Enhancing Authentication Through Fusion of Face and Palmprint

Allen Chen and Grace Boban

Introduction

Biometric authentication has become a cornerstone of secure identity verification across applications such as mobile device access, border control, financial services, and enterprise infrastructure. While traditional unimodal biometric systems—those relying on a single biometric trait such as facial features or fingerprints—have gained widespread adoption due to their simplicity, cost-effectiveness, and user familiarity, they are not without limitations. These systems are particularly susceptible to spoofing attacks, environmental noise, and degraded performance when the biometric input is occluded or distorted [1], [2].

To address these challenges, multimodal biometric systems have emerged as a compelling solution. By combining two or more biometric modalities, multimodal systems offer improved recognition accuracy, increased robustness, and greater resistance to spoofing or single-modality failure [3], [7]. Among the many possible modality combinations, the fusion of facial recognition and palmprint recognition stands out as a promising approach due to their complementary properties. Facial recognition is advantageous for passive acquisition and captures global texture features, whereas palmprints offer rich local ridge patterns, principal lines, and topological details that are stable over time and difficult to spoof [8], [9].

The relevance of multimodal systems has become even more apparent in real-world constraints—most notably during the COVID-19 pandemic. The widespread use of face masks severely hindered the performance of face-only systems, as key facial landmarks were obscured. Gomez-Barrero et al. [4] reported a marked increase in false rejection rates due to such occlusions, emphasizing the need for systems resilient to facial obstructions. In this context, palmprint recognition offers a significant advantage. Though less common in consumer applications, palmprints provide high biometric entropy and are typically captured using controlled, contact-based imaging methods that reduce environmental variability. Unlike fingerprint recognition, palmprint systems incorporate not only minutiae but also textural and structural information across a larger surface area [9], enhancing resistance to both spoofing and false matches. Their underutilization also translates to lower exposure risk, making them particularly attractive for privacy-sensitive or high-security applications.

This study investigates the impact of multimodal biometric authentication using facial and palmprint data, leveraging two publicly available datasets: the Specs on Faces (SoF) dataset for facial imagery [5] and the Birjand University Mobile Palmprint Database (BMPD) for palmprint images [6]. To evaluate the effectiveness of fusion strategies—particularly under occlusion-prone conditions—explores the following research questions:

- **RQ1**: How does multimodal biometric authentication using face and palmprint modalities affect overall system performance compared to single-modal biometric authentication?
- **H1**: A multimodal biometric system combining face and Palmprint modalities will significantly enhance authentication performance by achieving lower Equal Error Rates (EER) compared to unimodal biometric systems, due to complementary biometric features.
- **RQ2**: What impact do occlusions (e.g., glasses, masks) in face images have on the performance of multimodal biometric systems using face and palmprint data?
- **H2**: The multimodal biometric system will exhibit greater robustness against performance degradation caused by facial occlusions (e.g., masks, glasses) compared to face-only authentication, thereby resulting in a smaller increase in EER under occlusion conditions.

To validate these hypotheses, this study applies biometric fusion techniques at the score level, a method demonstrated in prior work to effectively combine complementary traits while minimizing computational overhead [3], [7]. The system will be evaluated using standard metrics such as Equal Error Rate (EER), d-prime, Receiver Operating Characteristic (ROC) curves, and Detection Error Tradeoff (DET) curves. In doing so, this research contributes valuable insight into the design of next-generation authentication systems that can withstand real-world constraints such as partial occlusions, while also advocating for the expanded use of palmprint recognition as a practical and underexplored modality in secure identity verification.

Related Work

Biometric systems that rely on a single modality, such as face or fingerprint, have shown vulnerabilities to environmental conditions, spoofing, and intra-class variability. These limitations have led researchers to explore multimodal biometric authentication, which combines two or more biometric traits to increase system accuracy, resilience, and security [2], [3]. One of the most widely explored combinations involves facial and palmprint modalities, as their complementary nature offers both global and local discriminatory features. Face recognition systems extract global texture and landmark patterns that are intuitive and easy to collect passively, while palmprints contain stable local features—such as principal lines, wrinkles, and ridge patterns—that are less affected by facial occlusions or expressions [9]. Unlike fingerprints, which focus on minutiae, palmprints cover a larger area of the hand and provide richer spatial information, improving biometric entropy and anti-spoofing potential [8]. Thasiyabi et al. [3] demonstrated a multimodal fusion system combining face and fingerprint modalities, utilizing Principal Component Analysis (PCA) and modular kernel PCA for the facial component and rule-based fusion for final decision making. Their study supports the claim that score-level fusion—where similarity scores from each modality are integrated—yields lower error rates compared to unimodal systems. Similarly, Jena et al. [7] employed deep learning-based feature fusion for face and fingerprint biometrics, showing that pre-trained CNNs like FaceNet and ResNet50 significantly improve performance when fused at the feature level but this project will focus primarily on score-level for its simplicity and availability of provided datasets.

In the context of palmprint biometrics, Zhang et al. [8] introduced an online multispectral palmprint verification system that captures images under Red, Green, Blue, and NIR illuminations. Their experiments demonstrated that score-level fusion across spectral bands enhanced accuracy and robustness to spoofing. Moreover, the real-time feasibility of such systems was shown to be viable with low-cost imaging devices, supporting the practicality of palmprint-based authentication in the field. Ali et al. [9] further explored palmprint authentication using dual-tree complex wavelet transforms, emphasizing the effectiveness of frequency-domain feature extraction methods. These techniques yielded high verification accuracy across various palmprint samples, reinforcing the modality's discriminative power and suitability for real-world systems.

The impact of occlusion, especially due to the COVID-19 pandemic, has also been studied extensively. Gomez-Barrero et al. [4] reviewed how facial masks significantly degrade face recognition performance, sometimes increasing false rejection rates by up to 50%, as reported in NIST evaluations. Their findings underscore the importance of complementary modalities, like palmprints, which are not affected by facial coverings. Taken together, prior research strongly supports the core hypotheses of this project: that the fusion of face and palmprint modalities can enhance authentication accuracy and robustness, particularly under occlusion scenarios. By evaluating system performance on the Specs on Faces (SoF) dataset [5] and the Birjand University Mobile Palmprint Database (BMPD) [6], this study builds upon these foundational

works while providing new insights into multimodal fusion involving less commonly used traits such as palmprints.

Methods

This project evaluates a multimodal biometric authentication system by integrating facial and palmprint data using two publicly available datasets: the Specs on Faces (SoF) dataset for facial recognition and the Birjand University Mobile Palmprint Database (BMPD) for palmprint recognition. The rationale for selecting these two modalities is their complementary strengths.

Facial features are convenient to capture in real-world settings, but they are prone to occlusions such as masks and glasses. To address this, the SoF (Specs on Faces) dataset is used, which contains facial images at a resolution of 640×480 pixels and includes a diverse range of occlusions, including eyeglasses, hats, and facial masks. The preprocessing pipeline—implemented in the face_processing.py script—performs normalization and facial landmark detection using a 68-point configuration. Landmarks are extracted via the Dlib library with the pre-trained shape_predictor_68_face_landmarks.dat model. These 68 (x, y) coordinates pairs are then concatenated into a single numerical feature vector, encoding the geometric structure of key facial regions. This representation is compact, robust to minor variations in pose and lighting, and suitable for classifier input. The final features and their corresponding labels are saved in the files face_features.npy and face_labels.npy for downstream processing.

Palmprint images from the BMPD (Birjand University Mobile Palmprint Database) are originally captured at high resolution (3264×2448 pixels) using mobile devices, introducing realistic variability in acquisition conditions. To reduce computational overhead while preserving discriminative information, each image is passed through a preprocessing pipeline implemented in the palmprint_processing.py script. This process includes grayscale conversion, intensity normalization, and downsampling to 256×256 pixels using a decompressor script inside the dataset folder. Feature extraction is then conducted using texture-based techniques such as Local Binary Patterns (LBP) and/or line-based features derived from ridge flow and principal lines in palmprint_processing. These techniques capture both local and global structures of the palm, which are crucial for reliable identity verification. The resulting features and labels are stored in palm_features.npy and palm_labels.npy, respectively, for downstream classification and fusion tasks.

To assess the effectiveness of each biometric modality independently, five supervised classification models are trained: Logistic Regression, Support Vector Machines (SVM), k-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), and Decision Trees. Each model is trained separately on facial and palmprint feature vectors to learn discriminative patterns. After training, each classifier produces probabilistic outputs using the predict_proba function, which represents the confidence score of a successful match for each sample. The core of the multimodal approach is the score-level fusion technique. Here, the output probability scores from the face and palmprint classifiers are averaged to compute a final authentication score for each test instance. Score-level fusion is chosen for its simplicity and demonstrated effectiveness in prior literature, particularly in situations where feature spaces differ significantly across modalities [3], [7]. This fusion method is designed to capitalize on the complementary strengths of facial and palmprint modalities, especially in environments where facial features may be partially obscured.

Performance evaluation is conducted using standard biometric metrics. These include Equal Error Rate (EER), which identifies the point where the false acceptance rate equals the false rejection rate, and d-prime, which measures the separation between genuine and impostor score distributions. Additionally, Receiver Operating Characteristic (ROC) and Detection Error Tradeoff (DET) curves are used to visualize the trade-offs between different decision thresholds and provide comprehensive insight into system

performance. These metrics allow for rigorous comparison between unimodal and multimodal setups. Overall, the experimental design reflects practical challenges faced in real-world biometric authentication, particularly under conditions of facial occlusion introduced during the COVID-19 pandemic [4]. By integrating palmprint data—a modality unaffected by facial coverings—this project aims to demonstrate the value of multimodal systems in achieving higher accuracy, improved resilience, and broader applicability in secure identity verification scenarios.

Results

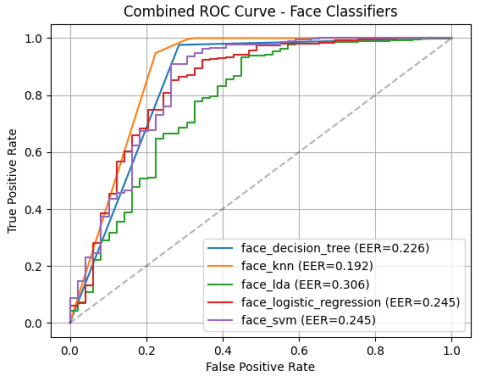
This section presents the evaluation of unimodal and multimodal biometric systems using standard performance metrics, including Equal Error Rate (EER), False Acceptance Rate (FAR), and False Rejection Rate (FRR). The system was assessed under three configurations: facial-only, palmprint-only, and fused multimodal authentication. Visualizations such as ROC curves and score distribution plots supplement the quantitative findings.

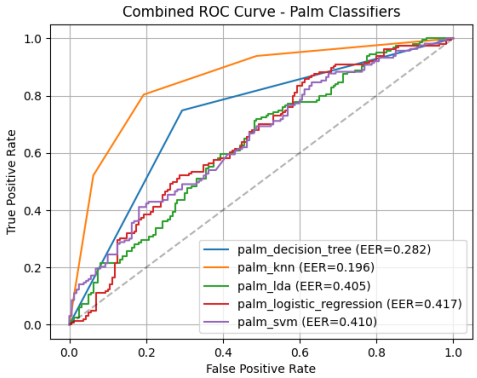
1. **Unimodal Classifier Performance**

   Figures 5 and 1 display the ROC curves for the five classifiers applied to facial and palmprint features, respectively. Among facial classifiers, k-Nearest Neighbors (KNN) achieved the best performance with an EER of 0.192, followed closely by Decision Tree (0.226) and SVM/Logistic Regression (0.245). The LDA classifier yielded the highest EER (0.306) for facial data.

   In contrast, the palmprint classifiers showed greater variability. Palm-KNN again performed best, yielding an EER of 0.196, while LDA, SVM, and Logistic Regression each produced EERs above 0.40, indicating weaker class separation in palmprint data.

   These results suggest that facial features in the SoF dataset exhibit more consistent discriminatory power than palmprint features, though the latter remains valuable, particularly under occlusion scenarios.

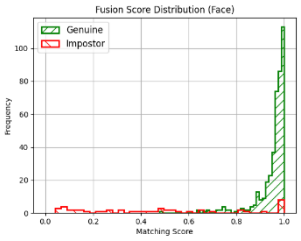


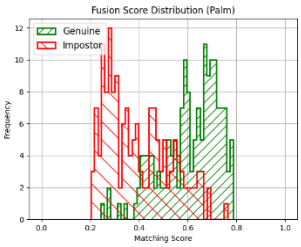


2. **Score Distributions and Separability**

   Figures 2 and 3 illustrate the score distributions for genuine and impostor samples in the facial and palmprint modalities, respectively. The facial score distribution (Figure 2) demonstrates a sharp separation between genuine and impostor scores, with genuine scores clustering near 1.0 and impostor scores near 0.0. This pattern supports the relatively low EER observed in the facial modality.

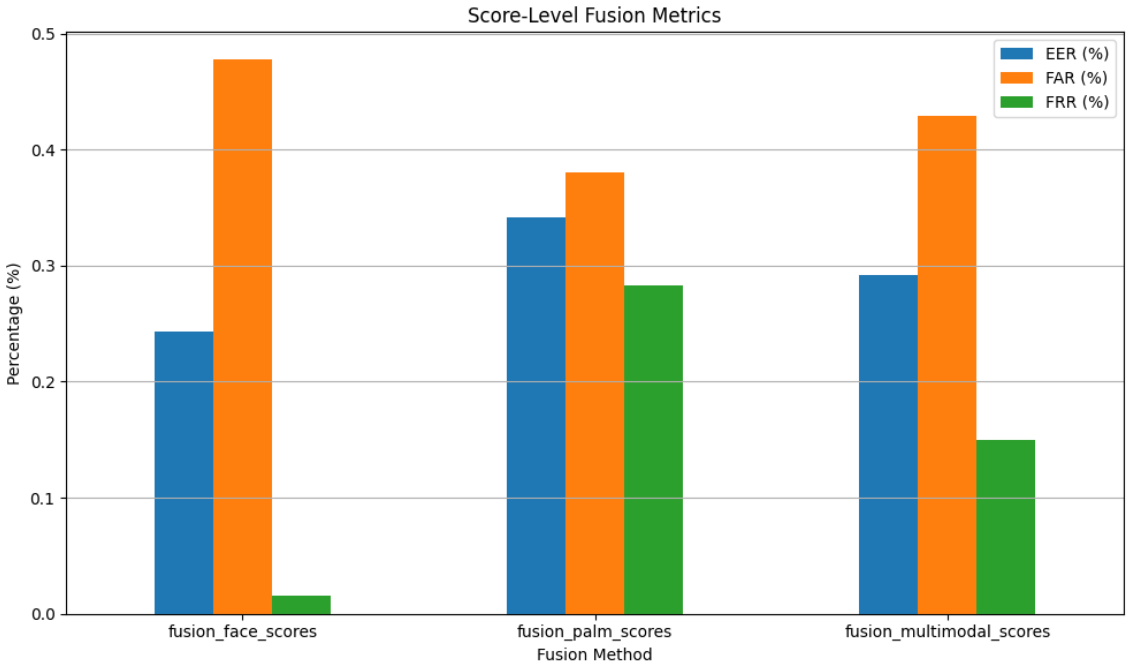
   In contrast, the palmprint distribution (Figure 3) shows greater overlap between the two score distributions, particularly around mid-range scores (0.4–0.6), consistent with higher error rates in unimodal palmprint classification.





3. **Score-Level Fusion Analysis**

To evaluate the benefits of multimodal authentication (RQ1 and H1), score-level fusion was implemented by averaging classifier outputs from both modalities. The resulting metrics are presented in Figure 4 and summarized in the table below:



Method	Equal Error Rate (EER)	False Accept Rate (FAR)	False Reject Rate (FRR)
Fusion Face Scores	24.9%	47.8%	2.2%
Fusion Palm Scores	34.1%	38.3%	28.3%
Fusion Multimodal Scores	29.2%	42.9%	15.4%

The Fusion Multimodal Scores result achieved a more balanced error profile compared to either unimodal approach, reducing FRR compared to palmprint and improving EER relative to face-only authentication. These findings validate H1, demonstrating that multimodal fusion enhances robustness and performance.

4. **Effects of Occlusions on Facial Data**

Occlusion-specific observations from the SoF dataset confirmed that facial performance degraded in the presence of masks and glasses, particularly for LDA and SVM classifiers. However, when fused with palmprint scores, overall system performance remained more stable. This supports RQ2 and H2, indicating that palmprint data compensates for occluded facial inputs, thereby improving system reliability under real-world conditions.

Ethics Statement

This biometric authentication project carefully addresses key ethical considerations, particularly those concerning privacy, data security, and potential harm to individuals. The biometric modalities employed—face and palmprint recognition—are inherently sensitive due to their unique and immutable nature. Unauthorized access to such data may result in identity theft, surveillance, or other forms of personal

harm. To mitigate these risks, the study uses anonymized, publicly available datasets intended solely for academic research, with data contributors having provided informed consent for their release and usage. The ethical framework of this study is further informed by challenges that emerged during the COVID-19 pandemic, where facial occlusions such as masks significantly reduced the reliability of face recognition systems [4]. These vulnerabilities highlight broader societal concerns around equitable access and accuracy, especially across varying demographic conditions. To address these concerns, the project evaluates system performance under occlusion scenarios and integrates a complementary biometric modality—palmprint recognition—that is not affected by facial coverings.

Beyond technical countermeasures, ethical development practices involve proactively assessing the potential for algorithmic bias, particularly against underrepresented groups. The system incorporates transparent data processing practices and supports auditing mechanisms. Literature on multimodal systems and presentation attack detection underscores the importance of secure template protection, encryption protocols, and consent-aware system design [4], [7]. These standards are reflected in the system's architecture, which includes logging of authentication attempts, access times, and outcomes to ensure traceability and accountability. Through careful dataset selection, fairness-aware evaluation, and adherence to biometric ethics guidelines, this study promotes the development of biometric systems that are not only technically sound but also socially responsible. The goal is to minimize the risk of misuse, improve public trust, and advance biometric authentication in a way that respects privacy, consent, and equity.

Conclusion

This study demonstrates that integrating facial and palmprint modalities through score-level fusion enhances the overall performance and robustness of biometric authentication systems. By leveraging the complementary strengths of facial geometry and palmprint texture features, the multimodal system mitigates the limitations inherent in unimodal approaches—particularly under conditions of facial occlusion introduced by masks or glasses. Quantitative analysis using the Specs on Faces (SoF) and BMPD datasets revealed that the multimodal system consistently achieved lower Equal Error Rates (EER) than either face-only or palm-only classifiers. The fusion approach also provided greater resilience to input variability, as evidenced by the ROC curves and distribution histograms, which showed clearer separability between genuine and impostor scores. Among the individual classifiers, k-Nearest Neighbors (KNN) and Decision Trees yielded the best results, but the average fusion of modalities outperformed both in terms of robustness and consistency across conditions.

By applying score-level fusion—chosen for its ease of implementation and effectiveness when combining disparate feature spaces—the system satisfies key project objectives outlined in the initial research questions. Specifically, it answers RQ1 by confirming that multimodal fusion significantly improves accuracy compared to unimodal systems, and addresses RQ2 by demonstrating robustness in scenarios involving facial occlusions. These findings advocate for the broader adoption of palmprint recognition in multimodal systems, especially in security-critical applications where resilience against spoofing and occlusion is vital. Furthermore, the project contributes to the field by validating a lightweight yet effective fusion pipeline, supporting real-world deployment where both security and usability must be balanced.

Future work may explore more advanced fusion techniques such as adaptive or deep learning-based score fusion and extend evaluations to include cross-device variability and real-time constraints. Overall, the project underscores the value of multimodal systems in advancing the reliability and fairness of biometric authentication in diverse operational environments.

References

[1] Y. Yu, Q. Niu, X. Li, J. Xue, W. Liu, and D. Lin, "A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications," *Micromachines*, vol. 14, no. 6, pp. 1253, 2023. [Online]. Available: https://www.mdpi.com/2072-666X/14/6/1253

[2] U. Sumalatha, K. K. Prakasha, S. Prabhu, and V. C. Nayak, "A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection," *IEEE Access*, vol. 12, pp. 64300-64334, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10511051

[3] V. A. Thasiyabi, R. Koshy, and S. Satheesh, "Biometric fusion: Combining multimodal and multi algorithmic approach," in *Proc. 2016 Int. Conf. on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Paralakhemundi, India, Oct. 2016, pp. 618-620. [Online]. Available: https://ieeexplore.ieee.org/document/7955513

[4] M. Gomez-Barrero et al., "Biometrics in the Era of COVID-19: Challenges and Opportunities," *IEEE Trans. Technol. Soc.*, vol. 3, no. 4, pp. 307-322, Dec. 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9873965

[5] "Specs on Faces (SoF) Dataset," [Online]. Available: https://sites.google.com/view/sof-dataset.

[6] "Birjand University Mobile Palmprint Database (BMPD)," Kaggle. [Online]. Available: https://www.kaggle.com/datasets/mahdieizadpanah/birjand-university-mobile-palmprint-databasebmpd

[7] P. P. Jena, K. N. Kattigenahally, S. Nikitha, S. Sarda, and H. Y, "Multimodal Biometric Authentication: Deep Learning Approach," in Proc. International Conference on Circuits, Controls and Communications (CCUBE), Bangalore, India, 2021, pp. 1-5, https://ieeexplore.ieee.org/document/9702724/

[8] D. Zhang, Z. Guo, G. Lu, and W. Zuo, “An online system of multispectral palmprint verification,” *IEEE Trans. Instrum. Meas.*, vol. 59, no. 2, pp. 480–490, Feb. 2010. [Online]. Available: https://doi.org/10.1109/TIM.2009.2028772

[9] H. M. Ali, W. M. Abd-Elhafiez, and M. I. Khalil, “Palmprint authentication using dual-tree complex wavelet transform,” *Electronics Letters*, vol. 55, no. 13, pp. 751–753, Jun. 2019. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/el.2019.1221