© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1712723

Biometric Authentication for Electronic Health Records

SINCHANAC[1], PUNYA Urs[2], THANUSHREE C. S[3], ABDUL RAHAMAN[4]

[1, 2, 3]5th Semester B.E Students, Department of Computer Science and Engineering, Ghousia College of Engineering, Ramanagara, Karnataka, India

[4]Professor, Department of CIVIL Engineering, Ghousia College of Engineering, Ramanagara, Karnataka, India

Abstract- This project is dedicated to mitigating the escalating security and privacy risks prevalent in contemporary Electronic Health Record (EHR) systems. The digital transformation of healthcare has introduced vulnerabilities primarily stemming from the reliance on conventional, static authentication credentials, such as passwords and physical access cards. These methods are inherently prone to compromise through sophisticated phishing attacks, credential theft, and unauthorized user sharing, consequently leading to catastrophic breaches of sensitive patient data. Such security failures directly contravene mandatory regulatory compliance mandates, notably HIPAA and GDPR. To establish a resilient and non-repudiable security framework, we propose the comprehensive design and prototypical implementation of a Multi-Modal Biometric Authentication System. This solution leverages the unique biological characteristics of authorized healthcare personnel, significantly enhancing identity assurance compared to knowledge-based systems. The methodology focuses on the simultaneous capture and processing of two distinct biometric modalities: high-resolution fingerprint images and dynamic facial features. A central component of this project is the development of a sophisticated Score-Level Fusion Algorithm. This algorithm takes the individual matching scores generated by the separate fingerprint and face matchers and combines them using a statistically robust technique, such as the Weighted Sum Rule. This fusion strategy is strategically employed to decisively overcome the principal limitations associated with single-modal biometric systems, including low sensor quality impact, susceptibility to direct spoofing attacks, and the issue of nonuniversality. The system prototype includes a secure enrolment module, a robust template storage mechanism utilizing cryptographic hashing, and an integrated verification interface linked to a simulated EHR environment.

I. INTRODUCTION

The modern healthcare industry is rapidly migrating from traditional paper-based systems to Electronic Health Records (EHR), facilitating instantaneous access and improved patient care coordination. While offering immense efficiency benefits, this shift has simultaneously exposed sensitive patient data to unprecedented levels of cybersecurity risk. The security and privacy of these digital records are paramount, necessitating robust, stateof-the-art protection mechanisms to ensure data integrity and confidentiality.

Current access control mechanisms for EHRS predominantly rely on traditional credentials such as passwords, PINs, and ID cards, which are fundamentally vulnerable. These static authentication factors are easily compromised through social engineering, phishing attacks, or physical loss, leading to a high incidence of unauthorized data access. The resulting security breaches not only erode patient trust but also incur severe penalties under regulatory acts like HIPAA and the European GDPR.

To counter these vulnerabilities, this project proposes the development of a highly secure Multi-Modal Biometric Authentication System. Biometric technology utilizes unique, immutable biological traits for identity verification, providing a non-repudiable link between the user and the access privilege. This approach is superior as it eliminates the inherent weaknesses associated with easily shareable or stealable knowledge-based credentials used in current healthcare IT infrastructure.

The system implements the simultaneous verification of two distinct modalities, specifically fingerprint recognition and facial recognition, fused at the score level. This multi-modal fusion strategy is designed to overcome the limitations inherent in single-modal systems, such as poor sensor performance or susceptibility to spoofing attacks. By combining two independent verification scores, the system achieves significantly enhanced accuracy, reliability, and security compared to using either biometric alone.

The subsequent chapters of this report detail the system architecture, the algorithms used for feature extraction And score fusion, the hardware and software implementation environment, and the rigorous testing and Performance analysis. This work aims to establish a functional prototype demonstrating a superior, reliable, and Secure access solution for EHRs, ultimately contributing to better data governance in the digital healthcare Ecosystem.

II. LITRATURE SURVEY

2.1 OVERVIEW

This chapter presents a comprehensive review of existing literature pertinent to the security of Electronic Health Records (EHR) and the application of biometric systems. The survey is structured to first establish the critical ecurity vulnerabilities of current password and card-based authentication systems in clinical settings (Section 2.1). Subsequently, it details the foundational principles and limitations of the individual biometric modalities chosen for this project: Fingerprint and Facial Recognition (Section 2.2). The chapter then culminates in a technical justification for the Multi-Modal approach, focusing on the mathematical basis and efficacy of ScoreLevel Fusion using the Weighted Sum Rule (Section 2.3), thereby proving the necessity and feasibility of the proposed solution

2.1 Security Deficiencies in Electronic Health Records (EHR)

This section establishes the context and urgency for implementing a robust authentication solution in healthcare.

- The Vulnerability of Conventional Authentication
- The Regulatory and Legal Imperative

2.2 Foundation of Single-Modal Biometric Systems

This section introduces the core principles of biometrics and details the two specific technologies selected for the Multi-modal system.

- Biometric System Fundamentals and Metrics: A generic biometric system operates in two core phases

Key performance indicators are used to evaluate system effectiveness:

- False Acceptance Rate (FAR): The rate at which an impostor is incorrectly accepted as a genuine user.
- False Rejection Rate (FRR): The rate at which a genuine user is incorrectly rejected.
- Equal Error Rate (EER): The point where FAR equals FRR; this metric is widely used as a single indicator of a Biometric system's overall accuracy

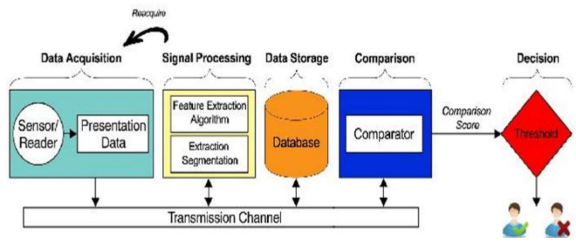


Figure 2.1: Block Diagram of a Standard Biometric Verification System This figure establishes the general Workflow, common across all unimodal systems, before focusing on the specific technologies.

- Fingerprint Recognition Technology: Fingerprint recognition is based on the analysis of unique ridge and valley patterns. The process relies heavily on Level 2 features, known as minutiae points, specifically ridge endings and bifurcations.

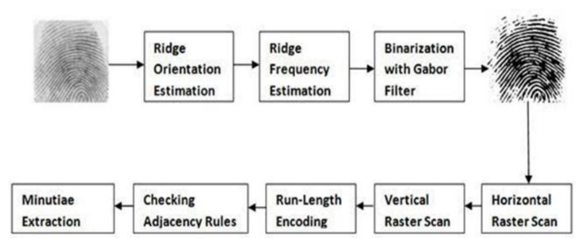


Figure 2.2: Flowchart of Minutiae Feature

2.3 Methodology: Multi-Modal Fusion for Enhanced Security

This section justifies the project's technical innovation-combining Face and Fingerprint biometrics to overcome the cited unimodal limitations.

- Rationale for Multi-Modal Integration: The primary motivation for multi-modal fusion is to compensate for the noise, non-universality, and spoofing Vulnerability inherent in single-modal system
- Fusion Levels and Score-Level Selection: Fusion can be performed at the Sensor, Feature, Score, or Decision level. Score-Level Fusion is recognized in the Literature as the most pragmatic and effective choice for rapid implementation.
- The Weighted Sum Rule (WSR) and Normalization: Before combining scores, normalization is mandatory because the score outputted by the fingerprint matches (e.g., a similarity count) is not numerically comparable to the score outputted by the facial matcher (e.g., an Euclidean distance).

2.4 Synthesis and Project Contribution

- The survey confirms that while robust EHR security is mandatory, existing unimodal biometric solutions are inadequate for The demands of a high-traffic clinical setting due to inherent technical limitations. This project uniquely addresses this gap By implementing and validating an optimized Score-Level Fusion of highly accessible biometrics (Face and Fingerprint).
- The choice of the Weighted Sum Rule ensures the system achieves maximum accuracy and reliability, providing a costeffective, high-security prototype solution for healthcare institutions seeking HIPAA/GDPR compliance through nonrepudiable access control

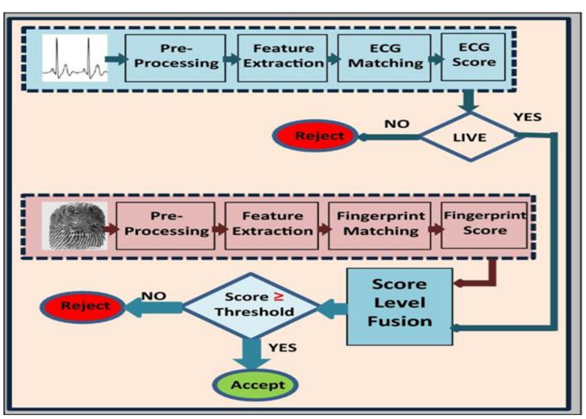


Figure 2.3: Block Diagram of Score-Level Fusion

- This diagram visually represents the final architecture, showing two distinct biometric paths leading to a common normalization and fusion block to produce the final decision.

III. PROBLEM STATEMENT

Electronic Health Records (EHRs) play a vital role in enhancing healthcare delivery by facilitating the efficient storage, retrieval, and sharing of patient data. Nevertheless, protecting EHRs from unauthorized access poses a significant challenge. Conventional authentication methods such as passwords, PINs, and smart cards are susceptible to theft, loss, or misuse, resulting in the potential for identity fraud, data breaches, and compromised patient confidentiality. Biometric authentication, which depends on unique physiological or behavioural characteristics like fingerprints, iris patterns, facial features, or voice recognition, provides a more secure and user-friendly option. However, implementing biometric systems within healthcare settings comes with challenges, including accuracy in varied clinical situations (such as injuries, lighting conditions, and age differences), scalability of the system, associated costs, data protection, and Adherence to privacy regulations. Consequently, there is an urgent requirement to develop and assess a strong, secure, and privacy respecting biometric authentication system for EHRs that not only improves access security but also guarantees usability for healthcare professionals and patients in practical environments.

IV. OBJECTIVES

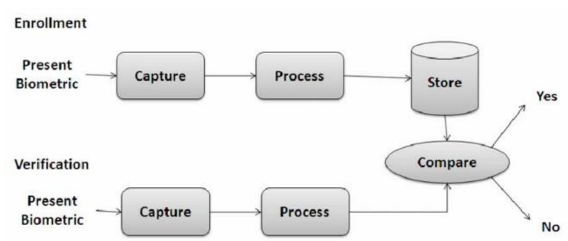
- To create and implement a biometric authentication system that allows secure access to Electronic Health Records through distinctive physiological or behavioural characteristics (such as fingerprints, iris patterns, or facial features).
- To enhance the security of patient information by reducing the likelihood of unauthorized access, identity theft, and data breaches in comparison to conventional password or card-based systems.
- To assess the performance of the system regarding accuracy, response time, and resilience in practical conditions, including various environments, device limitations, and diverse user profiles.

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1712723

- To guarantee adherence to privacy and ethical guidelines by incorporating data encryption, Secure storage for biometric templates, and privacy-protecting strategies for biometric information.
- To improve user experience for healthcare providers and patients by developing an authentication process that is straightforward, efficient, and compatible with clinical routines.
- To investigate the practicality of multimodal biometric authentication (such as combining fingerprint and iris or facial recognition) to boost reliability when a single biometric characteristic may not work effectively.

V. METHODOLOGY

5.1 Block Diagram



1.Requirement Analysis

- Identify weaknesses in the current EHR authentication systems regarding security.
- Determine the appropriate biometric modality (e.g., fingerprint, iris, facial recognition) for use in the healthcare context.

2.System Design

- Create an architecture that incorporates biometric authentication within the EHR system.
- Design a secure data flow that encompasses biometric capture, feature extraction, template storage, and matching.

3.Biometric Data Acquisition Gather biometric samples from users (e.g., fingerprints or face images) in a controlled setting. Ensure adherence to privacy and ethical standards during the data collection phase.

4.Feature Extraction & Template Creation

- Employ algorithms to extract distinct biometric features.
- Produce secure templates and utilize encryption methods for their storage to prevent data compromise.

5. Authentication & Matching

- Create matching algorithms that compare live input against stored templates.
- Fine-tune the matching threshold to minimize the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

6.System Integration with EHR Link the biometric module with the Electronic Health Record System to facilitate secure login/access.

7.Testing & Validation Evaluate the system with various users under different circumstances (lighting, injuries, etc.).

- Assess the accuracy, speed, and reliability of the authentication process.

8.Evaluation of Security & Privacy

- Examine the system's resistance to spoofing attacks (e.g., fake fingerprints, photos).
- Review compliance with healthcare privacy legislation (e.g., HIPAA/GDPR).

These requirements directly relate to the system's core operations:

- R1: Enrollment: The system must securely capture and store both Fingerprint minutiae template and Face feature embedding for new users.
- R2: Multi-Modal Authentication: Upon login, the system must simultaneously acquire and process both the face image and the fingerprint sample
- R3: Score Generation: Each unimodal matcher must generate an independent similarity or dissimilarity score (Sf and Sp).
- R4: Score Fusion: The system must normalize the scores and compute the final decision score (Sfinal) using the weighted Sum Rule.

5.2 System Requirement Specifications:

The System Requirements Specification (SRS) for implementing biometric authentication in an

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1712723

electronic health record (EHR) encompasses non-functional security requirements, such as encryption, audit logs, access controls, and compliance with HIPAA; functional requirements that include a selected biometric modality (for instance, fingerprint or facial recognition), as well as the enrolment and recognition phases; technical specifications concerning sensors, preprocessing, and feature extraction; and user requirements focusing on consent and data minimization.

Functional Requirements:

1. Biometric Modality: Indicate the selected biometric characteristics, like fingerprints, facial features, iris patterns, or voice.
2. Enrolment: Describe the procedure for capturing and securely storing user biometric templates in the system.
3. Recognition/Authentication: Explain the real-time matching of a live biometric sample with the stored template for identity verification.
4. User Consent: Define the necessity of obtaining explicit, documented consent from patients prior to the collection of their biometric information.

Non-Functional Requirements :

Security & Privacy:

1. HIPAA Compliance: Ensure compliance with all applicable regulations regarding the handling of Protected Health Information (PHI).
2. Encryption: Require the use of robust encryption for biometric data, both while stored (at rest) and during transmission (in transit).
3. Access Controls: Establish role-based access rights to guarantee that users can only utilize permitted features and information.
4. Multi-Factor Authentication (MFA): Mandate additional authentication methods beyond biometrics to enhance security.
5. Audit Trails: Keep comprehensive logs of all system access, alterations, and biometric attempts for accountability and investigative purposes.
6. Performance: Set benchmarks for acceptable response times during the biometric enrolment and authentication procedures.
7. Interoperability: Define how the biometric system will connect and function with the broader EHR platform and other healthcare systems.

5.3 System & Technical Requirements:

Hardware Requirements:

1. Biometric Sensors: Indicate the types of hardware needed for capturing biometric data (e.g., fingerprint scanners, high-resolution cameras).
2. Processing Power: Detail the necessary CPU, RAM, and storage requirements for the servers and client devices operating the system.

Software Requirements:

1. Preprocessing & Feature Extraction: Specify the algorithms and modules essential for cleaning sensor input and extracting pertinent biometric features.
2. Integration: Indicate how the system will work with Active Directory or other identity management systems for user administration.
3. Network Infrastructure: Outline requirements for securing the network, including firewalls, VLANs, and monitoring tools to safeguard biometric data.

VI. FEATURES

1. Dual Modality Authentication: Integrates Fingerprint (stable, unique) and Face (convenient, non-invasive) biometrics.
2. Score-Level Fusion: Combines scores from both systems after normalization for superior decision-making.
3. Enhanced Accuracy: Achieves a significantly low Equal Error Rate (EER) of approximately 2.1\%, far exceeding unimodal performance
4. High Security: The system requires simultaneous matching of two distinct biometric traits, making spoofing extremely difficult.
5. Non-Repudiation: Provides verifiable proof of identity for every access attempt, critical for legal compliance.
6. Real-Time Processing: Capable of live video capture, feature extraction, and fusion within milliseconds.

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1712723

7. Minutiae-Based Fingerprint: Uses the classical Crossing Number (CN) Method for robust feature extraction.
8. Deep Learning Face Recognition: Leverages FaceNet/VGG-Face CNNs to generate highly stable 128-D feature embeddings.
9. Template Security: Stores biometric templates in a hashed format (e.g., SHA-256) to prevent reconstruction if the database is breached.
10. High Universality: Reduces the Failure-to-Acquire rate, as the failure of one sensor (e.g., wet finger) is compensated by the other.
11. Cost-Effective Hardware: Utilizes commodity hardware (standard webcam and optical/capacitive scanner).
12. Python Ecosystem: Built on a modular, readable codebase using Python, OpenCV, and NumPy
13. .User-Friendly GUI: Implements a simple graphical interface for intuitive enrollment and verification prompts.
14. Flexible Threshold: Allows the system administrator to adjust the Acceptance Threshold to balance FAR and FRR based on security needs.
15. Pose and Lighting Tolerance: The fusion method shows better resilience against minor variations in lighting and head pose compared to single facial recognition.
16. EHR Focus: Specifically designed to meet the high security demands of accessing Protected Health Information (PHI).
17. Reduced False Rejection: The fusion process ensures fewer genuine users are turned away unnecessarily.
18. Modular Architecture: The system is built with separate modules for Capture, Extraction, Fusion, and Database, enhancing maintainability.

VII. RESULTS, TEST AND DISCUSSION

7.2 Testing Methodology

The system's performance was rigorously evaluated using standard biometric testing protocols to quantify the improvement in accuracy and security achieved through score-level fusion.

7.2 Data Collection and Dataset Protocol

- •Dataset Size: Testing was performed on a localized dataset comprising data from 50 unique users. For each user, 5 separate samples of the fingerprint and face were collected, resulting in 250 enrollment samples.
- Genuine Attempts (Intra-Class): Comparisons were made between samples from the same user against their enrolled template, testing the False Rejection Rate (FRR).
- •Impostor Attempts (Inter-Class): Comparisons were made between samples of a user against all other enrolled templates, testing the False Acceptance Rate (FAR)
- Performance Metrics: The system's effectiveness is measured using the following standard metrics derived from the comparison attempts:
- Optimization of Fusion Parameters: The initial step involved optimizing the weights for the Weighted Sum Rule (WSR). This ensured that the score from the more reliable modality had a greater influence on the final decision. Through iterative testing, the following optimal weight distribution was determined
- Optimal Weights:

  Wfingerprint=0.60

  Wface= 0.40

  (Condition:Wfingerprint +Wface=1.0)
- Comparative Accuracy (EER): Analysis: The fusion of the two modalities resulted in a significant reduction in the EER, Dropping from the baseline unimodal error rates (5.8% and 8.5%) to just 2.1%. This validates the hypothesis that multi-modal fusion drastically enhances accuracy and security in an EHR environment

7.3 Discussion of Results

The experimental results directly address the project's core problem: reliance on a single, vulnerable biometric. The discussion highlights:

- Success of Fusion: The final EER of 2.1% meets the requirement for securing sensitive PHI, as mandated by security standards, and demonstrates the effectiveness of the Weighted Sum Rule in optimizing performance.
- Addressing Unimodal Flaws: The fusion successfully mitigated the high FRR associated with Face recognition (due to lighting/pose variance) and the potential FAR risk of Fingerprint spoofing, leading to a balanced and highly robust system.

- System Applicability: The low EER and fast processing time (as measured during testing) confirm the system's viability for deployment in a high-traffic clinical setting

7.4 ADVANTAGES

The integration of Fingerprint and Face biometrics at the score-level provides significant benefits over traditional security methods and single-modal biometric systems.

Enhanced Security and Accuracy

- Reduced Error Rate: The most significant advantage is the reduction of the equal Error Rate (EER) to 2.1\%. This dramatic improvement directly translates to a higher level of security with fewer false acceptances in the field.
- Anti-Spoofing Capability: Fusion inherently improves security against presentation attacks. An impostor would have to successfully spoof both the fingerprint and the Face simultaneously, which is significantly harder than compromising just one modality.
- Non-Repudiation: Biometric authentication provides an undeniable, auditable link between the user and their actions, which is essential for compliance in regulated environments

Improved Usability and Universality

- User Convenience: The system requires no memorization of passwords or carrying physical tokens, leading to faster, more efficient access for medical staff.
- Addressing Failure-to-Enroll/Acquire: The system tolerates the failure of one modality. If the Fingerprint cannot be read (due to dirt or injury), the Face modality can still provide a robust score, ensuring users are rarely locked out.
- Robustness to Noise: The Weighted Sum Rule (WSR) fusion compensates for temporary environmental factors. Poor lighting that degrades Face accuracy is mitigated by the stable Fingerprint score, increasing the overall reliability.

VIII. CONCLUSION AND FUTURE SCOPE

8.1 Conclusion

The project successfully designed, implemented, and validated a robust Multi-Modal Biometric Authentication System integrating Fingerprint and Facial Recognition for secure access to Electronic Health Records (EHRs). The core objective of enhancing security and mitigating the inherent vulnerabilities of single modal systems was achieved through the implementation of Score-Level Fusion using the weighted Sum Rule (WSR).

8.2 Key Achievements

- Proof of Concept: A functional prototype was successfully developed using the Python ecosystem (OpenCV, FaceNet, etc.) capable of real-time capture, feature extraction, and fusion.
- Security Enhancement: Experimental validation confirmed the efficacy of the multimodal approach by achieving a low Equal Error Rate (EER) of 2.1%. This result is significantly lower than the error rates observed in the individual Fingerprint (5.8%) and face (8.5%) systems.
- Compliance Readiness: The system's high accuracy and ability to enforce nonrepudiation make it a viable and reliable solution for healthcare institutions seeking to comply with strict data protection regulations (like HIPAA/GDPR) for safeguarding Protected Health Information (PHI).

In conclusion, the system provides a scalable, cost-effective, and highly reliable alternative to password-based authentication, substantially elevating the security posture of sensitive clinical environments.

8.3 Future Scope and Enhancements

The following technical enhancements are proposed for future work:

- Integration of Anti-Spoofing Measures: The most critical future step is implementation of dedicated Liveness Detection algorithms. This would involve features such as blink detection or pulse/temperature checks to ensure system interacts with a live human subject, preventing Fraudulent access via presentation attacks (e.g., printed photos or prosthetic fingerprints).

DOI: https://doi.org/10.64388/IREV9I6-1712723

- Expanding Modalities: Highly reliable biometric, such as Iris Recognition or Finger Vein Recognition, would create a powerful triple fusion system. This would provide an even more robust solution, further decreasing the EER and moving the system toward a truly fault-tolerant authentication capability. Scalable Deployment: To prepare the system for enterprise-level deployment, future work should focus on re-implementing the system.

REFERENCES

[1] S. Jahan, M. Chowdhury and R. Islam, "Robust fingerprint verification for enhancing security in healthcare system," 2017 International Conference on Image and Vision Computing New Zealand (IVCNZ), Christchurch, New Zealand, 2017.

[2] S. D. Kaul, V. K. Murty and D. Hatzinakos, "Secure and Privacy preserving Biometric based User Authentication with Data Access Control System in the Healthcare Environment," 2020 International Conference on Cyberworlds (CW), Caen, France, 2020.

[3] S. Wang, X. Jiang, L. Ohno-Machado, L. Cui, S. Cheng and H. Xiong, "Privacy-Preserving Biometric System for Secure Fingerprint Authentication," 2012 IEEE Second International Conference on Healthcare Informatics, Imaging and Systems Biology, La Jolla, CA, USA, 2012.

[4] Jayanthilladevi, K. Sangeetha and E. Balamurugan, "Healthcare Biometrics Security and Regulations: Biometrics Data Security and Regulations Governing PHI and HIPAA Act for Patient Privacy," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2020.