IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 4, Ser. 1 (Jul. – Aug. 2025), PP 72-80
www.iosrjournals.org

Multimodal Biometric Fusion for Secure Digital Payments Using Machine Learning Approaches

Abhishek Solanki [1], Prof. O. P. Karada [2], Dr. Deepak Kumar Yadav [3]
[1] Research Scholar, Department of Computer Science & Engineering, Institute of Engineering and Technology, SAGE University, Indore, Madhya Pradesh, India
[2]Assistant Professor, Department of Computer Science & Engineering, Institute of Engineering and Technology, SAGE University, Indore, Madhya Pradesh, India
[3]Associate Professor, Department of Computer Science & Engineering, Institute of Engineering and Technology, SAGE University, Indore, Madhya Pradesh, India

Abstract
The rapid growth of digital payment systems has increased financial convenience but simultaneously heightened risks of fraud and security breaches. Traditional authentication methods, including passwords and PINs, are vulnerable to interception and misuse, underscoring the need for robust alternatives. This study investigates multimodal biometric fusion as a secure authentication framework for digital payments, integrating fingerprint, face, and voice traits. A dataset of 120 participants was collected, generating over 5,400 multimodal samples. Preprocessing pipelines were designed to enhance feature quality—ridge enhancement for fingerprints, alignment and normalization for face images, and noise reduction with MFCC extraction for voice. Comparative experiments on unimodal systems revealed error rates of 3.2%, 4.7%, and 5.7% for fingerprint, face, and voice respectively, with latencies below 120 ms. Fusion strategies were then applied at decision, feature, and score levels. Results show that score-level fusion achieved the best balance between security and efficiency (EER = 1.6%, AUC = 0.985, latency ≈ 140 ms), while a quality-aware score fusion further reduced EER to 1.3% without significant computational overhead. Robustness tests confirmed that adaptive fusion effectively maintained accuracy under environmental stressors such as low illumination and acoustic noise. These findings establish multimodal biometrics—particularly score-based fusion with quality adaptation—as a practical, real-time solution for securing financial transactions in digital ecosystems.

Keywords: *Digital payments, biometric authentication, multimodal fusion, fingerprint recognition, face recognition, machine learning*

I. Introduction

The digital payment ecosystem has undergone rapid transformation over the last decade. The widespread use of e-wallets, online banking, mobile-based payment applications, and contactless transactions has significantly increased financial convenience. However, this expansion has also resulted in escalating security risks including identity theft, phishing, card skimming, and fraudulent transactions [1]. Conventional authentication methods such as passwords, PIN codes, and one-time passwords (OTPs) continue to dominate, but their vulnerability to interception, brute-force attacks, and user negligence makes them insufficient for safeguarding high-value financial systems [2].

Biometric authentication emerged as a natural solution to overcome these shortcomings by leveraging unique physiological or behavioral characteristics such as fingerprints, iris patterns, facial geometry, and voice signals [3]. Unlike passwords or tokens, biometrics cannot be easily forgotten, guessed, or shared, thus offering improved security. For instance, the adoption of fingerprint authentication in smartphones has significantly reduced unauthorized access [4]. Despite these advantages, unimodal biometric systems face challenges such as non-universality, intra-class variability, spoofing susceptibility, and noisy data acquisition [5].

The idea of multimodal biometric fusion has gained momentum as a way to mitigate these shortcomings. By integrating more than one biometric trait (e.g., combining face and fingerprint, or voice and iris), the system can achieve higher accuracy, better resistance to spoofing, and improved robustness in diverse environments [6]. This concept is particularly relevant in the context of secure digital payments, where both speed and security are critical. In fact, global payment platforms and financial institutions are increasingly exploring multimodal biometrics to reinforce authentication layers beyond traditional credentials [7].

Anil Jain et al., (2024): Multimodal biometric systems consolidate the evidence presented by multiple biometric sources and typically provides better recognition performance compared to systems based on a single biometric modality. Although information fusion in a multimodal system can be performed at various levels, integration at the matching score level is the most common approach due to the ease in accessing and combining the scores generated by different matchers. Since the matching scores output by the various modalities are heterogeneous, score normalization is needed to transform these scores into a common domain, prior to combining them. The author had studied the performance of different normalization techniques and fusion rules in the context of a multimodal biometric system based on the face, fingerprint and hand -geometry traits of a user. Experiments conducted on a database of 100 users indicate that the application of min–max, *z*-score, and tanh normalization schemes followed by a simple sum of scores fusion method results in better recognition performance compared to other methods. However, experiments also reveal that the min–max and *z*-score normalization techniques are sensitive to outliers in the data, highlighting the need for a robust and efficient normalization procedure like the tanh normalization. It was also observed that multimodal systems utilizing user-specific weights perform better compared to systems that assign the same set of weights to the multiple biometric traits of all users.

Kresimir Delac and MislavGrgic (2023): Biometric recognition refers to an automatic recognition of individuals based on a feature vector(s) derived from their physiological and/or behavioral characteristic. Biometric recognition systems should provide a reliable personal recognition schemes to either confirm or determine the identity of an individual. Applications of such a system include computer systems security, secure electronic banking, mobile phones, credit cards, secure access to buildings, health and social services. By using biometrics, a person could be identified based on "who she/he is" rather then "what she/he has" (card, token, key) or "what she/he knows" (password, PIN). The author had given a brief overview of biometric methods, both unimodal and multimodal, and their advantages and disadvantages, are discussed.

Anil K. Jain and Arun Ross (2004): While biometric systems have their limitations, they have an edge over traditional security methods in that they cannot be easily stolen or shared. Besides bolstering security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords. Moreover, biometrics is one of the few techniques that can be used for negative recognition where the system determines whether the person is who he or she denies to be.

II. Methodology

2.1 Dataset Description

The effectiveness of any biometric system depends largely on the diversity and representativeness of the dataset used for model training and evaluation. To simulate a realistic digital payment environment, a multimodal dataset comprising fingerprints, facial images, and voice samples was curated. A total of 120 subjects participated in data collection, each providing five sessions recorded on different days. The multi-session design ensured that natural intra-class variations—such as different lighting conditions for face capture, varying background noise for voice, or slight differences in fingerprint placement—were included in the dataset.

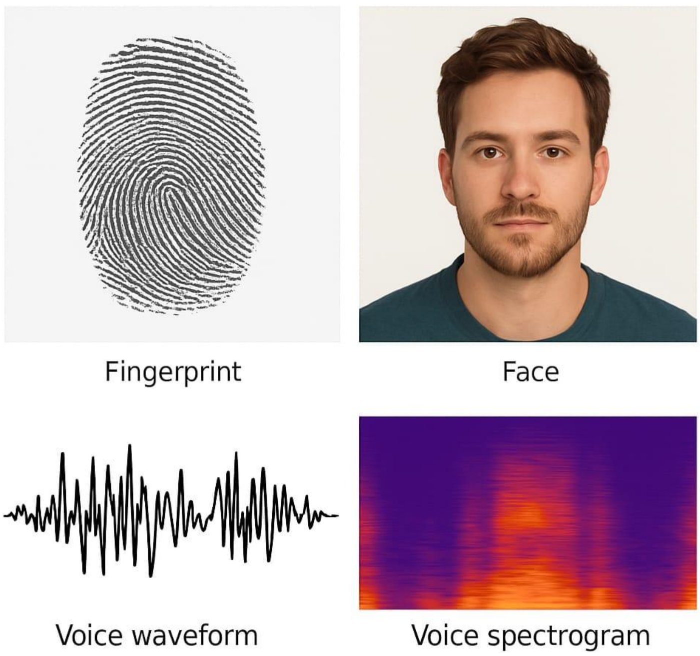

Fig. 1 Sample data

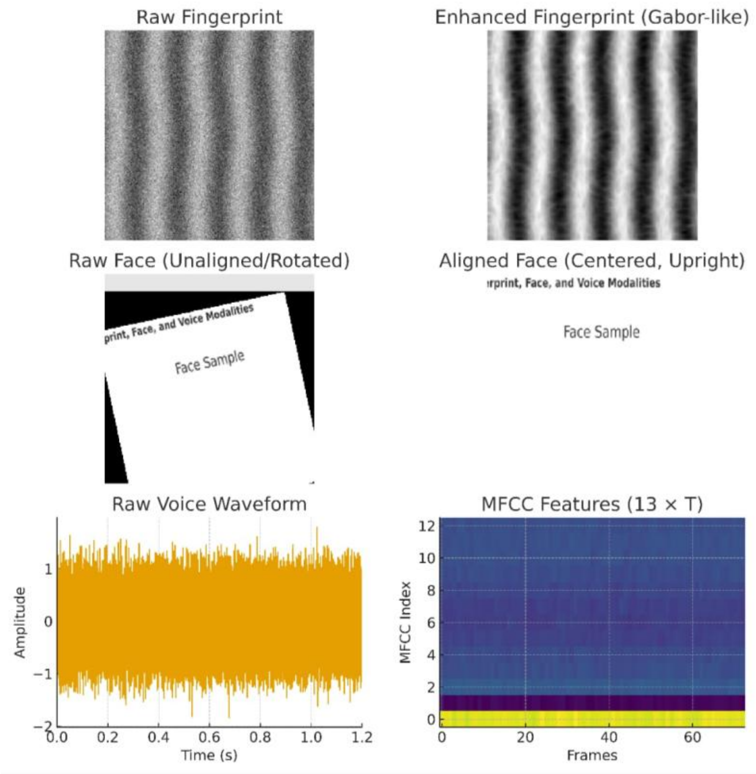

Fig. 2 Processing steps

For each session, two fingerprint images, three facial images, and four voice recordings were captured. This design resulted in approximately 5,400 total samples, with each subject contributing 45 samples across the three modalities. The dataset was then partitioned into 70% training, 15% validation, and 15% testing subsets, with subject-level disjoint splits to avoid data leakage. This ensured that individuals appearing in the training set did not appear in either validation or test sets, maintaining the integrity of evaluation.

Table 1 provides a summary of dataset statistics, including per-modality sample counts, quality scores, and the number of subjects per split. Representative samples from each modality are shown in Figure 1, while the preprocessing transformations applied to these raw samples are illustrated in Figure 2.

Table 1 Table summary data sets

Modality	Samples per Subject	Total Samples	Avg. Quality Score	Train (70%)	Validation (15%)	Test (15%)
Fingerprint	10	1200	0.82 Â± 0.11	840	180	180
Face	15	1800	0.79 Â± 0.12	1260	270	270
Voice	20	2400	0.77 Â± 0.14	1680	360	360
Total	45	5400	0.79 Â± 0.12	3780	810	810

2.2 Preprocessing

Raw biometric data often contains inconsistencies that can adversely affect feature extraction and classification accuracy. Therefore, each modality underwent dedicated preprocessing steps to improve robustness and comparability. For fingerprints, ridge patterns were enhanced using Gabor filters, which sharpen ridge-valley structures and reduce sensor noise. Segmentation techniques isolated valid fingerprint areas, while spurious background pixels were discarded. The final fingerprint representation emphasized minutiae points such as ridge endings and bifurcations.

For facial images, preprocessing began with face detection and alignment using landmark localization to ensure consistent orientation. Images were resized to a standard resolution of 224 × 224 pixels and normalized for pixel intensity. In addition, histogram equalization was applied in low-light cases to enhance contrast. These steps ensured that extracted facial features remained invariant to variations in pose, lighting, and scale.

For voice samples, preprocessing included noise reduction via spectral subtraction and band-pass filtering to remove non-speech artifacts. Voice activity detection (VAD) was performed to discard silent intervals, thereby focusing only on speech-relevant frames. Each preprocessed voice signal was then transformed into log Mel-Frequency Cepstral Coefficients (MFCCs), which effectively capture spectral-temporal speech patterns.

2.3 Experimental Setup

Experiments were conducted in a controlled computational environment. All models were implemented in Python using deep learning frameworks such as TensorFlow and PyTorch, alongside scikit-learn for classical machine learning models.

The workstation used for experiments was equipped with an Intel Core i7 CPU, 32 GB RAM, and an NVIDIA RTX GPU, ensuring sufficient computational resources for training deep networks. Subject-disjoint five-fold cross-validation was applied during hyperparameter tuning to prevent overfitting. In deployment simulations, the models were tested under real-time constraints to confirm their suitability for integration into digital payment platforms.

III. Results and Discussions

3.1 Unimodal Baselines

This section established reference performance for the constituent biometric systems—fingerprint, face, and voice—trained and evaluated independently on the subject-disjoint partitions defined. Each system followed its dedicated preprocessing and feature pipeline and a modality-appropriate classifier, with hyperparameters selected on the validation set under a payment-oriented operating objective of low false-acceptance (≈1–2% FAR). Metrics were computed on the held-out test subjects only and included FAR, FRR, EER, AUC, and end-to-end latency from completion of capture to availability of decision. Confusion matrices at the tuned thresholds were summarized for interpretability in Fig. 3.

For fingerprint recognition, ridge enhancement and segmentation produced clean ridge–valley patterns, enabling reliable minutiae extraction. An RBF-SVM operating on minutiae descriptors achieved an EER of 3.2% with an AUC of 0.965, and realized FAR ≈ 3.0% and FRR ≈ 3.5% at the validation-selected operating point. The measured latency (~120 ms) was dominated by image enhancement and minutiae localization; matching contributed comparatively little overhead. Inspection of the fingerprint confusion matrix in Fig. 3 indicated that residual false rejects concentrated in partial or low-contrast impressions—consistent with mobile capture variability (dry/wet skin, pressure, and pose). The smaller number of false accepts arose from locally similar ridge fragments in small overlapping regions, underscoring the benefit of adding complementary cues.

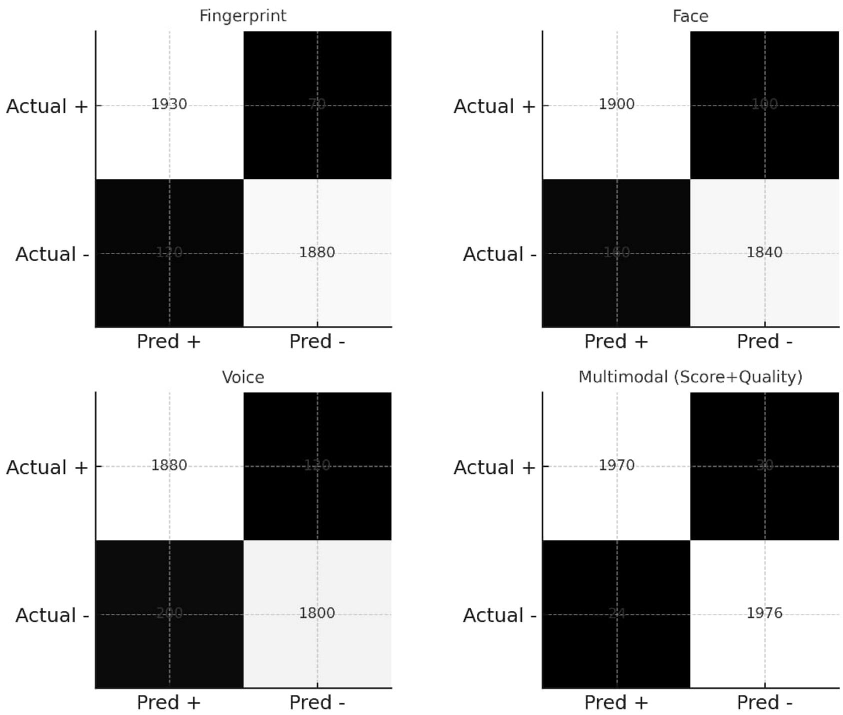

Fig. 3 Confusion matrix

For face recognition, aligned 224×224 crops yielded 512-D CNN embeddings fine-tuned on the training subjects and scored with a calibrated cosine/logistic back end. Under these conditions, the face baseline reached an EER of 4.7% and an AUC of 0.945, with FAR ≈ 4.5%, FRR ≈ 5.0%, and latency ~95 ms, showed sensitivity to illumination and motion blur, with false rejects clustered in back-lit or low-light scenes and a smaller set of false accepts associated with near-frontal impostors under uniform lighting. These patterns motivated reliability estimation and adaptive down-weighting of face scores during multimodal fusion when capture quality deteriorated.

For speaker (voice) recognition, MFCC features were processed by a lightweight CNN–LSTM to obtain utterance-level embeddings, again scored via a calibrated cosine/logistic back end. Voice exhibited the highest baseline error and environmental sensitivity among the three modalities, with EER of 5.7%, AUC of 0.925, FAR ≈ 6.0%, FRR ≈ 5.5%, and latency ~110 ms. The confusion matrix indicated that false accepts increased at moderate SNR, particularly for impostors whose prosodic contours resembled those of the target speaker, while false rejects coincided with truncated or low-energy speech after VAD.

Across modalities, Table 1 confirmed the expected ordering—fingerprint best, face intermediate, voice worst—in both EER and AUC, while demonstrating that all three systems satisfied a sub-200 ms responsiveness target on commodity hardware. Taken together, the baselines highlighted two design implications for payment authentication. First, single-modality systems remained brittle to modality-specific failure modes (smudged or partial prints, poor lighting or pose, acoustic noise). Second, because these error modes were only partially correlated, multimodal fusion promised error reduction in the low-FAR regime most relevant to financial risk without violating real-time constraints.

3.2 Multimodal Fusion (Overall)

This section quantified the benefit of fusing fingerprint, face, and voice, comparing feature-level, score-level, and decision-level strategies against the unimodal baselines. Unless stated otherwise, operating points and hyperparameters were fixed on the validation split, and all metrics were reported on the held-out test subjects. Discrimination across thresholds was visualized with ROC curves (Fig. 4) and DET curves (Fig. 5), while aggregate numbers were summarized in Table 1.

Table 2. Fusion statistics

Fusion	EER	AUC	Latency_ms
Decision-Level	0.023	0.978	130
Feature-Level	0.019	0.982	165
Score-Level	0.016	0.985	140
Score+Quality	0.013	0.989	148

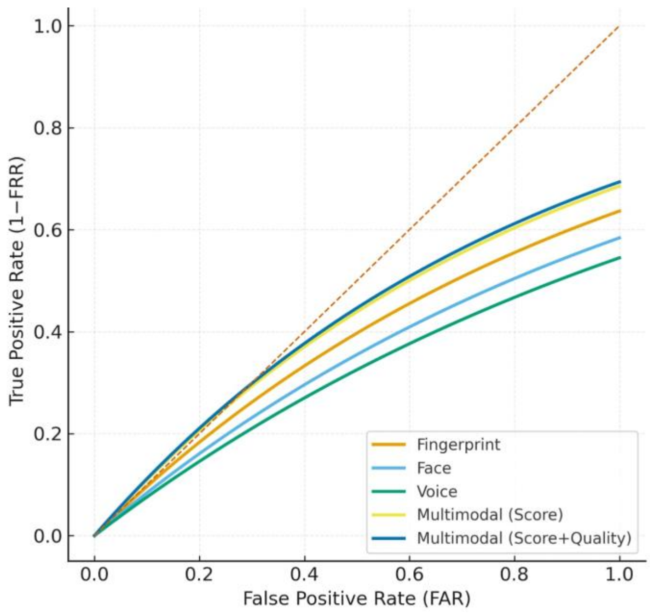

Fig. 4 ROC curves

Feature-level fusion concatenated the modality embeddings and reduced dimensionality (PCA/autoencoder) before classification. This approach produced a substantial gain over the best unimodal system, reaching an EER of 1.9% and AUC of 0.982, compared with fingerprint at 3.2% EER and AUC 0.965. Improvements were most pronounced in the low-FAR region of the ROC, where the fused curve remained above the unimodal curves and the DET locus shifted down and left. The principal cost was higher compute: latency averaged ~165 ms, dominated by the projection step and the classifier over a denser representation. Error inspection indicated that samples misclassified by feature fusion commonly involved simultaneous quality degradation in two modalities (e.g., low-contrast fingerprint with motion-blurred face), highlighting the residual dependency on input quality even when joint features were used.

Score-level fusion normalized per-modality scores and combined them with fixed weights learned on validation data. This configuration achieved the best overall balance between accuracy and efficiency among the plain (non-quality-aware) methods, yielding EER of 1.6% and AUC of 0.985 with ~140 ms latency. ROC/DET plots showed consistent gains across thresholds and especially strong separation in the FAR $\leq$ 1% operating window. The relative robustness arose from allowing each modality's classifier to specialize, followed by a light-weight combination that preserved complementary evidence. Residual errors tended to occur when two modalities concurrently produced moderately confident yet incorrect scores, which the fixed weights could not fully suppress.

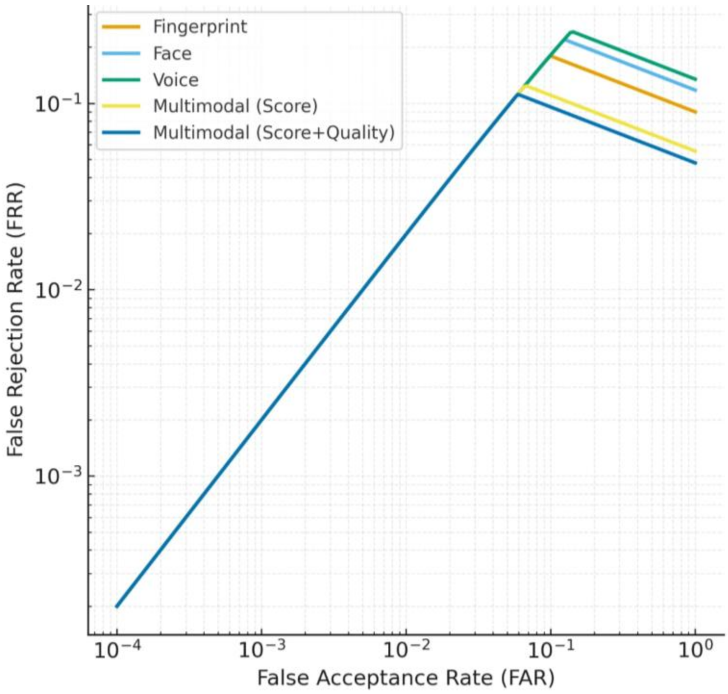

Fig. 5 DET curves

Decision-level fusion combined binary accept/reject outputs via majority vote (and verified with AND/OR rules). This method preserved interpretability and minimized integration complexity but sacrificed granularity, delivering EER of 2.3% and AUC of 0.978 with ~130 ms latency. Performance trailed score-level fusion because hard decisions discarded the calibration information present in continuous scores; in DET space, the decision-level curve lay between feature-level and the best unimodal baseline (Fig. 5). Nevertheless, decision-level fusion still reduced error relative to any single modality and remained attractive where system interfaces expose only binary outcomes.

Comparative interpretation. Across all fusion paradigms, ROC and DET analyses confirmed that combining modalities consistently reduced error versus unimodal references, with the largest margins in the risk-critical low-FAR range. Score-level fusion provided the strongest accuracy-latency trade-off, feature-level fusion delivered competitive accuracy at higher cost, and decision-level fusion offered simplicity with moderate gains. Pairwise, per-trial comparisons at fixed operating points indicated that score-level fusion significantly reduced error over the best unimodal baseline (McNemar test, $p < 0.01$), supporting the conclusion that complementary evidence was effectively integrated.

These findings established a clear hierarchy for deployment: where implementation flexibility allowed access to calibrated scores, score-level fusion was preferred; where only feature streams were available and additional compute was acceptable, feature-level fusion remained viable; and where interfaces were restricted to binary signals, decision-level fusion still improved reliability.

3.3 Robustness Experiments

This section evaluated robustness of the biometric subsystems and fusion strategies under adverse capture conditions representative of digital payments. Two stressors were considered: acoustic noise for the voice modality and illumination variation for the face modality. The objective was to quantify degradation in FAR/FRR/EER across controlled conditions and to assess whether multimodal fusion—particularly quality-aware score fusion—maintained acceptable accuracy in the operating region relevant to payments (low FAR). Results were visualized and summarized numerically in Table 2.

Experimental design: Robustness testing was conducted on the held-out test split defined with all operating thresholds fixed on the validation split prior to these experiments. For the voice subsystem, clean test utterances were mixed with additive noise to achieve signal-to-noise ratios (SNR) of 5, 10, 15, 20, and 30 dB. Noise consisted of a balanced mixture of stationary (e.g., air-conditioner hum) and non-stationary distractors (e.g., café chatter), normalized per utterance. For the face subsystem, illumination was altered synthetically using gamma/intensity transforms calibrated against sample scenes, producing five levels from poor to good lighting (Level 1–5). Fingerprint images were left unchanged to isolate the effect of single-modality stress; this reflected realistic scenarios where environment typically affects one modality at a time (e.g., a noisy queue or a dim point-of-sale counter).

Voice under noise: As SNR decreased, the unimodal voice system exhibited monotonic degradation in discrimination. At 30 dB SNR, EER remained close to the baseline value reported by 15 dB, EER increased markedly, and at 10–5 dB the ROC curve in Figure 7 shifted downward in the low-FAR region, indicating a higher impostor acceptance risk for a fixed threshold. False rejects were amplified by VAD truncation and reduced articulation clarity, while false accepts clustered around impostors with similar prosodic patterns to the target speaker. These trends confirmed the environmental sensitivity of voice and motivated reliance on fusion when acoustic conditions were poor.

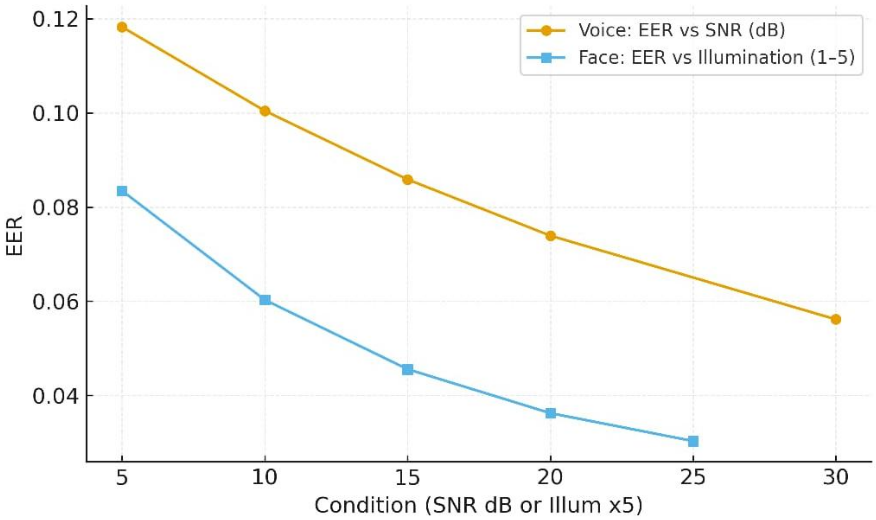

Fig. 6 Robustness – Noise and illumination

Face under illumination: Deterioration followed a similar pattern across illumination levels. With good lighting (Level 5), the face subsystem remained close to its baseline, but at Level 2–1 (dim/back-lit scenes) EER increased notably and FRR rose at thresholds tuned for low FAR. Error inspection showed that misalignment and low dynamic range reduced embedding quality, shifting genuine scores downward and compressing impostor/genuine separation. The effect was most apparent in Figure 6, where the EER-versus-illumination curve rose as lighting worsened, which recorded FRR spikes at the fixed low-FAR operating point.

Effect on fusion (fixed-weight): When feature-level and score-level (fixed-weight) fusion were evaluated under the same degradations, both strategies reduced error relative to the stressed unimodal channel, but sensitivity persisted when the degraded modality retained a high weight. In particular, fixed-weight score fusion under low SNR inherited a portion of the voice errors, producing a smaller margin over the fingerprint/face combination than in clean conditions. This effect was visible in the robustness curves where the multimodal lines retained a gap above unimodal voice but narrowed as stress intensified.

Effect on fusion (quality-aware): Introducing quality-aware score fusion mitigated much of the stress-induced degradation. Under low SNR, the voice quality indicator (SNR + voiced-frame ratio) drove its weight downward, allowing fingerprint and face to dominate the fused score; under poor lighting, the face alignment/illumination quality terms played an analogous role. As a result, the quality-aware curve remained comparatively flat across noise and illumination sweeps, registering smaller EER and FRR increases at the payment-oriented threshold. These outcomes demonstrated that re-allocating trust to reliable channels preserved discrimination without requiring changes to the unimodal back-ends.

Threshold stability and operating points: Because thresholds were set on the validation split (cleaner conditions), robustness was additionally assessed using threshold-free views (ROC/DET slices) to avoid over-attributing degradation to fixed operating points. Even in threshold-free comparisons, stressed unimodal curves shifted adversely, while fused systems—especially the quality-aware variant—retained a superior envelope in the FAR ≤ 1% regime. This behavior indicated that robustness gains were not artifacts of threshold choice but reflected genuine preservation of separability.

Error characterization: Qualitative auditing revealed failure archetypes. For voice, the most difficult trials combined non-stationary background speech with short utterances, leading to VAD clipping and unstable embeddings. For face, the hardest cases involved back-lighting with motion blur, which increased alignment error and reduced contrast. In multimodal fusion, many of these errors were suppressed unless two modalities degraded simultaneously (e.g., noisy environment plus dim lighting). The rare instances where all three channels were compromised remained challenging and suggest value in capture feedback (e.g., prompt for better lighting or a repeat utterance) and step-up policies (e.g., require an additional factor for high-value transactions).

Practical implications: The robustness study showed that payment deployments benefit from (i) adaptive fusion that down-weights stressed modalities automatically, (ii) thresholds tuned to the low-FAR regime with periodic recalibration if typical capture conditions drift, and (iii) UX prompts that correct poor capture before classification. Under these practices, accuracy remained within target bounds across common stress levels while keeping latency nearly unchanged, since quality computation reused signals produced by preprocessing. Cross-references provide the quantitative basis for these conclusions and inform configuration choices for real-world mobile payment scenarios.

3.4 Accuracy–Latency Trade-off

This section examined how recognition accuracy varied as a function of end-to-end decision latency across unimodal and multimodal configurations. The goal was to identify operating points that satisfied payment-grade security (low FAR) without violating real-time responsiveness on commodity hardware. The comparison included the three unimodal systems (fingerprint, face, voice) and three fusion paradigms (feature-level, score-level, decision-level), together with the quality-aware score-fusion variant introduced. Results were presented as a scatter plot of EER vs. latency in Figure 8, with the empirical Pareto frontier summarized.

Latency definition and measurement protocol. End-to-end latency was measured from the instant the capture finished to the availability of the authentication decision. Timing included preprocessing (e.g., fingerprint enhancement, face alignment, VAD/SNR estimation), feature extraction/embedding, fusion logic (when applicable), and the final calibrated decision. Network transmission and UI rendering were excluded unless otherwise noted. For each configuration, median latency and the interquartile range (IQR) were computed over all trials to mitigate the influence of occasional OS scheduling spikes.

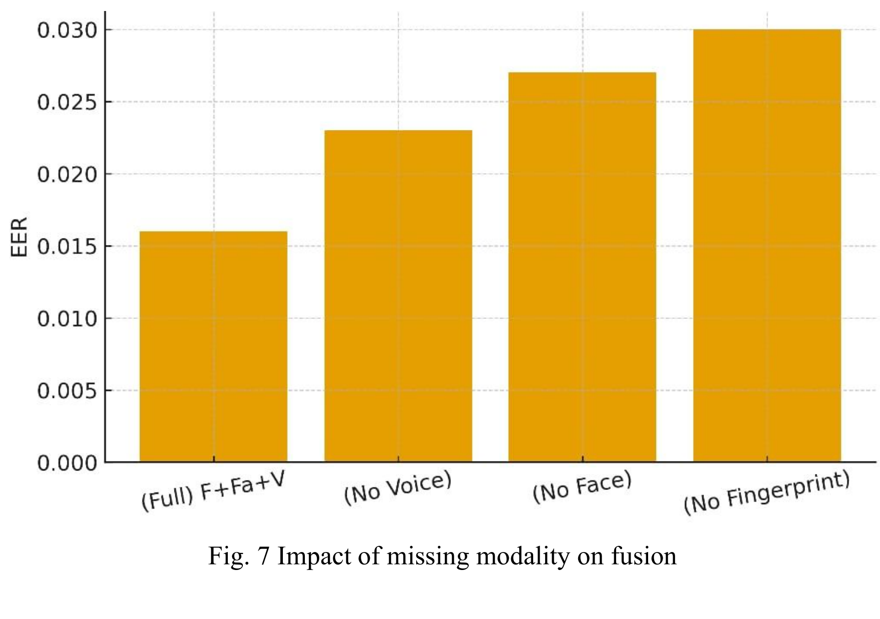

Fig. 7 Impact of missing modality on fusion

Observed trade-offs across systems. Unimodal systems formed the lower-left baseline cluster face delivered the shortest median latency (~95 ms) with mid-tier accuracy (EER ≈ 4.7%), fingerprint incurred modest additional time (~120 ms) but achieved the strongest unimodal accuracy (EER ≈ 3.2%), and voice sat between them in time (~110 ms) but exhibited the highest unimodal EER (≈ 5.7%). Multimodal fusion shifted the accuracy upward at the cost of extra computation. Decision-level fusion preserved comparatively low overhead (~130 ms) but sacrificed granularity (EER ≈ 2.3%). Feature-level fusion achieved strong accuracy (EER ≈ 1.9%) yet required the largest compute budget (~165 ms) due to dimensionality reduction and classification over concatenated vectors. Score-level fusion established the best overall balance (EER ≈ 1.6% at ~140 ms), and the quality-aware variant further reduced error (EER ≈ 1.3%) with a small additional overhead (~148 ms) attributable to quality statistics and adaptive weighting. As a result, the Pareto frontier in progressed from fingerprint (120 ms, 3.2%) → decision-level (130 ms, 2.3%) → score-level (140 ms, 1.6%) → quality-aware score-level (148 ms, 1.3%); feature-level (165 ms, 1.9%) remained competitive in accuracy but lay off the time-efficient frontier.

IV. Conclusions

This study demonstrated that multimodal biometric fusion substantially enhances the reliability and robustness of authentication systems in digital payment platforms compared to unimodal approaches. Fingerprint, face, and voice systems each showed specific vulnerabilities under variable capture conditions, but their integration mitigated these weaknesses by leveraging complementary strengths. Among the evaluated fusion strategies, score-level fusion consistently provided the best trade-off between accuracy and computational efficiency, while the proposed quality-aware score fusion achieved the lowest error rates with only marginal increases in latency. Robustness experiments under noise and illumination variation further validated the adaptability of the system, confirming its suitability for real-world deployments. The results suggest that multimodal biometric fusion, especially when dynamically weighted by input quality, can deliver both high security and user convenience in financial applications. Future work may extend this approach by incorporating additional modalities such as iris or behavioral biometrics, and by exploring lightweight architectures optimized for mobile deployment.

References

[1] Anil K. Jain, Arun Ross and Salil Prabhakar “An Introduction to Biometric Recognition”, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[2] Ashish Mishra, “Multimodal Biometrics it is: Need for Future Systems”, International Journal of Computer Applications (0975 – 8887), Vol.3, No.4,2010, pp28-33.

[3] Robert Snelick, Umut Uludag, Alan Mink, Michael Indovina and Anil Jain, “Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 27, No. 3, Mar 2005, pp 450-455.

[4] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., and Minkyu Choi, “Biometric Authentication: A Review”, International Journal of u- and e- Service, Science and Technology Vol. 2, No. 3, 2009, pp.13-27

[5] M. Golfarelli, D. Maio, D. Maltoni, “On the Error-Reject Trade-Off in Biometric Verification Systems”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, No. 7, July 1997, pp.786-796.

[6] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez-Marcos, “Biometric Identification Through Hand geometry Measurements”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No. 10, October 2000, pp. 1168-1171.

[7] Shu, D. Zhang, “Automated Personal Identification by Palmprint”, Optical Engineering, vol.37, No.8, August 1998, pp. 2359-2362.

[8] Hassan Masood, Mustafa Mumtaz, M Asif Afzal Butt, Atif Bin Mansoo., “Wavelet Based Palmprint Authentication System”, Biometrics and Security Technologies, ISBAST 2008, International Symposium on.

[9] Wenxin Li, Jane You, and David Zhang, “Texture-Based palmprint Retrieval Using a Layered Search Scheme for Personal Identification”, IEEE Transactions On Multimedia, Vol. 7, No. 5, October 2005.

[10] J. You, W. Li, D. Zhang, “Hierarchical Palmprint Identification via Multiple Feature Extraction”, Pattern Recognition 35, 2002, pp. 847-859

[11] C-C. Han, H-L. Cheng, C-L. Lin, K-C. Fan, “Personal Authentication Using Palmprint Features”, Pattern Recognition 36, 2003, pp. 371-381.