

Secure Fingerprint Authentication Using Machine Learning and Deep Learning

Rushad I. Sheikh¹, Deep Chirwatkar², Kiran P. Pustode³

¹Student, Department of Computer Applications, Karanjekar College of Engineering and Management, Sakoli

²Assistant Professor, Department of Computer Applications, Karanjekar College of Engineering and Management, Sakoli

³HOD, Department of Computer Applications, Karanjekar College of Engineering and Management, Sakoli

Abstract - Fingerprint authentication is among the most widely deployed biometric security mechanisms, yet its resilience against presentation attacks and cross-sensor variability remains an open research challenge. This paper presents a controlled comparative security evaluation of four machine learning and deep learning models: Convolutional Neural Network (CNN), Hybrid CNN with Batch Normalization and Dropout, Support Vector Machine (SVM) with Histogram of Oriented Gradients (HOG) feature extraction, and Random Forest ensemble, applied to binary genuine-versus-spoofed fingerprint classification. All models are trained on the publicly available Sokoto Coventry Fingerprint Dataset (SOCOFing) under identical preprocessing and evaluation conditions, with the False Acceptance Rate (FAR) as the primary security metric. The standard CNN achieves the best overall balance with 97.36% accuracy, FAR of 8.11%, and FRR of 0.82%, while SVM delivers the lowest FAR of 5.60%. External cross-sensor validation on a smartphone-captured dataset exposes significant distributional sensitivity in deep learning models and over-conservative rejection in classical models. Findings confirm that machine learning-based fingerprint authentication is technically feasible and highly adaptable, offering a strong foundation for next-generation biometric security systems.

Key Words: Fingerprint Authentication, Biometric Security, Convolutional Neural Network, Support Vector Machine, False Acceptance Rate, Presentation Attack Detection, HOG Feature Extraction, Deep Learning, Cross-Dataset Generalization.

1. INTRODUCTION

Biometric authentication has become a foundational component of modern cybersecurity infrastructure, progressively supplementing traditional knowledge-based credential systems across enterprise IT, financial services, healthcare, and government sectors [1]. Among available modalities, fingerprint recognition holds a dominant position due to the uniqueness of ridge patterns at population scale, morphological stability throughout a lifetime, and the maturity of capacitive and optical sensor technology [2].

Despite widespread deployment, fingerprint authentication remains subject to well-documented vulnerabilities. Traditional minutiae-based feature extraction exhibits degraded reliability under environmental noise, moisture variability, partial capture, cross-sensor hardware differences, and adversarial manipulation [6]. The most critical threat, the presentation attack, involves fabricating artificial artefacts from silicone, gelatin, or latex to impersonate enrolled users, producing False Acceptance events with severe security consequences [3].

Machine learning (ML) and deep learning (DL) approaches have emerged as technically superior alternatives. Convolutional Neural Networks (CNNs) learn discriminative spatial representations of ridge texture and liveness cues directly from raw image data [4]. Hybrid CNN architectures incorporating Batch Normalization and Dropout improve training convergence stability and reduce overfitting [5]. Classical methods including SVM with HOG descriptors and Random Forest ensembles provide computationally efficient, interpretable baselines [8],[9].

However, the existing literature predominantly evaluates individual architectures in isolation using aggregate accuracy, preventing valid cross-model security comparisons. This paper fills the gap through a controlled, head-to-head comparative evaluation of all four model types under identical conditions, using FAR as the primary security metric, supplemented by mandatory external cross-dataset validation for distributional robustness assessment.

2. LITERATURE REVIEW

2.1 Traditional and Classical Methods

Traditional fingerprint authentication relies on minutiae-based matching pipelines that extract ridge endings and bifurcations and compute similarity scores against enrollment templates. Rahman et al. [2] demonstrated that even parameterized template protection schemes remain vulnerable to distortion in adversarial environments. Maiti et al. [6] confirmed that standalone minutiae systems are inadequate against presentation attacks without supplementary liveness detection, and that cross-sensor variability is a persistent limitation. SVM classifiers applied to HOG feature descriptors, originally introduced for pedestrian detection by Dalal and Triggs [7], have demonstrated competitive fingerprint spoof detection performance with advantages in computational efficiency [8].

2.2 Deep Learning Approaches

CNNs have significantly advanced fingerprint authentication and liveness detection. Garg et al. [4] showed that CNNs with inversion and augmentation achieve superior generalization for limited training datasets with improved tolerance to acquisition variability. Nogueira et al. [10] established CNN-based liveness detection achieving high benchmark accuracy. Hussain et al. [5] proposed a hybrid deep learning model achieving 99.42% classification accuracy with FAR 0.31% and FRR 0.27%, demonstrating that Batch Normalization and Dropout provide quantifiable security metric improvements. Kothadiya et al. [12] provided evidence that regularization strategies systematically reduce the intra-to-cross-dataset performance gap.

2.3 Presentation Attack Detection

Li and Ramachandra [11] comprehensively surveyed deep

learning FPAD methods, identifying cross-material and cross-sensor generalization as the field's primary open challenge. Casula et al. [13] confirmed that cross-dataset testing reveals generalization failures invisible in single-dataset evaluations. Alduhailan et al. [1] highlighted the adversarial perturbation threat, demonstrating that Dropout regularization provides

incidental robustness benefits. Sonal et al. [9] showed complementary SVM and Random Forest strengths in multi-biometric frameworks, supporting the inclusion of both classical model types in comparative analysis.

3. METHODOLOGY

3.1 System Architecture and Flowchart

The system employs a dual-pipeline architecture. The deep learning pipeline feeds normalized 128x128 grayscale images directly into convolutional feature extractors. The classical ML pipeline first applies HOG feature extraction to generate descriptor vectors before classification. Both pipelines share a common preprocessing stage. Fig. 1 shows the system architecture flowchart.

Fig -1: System Architecture Flowchart

Stage	Process	Output
1. Input	SOCOFing Real + Altered Images	Raw fingerprint images
2. Preprocessing	Grayscale -> Resize 128x128 -> Normalize [0,1]	Normalized arrays
3. DL: Data Split	85% Train / 15% Val (ImageDataGenerator)	Batches of 32
4. ML: HOG Extract	16x16 cells, 2x2 blocks + 80/20 stratified split	Feature vectors
5. Model Training	CNN / Hybrid CNN / SVM (RBF) / Random Forest (200)	Trained classifiers
6. Evaluation	FAR, FRR, Accuracy, Precision, Recall	Security profiles
7. Ext. Validation	Smartphone dataset (print + replay attacks)	Cross-domain metrics

3.2 Dataset Acquisition

The Sokoto Coventry Fingerprint Dataset (SOCOFing) [14] is the primary dataset containing 6,000 genuine fingerprint images of 600 African subjects plus 55,249 synthetically altered images spanning three manipulation types (obliteration, central rotation, z-cut) at three severity levels (Easy, Medium, Hard). All genuine images are labeled "real" and all altered images "spoof." The external Biometric Fingerprint Spoofing dataset, captured on a Samsung Galaxy A53 5G smartphone, contains genuine fingerprints, print attacks (fingerprints printed on paper), and replay attacks (fingerprints displayed on screen), used exclusively for cross-dataset validation.

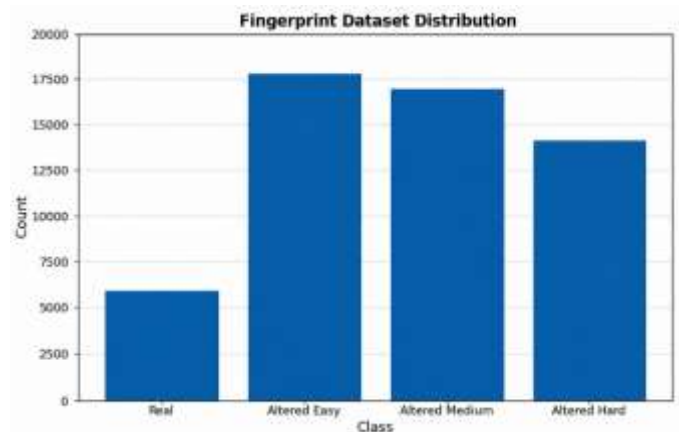


Fig -2: Dataset distribution

3.3 Preprocessing Pipeline

A uniform preprocessing pipeline is applied across all models: grayscale conversion eliminates irrelevant color variation; spatial rescaling to 128x128 pixels standardizes input dimensions; pixel normalization to [0, 1] stabilizes gradient-based optimization. The deep learning pipeline uses TensorFlow ImageDataGenerator with 85/15 training-validation split and batch size 32. For classical ML, up to 10,000 images per class are sampled to maintain computational feasibility for scikit-learn classifiers, with an 80/20 stratified train-test split at random seed 42.

3.4 Model Specifications

CNN: Three sequential Conv2D blocks with filter depths 32, 64, 128 and MaxPooling2D reduction, followed by Dense(128, ReLU) and sigmoid output. Hybrid CNN: Extends CNN with Batch Normalization after first two convolutional blocks, Dense(256), and Dropout(0.5) before sigmoid output. Both compiled with Adam optimizer, binary cross-entropy loss, trained for 10 epochs. SVM: RBF-kernel Support Vector Machine trained on HOG feature vectors with default scikit-learn hyperparameters. Random Forest: 200 decision trees trained on bootstrap samples with random feature subsets at each split.

3.5 Evaluation Framework

A unified evaluation function computes all metrics from the confusion matrix: FAR = FP/(FP+TN) is the primary security metric quantifying unauthorized access risk; FRR = FN/(FN+TP) is the primary usability metric; Accuracy = (TP+TN)/Total; Precision = TP/(TP+FP); Recall = TP/(TP+FN). The function is applied identically to all four models on both the primary SOCOFing test partition and the external validation dataset, producing eight complete security profiles.

4. EXPERIMENTAL RESULTS

4.1 Dataset Distribution

The SOCOFing dataset exhibits class imbalance: approximately 6,000 genuine samples versus over 49,000 altered samples across Easy (~18,000), Medium (~17,000), and Hard (~14,500) categories. The genuine-to-spoof ratio of approximately 1:8.2 directly influences FAR and FRR interpretation. Visual inspection confirms realistic manipulation characteristics: ridge obliteration, rotation artifacts, and z-cut distortions representative of real-world presentation attack instruments. The external spoofing dataset presents fundamentally different image characteristics: lower optical resolution, variable background illumination, and

different ridge contrast compared to controlled SOCOFing scanner acquisition.

4.2 Primary Dataset Results (SOCOFing)

Table -1: Models Comparative Analysis (Primary SOCOFing Dataset)

Model	Accuracy	FAR	FRR	Precision	Recall
CNN	97.36%	8.11%	0.82%	0.9734	0.9918
Hybrid CNN	95.18%	16.89%	0.78%	0.9462	0.9922
SVM (HOG)	93.38%	5.60%	8.37%	0.9056	0.9163
Random Forest	86.78%	5.45%	26.46%	0.8878	0.7354

CNN Performance: The CNN achieves 97.36% accuracy with FAR 8.11% and FRR 0.82%, the most balanced security-usability profile. Training curves show healthy convergence with validation accuracy closely tracking training accuracy, confirming minimal overfitting. High Recall (0.9918) demonstrates near-complete genuine user detection. The Hybrid CNN, despite incorporating Batch Normalization and Dropout, exhibits elevated FAR of 16.89% due to overfitting to SOCOFing-specific patterns, evidenced by validation accuracy instability around epoch 7.

Real Fingerprints



Fig -3: Real Fingerprints

Altered Fingerprints



Fig -3: Altered Fingerprints

SVM achieves the second-lowest FAR (5.60%) with competitive accuracy (93.38%), demonstrating strong security-oriented performance at the cost of higher FRR (8.37%) — rejecting approximately 1 in 12 legitimate users. The Random Forest achieves the lowest FAR (5.45%) but unacceptable FRR of 26.46%, rejecting over one-quarter of legitimate users, disqualifying it from practical deployment. This failure is attributed to the 1:8.2 class imbalance and inherent representational limitations of tree-based methods on spatially structured image data.

4.3 External Cross-Dataset Validation

Table -2: External Dataset Models Performances

Model	Accuracy	FAR	FRR	Behaviour
CNN	33.33%	100%	0%	All-genuine predictor
Hybrid CNN	50.00%	45%	60%	Partial generalization

Model	Accuracy	FAR	FRR	Behaviour
SVM	70.00%	0%	90%	Near-total rejection
Random Forest	66.67%	0%	100%	All-spoof predictor

The external validation reveals a stark architectural divide. The CNN collapses to an all-genuine predictor (FAR 100%, FRR 0%): spoof-detection features calibrated to SOCOFing scanner-specific obliteration and rotation artifacts are not triggered by smartphone-captured images with different pixel statistics and ridge contrast. The Hybrid CNN achieves partial cross-domain robustness (50% accuracy, FAR 45%, FRR 60%), with the improvement attributable to Batch Normalization and Dropout creating marginally more distribution-invariant representations.

Classical models switch to near-total or complete rejection due to severe HOG feature space covariate shift between optical scanner and smartphone camera. The SVM's 0% FAR and Random Forest's 0% FAR on the external dataset are operationally meaningless — achieved by rejecting virtually all inputs rather than genuine spoof discrimination. These findings validate the methodological necessity of mandatory cross-dataset testing in biometric authentication research.

5. DISCUSSION

The CNN emerges as the most practically deployable model under controlled acquisition conditions, achieving the optimal FAR-FRR trade-off. Its primary dataset FAR of 8.11% is within acceptable range for civilian authentication. Compared to state-of-the-art results by Hussain et al. [5] achieving FAR 0.31% with purpose-built hybrid architectures, the performance gap indicates significant improvement potential through targeted augmentation and adversarial training.

The Hybrid CNN's counterintuitive elevated FAR (16.89%) despite regularization components provides a critical practical lesson: architectural complexity without proportionate training data amplifies overfitting rather than reducing it. This aligns with Kothadiya et al. [12] who observed that regularization benefits are dataset-size dependent. The SVM's low FAR (5.60%) with higher FRR (8.37%) demonstrates the classical security-usability trade-off appropriate for high-assurance access control environments.

The complementary FAR-FRR profiles of deep learning (low FRR) and classical (low FAR) model families suggest a hybrid deployment architecture: CNN-based first-stage authentication for user accessibility followed by SVM-based second-stage security verification for spoof resistance. The external validation performance gap is not model failure but a well-documented deployment challenge [13]; the path forward lies in multi-condition training, transfer learning, and domain adaptation strategies standard in industry-grade biometric systems.

6. CONCLUSIONS

This paper presented a comprehensive, security-centric comparative evaluation of CNN, Hybrid CNN, SVM with HOG, and Random Forest for fingerprint authentication. Under controlled SOCOFing conditions, the CNN achieves the best balanced profile (97.36% accuracy, FAR 8.11%, FRR 0.82%) while SVM delivers the strongest security with FAR 5.60%.

The Hybrid CNN's elevated FAR (16.89%) despite regularization demonstrates that model complexity without proportionate data impairs security performance. The Random Forest's unacceptable FRR (26.46%) disqualifies it from deployment.

External cross-dataset validation reveals universal distributional sensitivity, confirming that benchmark performance cannot proxy for real-world deployment robustness. Complementary model family profiles provide practical design guidance for hybrid deployment architectures. Future research directions include multi-sensor training, domain adaptation, adversarial training, threshold optimization, and integration with multimodal biometric frameworks for cloud and IoT environments. The experimental methodology and findings provide a reproducible, evidence-based foundation for practitioner model selection in security-sensitive fingerprint authentication deployments.

ACKNOWLEDGEMENT

The authors sincerely acknowledge the guidance and support of the Department of Master of Computer Applications, Karanjekar College of Engineering and Management, Sakoli, affiliated to Dr. Babasaheb Ambedkar Technological University, Lonere. Special appreciation is extended to all faculty members of the MCA Department for their sustained academic support throughout this research work.

REFERENCES

- [1] A. Alduhailan, N. H. Kamarudin, S. N. H. S. Abdullah, and A. Dau, "Deep Learning in Biometric Authentication: Challenges, Recent Advancements, and Future Trends," *Journal of Advances in Information Technology*, vol. 16, no. 4, pp. 458-477, 2025.
- [2] M. M. Rahman, T. I. Mishu, and M. A. A. Bhuiyan, "Performance Analysis of a Parameterized Minutiae-Based Approach for Securing Fingerprint Templates," *Journal of Information Security and Applications*, vol. 67, p. 103209, 2022.
- [3] J. Saleem, U. Raza, M. Hammoudeh, and W. Holderbaum, "Machine Learning-Enhanced Attribute-Based Authentication for Secure IoT Access Control," *Sensors*, vol. 25, no. 9, p. 2779, 2025.
- [4] R. Garg, G. Singh, A. Singh, and M. P. Singh, "Fingerprint Recognition using Convolution Neural Network with Inversion and Augmented Techniques," *Systems and Soft Computing*, vol. 6, p. 200106, 2024.
- [5] A. Hussain, F. Murshed, M. N. Alandoli, and G. Aljafari, "A Hybrid Deep Learning Approach for Secure Biometric Authentication Using Fingerprint Data," *Computers*, vol. 14, no. 5, p. 178, 2025.
- [6] D. Maiti, M. Basak, and D. Das, "Fingerprint Biometric: Confronting Challenges, Embracing Evolution, and Extending Utility - A Review," *Journal of Engineering Research and Sciences*, vol. 3, no. 9, pp. 26-60, 2024.
- [7] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," *Proc. IEEE CVPR*, pp. 886-893, 2005.
- [8] J. Rachel and E. Devarasan, "Robust Contactless Fingerprint Authentication Using Dolphin Optimization and SVM Hybridization," *Frontiers in Big Data*, vol. 8, 2025.
- [9] Sonal, A. Singh, and C. Kant, "Optimized Hybrid SVM-RF Multi-Biometric Framework for Enhanced Authentication," *PeerJ Computer Science*, vol. 11, p. e2699, 2025.
- [10] R. F. Nogueira, R. de A. Lotufo, and R. C. Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks," *IEEE Trans. Information Forensics and Security*, vol. 11, no. 6, pp. 1206-1213, 2016.
- [11] H. Li and R. Ramachandra, "Deep Learning Based Fingerprint Presentation Attack Detection: A Comprehensive Survey," *arXiv:2305.17522*, 2023.