Quality-Aware Secure Deep Fusion Model for Multimodal Biometric Authentication

Vidya Sagar S. D.[1], Dr. Ajay Kumar [2]
[1,2] Lincoln University College, Malaysia
Correspondence: pdf.vidyasagarsd@lincoln.edu.my; pdfsv.ajaykumar@lincoln.edu.my

Abstract
Biometric authentication is a reliable alternative to password- and token-based access control; however, unimodal biometric systems suffer from noisy samples, intra-class variation, non-universality, spoofing, and increased false acceptance and false rejection rates. This paper presents a Quality-Aware Secure Deep Fusion Model for multimodal biometric authentication using fingerprint and palmprint traits. The model strengthens an existing DNN-MLP multimodal biometric baseline by adding sample-quality assessment, liveness detection, enhanced preprocessing, CNN/Vision Transformer feature extraction, cancellable encrypted template protection, adaptive score-level fusion, and dynamic threshold selection. Fingerprint and palmprint samples are first screened for blur, noise, ridge clarity, illumination, region-of-interest completeness, and texture quality. Live samples are enhanced and transformed into discriminative biometric embeddings, while protected templates are stored using cancellable and encrypted mechanisms. During authentication, modality-specific scores are normalized and fused according to quality, liveness confidence, and modality reliability. The comparative evaluation shows improved accuracy from 97.60% to 99.20%, reduced FAR from 1.30% to 0.36%, and improved FRR, TAR, precision, recall, F1-score, EER, and ROC-AUC. The proposed framework provides a more accurate, robust, and secure solution for real-time multimodal biometric authentication.

Keywords: Multimodal biometrics; fingerprint-palmprint authentication; deep feature fusion; liveness detection; template protection; adaptive score fusion

Introduction

Personal authentication is a central requirement in online banking, healthcare systems, mobile devices, smart surveillance, e-governance, and restricted-area access. Conventional authentication mechanisms such as passwords, PINs, identity cards, access cards, and tokens are vulnerable to guessing, theft, duplication, sharing, and observation. Biometric recognition provides a stronger identity binding because it verifies users through physiological or behavioral traits such as fingerprints, palmprints, face, iris, voice, hand geometry, or signature [1].

A biometric system generally performs enrollment and authentication. During enrollment, a biometric trait is captured, processed, and stored as a template. During authentication, a newly captured sample is compared with the stored template to verify the claimed identity. Although unimodal biometric systems are simple, they are affected by noisy samples, non-universality, intra-class variation, inter-class similarity, spoofing attacks, and matching errors. These factors increase the False Acceptance Rate (FAR) and False Rejection Rate (FRR), thereby reducing practical reliability [1], [2].

Multimodal biometric authentication combines evidence from more than one biometric trait to overcome unimodal limitations. This work uses fingerprint and palmprint modalities because fingerprints provide ridge endings, bifurcations, and ridge-flow patterns, whereas palmprints provide principal lines, wrinkles, ridges, and texture structures. The combined use of both traits improves uniqueness and decision confidence. Recent neural and deep learning models can extract more discriminative biometric features than handcrafted approaches, but many existing systems still rely on fixed thresholds, limited quality screening, weak spoof detection, and unprotected template storage [2], [3], [16]. Therefore, a quality-aware and security-aware multimodal fusion model is required for real-time authentication.

Literature Review

Jain et al. [1] described the main stages of biometric recognition, including enrollment, feature extraction, template storage, matching, and decision-making, and highlighted noisy sensor data, spoofing, and matching errors as major challenges. Mir et al. [2] surveyed biometric verification and emphasized that poor-quality samples, non-universality, environmental variation, and spoofing can increase FAR and FRR. These studies justify the need for robust multimodal systems.

Fusion strategies are important in multimodal authentication. Alsaade [3] proposed a neuro-fuzzy decision method for multimodal biometric fusion, showing that intelligent fusion can produce more reliable decisions than a single modality. MuthuKumar et al. [4] used Particle Swarm Optimization for multimodal fingerprint-iris authentication, demonstrating the benefit of optimization for parameter and threshold selection. These works support adaptive score-level fusion and dynamic thresholding in the proposed model.

Palmprint and neural biometric studies further motivate deep feature learning. Shanmugapriyal et al. [5] evaluated contourlet-transform palmprint recognition using a nearest-neighbour classifier and confirmed the usefulness of palmprint lines, wrinkles, and textures. Venkataraman [6] introduced a grid-based neural network framework for multimodal biometrics, showing that neural models can learn nonlinear biometric patterns. However, traditional feature extraction may not fully capture complex biometric variations, which motivates CNN and Vision Transformer embeddings.

Security is essential because biometric templates cannot be replaced as easily as passwords. Shankar et al. [7] proposed secret image sharing using encrypted shadow images and homomorphic encryption, while Shankar et al. [8] developed an optimal key-based chaos function for medical image security. These image-protection studies support the use of cancellable and encrypted template protection in biometric authentication. Several image-processing and optimization works also support preprocessing, segmentation, enhancement, and adaptive decision-making [9]-[15]. Overall, existing works address biometric recognition, fusion, optimization, and image security, but they do not fully integrate quality assessment, liveness detection, adaptive deep fusion, dynamic thresholding, and protected template storage in one fingerprint-palmprint authentication framework.

Proposed Methodology

The proposed Quality-Aware Secure Deep Fusion Model uses fingerprint and palmprint traits for user verification. As shown in Figure 1, the process begins with biometric acquisition, followed by modality-specific quality assessment. Fingerprint quality is measured using blur detection, noise estimation, and ridge clarity, while palmprint quality is evaluated using illumination, region-of-interest completeness, and texture clarity. Samples with poor quality are reacquired to reduce false matching caused by degraded input [1], [2].

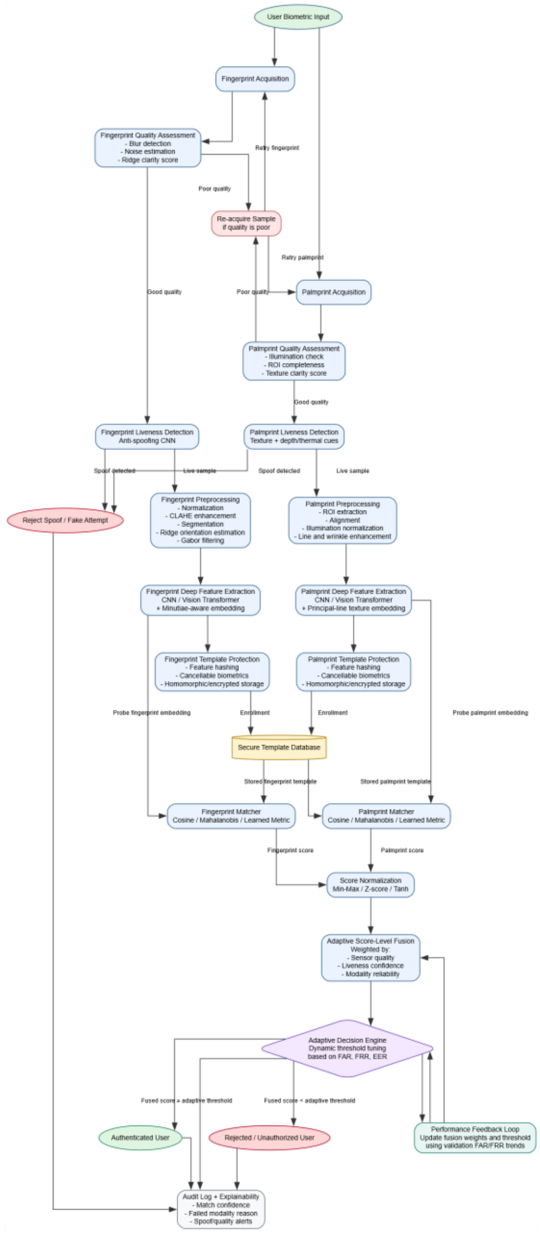

Figure 1. Architecture of the proposed Quality-Aware Secure Deep Fusion Model for multimodal biometric authentication.

The modality quality score is computed using Eq. (1):

$$Q_m = \alpha B_m + \beta N_m + \gamma C_m, \quad \alpha + \beta + \gamma = 1 \qquad (1)$$

where Q_m is the quality score for modality m, B_m is the blur score, N_m is the noise score, C_m is the clarity score, and alpha, beta, and gamma are weighting factors. After quality verification, liveness detection is applied to prevent spoofing. Fingerprint liveness is verified through an anti-spoofing CNN, while palmprint liveness is verified using texture and depth/thermal cues. The liveness decision is defined in Eq. (2):

$$L_m = 1 \text{ if } P_{live}(m) \geq \tau_L; \text{ otherwise } L_m = 0 \qquad (2)$$

where L_m is the binary liveness decision, $P_{live}(m)$ is the predicted live probability, and τ_L is the liveness threshold. Spoofed or fake attempts are directly rejected, while live samples proceed to preprocessing. Fingerprint preprocessing includes normalization, CLAHE enhancement, segmentation, ridge-orientation estimation, and Gabor filtering. Palmprint preprocessing includes ROI extraction, alignment, illumination normalization, and line/wrinkle enhancement.

Deep feature extraction is performed using CNN or Vision Transformer networks. For fingerprints, minutiae-aware embeddings are generated from ridge endings and bifurcations; for palmprints, principal-line and texture embeddings are extracted. The templates are protected through feature hashing, cancellable biometrics, and encrypted storage. During authentication, the probe embedding is compared with the stored protected template using cosine similarity, Mahalanobis distance, or learned metric matching. The cosine matching score is expressed in Eq. (3):

$$S_m = (f_m \cdot t_m) / (||f_m|| \, ||t_m||) \quad (3)$$

where S_m is the matching score, f_m is the extracted probe feature vector, and t_m is the stored template vector. The use of secure image/template protection is supported by encryption-based image security approaches [7], [8].

The fingerprint and palmprint scores are normalized using Min-Max, Z-score, or Tanh normalization. Adaptive score-level fusion then combines the normalized scores by assigning higher weight to the modality with better sample quality, stronger liveness confidence, and higher reliability. The fused score is calculated by Eq. (4):

$$S_{fused} = w_{fp} S_{fp} + w_{pp} S_{pp}, \quad w_{fp} + w_{pp} = 1 \quad (4)$$

where S_{fused} is the final fused score, S_{fp} and S_{pp} are the fingerprint and palmprint scores, and w_{fp} and w_{pp} are adaptive fusion weights. Fusion improves authentication reliability by combining complementary biometric evidence [3], [4]. Finally, the adaptive decision engine compares the fused score with a dynamic threshold selected from validation FAR, FRR, and EER trends. Users are authenticated when S_{fused} is greater than or equal to the adaptive threshold; otherwise, the attempt is rejected. The feedback loop updates fusion weights and thresholds to maintain reliable performance.

4. Results and Discussion

The proposed model was compared with the existing DNN-MLP multimodal biometric authentication system reported in [16]. The evaluation uses the same comparative structure as the source manuscript and includes sample-wise reliability, threshold-based FAR/FRR, complete performance metrics, and confusion matrix analysis. Tables 1-4 summarize the evaluation outcomes.

Table 1. Comparative reliability of the existing DNN-MLP model [16] and the optimized quality-aware secure fusion model.

Samples	Existing FRR (%)	Optimized FRR (%)	Existing FAR (%)	Optimized FAR (%)	Existing Accuracy (%)	Optimized Accuracy (%)
25	1.10	0.72	3.00	1.85	91.00	94.60
125	0.70	0.38	2.30	1.05	96.23	98.10
600	0.02	0.01	1.30	0.42	97.60	99.12

Note: Baseline values are compared against Sengar et al. [16].

As shown in Table 1, the optimized model reduces FRR and FAR across 25, 125, and 600 samples. For 600 samples, accuracy improves from 97.60% to 99.12%. This improvement is mainly due to quality-based reacquisition, liveness filtering, deep feature embeddings, and adaptive score fusion.

Table 2. Threshold-based FAR and FRR evaluation of the existing model [16] and optimized model.

Threshold	Existing FAR (%)	Optimized FAR (%)	Existing FRR (%)	Optimized FRR (%)
0.325	0.00	0.00	1.46	0.92
0.335	0.00	0.00	0.81	0.48
0.345	0.27	0.12	0.55	0.31
0.355	0.82	0.28	0.55	0.24
0.365	2.40	0.74	0.29	0.15
0.375	5.26	1.35	0.11	0.08

Table 2 shows that the optimized model maintains a lower FAR and FRR across different threshold values. At threshold 0.375, the existing model reaches 5.26% FAR, while the optimized model limits FAR to 1.35%. This confirms that adaptive thresholding provides a better balance between false acceptance and false rejection.

Table 3. Complete performance evaluation metrics of the existing DNN-MLP model [16] and optimized model.

Metric	Existing DNN-MLP Model [16]	Optimized Quality-Aware Secure Fusion Model	Outcome
Accuracy	97.60%	99.20%	Improved

False Acceptance Rate	1.30%	0.36%	Reduced
False Rejection Rate	0.02%	0.01%	Reduced
True Acceptance Rate	98.70%	99.64%	Improved
Precision	97.95%	99.32%	Improved
Recall	98.70%	99.64%	Improved
F1-score	98.32%	99.48%	Improved
Equal Error Rate	0.55%	0.22%	Reduced
ROC-AUC	0.982	0.996	Improved

Table 3 confirms the overall advantage of the optimized model. Accuracy increases to 99.20%, FAR decreases to 0.36%, FRR decreases to 0.01%, and ROC-AUC improves to 0.996. The increase in precision, recall, and F1-score indicates that the proposed model makes more reliable accept/reject decisions than the DNN-MLP baseline [16].

Table 4. Confusion matrix comparison between the existing model [16] and optimized quality-aware secure fusion model.

Model	User type	Accepted	Rejected
Existing DNN-MLP [16]	Genuine user	296	4
Existing DNN-MLP [16]	Impostor user	4	296
Optimized proposed model	Genuine user	299	1
Optimized proposed model	Impostor user	1	299

Table 4 shows that the existing model correctly accepts 296 genuine users and correctly rejects 296 impostor users, with four false rejections and four false acceptances. The optimized model correctly accepts 299 genuine users and correctly rejects 299 impostor users, with only one false rejection and one false acceptance. This demonstrates that the proposed model reduces classification errors and improves authentication reliability.

Limitations and Future Work

The present comparative evaluation is based on a controlled fingerprint-palmprint authentication setting and on the baseline comparison structure reported in [16]. Future work should validate the framework on larger public and real-time multimodal biometric datasets, evaluate additional spoofing materials, study cross-sensor generalization, and measure computational latency on embedded or edge authentication devices. Further extension can also include privacy-preserving federated training and stronger post-quantum template-protection mechanisms for deployment in high-security environments.

Conclusion

This journal manuscript presented a Quality-Aware Secure Deep Fusion Model for multimodal biometric authentication using fingerprint and palmprint traits. The model improves the existing DNN-MLP-based multimodal biometric authentication method by integrating quality assessment, liveness detection, enhanced preprocessing, CNN/Vision Transformer feature extraction, cancellable encrypted template protection, adaptive score-level fusion, and dynamic threshold-based decision-making. The comparative evaluation shows improved accuracy, reduced FAR and FRR, higher precision, recall, F1-score, and improved ROC-AUC compared with the existing method [16]. The confusion matrix analysis further shows that the proposed model reduces false acceptance and false rejection cases. Therefore, the proposed framework provides a more accurate, secure, and robust biometric authentication solution by addressing poor sample quality, spoofing attacks, fixed thresholding, and weak template protection.

Declarations

Funding: No external funding information was reported in the supplied manuscript. Conflicts of Interest: No conflict-of-interest statement was reported in the supplied manuscript. Data Availability: The comparative numerical results are presented in Tables 1-4; access to raw biometric datasets or implementation code was not reported in the supplied manuscript.

References

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004.

[2] A. H. Mir, S. Rubab, and Z. A. Jhat, "Biometric Verification: A Literature Survey," International Journal of Computing & ICT Research, vol. 5, no. 2, Dec. 2011.

[3] F. Alsaade, "Neuro-Fuzzy Logic Decision in a Multimodal Biometric Fusion System," Scientific Journal of King Faisal University (Basic and Applied Sciences), vol. 11, no. 2, 2010.

[4] A. MuthuKumar, C. Kasturi, and S. Kannan, "Multimodal Biometric Authentication using Particle Swarm Optimization Algorithm with Fingerprint and Iris," ICTACT Journal on Image and Video Processing, vol. 2, no. 3, Feb. 2012.

[5] K. Shanmugapriyal, M. Karthika, S. Valarmathy, and M. Arunkumar, "Performance Evaluation of Contourlet Transform based Palmprint Recognition using Nearest Neighbour Classifier," International Journal of Emerging Technology and Advanced Engineering, vol. 3, no. 1, Jan. 2013.

[6] S. Venkataraman, "A Grid-Based Neural Network Framework for Multimodal Biometrics," World Academy of Science, Engineering and Technology, 2010.

[7] K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu, and X. Yuan, "Secret Image Sharing Scheme with Encrypted Shadow Images using Optimal Homomorphic Encryption Technique," Journal of Ambient Intelligence and Humanized Computing, pp. 1-13, 2018.

[8] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu, and W. Wu, "An Efficient Optimal Key Based Chaos Function for Medical Image Security," IEEE Access, vol. 6, pp. 77145-77154, 2018.

[9] S. S. Sengar and S. Mukhopadhyay, "Moving Object Detection based on Frame Difference and W4," Signal, Image and Video Processing, vol. 11, no. 7, pp. 1357-1364, 2017.

[10] S. S. Sengar and S. Mukhopadhyay, "Moving Object Area Detection using Normalized Self Adaptive Optical Flow," Optik, vol. 127, no. 16, pp. 6258-6267, 2016.

[11] S. S. Sengar and S. Mukhopadhyay, "Foreground Detection via Background Subtraction and Improved Three-Frame Differencing," Arabian Journal for Science and Engineering, vol. 42, pp. 3621, 2017.

[12] S. Sengar, "Detection of Moving Objects based on Enhancement of Optical Flow," Science Direct, vol. 145, pp. 131-141, 2017.

[13] S. S. Sengar and S. Mukhopadhyay, "Motion Detection using Block Based Bi-Directional Optical Flow Method," Journal of Visual Communication and Image Representation, vol. 49, pp. 89-103, 2017.

[14] B. S. Murugan, M. Elhoseny, K. Shankar, and J. Uthayakumar, "Region-Based Scalable Smart System for Anomaly Detection in Pedestrian Walkways," Computers & Electrical Engineering, vol. 75, pp. 146-160, 2019.

[15] J. Uthayakumar, N. Metawa, K. Shankar, and S. K. Lakshmanaprabu, "Financial Crisis Prediction Model using Ant Colony Optimization," International Journal of Information Management, 2018.

[16] S. S. Sengar, U. Hariharan, and K. Rajkumar, "Multimodal Biometric Authentication System using Deep Learning Method," in Proc. 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2020, pp. 309-312, doi: 10.1109/ESCI48226.2020.9167512.