Ren, S., Sun, J. (2016). Deep Residual Learning for Image Recognition (ResNet). Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).

