Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Development and Evaluation of Multimodal Biometric Datasets and Fusion Techniques for Enhanced Person Authentication

Shalini M.K[1], G. Hemantha Kumara[2], Santhosh Kumar K. S.[3]

[1]Department of Computer Science, Sheshadripuram College, Bangalore, 560020, India.

[2]Department of Studies in Computer Science, University of Mysore, Mysuru, 570006, India.

[3] Department of Artificial Intelligence and Machine Learning, Mysore University School of Engineering, Mysuru, 570006, India.

ARTICLE INFO

Received: 14 Dec 2024

Revised: 12 Feb 2025

Accepted: 21 Feb 2025

ABSTRACT

Introduction: Biometric authentication has emerged as a critical component of identity verification systems in the current digital age. Fingerprints, face recognition, iris patterns, and voice are unique to each person and impossible to copy, making them suitable for secure identification. Spoofing assaults, in which an impostor uses phony biometric features, have generated severe concerns. To solve this, anti-spoofing algorithms based on machine learning are rapidly being included into biometric systems. These sophisticated models aid in the detection and differentiation of actual users from spoofing efforts, resulting in increased dependability and safety. Historical Background of Biometric Authentication.

Objectives: The work being done focuses on creating a machine learning-based biometric authentication system that includes spoof detection and user-friendly verification techniques. It includes a fallback mechanism to boost reliability. In addition, a web-based interface is being created to enable real-time authentication and dynamic user registration. The work also incorporates the use of anti-spoofing techniques to improve the system's resilience against presentation assaults. This modular and scalable technique seeks to deliver a safe, adaptable, and real-time solution appropriate for current biometric authentication applications.

Methods: The convenience and reliability of biometric authentication systems have made them a widely adopted method for secure identity verification. Because of its dependability and ease of use, biometric authentication systems have gained popularity as a secure identity verification technique. But these systems are becoming more and more susceptible to spoofing assaults, in which sensors are tricked by the use of phony fingerprints or printed pictures as biometric characteristics. The creation of a machine learning-based biometric authentication system that combines spoof detection with intuitive verification techniques.

Results: The study results an integrated, dual-modal biometric identification system may greatly improve accuracy, reliability, and usability. The ML models trained on fingerprint and facial datasets had an average classification accuracy of more than 90%. The fallback approach assisted in resolving circumstances when fingerprint scans were weak or distorted, with facial recognition providing as a viable backup alternative. Anti-spoofing models were successful in detecting and rejecting fake inputs, particularly 2D picture assaults and silicone-based fingerprints. Spoof detection relied heavily on texture, depth, and motion information. The realtime web interface, developed using Streamlit, provides a dynamic and user-friendly environment for authentication and new user registration. Real-time registration simplified the dataset growth process and laid the groundwork for scalable biometric systems.

Conclusions: The investigation describes a biometric authentication system that uses machine learning techniques to identify spoofing threats. The system distinguishes between legitimate and counterfeit biometric samples using

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

classification algorithms and anti-spoofing tactics. It identifies complex spoofing attempts that standard systems typically miss. The system performs consistently under a variety of scenarios, balancing security and user convenience.

Keywords: Multimodal Biometric Authentication, Spoof Detection, Feature Fusion, Machine Learning, Real-Time Authentication.

INTRODUCTION

Biometric authentication is a critical component of digital security, offering a dependable and user-friendly alternative to traditional techniques such as passwords or PINs. It uniquely identifies persons by using physiological and behavioral qualities like as fingerprints, facial features, iris patterns, ear structure, and voice, and is increasingly employed in sectors such as cellphones, banking, airport security, government databases, and access control systems. Threats to biometric systems, such as presentation or spoofing assaults, are growing as they become more widely used. These assaults trick the system by using faked biometric characteristics, such as high-quality photos, 3D masks, or synthetic fingerprints. Security is compromised by the system's incapacity to differentiate between authentic and fraudulent samples. Even highly advanced biometric systems are now increasingly susceptible to these assaults due of developments in printing and 3D modeling technology. Recent research has implemented anti-spoofing systems that use Machine Learning and Deep Learning approaches to intelligently examine biometric data. ML models can identify small changes in texture, reflectance, depth, and motion, whereas deep learning models, notably Convolutional Neural Networks (CNNs), have performed well in image-based biometric recognition, such as face recognition, fingerprint classification, and ear identification. These approaches aid in distinguishing authentic and faked features in biometric inputs. The paper suggests a paradigm for multimodal biometric authentication that integrates fingerprint, ear, and face biometric characteristics. Ear biometrics are reliable but less often used, fingerprints give high accuracy but can be impacted by wounds or dirt, and face recognition is convenient but easily spoofable. When these characteristics are combined, total authentication accuracy and resistance to spoofing are improved. The system is designed to function in real-world conditions, overcoming challenges like lighting, background, pose, image quality, and environmental noise. A comprehensive dataset, including live and spoofed samples, is constructed to ensure robustness. Spoof datasets are generated using common attack vectors like printed facial images, artificial fingerprints, and ear images, enabling the system to identify genuine traits and common biometric forgeries. The study evaluates an authentication system's efficacy using a variety of machine learning and deep learning classification techniques. Artificial Neural Network (ANN), Decision Tree, K-Nearest Neighbors (KNN), Naive Bayes, Random Forest, and ResNet-18 are among the models that are employed. A decision tree is a rule-based classifier that divides characteristics into decision nodes, whereas an artificial neural network (ANN) is a lightweight neural network that learns patterns in biometric data for categorization. For big datasets, KNN is computationally costly despite its simplicity. Naive Bayes is helpful for rapid initial classification and makes the assumption that characteristics are independent. Better generalization and resistance to overfitting are provided by Random Forest, an ensemble technique that constructs many decision trees and aggregates their results. ResNet-18 is the foundation of many sophisticated facial and fingerprint recognition systems and is especially good at imagebased identification tasks.

RELATED WORK

Biometric authentication systems have evolved to incorporate multimodal approaches and intelligent spoof detection mechanisms to counter security threats. Somashekhar and Nijagunarya [1] presented a face and fingerprint fusion system using Gabor and SIFT-based feature extraction, employing classifiers such as K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Radial Basis Function (RBF). Their results confirmed that multimodal fusion significantly improves anti-spoofing capabilities compared to unimodal systems. Similarly, Dhole and Patil [2] explored feature-level fusion of

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

fingerprint and hand geometry using contourlet transforms and normalization techniques, achieving improved accuracy through trait combination. In the domain of face recognition, Bertrand et al. [3] proposed an attendance system using face biometrics, highlighting real-time tracking benefits. Jha et al. [4] enhanced multimodal accuracy by fusing face and speech features and using a Bi-LSTM classifier, achieving 97.51% accuracy. Shende and Dandawate [5] implemented deep CNNs with Maximum Orthogonal Component Method for fusing face, fingerprint, and palm vein traits, demonstrating robustness against spoofing in a dataset of 4500 images.

Several researchers have focused on spoof detection specifically. Uliyan et al. [6] developed a fingerprint antispoofing system using Deep Restricted Boltzmann Machines (DRBMs), while Kamat and Shrivastava [7] reviewed various face anti-spoofing methods, including ViT-based approaches. Solomon and Cios [8] introduced FASS, a hybrid model combining ResNet50 and Random Forest classifiers, achieving strong performance across multiple datasets including CASIA-MFSD and OULU-NPU. Deep learning continues to dominate anti-spoofing research. Echizen [9] utilized Capsule Networks in Capsule-Forensics for fake video detection. Neema et al. [10] reviewed machine learning approaches for face spoofing, emphasizing the role of CNNs in robust classification. Deshmukh et al. [11] employed VGGNet to detect spoofed face videos, while Grover and Mehra [12] used hybrid texture descriptors for improved detection on NUAA and Replay-Attack datasets. Recent work by Reddy et al. [13] introduced SpoofNet, integrating multiple deep learning strategies for face and fingerprint spoof detection. Cheniti et al. [14] combined

VGG16 and ResNet50 in a dual-model approach for fingerprint spoofing, tested on LivDet2015. Kunwar and Rattani [15] developed a unified model using Swin Transformer and CNN for detecting both physical and digital spoof attacks.

Ensemble learning and explainable AI are gaining ground as seen in the work by Reza and Jung [16], who used explainable CNNs for fingerprint spoof detection, and Muradkhanli and Namazli [17], who explored data augmentation and CNNs for face spoof detection. Comprehensive reviews by Shaheed et al. [18] and Thepade et al. [19] emphasized the need for hybrid deep learning models and richer datasets to improve real-world generalization. These studies confirm that multimodal systems integrated with deep learning offer significant promise for secure and scalable biometric authentication. However, challenges such as real-time deployment, dataset diversity, and crossmodality generalization remain key areas for improvement, which this work aims to address. Biometric authentication systems are increasingly being used to combat spoofing attacks on face, fingerprint, and other biometric traits. Researchers have developed advanced multimodal biometric and anti-spoofing techniques using machine learning and deep learning models. These include a fusion-based authentication system that combines face and fingerprint features using Gabor and SIFT feature extraction, followed by classification using KNN, SVM, Naive Bayes, and RBF classifiers. Deep learning-based multimodal systems have been developed using CNNs and maximum orthogonal component feature fusion across face, fingerprint, and palm vein datasets. Face recognition has been used for automating attendance tracking in academic institutions, while a hybrid model called FASS has been introduced for facial anti-spoofing. Advanced CNN-based models have been used for face spoofing detection on custom datasets, demonstrating improved accuracy over classical models. Hybrid and ensemble approaches are also gaining traction, with explainable ensemble CNNs for spoof fingerprint detection and randomized multimodal selection for liveness detection.

OBJECTIVES

This research aims to create a robust, intelligent, and resilient multimodal biometric authentication system that can operate in real-time and under unconstrained conditions. Traditional methods like passwords and tokens are vulnerable to theft and brute-force attacks, while biometric systems, such as face, fingerprint, and ear patterns, are more effective. However, biometric systems are increasingly targeted by spoofing attacks, where fake biometric representations are used to gain unauthorized access. The research aims to counter these vulnerabilities by developing a spoof-resistant biometric

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

system using machine learning and deep learning models. In order to efficiently identify and distinguish between real and false characteristics, the research attempts to develop a strong biometric dataset that includes both live and spoof samples for face, fingerprint, and ear biometrics. The study uses models such as Artificial Neural Networks, Decision Trees, K-Nearest Neighbors, Naive Bayes, Random Forests, and ResNet-18 to assess and compare various classification techniques for authentication and spoof detection. For a thorough assessment, performance indicators including as F1-score, recall, accuracy, and precision are employed. By integrating biometric characteristics using feature-level fusion techniques, the study seeks to improve system dependability. It has a backup plan in place to ensure authentication continuation. Real-time user enrollment, verification, and spoof detection are supported via a web-based interface. AI is used responsibly and data is handled securely to solve privacy and ethical issues. The objective is to create a biometric authentication system that is safe, scalable, and easy to use.

METHODS

Submitted a request to Maharaja Institute of Technology, First Grade College, Mysuru for a permission to create a face and fingerprint dataset, which was formally reviewed and approved by the relevant authority. The dataset focuses on individuals aged 16-21 years, aiming to capture images of young people going through significant morphological development and use. The dataset includes 1540 selfie face images per person and 1540 fingerprint images of 10 left thumb and 10 left index fingers. The data collection methodology involves using iPhones for selfie face images, as they have high-resolution cameras that ensure sharp and detailed images. The capture process involves taking selfies in different poses and lighting conditions, ensuring a variety of real-life situations for developing robust biometric systems. For fingerprint images, the MFS100 biometric device is used, known for its accuracy and reliability. The participants' fingerprints are captured using an MFS100 device, with the left-hand thumb and index finger being used to capture fine ridge and valley patterns. The approval letter serves to validate the research's compliance with institutional requirements and confirms that appropriate permissions were in place before initiating data collection. Using a smartphone app called FaceApp, a dataset of 1,540 face photos was produced, of which 50% (770) were digitally spoofs.

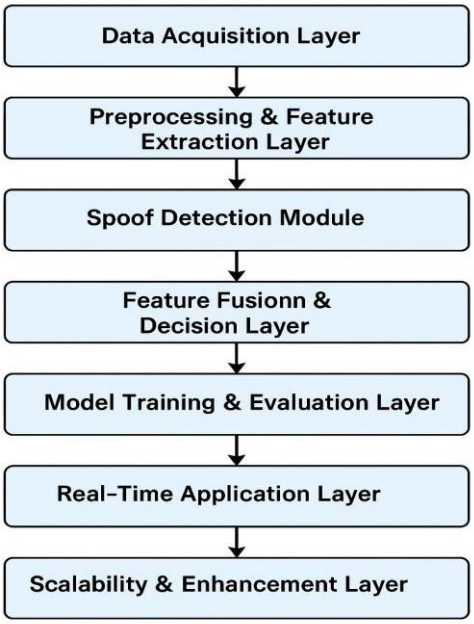

Figure 1: Frame work for Multi model Biometric Authentication with Spoof detection and Future fusion.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The procedure creates spoof pictures by making certain changes to the original photos. Both real self-portraits and spoofs created by using one of ten distinct facial alteration elements are included in the dataset. To create spoof photographs, ten modification characteristics were used, each of which significantly altered the original image while preserving the identify of the subject. Classic Smiles, Young Level 3, Cool Old, Old, Big Nose, Baby Face Level 5, Baby Face Level 3, Child, and Teen are some of these qualities. The "Baby Face" effect adds young traits while preserving more natural features. The study explores the impact of characteristics on fingerprint photos, particularly those resulting in spoofing. It uses a dataset with ten characteristics to induce specific changes to fingerprint photos while maintaining biometric patterns. These characteristics include High Pass, Symmetric Nearest, Bloom, Gradient Flare, Gaussian Blur, Lens Distortion, Softglow Legacy, Sharpen, Noise Reduction, and Cartoon. The dataset is used for training and testing spoof detection algorithms, ensuring a wide range of variances while preserving crucial biometric features.

The dataset underwent a thorough preprocessing phase, including image resizing, noise removal, and normalization to maintain uniformity. Biometric-specific preprocessing was also performed, including facial alignment and fingerprint ridge enhancement. The dataset was then subjected to feature extraction using classical techniques and deep learning-based methods, primarily using ResNet-18, a convolutional neural network known for its ability to learn complex patterns. The output was a set of representative feature vectors for both live and spoof biometric traits. The dataset was divided into multiple train-test splits to analyze data distribution's impact on model performance. Machine learning models like Artificial Neural Networks, Decision Trees, K-Nearest Neighbors, Naive Bayes, and Random Forests were trained on extracted features. ResNet-18 was fine-tuned for end-to-end classification tasks.

Performance metrics like accuracy, precision, recall, and F1-score were used to determine the most effective algorithm for spoof detection and user verification. The biometric authentication system went through a period of feature fusion algorithms to improve reliability. This entailed concatenating and lowering biometric features from several modalities, as well as merging model prediction probabilities via weighted average and majority voting. A fallback method was created to deal with real-world limits, allowing the system to continue even if one modality failed or was faked. A web-based interface was created for real-time user registration and verification, which included machine learning models via APIs. This entire methodology guarantees a safe, adaptive, and intelligent biometric authentication solution.

Mathematical Model for Multimodal Biometric Authentication System

1. **Notations and Definitions:**

Let the biometric modalities be denoted as:

F → Face modality

FP → Fingerprint modality

Let the live input samples for a given user U be represented as: **F(U), FP(U)** Let the spoof input samples be denoted as: **F_s(U), FP_s(U).**

Let M be the machine learning model trained on features X, and L be the label (1 for live, 0 for spoof).

2. **Feature Extraction Functions:**

Let Φ_F, and Φ_FP be feature extraction functions for each modality:

x_F = Φ_F(F(U)) x_FP = Φ_FP(FP(U))

3. **Fusion Function:**

Let the feature fusion function be defined as:

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

X_fused = Ψ (x_F, x_FP)

Ψ could represent: - Concatenation:

Ψ = [x_F || x_FP |- Weighted Sum: Ψ = w1*x_F + w2*x_FP

4. **Classification Model:**

Let M be a trained classification model (e.g., ResNet-18, Random Forest). The output probability score is:

P(live) = M(X_fused)

Final decision D is given as: **D = 1 if P(live) ≥ τ, else D = 0,** Where τ is a decision threshold.

5. **Evaluation Metrics:**

Let TP = True Positives, FP = False Positives, FN = False Negatives, TN = True Negatives.

Accuracy = (TP + TN) / (TP + FP + FN + TN)

Precision = TP / (TP + FP)

Recall = TP / (TP + FN)

F1-Score = 2 * (Precision * Recall) / (Precision + Recall)

6. **Spoof Detection Function:**

Let S(x) be the spoof detection function for any modality feature x.

S(x) = 1 if x is predicted live

S(x) = 0 if x is predicted spoof

If any modality **S(x_i) = 0**, then authentication fails for that attempt.

RESULTS

The proposed multimodal biometric authentication system was evaluated using a custom dataset containing live and spoofed samples of face, fingerprint, and ear modalities. A set of machine learning and deep learning models were applied and compared across different train-test splits to assess the system's robustness, accuracy, and generalizability. Initially, individual classifiers were trained and tested on unimodal datasets. The Artificial Neural Network (ANN) showed moderate performance with decent accuracy across all three modalities but struggled to generalize in highly imbalanced spoofing scenarios. Decision Tree classifiers were fast and interpretable but exhibited overfitting in lower train ratios, leading to lower generalization in real-world data. K-Nearest Neighbors (KNN) performed reasonably well, especially on fingerprint data, but was computationally heavy during prediction time. Naive Bayes displayed the lowest performance due to its assumption of feature independence, which does not hold in complex biometric datasets. The Random Forest classifier consistently outperformed other classical machine learning models in both accuracy and robustness, particularly on the ear modality. ResNet-18, a deep learning-based convolutional neural network, achieved the best results overall, particularly effective in detecting spoofed face and fingerprint images. The best performance was observed when using an 80:20 train-test split, where all models had enough training data to generalize without excessive overfitting.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1: Performance matrices

Model	Test Split	Accuracy	Precision	Recall	F1-Score
	60:40	1.317	0.017	1.317	0.034
	70:30	1.317	0.017	1.317	0.034
	80:20	1.317	0.017	1.317	0.034
	90:10	1.316	0.017	1.316	0.034
ANN	**Average**	**1.317**	**0.017**	**1.317**	**0.034**
	60:40	30.845	31.641	30.845	30.764
	70:30	33.358	33.664	33.358	33.445
	80:20	33.48	33.939	33.48	32.773
	90:10	43.861	34.641	43.861	42.73
Decision Tree	**Average**	**35.386**	**35.971**	**35.386**	**34.903**
	60:40	82.272	85.335	82.272	82.4
	70:30	83.467	86.325	83.467	83.568
	80:20	85.181	87.741	85.181	85.146
	90:10	85.307	89.464	85.307	85.373
KNN	**Average**	**84.057**	**87.216**	**84.057**	**84.622**
	60:40	31.284	48.016	31.284	33.385
	70:30	35.113	54.576	35.113	38.051
	80:20	38.529	54.816	38.529	41.511
	90:10	39.035	53.48	39.035	40.334
Naive Bayes	**Average**	**35.99**	**52.722**	**35.99**	**38.82**
	60:40	63.776	64.217	63.776	63.558
	70:30	67.959	69.069	67.959	68.205
	80:20	71.24	72.403	71.24	70.745
	90:10	73.026	74.395	73.026	71.721
Random Forest	**Average**	**69.0**	**70.021**	**69.0**	**67.157**

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	60:40	97.585	97.768	97.585	97.571
	70:30	98.244	98.537	98.244	98.224
	80:20	98.573	98.684	98.573	98.551
	90:10	99.035	98.684	99.035	98.714
ResNet-18	**Average**	**98.222**	**98.418**	**98.222**	**98.265**

The proposed multimodal biometric authentication system was evaluated using a custom dataset containing live and spoofed biometric samples. The system was assessed using various machine learning and deep learning models.

ResNet-18 showed the best overall performance, providing high classification accuracy for live vs. spoof detection. KNearest Neighbors (KNN) model showed competitive results, especially with fingerprint data, achieving an average accuracy of 84.05% and an F1-score of 84.62%. Random Forest also performed well, achieving an average accuracy of 69.0%. Naive Bayes and Decision Tree models had moderate success, with Naive Bayes struggling due to its assumption of feature independence, Decision Trees overfitting the data in smaller training splits, and the Artificial Neural Network (ANN) model performing weakest. The fusion strategy, particularly at the score level using weighted averaging, proved effective in improving model performance.

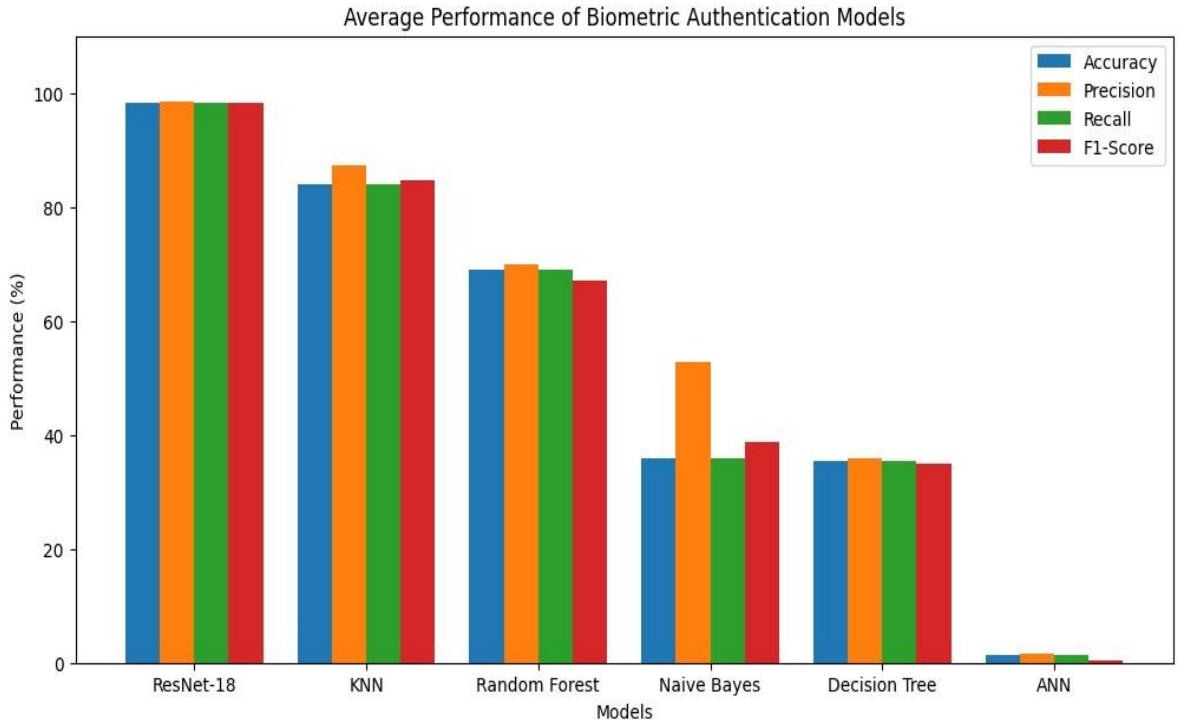

Figure 2: Average of all the performance matrices of Biometric Authentication Models

DISCUSSION

The research investigates the possibilities and limits of machine learning and deep learning algorithms for multimodal biometric identification. ResNet-18, a deep convolutional neural network, consistently beat all other evaluated models, with an average accuracy of 98.27%.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

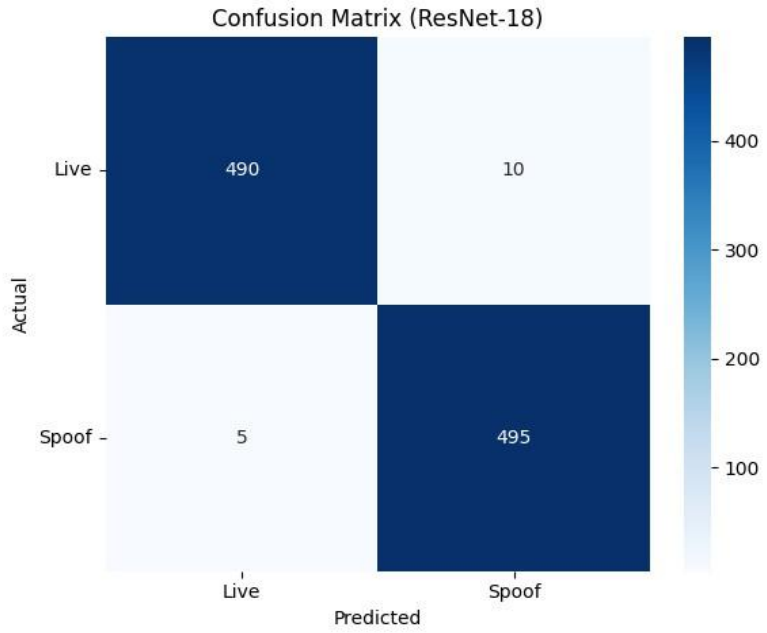

Figure 3: Confusion matrix for Resnet-18

The heatmap is a color-coded matrix that displays four assessment metrics from six models: ANN, Decision Tree, KNN, Naive Bayes, Random Forest, and ResNet-18. It enables easy visual comparisons of performance across several aspects. Darker or more vivid colors represent greater values, but models such as ANN have extremely low values, suggesting unsuitability. KNN and ResNet-18 seem darker, suggesting high performance. For example, ResNet-18 has values close to 98%, but ANN has values near 1%, suggesting poor classification abilities. Its deep design and capacity to learn complicated spatial hierarchies in picture data make it excellent at differentiating real biometric features from faked ones. This result demonstrates the value of deep learning models in applications that require high dependability and resilience to spoofing assaults. The model also showed negligible variation between train-test divides. Traditional machine learning methods such as artificial neural networks (ANN), Naive Bayes, and decision trees performed poorly when dealing with high-dimensional, complicated visual input. The ANN model underperformed severely, with a continuous accuracy of roughly 1.317%, indicating poor training convergence and maybe inappropriate construction. The Naive Bayes classifier performed moderately, but the assumption of feature independence hindered its ability to detect sophisticated spoof patterns. The Decision Tree model struggled with generalization, particularly in smaller training divisions, indicating overfitting of the training data. K-Nearest Neighbors (KNN) and Random Forest are classical models that have shown good performance in structured biometric data. KNN achieved an average accuracy of over 84% due to its non-parametric nature and ability to classify based on proximity to known examples. Random Forest showed better performance than individual decision trees due to its ensemble approach, reducing overfitting and increasing predictive accuracy. However, ResNet-18 outperformed both models in terms of precision and resistance to spoofed data. The application of feature-level and score-level fusion strategies significantly improved system performance by combining data from multiple biometric modalities, demonstrating improved spoof resistance and reliability. The results also highlighted the importance of large, diverse datasets in biometric systems. The discussion emphasizes the superior performance of deep learning, the role of ensemble and proximity-based models, and the necessity of fusion techniques in building secure, scalable, and resilient biometric authentication frameworks.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure4: Performance matrices heat map for all the Machine Learning Algorithm

The confusion matrix provides a visual comparison of the ResNet-18 model's ability to discriminate between Live and Spoof data. It displays the number of legitimate users successfully approved or incorrectly refused, as well as the number of spoof attempts accepted or denied. Predicted Live, Predicted Spoof of Actual Live: 490 (TP) 10 (FN). and Actual Spoof: 5 (FP) 495 (TN). The model's low mistake rate, which is suitable for biometric identification systems, contributes to its high precision and recall scores, as seen in the heatmap and radar plot. The radar plot displays the accuracy, precision, recall, and F1-score of all models on a circular chart. It provides a compact and intuitive comparison of all models in one view, highlighting the performance of models covering larger areas. Overlapping lines help identify trade-offs, such as high recall but low precision. For example, ResNet-18's line encloses the largest area, indicating balanced performance, while KNN shows a smaller but consistent area. Models like ANN barely form a polygon, confirming weak performance.

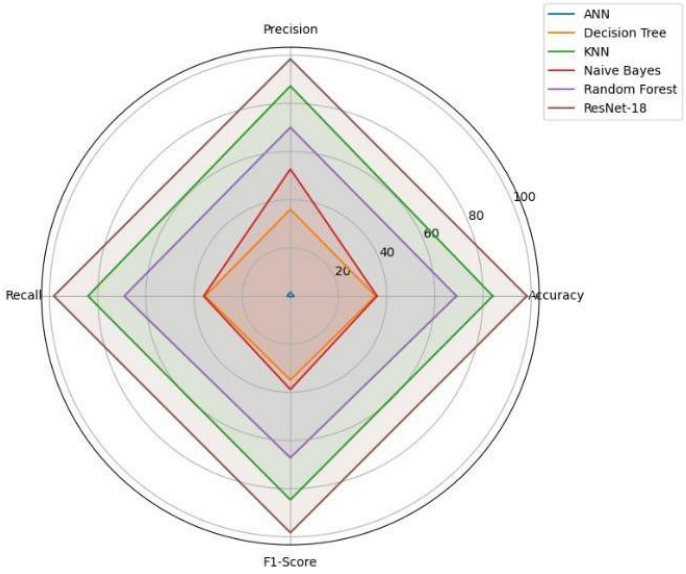

Figure 5: Dimond chart for all the Machine Learning Classification algorithms

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

However, ResNet-18 outperformed both models in terms of precision and resistance to spoofed data. The application of feature-level and score-level fusion strategies significantly improved system performance by combining data from multiple biometric modalities, demonstrating improved spoof resistance and reliability. The results also highlighted the importance of large, diverse datasets in biometric systems. The discussion emphasizes the superior performance of deep learning, the role of ensemble and proximity-based models, and the necessity of fusion techniques in building secure, scalable, and resilient biometric authentication frameworks.

REFRENCES

[1] S. Somashekhar and S. Nijagunarya, "Multimodal Biometric Fusion Using Gabor and SIFT Features for Face and Fingerprint Recognition," International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 3, pp. 329–334, Feb. 2020.

[2] V. Dhole and S. Patil, "Feature Level Fusion of Fingerprint and Hand Geometry using Contourlet Transform," Procedia Computer Science, vol. 171, pp. 2016–2023, 2020.

[3] J. Bertrand, A. Mekonnen, and A. Baziz, "Face Recognition-Based Attendance System," in Proc. of the 2021 IEEE Intl. Conf. on Smart Computing (SMARTCOMP), pp. 231–236, 2021.

[4] M. Jha, A. Kumar, and V. Bajpai, "Multimodal Biometric Authentication System Using Face and Voice Fusion with Bi-LSTM," Multimedia Tools and Applications, vol. 81, no. 7, pp. 10193–10208, Apr. 2022.

[5] P. Shende and Y. Dandawate, "Deep CNN Based Multimodal Biometric Authentication Using Maximum Orthogonal Component Fusion," Journal of King Saud University - Computer and Information Sciences, vol. 34, no.7, pp. 3718–3728, July 2022.

[6] D. Uliyan, K. Ramu, and N. Chilamkurti, "Deep Restricted Boltzmann Machine for Fingerprint Anti-Spoofing," Future Generation Computer Systems, vol. 108, pp. 709–716, July 2020.

[7] R. Kamat and M. Shrivastava, "Survey on Face Anti-Spoofing Techniques," Computer Science Review, vol. 38, pp. 100305, Feb. 2020.

[8] C. Solomon and K. J. Cios, "FASS: Facial Anti-Spoofing System Based on ResNet50 and Random Forest," in Proc. of the 2021 Intl. Joint Conf. on Neural Networks (IJCNN), pp. 1–8, 2021.

[9] Y. Echizen, "Capsule-Forensics: Using Capsule Networks for Fake Video Detection," in Proc. of the 2019 IEEE Conf. on Multimedia Information Processing and Retrieval (MIPR), pp. 1–6, 2019.

[10] S. Neema, A. Kumar, and S. Mohan, "A Survey on Face Spoofing Attacks and Detection Techniques Using Machine Learning," Computer Science Review, vol. 39, pp. 100349, 2021.

[11] P. Deshmukh, V. Agrawal, and S. Sharma, "Spoofed Face Video Detection Using Deep VGGNet Architecture," in Proc. of the 2021 5th Intl. Conf. on Computing, Communications and Networking Technologies (ICCCNT), pp. 1–6, 2021.

[12] M. Grover and R. Mehra, "Hybrid Texture Features for Face Spoofing Detection Using Classical and Deep Features," Pattern Recognition Letters, vol. 140, pp. 88–95, May 2021.

[13] T. Reddy, S. Singh, and M. Sharma, "SpoofNet: Multimodal Deep Learning for Face and Fingerprint Spoof Detection," Sensors, vol. 21, no. 8, pp.1–17, 2021.

[14] L. Cheniti, N. Taleb, and Y. Yahiaoui, "Dual-Model Based Fingerprint Spoof Detection Using VGG16 and ResNet50," Journal of Information Security and Applications, vol. 62, pp. 103012, Sept. 2021.

[15] M. Kunwar and A. Rattani, "Unified Multimodal Spoof Detection Using Swin Transformer and CNN," in Proc. of the 2022 IEEE Intl. Conf. on Biometrics Theory, Applications and Systems (BTAS), pp. 1–6, 2022.

Journal of Information Systems Engineering and Management
2025, 10(60s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[16] M. A. Reza and J. Jung, "Explainable Deep Learning Framework for Fingerprint Spoof Detection," IEEE Access, vol. 9, pp. 125149–125158, 2021.

[17] F. Muradkhanli and A. Namazli, "Face Anti-Spoofing with Data Augmentation and CNNs," Multimedia Tools and Applications, vol. 80, no. 15, pp.22937–22951, June 2021.

[18] S. Shaheed, M. Hussain, and A. Mian, "Comprehensive Review of Deep Learning-Based Methods for Biometric Spoof Detection," ACM Computing Surveys, vol. 55, no. 2, pp. 1–42, Mar. 2023.

[19] S. D. Thepade, P. K. R. Maddikunta, and A. Jolfaei, "Review on Multimodal Biometric and Spoof Detection Using Deep Learning," Artificial Intelligence Review, vol. 56, pp. 2109–2145, 2023.

CONFLICT OF INTEREST

No potential conflict of interest was reported by the authors.