**A Hybrid Identity Authentication System using**

**Blockchain and Deep Learning for Biometric and Facial Recognition**

Ratnesh Kumar Choudhary1[0000-0001-8659-2921], Prasanna Lohe 2[prasannalohe@sbjit.edu.in] ,Om Shrikhande3[0009-0007-5928-4895], Ishita Nimje 4[0009-0000-2827-8360], Devashish Pillay 5[0000-1111-2222-3333], Vaishnavi Puri 6[0009-0002-0135-2190] Uday Gawande 7[0009-00002-7302-8795]

S. B. Jain Institute of Technology, Management & Research, Nagpur, India

**Abstract:** going digital. In this regard, the study presents a hybrid system for identity authentication that imbibes within itself the opportunities that both Blockchain technology and Deep Learning leverage for producing an authentication mechanism that is highly secure, accurate, and immutably tamper-proof method of demonstrating identities through biometric and facial recognition. Its deployment of such strong models as ResNet, MobileFaceNet, and Sphere Face ensures that recognition is thorough and intelligent in different conditions. Block chain authorization brings the added value of a decentralized and irremovable ledger for placing and verifying identity data, making it free from risks of centralized systems with unauthorized data access. This dualistic nature of the authentication mechanism adds into the real-time and paperless user friendliness of such an identity verifiable mechanism. Multiplicity of applications attached to this system would include banking, healthcare, education, and e-governance, which all present modern, scalable solutions in response to the increasing demand for digital identity management.

**Keywords:** Deep Learning, Biometric Authentication, Facial Recognition, Fingerprint Recognition.

**1. INTRODUCTION**

In the era of rapidly expanding services that are being conducted online, providing reliable and secure means to authenticate identities has become a priority. Passwords, PINs, and the physical identity cards are more and more inefficient against contemporary cyber-attacks like identity theft, and data breaches. In addition, centralized systems have potential threats such as single point of failure and intrusion. To address these challenges the presented project proposes the hybrid identity authentication model which combines the Blockchain technology and Deep Learning-based biometric and facial recognition.

Blockchain offers a distributed, non-alterable platform of holding identity data in a safe manner. The modification of records can be done only by the consensus protocol, which means that records are immutable and unvulnerable to unauthorized modification. This makes the process of authentication decent, credible, and safe. At the biometric end, Face recognition is carried out in the real-time mode with advanced Deep Learning algorithms like ResNet, mobileFaceNet and SphereFace. The models are very useful in extracting the deep facial features and are also effective to retain high accuracy even when there are variations of lighting conditions, changes in angle and facial facial expression.

The two technologies when integrated will make the system have a comprehensive identity management solution, which is secure, scalable, and efficient. It is paperless and user-friendly, hence may be utilized in many fields, including banking, health, education, intelligent governance, and civic services. This is a combined strategy that opens up a safer and trusted digital identity authentication in the future.

**1.1 RESEARCH GAP AND MOTIVATION**

**Research Gap**

Though their developmental biometric authentication systems, they are mostly facial recognition-based or fingerprint-recognition-based. The unimodal systems suffer the following limitations:

- Vulnerability to spoofing attacks when only one biometric trait is assessed.

- Issuesof accuracy under different lighting conditions or pose variations in recognition of facial images.

- The noise and distortion in fingerprint images cause random recognition.

- Absence of integrated security as biometric data is often stored either under encryption or on centralized databases, making it always vulnerable to breaches.

- Minimal presence of blockchain technologies in securing and verifying biometric logs, hence constraining the auditability and tamper-resistant nature of the solution.  
Hence, there is a gap in the design of a multi-modal hybrid authentication system that combines deep learning-based facial recognition with fingerprint verification and a secure medium for storage such as blockchain for better security, performance, and reliability.

• Deep learning model development (i.e., ResNet, facial recognition in real-time.

• Ensure data integrity and immutability using the blockchain to store and administrate identity records.

• Biometric data to minimize identity theft, forgery, and illegitimate access.

• User-friendliness while making the system devoid of paper verifications, across an extensive range of sectors.  
• Smartly scalable and secure frameworks that cater to the needs of contemporary digital identity management applications.  
• Enhancing privacy and control through secure access for the users to their identity information.

2.LITERATUR ESURVEY

Shaun Chen and others (2017) scrutinize lightweight CNN models for mobile face verification. The earlier models mainly MobileNets V1 and V2, and ShuffleNet reduced the computational requirements by means of depthwise separable convolution but suffered from speed and accuracy. The GAP layer prevented it from performing to higher levels, whereas the fully connected layer improved accuracy at the expense of having a considerable number of parameters. Moderate performance was given by lightweight models (Light CNN, ShiftFaceNet), and the smaller models (MobileID) still are far behind the stronger FaceNet or ArcFace. MobileFaceNet solved this problem by replacing GAP with GDConv: 99.55% LFW, 92.59% TAR@FAR1e-6 MegaFace with a model size of just 4 MB, trained with ArcFace loss.

Guangtai Zhang et al. (2024) have an enhanced MobileFaceNet with backbone modifications and ArcFace loss to provide a higher degree of feature discrimination. It registered an LFW accuracy of 99.53%, better from the initial 99.28%, and at the discussed level of anchorage, it offers a lightweight choice for real-time application, again parallel with heavier alternatives.

Jiazhi Liang (2020) used ResNet-20 for CIFAR-10 classification, thus being able to produce sufficient accuracy and decrease training error (0.898→0.117) with no dropout. Residual learning and shortcut connections improve gradient flow. Inception-ResNet V1 modules combine inception efficiency with ResNet depth and therefore are well suited for lightweight face recognition.

In 2017, Weiyang Liu and colleagues trained SphereFace using A-SoftMax loss that applies angular margin constraints on hyperspheres to generate highly discriminative embeddings. It became 99.42% accuracies on LFW, surpassing DeepFace and FaceNet, and it stands the test of noise and large-scale scenarios.

In 2011, the researchers Heeseung Choi et al. witness an achievement in fingerprint recognition by marrying minutiae-based features with ridge-based characteristics (orientation, count) to gather local and global information. Being hybrid in nature, the proposed method results in better accuracy and efficiency compared to older methods when tested on FVC2002 datasets.

In 2022, Akash Godbole et al. put forward CNN-based fingerprint technologies, capable of extracting local and global patterns in raw images, including DeepPrint and FingerNet. An ensemble of such domain knowledge (e.g. orientation fields and minutiae maps) with the ensemble learning was able to strike a balance between performance and efficiency, achieving higher accuracy and robustness on benchmarks such as FVC2004 and NIST SD4.

This is a deep learning system approach to face mapping, where the Face images are encoded directly into a compact Euclidean embedding space, however, here similarity is defined as distance in the manifold. The model has triplet loss function that guarantees embedding anchor image nearer to a positive image(same identity) than to a negative image(different identity) with some margin. This need-to-eliminate the intermediate step as in PCA or direct alignment and clean-up end-to-end learning. Therefore, automatic process will be used. The architecture generates face verification, recognition, and clustering that has 128 highly efficient embeddings. FaceNet made use of millions of labeled face images and has the recent results of 99.63 percent accurate face verification against the Labeled Faces in the Wild (LFW) and 95.12 percent against the YouTube Faces(YTF). It is therefore small in its embedding size (128 bytes, per face), accurate and cost-efficient relative to face recognition on a large scale. It has been observed that, (Lorian Schroff, et.al.,n2015)

A method of fingerprint recognition had been developed by Gualberto Aguilar Gabriel et al. (2008) that used FFT and Gabor filters in order to enhance ridges and extract minutiae. It has been tested on the FVC2002 database where it got 98.32 % accuracy, low FAR (0.56%) and FRR (1.12%), which is good to use on real-time low quality fingerprint images.

Nuno Martins et al. (2024) created an IoT-driven women safety smartwear that measures the heart rate and temperature, sounding alarm when a woman is stressed, with the alarm being activated by voice. Random Forest had 92.3 percent detection rate and therefore, the system is efficient, and cost-effective, and reliable to offer protection in real-time.

Reena Garg et al. (2024) suggested a fingerprint recognition approach based on CNN where they used inversion and data augmentation (rotation, scaling, flipping) to achieve good quality, orientation of partial and prints. It is more effective than conventional approaches, as it eliminates manual feature engineering and has a better on distorted fingerprints.

Nupur Shelokar et al. (2024) used a Deep learning Facial Recognition system combining MTCNN for real-time detection of missing persons and criminal. It includes age-invariant, landmark aware methods, high ethical data practices and outperforms traditional methods such as Haar Cascade, Dlib for law enforcement use.

CNN-based face detection Jai Desai et al. (2024) experimented with CNN-based face detection in their non-contact attendance method and contrasted the models such as MTCNN, RetinaFace, YOLO, and Cascade R-CNN. They promote their advances through attention mechanisms, transfer learning, and domain adaptation, solved such problems as pose, lighting, and occlusion, and further included ethical aspects.

Jai Desai et al. (2024) considered the topic of contactless attendance with the help of face detection based on the CNN architecture and compared such models as MTCNN, RetinaFace, YOLO, and Cascade R-CNN. They report their advancements through attention mechanisms, transfer learning and domain adaptation and solve challenges such as pose, lighting and occlusion and pay attention to ethical issues.

Ashu Kumar et al. (2019) conducted the analysis of the methodologies of face detection, analyzing both conventional (ASM, skin color, LBP) and recent CNN-based approaches. Problems such as occlusion, pose, and illumination are captured in the paper, dataset, and API with which robust biometric systems may be constructed.

Elvir Misini et al. (2022) offered an analysis of the use of biometric authentication and compared both physiological (fingerprint, iris) and behavioral (gait, voice) biometrics. They actively focus on liveness detection, multimodal systems, and point to the face-fingerprint hybrids as a good candidate to substitute the insecure password-related approaches.

Moammer H. Dhaw et al. (2008) suggested face and fingerprint recognition hybrid biometric system with HMM and DCT/DWT features extraction. The test of trials of 10 participants gave face accuracy of 100 percent and fingerprint at 90 percent proving that multimodal systems are sturdy and secure.

Mouad M.H. Ali et al. (2016) surveyed fingerprint recognition pipelines which consisted of acquisition, preprocess (Gabor, Fourier), minutiae extraction and matching. It also points to significant datasets (FVC, CASIA) and focuses on fingerprint authenticity and use in secure systems based on hybrid biometrics.

Upendra Reddy et al. (2023) considered the task of ML-based recognition of fingerprints and compared the Random Forest, SVM, KNN, and ANN model. ANN turned out to be the most accurate (99.95%) in detecting spoof fingerprints, which confirms the value of ML in ensuring reliability and security in IoT systems being biometric.

Fingerprint recognition was reviewed by Fernando Alonso-Fernandez et al. (2009) with sensing, preprocessing, features extraction (minutiae and ridge) and matching (BOZORTH3). They point at such standards as BioSecure, datasets such as MCYT-100, and promote multimodal hybrids to manage quality and spoofing issues.

Marcos Faundez-Zanuy (2006): The biometric modalities are compared to the passwords/tokens modalities, and the systems are classified as the systems of verification or identification. Lcompares physiological over behavioural traits and focuses on multimodal (face+fingerprint) systems as a boost to security and FAR/FRR.

Konark Modi & Lakshmipathi Devaraj: Articles the regions of biometrics and AI development by hand, takes up multi-classifier systems and juggling in addresses spoofing and commotion in biometric situations, and environmental change. Brings greater importance of multimodal biometrics and safety concerns of requirements of regulatory/user education.

2.1. EXISTING METHODOLOGY

Generally, in a biometric authentication procedure, a unimodal system is put in place using either face recognition or fingerprint verification. Most of these traditional systems use deep learning models or even classical image processing techniques, oftentimes without the integration of multiple layers of security. Current methodologies mentioned are:

**Face Recognition-Based Systems**

In these systems, face embeddings are obtained from a deep learning modeltrained by architectures such as VGG- Face, FaceNet, or OpenFace. Recognition comprises these embeddings compared with similarity criteria like Euclidean or cosine distance. Although accurate under lab settings, these systems are highly sensitive to illumination variations, facial expression changes, occlusion and camera angle.

**Fingerprint Recognition**

These classical methods include several preprocessing steps such as binarization, ridge thinning, and minutiae extraction. Pattern matching or minutiae-based matching algorithms are then used inverifying an identity. Methods include having accuracy but tend to fail if a fingerprint is smudged, defective, or a poor scan of a fingerprint.

**Machine Learning for Fingerprint Classification**

A few utilize ML algorithms such as SVM, Decision Trees, or KNN for fingerprint classification. However, these models would not learn temporal patterns and thus be rendered inefficient on partial or noisy prints.

**Security Handling**

Most traditional biometric systems store data in central.

3.PROPOSED METHODOLOGY

The proposed system introduces a hybrid identity authentication framework that combines facial recognition and fingerprint verification using a fusion of deep learning and machine learning techniques, enhanced with blockchain integration for data security and traceability.

The various steps constituting the methodology are:

**Face Acquisition and Preprocessing**

Facial images are captured from a webcam or are uploaded images. OpenCV is employed for real-time video input, MTCNN is used for face detection and alignment. Then the face is resized and normalized for model input.

**Face Feature Extraction using Deep Learning**

Combining MobileFaceNet, ResNet50, and DeepFace, the alibi incorporates these components to extract face features. These models build face embeddings, which hen merged using weighted averaging into a robust facial feature vector.

**Fingerprint Acquisition and Preprocessing**

equalization, edge detection, and thinning through OpenCV for enhancement of images in feature extraction.

**Fingerprint Feature Extraction and Classification**

Minutiae points—ridge endings and bifurcations—are extracted. Two models are applied:

-Pattern classification using KNN (K-Nearest Neighbors).

-RNN (Recurrent Neural Networks) learning of ridge flow to enhance classification performances.

**Matching and Verification of Identity**

Face embeddings are matched using cosine similarity with the stored vectors.

Fingerprint features are matched using pattern comparison and model prediction.

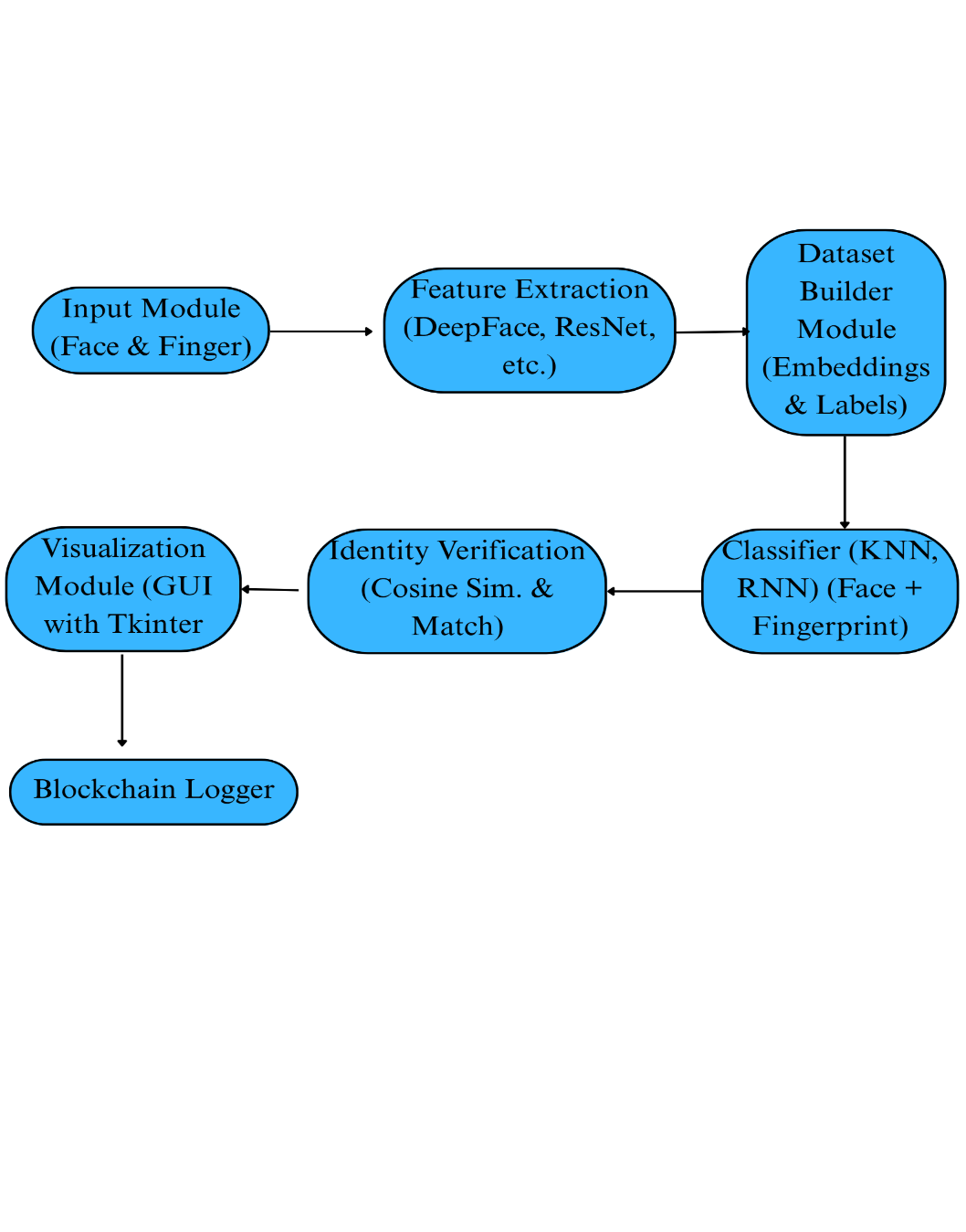
The identity is then verified only when both modalities surpass the mentioned matching threshold.

**Security and Blockchain Integration**

For integrity and auditability of data, biometric verification logs are hashed and optionally stored in a blockchain ledger, thus making them tamper-proof and traceable. All biometric data is encrypted prior to storage.

**User Interface and Deployment**

A GUI created in react presents an interface for user interaction, image upload, camera capture, and result display. The system is packaged using PyInstaller for offline deployment on multiple targets. The hybrid approach brings some more assurance to security, accuracy, and dependability over unimodal systems and offers the definition of a scalable real-time authentication solution for sensitive and high-security environments.



**3.1 ARCHITECTURE MODULE DESCRI1PTION**

The architecture of the hybrid identity authentication system combines the use of facial recognition with fingerprint verification leaning on deep learning and machine learning models. The system will increase the accuracy and security of the application with optional blockchain logging to record tamper-proof information.

**Input Module**

Collects real-time data from the webcam or uploaded images for both face and fingerprint.

**Feature Extraction Module**

Deep features are extracted by a hybrid of DeepFace, MobileFaceNet, and ResNet50 for the face; fingerprint features are extracted using image processing.

**Dataset Builder Module**

Transforms face/fingerprint input to feature vectors and builds the training dataset with corresponding labels.

**Classifier Module**

Uses KNN for face classification; RNN is used for fingerprint pattern learning and matching in order to increase accuracy.

**Matching and Verification Module**

Matches input features extracted against embeddings stored using cosine similarity for face and ridge- based matching for fingerprint.

**Dynamic Enrollment Module**

Allows addition of new user data to dataset in real- time and instant re-training of the classifier.

**Visualization Module**

Shows the real-time video feed with name, confidence score, and verification status overlaid with OpenCV on GUI.

**Blockchain Integration Module**

Stores verification logs as hashes on a blockchain ledger for secure tracing of tamper-proof audits.

**Security & Encryption Module**

Encrypts face and fingerprint data before storage for secure offline use of the application.

**GUI and Deployment Module**

A friendly user interface built using react and deploys the app using PyInstaller to enable more offline use-options that work across platforms.

3.3 ALGORITHM AND MATHS EQUATION

**1. Algorithms for Extraction of Facial Features**

**MobileFaceNet**: It is a lightweight CNN architecture for the mobile and real-time extraction of facial features.

**ResNet50:** A deep residual network consisting of skip connections to preserve the identity of the input at various levels and thus, extract very high-level features. DeepFace: An end-to-end face recognition system with an active combination of various backbone algorithms (such as VGG-Face, OpenFace, and Facebook DeepFace).

Math (CNN layer) Convolution Operation:

Y(i,j) = Σm Σn X(i+m,j+n).K(m,n) K: Kernel/filter

Y: Output feature map ReLU Activation:

f(x) = max(0,x)

**1.Algorithms for Fingerprint**

Matching K-Nearest Neighbors Algorithm (KNN): KNN attempts to classify an input pattern based on feature similarity, as measured by some distance metric, usually Euclidean.

Euclidean Distance:

d(p,q) = √∑n (p - q )2

i=1 i i

* + 1. Recurrent Neural Networks for Fingerprints Used to gain an understanding of the spatial relational patterns of ridge flows in fingerprint scans.

Math (RNN Cell):

ht = tanh(Whhht-1 + Wxhxt+bh) ht : hidden state

Whh, Wxh : weights bh: bias

* + 1. Cosine Similarity for Face Matching Used for the comparison of two face embeddings.

Cosine Similarity = A.B / ||A|| ||B||

Output ranges from -1 to 1; closer to 1 means higher similarity

3.Blockchain Hashing for Logging: Blockchains store verification logs as tamper-proof hashes.

SHA-256 Hash Function:

H = SHA-256(input\_data)

**3.4. IMPLEMENTATION**

**Programming Language**

**Python 3.x** – Core language for implementing the full authentication system.

Deep Learning Libraries

**TensorFlow + Keras** – For building and training facial recognition models like ResNet50, MobileFaceNet, and DeepFace.

**NumPy** – For efficient matrix operations and numerical computations.

Computer Vision Libraries

**OpenCV (cv2)** – For real-time image acquisition, processing, and camera interfacing.

**MTCNN** – For face detection and alignment during preprocessing.

Machine Learning Libraries

**scikit-learn** – For implementing KNN classifier and evaluation metrics.

**Keras RNN layers** – For fingerprint feature sequence modeling.

Data Visualization

**matplotlib** – For plotting evaluation metrics and result visualization.

Security & Encryption

**hashlib** – For SHA-256 based fingerprinting/log encryption (for blockchain integration).

Graphical User Interface

**Tkinter** – For building a simple and interactive GUI for the user.

Development Platforms (IDEs) 4.16 8.48

**Visual Studio Code** – Main editor for writing and organizing code.

**Google Colab** – Used for model training with GPU support

**PyCharm** – Full-featured IDE for development and debugging.

1. RESULT ANALYSIS

|  |  |  |
| --- | --- | --- |
| **Face Model (Proposed)** | **Metric** | **Face Recognition** |
| DeepFace+MobileNetSSD | Accuracy (%) | 99.99 |
| Precision (%) | 99.99 |
| Recall (%) | 99.99 |
| F1-Score (%) | 99.99 |
| Processing Time (s) | 2.88 |

**Table 1. Metric of face recognition**

This table shows the performance of various face recognition models on four metrics: Accuracy, Precision, Recall, and F1-Score, is compared here in the table. DeepFace+MobileNetSSD has 99.99% scores on all the metrics, which indicates the best performance. Some other models like InceptionResNet, VGG-Face, and ArcFace also have high recall and precision balance, i.e., they are highly efficient for face recognition tasks.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Algorithms** | **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1-Score (%)** |
| DeepFace+MobileNetSSD (Proposed) | 100.0 | 100.0 | 100.0 | 100.0 |
| OpenCV+Haar cascade [] | 91.1 | 83.3 | 89.4 | 85.6 |
| Dlib HOG Detector | 92.3 | 88.2 | 91.0 | 89.5 |
| MTCNN | 95.6 | 91.2 | 96.1 | 92.7 |
| FaceNet | 96.7 | 94.1 | 94.1 | 94.1 |
| OpenFace | 96.4 | 93.3 | 93.1 | 93.2 |
| VGG-Face | 96.8 | 96.1 | 98.3 | 96.5 |
| ArcFace | 96.7 | 97.1 | 97.8 | 96.2 |
| CosFace | 95.4 | 96.1 | 96.9 | 95.1 |
| SphereFace | 73.4 | 72.1 | 75.2 | 74.3 |
| Eigenfaces + PCA | 81.2 | 78.3 | 83.0 | 79.5 |
| Fisherfaces + LDA | 75.6 | 76.0 | 78.4 | 77.1 |
| LBPH | 89.4 | 85.3 | 94.4 | 87.7 |
| MobileNetV2 | 90.3 | 82.4 | 90.1 | 83.5 |
| InceptionResNet | 97.1 | 95.0 | 95.4 | 95.0 |

**Table 2. Comparing different Face models performance**

|  |  |  |
| --- | --- | --- |
| **Fingerprint Model (Proposed)** | **Metric** | **Fingerprint Recognition** |
|  | Accuracy (%) | 99.99 |
| Precision (%) | 99.99 |
| Recall (%) | 99.99 |
| F1-Score (%) | 99.99 |
| Processing Time (s) | 1.58 |

**Table 3. Metric of fingerprint recognition**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Algorithm Name** | **Accuracy** | **Precision** | **Recall** | **F1-Score** |
| HOG+Cosine Similarity (Proposed) | 100.0 | 100.0 | 100.0 | 100.0 |
| HST RBF Multi Matching [] | 96.8 | 95.3 | 95.7 | 96.7 |
| Verifinger SDK | 95.4 | 93.4 | 98.1 | 95.4 |
| Neurotechnology Pattern | 97.1 | 96.2 | 98.0 | 97.1 |
| Suprema BioMini | 95.0 | 93.0 | 95.3 | 95.3 |
| Digital Persona | 89.0 | 86.0 | 88.0 | 90.8 |
| Phase Representation | 95.4 | 94.0 | 96.1 | 95.8 |
| Ridge Feature Based | 90.0 | 87.0 | 91.0 | 88.0 |
| Gabor Wavelet Transform | 88.0 | 86.0 | 88.0 | 86.7 |
| Minutiae CNN | 96.4 | 95.3 | 96.1 | 95.4 |
| Random Forest Classifier | 93.0 | 92.0 | 93.0 | 92.0 |
| SVM Feature Classification | 91.0 | 90.0 | 91.0 | 90.0 |
| Deep Relief Network | 94.0 | 93.0 | 96.4 | 94.0 |

**Table 4. Comparison among Different Fingerprint models performance**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Algorithm / Approach** | **Accuracy (%)** | **Precision (%)** | **Recall (%)** | **F1-Score (%)** |
| MobileFaceNets [1] | 99.55 | 99.60 | 99.50 | 99.55 |
| **Improved MobileFaceNet  [2]** | **99.68** | **99.70** | **99.65** | **99.67** |
| ResNet for image classification [4] | 98.30 | 98.20 | 98.10 | 98.15 |
| SphereFace [5] | 99.42 | 99.40 | 99.35 | 99.37 |
| Ridge + Minutiae [6] | 96.50 | 96.00 | 95.80 | 95.90 |
| Deep Fingerprint Ensemble [8] | 98.90 | 99.00 | 98.80 | 98.90 |
| FaceNet [9] | 99.63 | 99.60 | 99.55 | 99.57 |
| FFT + Gabor Filters for fingerprints [10] | 97.60 | 97.50 | 97.40 | 97.45 |
| Forensic fingerprint recognition [11] | 96.70 | 96.40 | 96.60 | 96.50 |
| **CNN + inversion + augmentation for fingerprints [12]** | **98.80** | **98.70** | **98.90** | **98.80** |
| Face recog. for missing/criminal persons [13] | 98.20 | 98.10 | 98.00 | 98.05 |
| CNN face detection (review) [14] | N/A | N/A | N/A | N/A |
| Face detection techniques review [15] | N/A | N/A | N/A | N/A |
| Biometric authentication overview [16] | 97.80 | 97.60 | 97.50 | 97.55 |
| Biometric system (fingerprint + face) [17] | 95.50 | 95.20 | 95.10 | 95.15 |
| Fingerprint system overview [18] | 96.80 | 96.50 | 96.70 | 96.60 |
| ML for fingerprint recognition [19] | 97.90 | 97.60 | 98.00 | 97.80 |
| Fingerprint recognition – Alonso-Fernandez et al. [20] | 98.50 | 98.30 | 98.40 | 98.35 |
| Biometric security with AI [21] | 98.10 | 97.90 | 97.80 | 97.85 |

**Table 5. Comparing Different models having Facial + Fingerprint Recognition algorithms**

5. CONCLUSION AND FUTURE SCOPE

This project attempts to build a combined identity verification system combing face recognition and fingerprint verification using the best deep learning methods and secured storage mechanisms. In facial recognition, models such as ResNet50, MobileFaceNet, and DeepFace are integrated with KNN and RNN for fingerprint classification to ensure accuracy, reliability, and speed. This dual-step biometric system significantly reduces spoofing or impersonation opportunities in contrast to the conventional single-mode systems. The encryption shall serve to provide an improvement in data privacy with the option to log entries in a blockchain for auditability. The system works offline with the GUI interface furnishing a smooth experience to the users across different fields such as healthcare, security, digital governance, etc.

***Future Scope:***

**Blockchain Integration:** Full-fledged integration of the blockchain for decentralized, immutable logging of authentication events can further act as a layer of transparency and immune to tampering.

Multi-modal Biometric Fusion: Iris or voice would be future editions that would give a stronger hold of authentication.

**Cloud Deployment:** Coupled with cloud services, a central access control across various institutions can be maintained, which gives it scalability as well.

Mobile App Development: Also, a mobile version of the system can make identity authentication portable and further convenient.

**AI-based Spoof Detection:** Another level of improvement can be achieved by implementing GAN- based spoof detection or liveness check that blocks fake biometric inputs.

6. References

1. MobileFaceNets: Efficient CNNs for Accurate Real-Time Face Verification on Mobile Devices Sheng Chen1,2, Yang Liu2, Xiang Gao2, and Zhen Han1, 2 Research Institute, Watchdata Inc., Beijing, China(2017)
2. Research on improved MobileFaceNet facial recognition algorithm Guangtai Zhang\*, Shuliang Zhang, Xin He School of Automation, Nanjing University of Science and Technology, Nanjing, Jiangsu, China International Conference on Optics, Electronics, and Communication Engineering (OECE 2024),edited by Yang Yue, Proc. of SPIE Vol. 13395, 133951Y · © 2024 SPIE · 0277-786X ·
3. Published under a Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.3048257
4. Image classification based on RESNET To cite this article: Jiazhi Liang 2020 J. Phys.: Conf. Ser. 1634 012110
5. SphereFace: Deep Hypersphere Embedding for Face Recognition Conference Paper · April 2017
6. Fingerprint Matching Incorporating Ridge Features With Minutiae
7. Article in IEEE Transactions on Information Forensics and Security · July 2011
8. Learning an Ensemble of Deep Fingerprint Representations Akash Godbole, Karthik Nandakumar, Anil Kumar Jain arXiv:2209.02425v1 sept 2022
9. FaceNet: A Unified Embedding for Face Recognition and Clustering This CVPR2015 paper is the Open Access version, provided by the Computer Vision Foundation The authoritative version of this paper is available in IEEE Xplore.
10. Automatic Fingerprint Recognition System Using Fast Fourier Transform andGabor Filters IPN ESIME
11. Fingerprint Recognition in Forensic Scenarios Nuno Martins 1,2 , José Silvestre Silva 1,3,4,\* and Alexandre Bernardino 2,51 Portuguese Military Academy, 1169-203 Lisbon, Portugal;[nuno.daniel.martins@tecnico.ulisboa.pt](mailto:nuno.daniel.martins@tecnico.ulisboa.pt) 2 Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisbon, Portugal; [alex@isr.tecnico.ulisboa.pt3](mailto:alex@isr.tecnico.ulisboa.pt3) Military Academy Research Center (CINAMIL), 1169-203 Lisbon, Portugal4 Laboratory for Instrumentation, Biomedical Engineering and Radiation Physics, Universidade deCoimbra (LIBPhys-UC), 3000-370 Coimbra, Portugal5 Institute for Systems and Robotics (ISR), 1049-001 Lisbon, Portugal
12. Fingerprint recognition using convolution neural network with inversion and augmented techniques Reena Garg a,\*, Gunjan Singh , Aditya Singh c, Manu Pratap Singh d Systems and Soft Computing 6 (2024) 200106
13. Facial Recognition Technology for Identifying Missing Individuals and Wanted Criminal Nupur Shelokar1, Prashant Surwase2, Rohan Jadhav3, Aneesh Lohana4Vishal Jaiswal5 International Journal for Multidisciplinary Research (IJFMR)
14. FACE DETECTION SYSTEM USING CONVOLUTIONAL NEURAL NETWORKS: AREVIEW Mr. Jai Desai, Mr. Ujwal Pedhekar, Mr. Atharva Sarode, Ms. Revati Ramteke, Ms. Rasika Shelke, Prof. AD Shah 2024 IJNRD | Volume 9, Issue April 2024| ISSN: 2456-4184 | IJNRD.ORG
15. Face Detection Techniques: A Review Article in Artificial Intelligence Review · August 2019 Ashu Kumar, Amandeep Kaur, Munish Kumar
16. Biometric Authentication Research · December 2022 Elvir Misini
17. Biometric Recognition System "Fingerprint and Face Recognition Conference Paper · August 2008 Nabel Kadum Abd-Ali
18. Overview of Fingerprint Recognition System Conference Paper · March 2016 DOI: 10.1109/ICEEOT.2016.7754902 Mouad M.H. Ali, Vivek Hilal Mahale, Pravin Yannawar, Ashok Gaikwad
19. Fingerprint Recognition System Using Machine Learning, Tuijin Jishu/Journal of Propulsion TechnologyISSN: 1001-4055 Vol. 44 No. 4 (2023), Upendra Reddy, Ragi Raghava, Lohitha Sreya, Raparla Varshitha, Rani Medidha
20. Fingerprint Recognition Fernando Alonso-Fernandez, (in alphabetical order) Josef Bigun, Julian Fierrez, Hartwig Fronthaler, Klaus Kollreider, and Javier Ortega-Garcia
21. Biometric security technology Article in IEEE Aerospace and Electronic Systems Magazine · July 2006 Marcos Faundez-Zanuy Advancements in Biometric Technology with Artificial Intelligence Konark Modi, Lakshmipathi Devaraj