© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715456

Biometric Based Electronic Health Record and Patient Identification System for Improved Healthcare Delivery in Nigeria

EKUNDAYO[1], AYOOLA SUNDAY[2], PROF. O. OLABODE[3]
[1]*Health Information Management Department, Achievers University, Owo*
[2]*School of Computing, computer science department Federal University of Technology, Akure*

Abstract- ***Accurate patient identification is critical to patient safety and effective healthcare delivery. In many developing countries, including Nigeria, healthcare institutions continue to rely on manual patient identification systems that are prone to errors, record duplication, and delays in accessing medical information. These challenges undermine the effectiveness of electronic health record (EHR) systems and compromise quality of care. This study designed, implemented, and evaluated a facial biometric–based electronic health record and patient identification system as a secure, contactless, and scalable solution for Nigerian healthcare settings. An experimental research design was adopted. Facial images were collected from 50 patients at a Nigerian tertiary healthcare institution, with three facial samples per participant, resulting in a dataset of 150 images. The system was developed using Java, OpenCV, and a MySQL database. Performance evaluation was conducted using standard biometric metrics, including face detection accuracy, face recognition accuracy, false acceptance rate (FAR), false rejection rate (FRR), and average system response time.The developed system achieved a face detection accuracy of 98.67% and a face recognition accuracy of 94.67%. Both FAR and FRR were recorded at 2.67%, while the average response time was 1.82 seconds. These findings demonstrate that facial recognition technology can effectively support real-time patient identification and electronic health record retrieval in clinical environments. The study concludes that facial biometric-based EHR systems can significantly enhance patient safety, reduce record duplication, and improve healthcare efficiency in low-resource settings. Future work should explore multi-modal biometric integration, large-scale deployment, and robust data privacy frameworks.***

Index Terms- ***Facial recognition; Biometrics; Electronic health records; Patient identification; Health informatics; Nigeria***

I. INTRODUCTION

Accurate patient identification is a foundational requirement for safe and effective healthcare delivery. Patient misidentification has been associated with medication errors, incorrect diagnoses, inappropriate clinical procedures, and fragmented continuity of care (World Health Organization [WHO], 2019). Globally, patient identification errors are recognized as a major contributor to preventable adverse events, particularly in low- and middle-income countries where healthcare systems often face infrastructural and resource constraints.

In Nigeria, patient identification practices in many public healthcare institutions remain largely manual. Patients are commonly identified using hospital numbers, paper folders, and demographic attributes such as names and dates of birth. These identifiers are often unreliable due to spelling variations, cultural naming practices, missing demographic information, and the absence of a national unique patient identifier (Ojo & Popoola, 2020). As a result, healthcare facilities frequently experience duplicated patient records, misplaced folders, prolonged waiting times, and delays in clinical decision-making (Olatunji et al., 2022).

Electronic health record (EHR) systems have been introduced to improve the management of patient information by enabling digital documentation, fast retrieval of records, and improved continuity of care. Evidence suggests that effective EHR implementation can enhance healthcare quality, reduce medical errors, and support clinical decision-making (Adler-Milstein et al., 2020). However, the

benefits of EHR systems are significantly undermined when patient identification mechanisms are weak. Without reliable identification, electronic systems merely digitize existing inefficiencies and errors (Healthcare Information and Management Systems Society [HIMSS], 2021).

Biometric technologies provide a promising solution to the challenge of patient identification by leveraging unique physiological characteristics for identity verification. Common biometric modalities include fingerprints, iris patterns, facial features, and voice recognition. Among these, facial recognition has gained increasing attention in healthcare due to its contactless nature, ease of deployment, and high user acceptability (Jain et al., 2019). Unlike fingerprint-based systems, facial recognition does not require physical contact with sensors, making it particularly suitable for infection-sensitive clinical environments.

Advances in computer vision algorithms and the availability of open-source libraries such as OpenCV have further enhanced the feasibility of deploying facial recognition systems in resource-constrained healthcare settings (Bradski & Kaehler, 2018; Li & Deng, 2022). Despite these advancements, empirical studies evaluating facial biometric-based EHR systems in Nigerian healthcare institutions remain limited. This study addresses this gap by designing, implementing, and experimentally evaluating a facial biometric-based electronic health record and patient identification system using real patient data from a Nigerian tertiary hospital.

The study was guided by the following research questions:

1. Can a facial recognition model accurately identify patients in a hospital environment?
2. Can a facial biometric-based EHR system be effectively implemented using open-source programming tools?
3. What is the efficiency level of the developed system in terms of accuracy, reliability, and response time?

II. LITERATURE REVIEW

2.1 Patient identification in healthcare

Patient identification refers to the accurate matching of patients to their health records, treatments, and clinical services. Traditional identification methods, such as names, hospital numbers, and identity cards, are widely used but have been shown to be unreliable, particularly in high-volume healthcare environments (Greenly et al., 2020). Errors in patient identification have been linked to adverse clinical outcomes and increased healthcare costs.

In developing countries, patient identification challenges are often exacerbated by inadequate health information infrastructure and poor record management practices. Studies conducted in Nigerian hospitals report frequent duplication of patient records and difficulties in retrieving medical folders due to manual filing systems and inconsistent identifiers (Adebayo et al., 2021).

2.2 Electronic health records and patient safety

Electronic health records are digital repositories of patient health information, including demographic data, medical history, laboratory results, and treatment plans. EHR systems are designed to improve healthcare efficiency, data accuracy, and continuity of care. Research has demonstrated that EHR adoption can reduce medical errors and improve patient outcomes when effectively implemented (Kellermann & Jones, 2019).

However, patient matching errors remain one of the most significant threats to EHR effectiveness. HIMSS (2021) emphasized that inaccurate patient identification undermines data integrity and clinical decision-making, regardless of the sophistication of the EHR platform.

2.3 Biometrics in healthcare systems

Biometric authentication systems have been increasingly adopted in healthcare for patient identification, access control, and data security. Fingerprint recognition is one of the most commonly used biometric modalities but faces challenges related to hygiene concerns, worn fingerprints, and sensor dependency (Ratha et al., 2020). Iris recognition offers high accuracy but requires specialized and costly equipment, limiting its suitability for low-resource settings.

Facial biometrics provides a non-intrusive alternative that balances accuracy, cost, and user convenience. Studies have reported high acceptance of facial recognition systems among patients and healthcare workers due to their ease of use and contactless operation (Li & Deng, 2022).

2.4 Facial recognition technologies in healthcare

Facial recognition systems typically involve three stages: face detection, feature extraction, and face recognition. Classical algorithms such as the Viola–Jones face detection algorithm and Eigenfaces-based recognition have been widely used in real-time applications due to their computational efficiency (Viola & Jones, 2004; Turk & Pentland, 1991).

Recent studies report facial recognition accuracy exceeding 90% in controlled healthcare environments, supporting the feasibility of facial biometrics for patient identification (Zhang et al., 2021; Kumar et al., 2023). However, there remains a paucity of empirical studies evaluating facial biometric-based EHR systems within Nigerian healthcare institutions, highlighting the need for context-specific research.

Biometrics in Healthcare involves the use of unique biological and physiological characteristics for identifying individuals, typically for security and authentication purposes. Globally, biometrics is increasingly integrated into healthcare systems due to its potential to enhance patient identification accuracy, reduce fraud, and streamline administrative processes. Biometric data includes fingerprints, facial recognition, iris scans, and other modalities that are considered unique to each individual. The technology's appeal lies in its ability to provide a reliable, non-transferable means of identification, which is crucial in healthcare settings where accurate patient identification is critical.

The historical development of biometric technologies dates back to the 19th century, with the introduction of fingerprint analysis for criminal identification. Since then, the technology has evolved significantly, with advancements in computing power, sensor technology, and data analytics contributing to the development of more sophisticated biometric systems. In the 21st century, the adoption of biometrics has expanded beyond law enforcement and into sectors such as healthcare, where it is used to improve the accuracy and security of patient identification processes (Jain and Kumar, 2019).

In healthcare, commonly used biometric modalities include fingerprint recognition, facial recognition, and iris scanning. Fingerprint recognition is perhaps the most widely adopted due to its relatively low cost and ease of implementation. It involves capturing the unique patterns of ridges and valleys on a person's finger, which can then be compared against a stored database for identification purposes. Despite its widespread use, fingerprint recognition is not without challenges, particularly in populations with worn or damaged fingerprints, such as manual laborers or the elderly (Rodriguez and Alonso, 2020).

Facial recognition is another biometric modality that has gained traction in healthcare. This technology analyzes the unique features of a person's face, such as the distance between the eyes, the shape of the jawline, and other facial contours. Facial recognition is often used in conjunction with other biometric modalities to enhance accuracy and reliability. However, it also raises significant privacy concerns, particularly in light of the potential for misuse in surveillance (Dutta and Bhattacharya, 2021).

Iris scanning is considered one of the most accurate biometric modalities, as the patterns in a person's iris are highly unique and stable over time. This technology involves capturing a high-resolution image of the iris, which is then converted into a digital template for comparison. Iris scanning is particularly useful in healthcare settings where high levels of accuracy are required, such as in the identification of unconscious or unresponsive patients. However, the high cost of iris scanning technology can be a barrier to its widespread adoption, particularly in resource-constrained settings (Ali et al., 2022).

In Africa, the adoption of biometric technologies in healthcare is gradually increasing, driven by the need to improve patient identification and reduce healthcare fraud. However, the continent faces unique challenges in implementing these technologies, including infrastructural limitations,

data privacy concerns, and the high cost of deployment. In some African countries, biometric systems have been introduced as part of broader efforts to digitize healthcare services, with mixed results. For instance, in Kenya, the use of biometric systems in hospitals has improved patient tracking but also highlighted issues related to data security and interoperability (Ngugi et al., 2021).

West Africa, a subregion with diverse healthcare challenges, has seen a slower adoption of biometric technologies. The region's healthcare systems are often under-resourced, and the introduction of new technologies like biometrics can be met with resistance due to concerns about cost and sustainability. However, pilot projects in countries like Ghana and Nigeria have shown promise, particularly in urban areas where infrastructure is more developed. These projects have demonstrated the potential of biometrics to improve healthcare delivery, although challenges related to data privacy and system integration remain significant (Osei and Agyeman, 2020).

In Nigeria, the adoption of biometric systems in healthcare varies across states, reflecting the country's diverse socio-economic landscape. In urban areas like Lagos and Abuja, biometric technologies are being integrated into healthcare systems to improve patient identification and reduce administrative inefficiencies. However, in rural areas, where healthcare infrastructure is often lacking, the implementation of these systems is more challenging. Issues such as unreliable electricity, limited internet connectivity, and a shortage of trained personnel hinder the effective use of biometric technologies (Akinwande et al., 2023).

Ondo State provides a specific example of the challenges and opportunities associated with the implementation of biometric systems in healthcare in Nigeria. In recent years, the state government has launched initiatives to improve healthcare services, including the introduction of biometric identification systems. These systems aim to streamline patient registration processes, reduce healthcare fraud, and improve the accuracy of medical records. However, the rollout of these technologies has been uneven, with significant disparities between urban and rural areas (Ajayi and Okunola, 2022).

The implementation of biometric systems in Ondo State has highlighted several key issues, including the need for robust data protection measures and the importance of community engagement. In some rural communities, there is skepticism about the use of biometric technologies, fueled by concerns about data privacy and the potential misuse of personal information. To address these concerns, the state government has launched public awareness campaigns to educate residents about the benefits of biometric systems and the safeguards in place to protect their data (Fasoranti, 2024).

Moreover, the success of biometric systems in Ondo State depends on the integration of these technologies with existing healthcare infrastructure. This requires not only technological investments but also improvements in the overall healthcare delivery system, including training for healthcare workers and the development of standard operating procedures for the use of biometric data. Without these complementary measures, the effectiveness of biometric systems in improving healthcare outcomes may be limited (Olawale and Adebisi, 2021).

Different BPI techniques

Biometric Patient Identification (BPI) refers to the application of biometric technologies to verify and manage patient identities based on their unique physiological or behavioral characteristics. The increasing demand for accurate, secure, and efficient identification in healthcare has led to the adoption of various biometric modalities that help reduce medical errors, eliminate duplicate records, and ensure that patients receive the appropriate care. Several techniques are currently in use across the world, with five being particularly prominent: facial recognition, iris scanning, fingerprint recognition, voice recognition, and palm vein recognition.

2.8.2.2 Facial recognition

Facial recognition has gained widespread adoption due to its contactless nature and ease of integration with surveillance and access control systems. It works by analyzing specific facial features such as the distance between the eyes, nose, and jawline, and

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715456

uses advanced machine learning algorithms to map these features against stored images. The technology is particularly useful in post-COVID-19 environments due to its hygienic advantage, enabling hospitals to identify patients at entry points and retrieve records without physical interaction. Despite these benefits, facial recognition systems can be affected by external factors such as lighting, facial hair, or the wearing of masks, and also raise privacy concerns due to their association with surveillance. Nonetheless, studies affirm its effectiveness in patient identification, especially when combined with AI-based electronic health records (Dutta & Bhattacharya, 2021; Fasoranti, 2023).

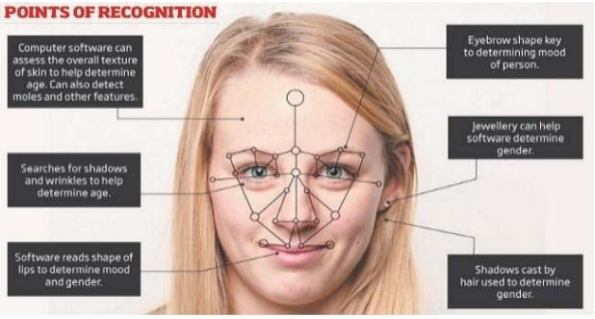

Figure 2.1 Biometric facial recognition technique (All internet security, 2024).

2.8.2.3 IRIS SCANNING

Iris scanning is another highly reliable biometric technique that captures the intricate and unique patterns of the iris, which remain stable over a person's lifetime. This method provides exceptionally high accuracy and is nearly impossible to forge, making it ideal for healthcare settings where security is paramount. Iris scanning is contactless and can differentiate even between identical twins. However, it is relatively expensive to implement and can be hindered by occlusions like eyelashes or poor lighting. Nevertheless, several hospitals and national health projects, especially in Asia and the Middle East, have adopted iris scanning for both patient identification and controlled access to sensitive healthcare data(Ali, Rahman, & Rahman, 2022).

How Iris scanned Records Identities

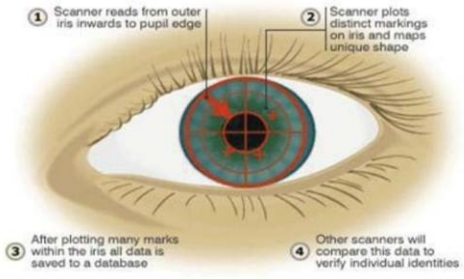

Figure 2.2 Biometric iris scanning technique (Le & Jain, 2009).

2.8.2.4.Finger print

Fingerprint recognition remains the most traditional and widely used biometric system in healthcare. It relies on the unique ridge patterns on a person's fingertips and is favored for its affordability and established infrastructure. In many low- and middle-income countries, including Nigeria and India, fingerprint recognition systems are deployed at the outpatient level for patient registration, medication tracking, and access to medical histories. However, this method requires physical contact, which poses hygiene challenges and may be less effective for elderly patients or individuals with worn-out fingerprints (Rodriguez & Alonso, 2020; Olowokere et al., 2023). Despite these limitations, its reliability and low cost make it a valuable tool in biometric-driven healthcare systems.

Figure 2.3 Finger on sensor device, a scanner (RightPatient, 2024)

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715456

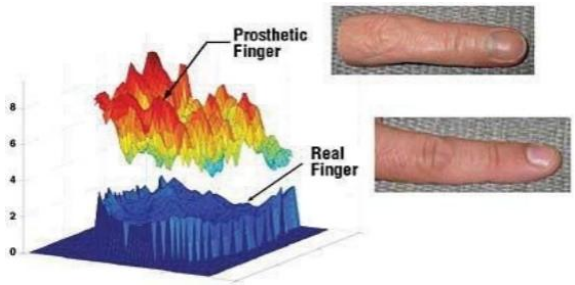

Figure 2.4 Fingerprinting: spoofing versus real (Rowe, 2005).

3.7.2.4 Voice Recognition

Voice recognition, or speaker recognition, is an emerging technique that identifies individuals by analyzing vocal features such as pitch, tone, and speech patterns. It is particularly suitable for remote healthcare services, including telemedicine, patient portals, and interactive voice response systems. One of its key advantages is that it can be used hands-free, making it accessible for people with disabilities. However, it may struggle in noisy environments or when a patient's voice is altered due to illness or emotional distress. Voice biometrics continue to gain traction in healthcare, especially for secure remote authentication (Kumar & Ghosh, 2023; Ngwakongnwi & Agboola, 2021).

2.7.2.5Hand-Palm Veins

Palm vein recognition is a highly secure and contactless biometric modality that uses near-infrared light to capture the unique vein patterns inside a person's hand. As these patterns are internal and cannot be easily forged or observed, palm vein technology offers high resistance to spoofing. It is especially suitable in healthcare contexts where hygiene and security are critical. While more expensive than fingerprint or voice recognition, it is increasingly being adopted in high-end hospitals across Asia, the UAE, and some African urban centers. Its non-intrusive and hygienic nature makes it ideal for environments involving immunocompromised patients (Mensah & Dlamini, 2020; Fasoranti, 2024).

Each of these biometric techniques presents distinct advantages and challenges. While some are favored for their affordability and simplicity (e.g., fingerprint), others offer superior accuracy and security at a higher cost (e.g., iris and palm vein recognition). The selection of an appropriate BPI method in any healthcare setting depends on a range of factors including patient demographics, infrastructure availability, privacy considerations, and cost. Recent advancements also support the deployment of multimodal systems, which combine two or more biometric techniques to enhance overall accuracy and reliability (Almeida & Silva, 2022).

Ultimately, the integration of biometric technologies into healthcare systems represents a significant advancement in ensuring accurate, efficient, and secure patient identification. These systems help mitigate the risks associated with medical errors, improve administrative efficiency, and promote trust in digital health records. As adoption continues to grow, the focus must also include the establishment of strong legal and ethical frameworks to govern data protection and patient privacy.

Figure 2.5 Hand palm vein scanning technique (Ruiz-Blondet, 2014)

2.7.3 Non-Biometric Patient Identification Methods

Non-biometric patient identification (NBPI) methods continue to serve as essential alternatives to biometric systems, especially in healthcare environments where biometric infrastructure is underdeveloped, or where patients express concerns regarding privacy and data protection. These methods are typically based on the use of physical objects or digital artifacts—such as proximity cards and security tokens—that rely on possession or knowledge rather than intrinsic biological features (Patel & Singh, 2021). Although they may not offer the inherent security of biometrics, NBPI systems provide practical, scalable,

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715456

and affordable solutions for secure access and identity verification in clinical settings.

Among the most widely adopted non-biometric techniques are proximity cards, hard tokens, and soft tokens. Each method exhibits distinct characteristics in terms of security level, usability, implementation cost, and risk.

2.7.3.1 Proximity card

Proximity cards, also referred to as radio-frequency identification (RFID) cards or contactless smart cards, are frequently used in hospitals for patient registration, staff authentication, and building access. These cards contain embedded microchips and antennas that transmit a unique identifier when held near a reader. Due to their contactless nature, they offer hygienic interaction, reduce wear and tear, and facilitate quick access to electronic health records (Mensah & Agyeman, 2021). However, they present certain vulnerabilities, including the risk of being lost, stolen, or cloned, particularly if encryption standards are weak (Patel et al., 2023).

Figure 2.6 Proximity card (Ultra Electronics, 2024).

3.7.3.2 Tokens: Hard and Soft

Hard tokens are physical devices that generate dynamic, one-time passwords (OTPs) based on either time or event-triggered algorithms. They are often used by healthcare personnel to access patient databases, prescription systems, or confidential clinical dashboards. Examples of hard tokens include smartcards, USB security keys, and fobs with LCD displays (Lee & Kim, 2022). These tokens offer higher levels of security compared to proximity cards and can function without internet connectivity. However, they come with limitations such as higher cost, susceptibility to loss or damage, and limited scalability for large patient populations (Kim & Lee, 2023).

Soft tokens function similarly to hard tokens but exist in software form, typically as mobile apps. Applications like Google Authenticator and Microsoft Authenticator generate OTPs that expire within a short window, ensuring time-bound access to secure platforms. In healthcare, soft tokens are increasingly used in telemedicine, mobile patient portals, and self-service appointment systems (Kaur & Yadav, 2023). Their advantages include convenience, widespread availability, and lower implementation cost. However, their effectiveness depends on the user's smartphone security, battery availability, and device literacy. They are also vulnerable to malware, phishing attacks, or SIM-swapping if not properly managed (Patel et al., 2023). When compared to biometric modalities such as fingerprint, facial recognition, or iris scanning, these non-biometric systems are less secure due to their reliance on possession. Nonetheless, they remain critical for augmenting security in resource-limited environments and for patients unwilling or unable to enroll in biometric systems. Their integration into multi-factor authentication (MFA) frameworks, combining something the user has (e.g., token or card) with something they know (e.g., password) or something they are (e.g., fingerprint), significantly enhances overall system integrity (Kim & Lee, 2023).

III. METHODOLOGY

3.1 Research design

An experimental research design was adopted for this study. This design enabled the development, implementation, and systematic evaluation of a facial biometric-based patient identification system under real clinical conditions.

3.2 Study area and population

The study was conducted at a tertiary healthcare institution in southwestern Nigeria. The study population comprised registered patients attending outpatient services during the study period. A purposive sampling technique was used to select 50 patients who consented to participate in the study.

3.3 Data collection

Facial images were captured using a standard webcam under normal hospital lighting conditions. Each participant's face was captured three times to

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715456

account for minor variations in facial expression and posture, resulting in a total of 150 facial images. Demographic and clinical attributes, including age, gender, blood group, and genotype, were also collected.

Table 1. Demographic characteristics of study participants (n = 50)

Variable	Category	Frequency	Percentage (%)
Gender	Male	28	56
	Female	22	44
Age group	18–30	14	28
	31–45	21	42
	46–60	10	20
	>60	5	10

3.4 System architecture

The developed system consisted of four major modules: image acquisition, face detection and recognition, database management, and user interface. Java was used for system development, OpenCV for image processing, and MySQL for data storage.

Figure 1. System architecture of the facial biometric-based EHR system.

Figure 1 illustrates the interaction between the webcam-based image acquisition module, the facial recognition engine, the database server, and the user interface during patient registration and identification.

The overall architecture of the proposed facial biometric-based electronic health record system is illustrated in Figure 1. The system consists of an image acquisition module, a facial recognition engine, a relational database for biometric and clinical data, and a Java-based clinical user interface

3.5 Performance evaluation metrics

System performance was evaluated using standard biometric metrics recommended by ISO/IEC 19795-1 (2021): face detection accuracy, face recognition accuracy, false acceptance rate (FAR), false rejection rate (FRR), and average system response time.

IV. RESULTS

The performance evaluation results indicate that the developed system achieved high accuracy and efficiency.

Table 2. Performance metrics of the facial recognition system

Metric	Value
Face detection accuracy	98.67%
Face recognition accuracy	94.67%
False acceptance rate (FAR)	2.67%
False rejection rate (FRR)	2.67%
Average response time	1.82 seconds

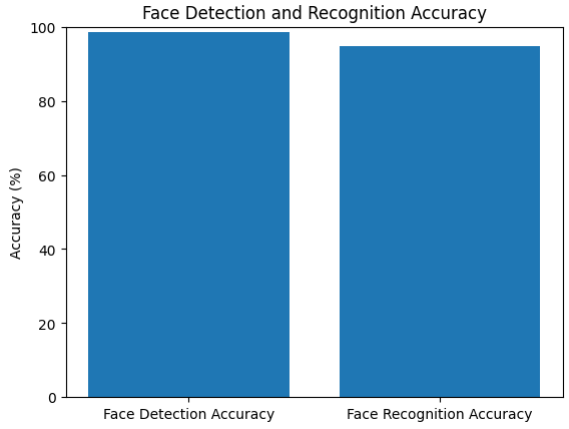

Figure 2. Face detection and recognition accuracy comparison. Figure 2 presents a bar chart comparing face detection accuracy and face recognition accuracy, demonstrating consistently high system performance.

Figure 2 presents the comparative performance of the face detection and face recognition components of the developed system. The face detection module achieved an accuracy of 98.67%, while the face recognition module recorded 94.67%. The high detection accuracy indicates effective localization of facial regions under real hospital conditions, while

© MAR 2026 | IRE Journals | Volume 9 Issue 9 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715456

the recognition accuracy confirms reliable patient identification once facial features were extracted

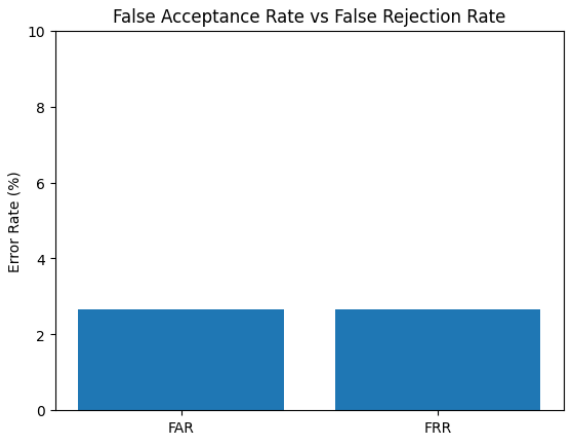

Figure 3. False acceptance rate and false rejection rate. Figure 3 illustrates the low FAR and FRR values recorded by the system, indicating strong reliability.

As shown in Figure 3, the False Acceptance Rate (FAR) and False Rejection Rate (FRR) were both 2.67%. These low error rates demonstrate strong system reliability and suggest that the likelihood of misidentifying patients or rejecting valid patients is minimal, which is critical for clinical deployment.

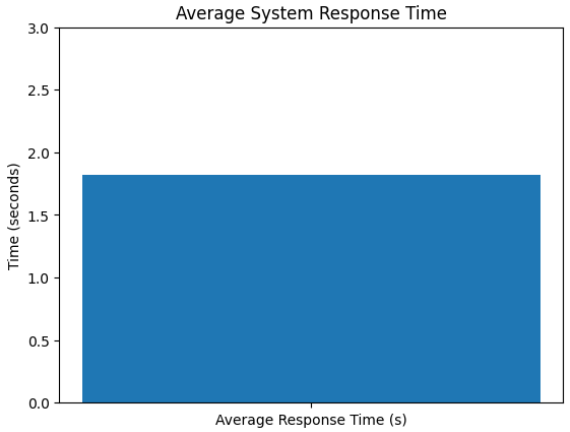

Figure 4. Average system response time. Figure 4 shows the average time required for patient identification and record retrieval. Figure 4 illustrates the average system response time recorded during patient identification and record retrieval. The system achieved an average response time of 1.82 seconds, indicating that biometric authentication and EHR retrieval can be performed in near real time without disrupting clinical workflows.

V. DISCUSSION

The face detection accuracy of 98.67% demonstrates the effectiveness of the detection algorithm under real hospital conditions. The recognition accuracy of 94.67% is consistent with results reported in similar healthcare biometric studies (Zhang et al., 2021; Kumar et al., 2023). Low FAR and FRR values indicate that the system minimizes both false matches and false rejections, which is essential for patient safety.

The average response time of 1.82 seconds suggests that the system can support real-time patient identification without disrupting clinical workflows. These findings confirm that facial recognition is a viable biometric modality for patient identification in Nigerian healthcare environments.

VI. ETHICAL CONSIDERATIONS

Ethical approval was obtained from the hospital management. Participation was voluntary, and informed consent was obtained from all participants. All biometric and clinical data were securely stored and used strictly for research purposes.

VII. CONCLUSION

This study designed, implemented, and evaluated a facial biometric-based electronic health record and patient identification system suitable for deployment in low-resource healthcare settings. The system demonstrated high accuracy, low error rates, and fast response time, confirming its suitability for real-time clinical use. The findings contribute empirical evidence to health informatics literature and support the adoption of facial biometrics in Nigerian healthcare institutions.

VIII. LIMITATIONS AND FUTURE WORK

The study was limited by a relatively small sample size and single-institution setting. Future research should involve multi-center evaluations, integration

of multi-modal biometrics, cloud-based architectures, and comprehensive data privacy frameworks.

REFERENCES

[1] Adler-Milstein, J., Holmgren, A. J., Kralovec, P., Worzala, C., Searcy, T., & Patel, V. (2020). Electronic health record adoption in US hospitals: The emergence of a digital advanced use divide. *Journal of the American Medical Informatics Association, 27*(4), 567–575. https://doi.org/10.1093/jamia/ocz204

[2] Adebayo, O. A., Salami, A. O., & Musa, I. T. (2021). Health information management practices in Nigerian tertiary hospitals. *African Journal of Health Information Management, 5*(2), 45–58.

[3] Bradski, G., & Kaehler, A. (2018). *Learning OpenCV 3: Computer vision in C++ with the OpenCV library*. O'Reilly Media.

[4] Greenly, M., McElroy, T., & Shaw, R. (2020). Patient identification errors: Causes and prevention strategies. *Journal of Patient Safety, 16*(3), e150–e156. https://doi.org/10.1097/PTS.0000000000000478

[5] Healthcare Information and Management Systems Society. (2021). *Patient identification and matching in healthcare*. HIMSS.

[6] International Organization for Standardization/International Electrotechnical Commission. (2021). *Biometric performance testing and reporting (ISO/IEC 19795-1)*. ISO.

[7] Jain, A. K., Ross, A., & Nandakumar, K. (2019). *Introduction to biometrics*. Springer.

[8] Kellermann, A. L., & Jones, S. S. (2019). What it will take to achieve the as-yet-unfulfilled promises of health information technology. *Health Affairs, 38*(10), 1700–1705. https://doi.org/10.1377/hlthaff.2019.00745

[9] Kumar, R., Singh, S., & Verma, P. (2023). Facial recognition-based patient identification system for smart healthcare. *International Journal of Medical Informatics, 171*, 104998. https://doi.org/10.1016/j.ijmedinf.2023.104998

[10] Li, S. Z., & Deng, W. (2022). Deep facial recognition: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 44*(9), 4976–4999. https://doi.org/10.1109/TPAMI.2020.3036097

[11] Ojo, A. I., & Popoola, S. O. (2020). Medical records management and service delivery in Nigerian hospitals. *Health Information Management Journal, 49*(2–3), 82–90. https://doi.org/10.1177/1833358319872884

[12] Olatunji, O. M., Adewale, B. A., & Aremu, A. S. (2022). Challenges of electronic health record implementation in Nigeria. *Journal of Health Informatics in Developing Countries, 16*(1), 1–15.

[13] Turk, M., & Pentland, A. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience, 3*(1), 71–86. https://doi.org/10.1162/jocn.1991.3.1.71

[14] Viola, P., & Jones, M. (2004). Robust real-time face detection. *International Journal of Computer Vision, 57*(2), 137–154. https://doi.org/10.1023/B:VISI.0000013087.49260.fb

[15] World Health Organization. (2019). *Patient identification*. WHO.

[16] Zhang, Y., Wang, L., & Liu, H. (2021). Facial recognition-based healthcare authentication system. *IEEE Access, 9*, 128345–128356. https://doi.org/10.1109/ACCESS.2021.3112634