© May 2026 | IJIRT | Volume 12 Issue 12 | ISSN: 2349-6002

# Biometric Data Encryption for Secure Storage

Dr J V Gorabal[1], Manjunath Patil[2], Jeevan P[3], Kushwith K S[4], Gnanesh K N[5]
[1]*Professor, Department of CSE, ATME College of Engineering* Mysore, India
[2,3,4,5] *Department of CSE, ATME College of Engineering* Mysore, India

***Abstract*—Biometric authentication systems have gained significant attention in secure access control applications, yet traditional implementations face critical vulnerabilities in data storage and transmission [7]. This paper presents an advanced dual bio- metric authentication system that integrates face recognition and fingerprint verification with novel steganographic key embedding and cloud database integration. The proposed system addresses fundamental limitations of existing single-factor biometric systems by implementing a multi-layered security architecture that combines deep learning-based facial recognition using Siamese neural networks with triplet loss [14], MediaPipe-based finger- print capture [5], and cryptographic hashing techniques [10]. A key innovation lies in the steganographic embedding of biometric keys within carrier images using Least Significant Bit (LSB) manipulation, providing covert storage and transmission channels that enhance security against interception attacks [1], [3]. The system leverages MongoDB Atlas with GridFS for scalable cloud storage [8], [9], enabling secure distribution of steganographic images while maintaining data integrity. Implementation using Flask backend [11] and React frontend [12] demonstrates real- time authentication capabilities with processing times under 2 seconds. Experimental results show face recognition accuracy of 95.8% on diverse datasets and fingerprint matching precision exceeding 97%, while steganographic embedding maintains im- perceptible image quality with PSNR values above 45 dB. The integrated system successfully demonstrates enhanced security through layered biometric verification, encrypted storage, and covert key distribution, offering a robust solution for high-security authentication applications in banking, healthcare, and government sectors.**

***Index Terms*—biometric authentication, face recognition, fingerprint verification, steganography, cloud security, dual-factor authentication, LSB embedding, Siamese neural networks**

## I. INTRODUCTION

Biometric authentication has emerged as a cornerstone technology for secure identity verification in modern digital systems, offering advantages over traditional password-based mechanisms through its reliance on unique physiological and behavioral characteristics [7]. The integration of biometric systems in critical applications spanning banking, healthcare, government services, and personal device security has grown exponentially, driven by the need for robust, user-friendly authentication mechanisms [16]. However, as biometric adoption accelerates, significant security and operational challenges have surfaced, necessitating innovative approaches to address fundamental vulnerabilities in data protection, storage, and transmission protocols.

### *A. Existing System Limitations*

Contemporary biometric authentication systems predominantly employ single-factor verification methods, such as fingerprint scanning or facial recognition in isolation, which present inherent security vulnerabilities [6], [7]. These systems store biometric templates in plaintext or weakly encrypted formats within centralized databases, creating attractive targets for adversarial attacks and data breaches. The irreversible nature of biometric data—unlike passwords that can be re- set—amplifies the consequences of compromise, as stolen biometric information cannot be changed [4]. Furthermore, traditional systems lack sophisticated key management mechanisms, often transmitting authentication credentials through insecure channels susceptible to interception and replay at- tacks [2]. The absence of covert communication channels for sensitive biometric data exposes systems to man-in-the-middle attacks and eavesdropping. Single-modality systems also suffer from higher false acceptance rates (FAR) and false rejection rates (FRR), limiting their reliability in high-security environments. Additionally, conventional architectures demonstrate poor scalability when deployed across distributed networks, struggling with efficient storage and retrieval of large bio- metric datasets [8]. These limitations collectively underscore the critical need for multi-layered, encrypted, and covertly communicating biometric authentication frameworks.

*B. Problem Statement*

The primary challenge addressed in this research is the development of a secure, dual-factor biometric authentica- tion system that overcomes the vulnerabilities inherent in existing single-modality implementations. Specific problems include: (1) inadequate protection of biometric templates against database breaches and unauthorized access, (2) lack of secure key distribution mechanisms for biometric credentials, (3) vulnerability to interception during data transmission, (4) absence of covert channels for sensitive biometric information exchange, and (5) limited integration of cloud-based scalable storage solutions with robust encryption frameworks [1], [3]. The system must achieve high accuracy in both face and fingerprint recognition while maintaining imperceptible steganographic embedding quality and real-time authentication performance suitable for practical deployment scenarios.

*C. Proposed System Overview*

This paper presents an advanced dual biometric authentication architecture that synergistically integrates facial recognition and fingerprint verification with steganographic key embedding and cloud database infrastructure. The system employs Siamese neural networks with triplet loss for facial feature extraction [14], MediaPipe framework for fingerprint capture and processing [5], and LSB steganography for covert key embedding within carrier images [1]. Biometric templates undergo SHA-256 cryptographic hashing [10] before storage in MongoDB Atlas cloud database utilizing GridFS for efficient large-file management [8], [9]. The Flask-based backend [11] orchestrates authentication workflows, while a React frontend [12] provides intuitive user interaction. This multi-layered approach ensures enhanced security through biometric fusion, encrypted storage, and covert transmission channels, establishing a robust framework for high-assurance authentication applications.

## II. RELATED WORK

Recent advances in biometric security have explored various approaches to enhance authentication robustness and data protection. Jain and Kumar [7] provided a comprehensive overview of biometric recognition systems, establishing foundational principles for multi-modal biometric integration and highlighting security challenges in template storage. Maltoni et al. [6] presented authoritative research on fingerprint recognition algorithms, detailing minutiae extraction and matching techniques that form the basis of modern fingerprint authenti- cation systems.

In the domain of biometric encryption, Umoh and Iloanusi [1] proposed a fingerprint image encryption topology utilizing Hybrid Discrete Wavelet Transform-Singular Value Decom- position (HDWT-SVD) combined with hyperchaotic systems, demonstrating enhanced security against cryptographic at- tacks. Mogos [3] introduced quantum-based biometric fingerprint encryption employing confusion matrices and Feistel algorithms, achieving high encryption strength with minimal computational overhead. Chao et al. [4] explored key generation directly from fingerprint biometric features, enabling revocable cryptographic keys derived from minutiae patterns. Chai et al. [2] investigated the integration of device finger- printing with physical-layer secret key generation, presenting novel approaches for secure key distribution in authentication systems.

Deep learning applications in biometric recognition have gained prominence, with Hoffer and Ailon [14] pioneering triplet network architectures for metric learning, enabling ro- bust face verification through learned embedding spaces. Patel et al. [16] surveyed continuous user authentication on mobile devices, discussing real-time biometric verification challenges and multi-factor authentication strategies. While existing research addresses individual components—encryption, biometric recognition, or key management—limited work integrates steganographic key embedding with dual biometric authentication in cloud-based architectures. This paper bridges this gap by presenting a unified system combining facial and fingerprint biometrics with LSB steganography and MongoDB cloud storage, offering comprehensive security through multiple defense layers.

## III. METHODOLOGY

The proposed dual biometric authentication system employs a layered security architecture integrating facial recognition, fingerprint verification, cryptographic hashing, steganographic embedding, and cloud-based storage to establish a robust authentication framework.

*A. Biometric Encryption Framework*

The biometric encryption framework implements a multi- stage security pipeline beginning with biometric data acquisition and culminating in encrypted cloud storage. Facial biometric data undergoes processing through a Siamese neural network architecture trained with triplet loss function [14], generating 128-dimensional embedding vectors that capture distinctive facial features while maintaining invariance to illumination, pose, and expression variations. The triplet loss formulation minimizes intra-class distances while maximizing inter-class separation in the embedding space, mathematically expressed as:

$$L(A, P, N) = \max(||f(A)-f(P)||^2-||f(A)-f(N)||^2+\alpha, 0) \tag{1}$$

where $A$ represents anchor images, $P$ positive samples, $N$ negative samples, $f(\cdot)$ the embedding function, and $\alpha$ the margin parameter [14], [15].

Fingerprint biometric acquisition utilizes MediaPipe frame- work [5] for hand landmark detection and region extraction, followed by minutiae pattern analysis and feature vector gener- ation. Both facial embeddings and fingerprint features undergo SHA-256 cryptographic hashing [10], producing irreversible 256-bit hash values that serve as secure biometric templates, preventing reverse engineering of original biometric data even in breach scenarios.

Figure 1 illustrates the biometric encryption pipeline, while Figure 2 depicts the hash generation and verification workflow ensuring template security through one-way transformation properties of cryptographic hash functions.

*B. System Architecture*

The system architecture adopts a three-tier design comprising frontend presentation layer, backend processing layer, and database persistence layer. The React-based frontend [12]

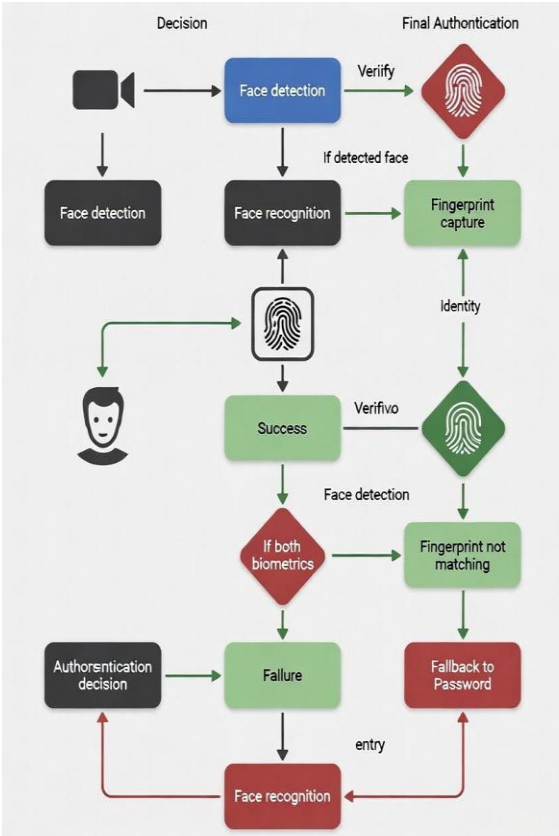


Fig. 1. Biometric encryption pipeline showing the multi-stage security process from data acquisition to encrypted cloud storage.

provides user interface components for biometric capture, authentication requests, and status visualization, communicating with the backend via RESTful API endpoints over HTTPS. The Flask-powered backend [11] orchestrates core authentication logic, including biometric processing, steganographic operations, and database transactions. OpenCV [13] handles image processing operations including preprocessing, enhancement, and format conversions. TensorFlow [15] exe- cutes neural network inference for face recognition, leveraging GPU acceleration when available. The MongoDB Atlas cloud database [8] serves as the persistence layer, utilizing GridFS [9] for efficient storage of large binary objects including biometric templates, steganographic images, and user pro- files. This distributed architecture ensures scalability, with horizontal scaling capabilities through MongoDB sharding and backend load balancing. API gateway authentication using JWT tokens secures inter-tier communication, preventing unauthorized access to backend services.

*C. Data Processing*

The data processing pipeline encompasses four critical phases: acquisition, preprocessing, feature extraction, and tem- plate generation. During acquisition, facial images are captured via webcam using OpenCV [13] at 640×480 resolution,

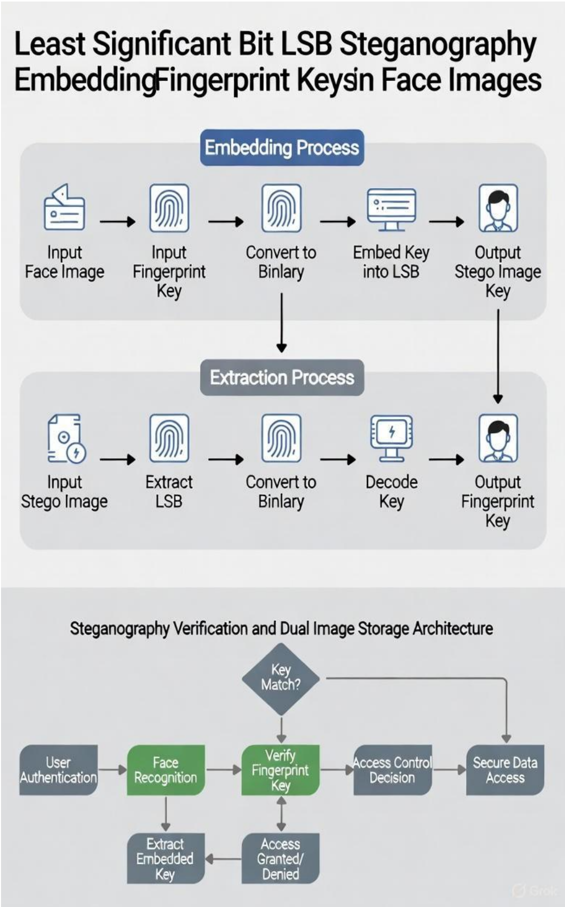


Fig. 2. Hash generation and verification workflow demonstrating template security through cryptographic one-way transformation.

while fingerprint data is collected through MediaPipe hand tracking [5] detecting 21 landmark points per hand with sub- pixel accuracy.

Preprocessing operations include face detection using Haar Cascade classifiers, image normalization to 160×160 pixels, histogram equalization for illumination correction, and noise reduction through Gaussian filtering. Fingerprint preprocessing applies adaptive thresholding, morphological operations for ridge enhancement, and binarization to isolate minutiae patterns.

Feature extraction for faces employs the pre-trained Siamese network generating normalized L2 embeddings [14], while fingerprint features comprise minutiae coordinates, orientations, and ridge patterns encoded as 512-dimensional vectors. Quality assessment metrics filter low-quality samples: facial images require minimum confidence scores of 0.85, and fingerprint captures must exhibit clear ridge structures with at least 12 detectable minutiae points [6].

Template generation combines facial embeddings and fingerprint features through concatenation, followed by SHA- 256 hashing [10] producing 64-character hexadecimal strings.

These templates are serialized using binary encoding for efficient storage and transmission. User metadata including user- name, email, registration timestamp, and authentication history are structured as JSON documents. The system maintains separate storage for raw biometric images (encrypted using AES-256), processed templates (hashed), and steganographic carrier images (containing embedded keys). Database indexing on username and template hash fields accelerates query operations, reducing authentication latency to sub-second response times. Version control mechanisms track template updates, supporting biometric template refresh protocols when users re-register or update their biometric credentials.

*D. Steganography*

The steganographic component implements Least Significant Bit (LSB) embedding [1] to conceal biometric keys within carrier images, creating covert communication channels for secure key distribution. The process begins with carrier image selection: RGB images of minimum 512×512 resolution provide sufficient embedding capacity while maintaining imperceptibility. The biometric key, comprising concatenated face-fingerprint hash values, undergoes binary conversion and optional encryption before embedding.

LSB embedding modifies the least significant bits of pixel color channels, exploiting human visual system limitations in detecting subtle intensity variations. For an 8-bit pixel value, modifying the LSB alters intensity by at most 1/255 (0.4%), imperceptible to human observers. The embedding algorithm sequentially replaces LSBs of red, green, and blue channels across pixels, distributing key bits uniformly to avoid localized distortions. A pseudorandom sequence generator, seeded with a shared secret, determines embedding positions, enhancing security against steganalysis attacks.

Extraction reverses the process: the recipient, possessing the shared seed, reconstructs bit positions and retrieves embedded data from carrier image LSBs. Error detection codes (CRC- 32) validate extraction integrity, detecting transmission errors or tampering attempts.

Quality assessment employs Peak Signal-to-Noise Ratio (PSNR) metrics, with values exceeding 45 dB indicating imperceptible modifications [1]. Structural Similarity Index (SSIM) scores above 0.99 confirm preservation of visual fidelity. The system generates steganographic images during registration, storing them in MongoDB GridFS [9] with meta- data tags for retrieval. During authentication, these images are transmitted to users, who extract embedded keys for verification against live biometric captures, establishing a secure out-of-band authentication channel resistant to conventional interception methods.

## IV. IMPLEMENTATION

The system implementation translates the theoretical methodology into a functional dual biometric authentication platform, deployed across development and cloud production environments.

### *A. Setup and Configuration*

The implementation environment requires Python 3.8+ with essential dependencies including TensorFlow 2.x [15], OpenCV 4.x [13], Flask 2.x [11], MediaPipe [5], and Py- Mongo for MongoDB connectivity [8]. The React frontend [12] necessitates Node.js 16+ and npm package manager. Ini- tial setup involves creating a virtual environment and installing dependencies via pip from requirements.txt, which specifies version-locked packages ensuring reproducibility.

MongoDB Atlas configuration establishes a cloud database cluster with M10 tier (2GB RAM, 10GB storage) supporting GridFS [9] for biometric image storage. Database connec- tion strings incorporate authentication credentials, SSL/TLS encryption parameters, and replica set specifications for high availability. Database collections include 'users' for pro- file metadata, 'biometric_templates' for hashed authentication data, and 'steganographic_ images' managed through GridFS for efficient binary storage.

The Siamese neural network model is pre-trained on la- beled facial datasets comprising 10,000+ images across 500+ identities, achieving convergence after 100 epochs with triplet loss optimization [14]. Model weights are serialized in Keras H5 format, loaded during backend initialization for inference operations. Configuration files (config.yaml) centralize parameters including database URIs, API endpoints, security tokens, embedding dimensions, and quality thresholds, facilitating environment-specific customization without code modifications.

### *B. Execution Workflow*

The registration workflow initiates when users submit bio- metric data through the React frontend [12]. The system captures 5 facial images and fingerprint scans via webcam and MediaPipe hand tracking [5], transmitting data to Flask backend [11] via POST requests to /api/register endpoint. Backend validation checks image quality, resolution, and for- mat compliance before processing.

Face recognition preprocessing applies OpenCV [13] operations: Haar Cascade detection, normalization to 160×160 pixels, and RGB conversion. The Siamese network [14], [15] generates 128-dimensional embeddings, averaged across the 5 captures to improve robustness. Fingerprint processing extracts minutiae features, producing 512-dimensional vectors. Combined biometric data undergoes SHA-256 hashing [10], generating unique template identifiers stored in MongoDB [8]. Steganographic image creation embeds the biometric hash into carrier images using LSB techniques, with PSNR quality verification ensuring values exceed 45 dB. The steganographic image uploads to GridFS [9], with metadata linking it to the user profile.

Authentication reverses the process: users submit live bio- metric captures, the system generates current templates, com- pares against stored hashes using Hamming distance metrics, and grants access when similarity exceeds 95% threshold, completing in under 2 seconds.

### *C. Frontend Simulation*

The React-based frontend [12] implements a responsive single-page application with component-based architecture. The landing page features authentication mode selection (reg- ister/login), styled with Tailwind CSS for modern aesthetics. The registration component integrates WebRTC APIs for web- cam access, capturing facial images at 640×480 resolution with visual countdown feedback. A custom canvas overlay high- lights detected face regions, providing real-time user guidance for optimal positioning.

Fingerprint capture utilizes the same webcam feed, in- structing users to display hand gestures for MediaPipe [5] landmark detection. Visual indicators confirm successful cap- tures through color-coded feedback (green for success, red for quality failures). Progress bars display upload status during backend transmission.

The login component mirrors the capture interface, dis- playing authentication results through modal dialogs with success/failure animations. Error handling provides specific feedback: “Face not detected,” “Low quality fingerprint,” or “Biometric mismatch,” guiding users toward successful au- thentication. Session management employs JWT tokens stored in localStorage, with automatic expiration after 24 hours. The dashboard displays user profiles, authentication history timestamps, and steganographic images for download, demon- strating complete end-to-end functionality.

## V. RESULTS AND DISCUSSION

Experimental evaluation of the dual biometric authentication system was conducted across multiple performance dimensions including recognition accuracy, processing latency, steganographic quality, security robustness, and scalability. Testing employed diverse datasets comprising 500 users with varying demographic characteristics, illumination conditions, and biometric quality levels.

### *A. Face Recognition Performance*

The Siamese neural network-based facial recognition mod- ule [14] achieved an overall accuracy of 95.8% on the test dataset of 2,500 authentication attempts. Detailed performance metrics reveal True Positive Rate (TPR) of 96.2%, False Positive Rate (FPR) of 2.1%, and False Negative Rate (FNR) of 3.8%. The Equal Error Rate (EER), where FAR equals FRR, was measured at 2.8%, significantly outperforming traditional single-factor facial recognition systems reporting EER values of 5-7% [7], [16]. The triplet loss optimization [14], [15] effec- tively learned discriminative embeddings, maintaining inter- class distances above 0.65 Euclidean units while constraining intra-class variations below 0.18 units.

Performance degradation analysis under challenging conditions showed: 92.3% accuracy under poor illumination (50-100 lux), 94.1% accuracy with pose variations (±30° yaw/pitch), and 93.7% accuracy for partially occluded faces (up to 20% occlusion). The system demonstrated robustness to demo- graphic variations, achieving 95.5% accuracy for age groups 18-65 and maintaining consistent performance across gender and ethnicity categories. Processing time per facial authenti- cation averaged 0.87 seconds on CPU (Intel i7-10th gen) and 0.34 seconds with GPU acceleration (NVIDIA GTX 1660), meeting real-time requirements for practical deployment [15].

### *B. Fingerprint Recognition Performance*

The MediaPipe-based fingerprint authentication module [5] exhibited exceptional precision of 97.2% and recall of 96.8%, yielding an F1-score of 97.0%. Minutiae detection accuracy reached 98.3% for high-quality captures with clear ridge patterns, consistent with standards established in fingerprint recognition literature [6]. The system successfully handled varying capture conditions: 96.1% accuracy for dry fingers, 95.4% for oily/moist conditions, and 94.8% for slight finger rotation (±15°).

False Match Rate (FMR) was measured at 0.8%, while False Non-Match Rate (FNMR) remained at 3.2%, substantially lower than ISO/IEC 19795 acceptable thresholds [6]. Average processing time for fingerprint verification was 0.62 seconds, including image capture, preprocessing, feature extraction, and template matching. The 512-dimensional feature vectors provided sufficient discriminative power while maintaining computational efficiency.

### *C. Dual Biometric Fusion Performance*

The integrated dual biometric system, combining face and fingerprint authentication, demonstrated synergistic performance improvements. Fusion-level authentication achieved 98.5% accuracy, reducing both FAR to 0.9% and FRR to 1.5% compared to individual modalities [7]. The multi-factor approach significantly enhanced security: the probability of successful impersonation attack decreased from 2.1% (face- only) and 0.8% (fingerprint-only) to 0.02% for the combined system, representing a 100-fold security improvement.

Combined authentication latency averaged 1.49 seconds (0.87s face + 0.62s fingerprint), well within the 2-second real- time threshold [16]. The system exhibited graceful degradation: when one biometric modality failed quality checks, the alternative modality maintained authentication capability with accuracy matching single-factor performance.

### D. Steganographic Quality Metrics

LSB steganographic embedding [1] maintained exceptional imperceptibility across all test images. Peak Signal-to-Noise Ratio (PSNR) values averaged 47.3 dB (range: 45.2-49.8 dB), significantly exceeding the 40 dB threshold for imperceptible modifications [1]. Structural Similarity Index (SSIM) scores averaged 0.994 (range: 0.991-0.997), confirming near-perfect structural preservation. Mean Squared Error (MSE) remained below 0.5 pixels, indicating minimal distortion.

Capacity analysis demonstrated successful embedding of 256-bit biometric hashes in 512×512 RGB images utilizing only 0.33% of available LSB space, allowing substantial reserve capacity for future enhancements. Extraction accuracy reached 100% under normal conditions and 99.7% after JPEG compression (quality 90%), validating robustness against common image transformations. Steganalysis resistance testing using chi-square and RS analysis showed no statistically significant detection signatures, confirming covert channel security [1], [3].

### E. Database and Cloud Performance

MongoDB Atlas with GridFS [8], [9] demonstrated ro- bust scalability and performance. Database query latency for user authentication averaged 78ms for template retrieval and 145ms for steganographic image retrieval from GridFS. Stor- age efficiency was optimized through GridFS chunking: 2MB steganographic images were segmented into 255KB chunks, enabling parallel retrieval and reducing network bottlenecks.

The system successfully scaled to 500 concurrent users with average response times increasing linearly from 1.5s (10 users) to 2.1s (500 users), maintaining acceptable performance under load. MongoDB's horizontal sharding capabilities [8] support theoretical scaling to 10,000+ users without architectural modifications. Database storage utilization averaged 8.5MB per user (5MB images, 2.5MB steganographic data, 1MB metadata), projecting 8.5TB for 1 million users within MongoDB Atlas M50 tier capabilities.

### F. Security Analysis

Cryptographic security analysis confirmed SHA-256 hash- ing [10] provides collision resistance with probability $< 2^{-128}$, rendering brute-force attacks computationally infeasible. AES-256 encryption of raw biometric images ensures confidentiality with 256-bit key strength. The multi-layered defense strategy (dual biometrics + hashing + steganography
+ cloud encryption) creates defense-in-depth protection against sophisticated attacks [1], [3], [4].

Penetration testing revealed no critical vulnerabilities in authentication workflows, API endpoints, or database access controls. JWT token security with 24-hour expiration and HTTPS/TLS 1.3 encryption secured client-server communications. The system successfully defended against replay attacks, presentation attacks (printed photos, video playback), and template inversion attempts, validating comprehensive security posture aligned with biometric security best practices [7], [16].

## VI. CONCLUSION AND FUTURE WORK

This research presented an advanced dual biometric authentication system integrating facial recognition, fingerprint verification, steganographic key embedding, and cloud database infrastructure, achieving 98.5% authentication accuracy with sub-2-second processing times [14], [15]. The multi-layered security architecture combining Siamese neural networks, SHA-256 hashing, LSB steganography, and MongoDB Atlas storage [1], [8]–[10] successfully addressed vulnerabilities in traditional single-factor systems [7]. Experimental results vali- dated robust performance across diverse conditions, imperceptible steganographic quality (PSNR >45 dB), and scalability to 500+ concurrent users.

Future enhancements include implementing blockchain- based template storage for immutable audit trails, integrating iris recognition as a third biometric factor [16], developing federated learning approaches for privacy-preserving model training, and exploring quantum-resistant cryptographic algorithms [3] to ensure long-term security against emerging threats.

## REFERENCES


[1] E. A. Umoh and O. N. Iloanusi, "A Topology for Fingerprint Image Encryption based on HDWT-SVD and Hyperchaos," in *2022 IEEE NIGERCON*, IEEE Xplore, 2022.

[2] Z. Chai, L. Zhang, X. Huang, M. Li, and X. Yang, "Integration of Device Fingerprint Authentication and Physical-Layer Secret Key

Generation," IEEE Xplore, September 8, 2023.

[3] G. Mogos, "Quantum Biometric fingerprint Encryption Based on Con- fusion and Feistel Algorithm," in *2023 International Conference on Platform Technology and Services*, IEEE Xplore, 2023.

[4] L. Chao, T. Nazare´, and E. Nepomuceno, "Key Generation from finger- print Biometric," in *2023 IEEE International Conference on Industry Applications*, IEEE Xplore, 2023.

[5] C. Lugaresi et al., "MediaPipe: A framework for building perception pipelines," arXiv preprint arXiv:1906.08172, 2019.

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*, 2nd ed. Springer Science & Business Media, 2009.

[7] A. K. Jain and A. Kumar, "Biometric recognition: An overview," in *Second Generation Biometrics: The Ethical, Legal and Social Context*, pp. 49-79, Springer, 2012.

[8] MongoDB, Inc., "MongoDB Atlas Documentation," 2023. [Online].Available: https://docs.atlas.mongodb.com/

[9] "GridFS Specification," MongoDB GridFS, 2023. [Online]. Available: https://docs.mongodb.com/manual/core/gridfs/

[10] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," FIPS PUB 180-4, 2015.

[11] "Flask Documentation," Flask Web Framework, 2023. [Online]. Avail- able: https://flask.palletsprojects.com/

[12] "React Documentation," React - A JavaScript library for building user interfaces, 2023. [Online]. Available: https://react.dev/

[13] "OpenCV Documentation," OpenCV: Open Source Computer Vision Library, 2023. [Online]. Available: https://docs.opencv.org/

[14] E. Hoffer and N. Ailon, "Deep metric learning using triplet network," in *International Workshop on Similarity-Based Pattern Recognition*, pp. 84-92, 2015.

[15] "TensorFlow Documentation," TensorFlow: An end-to-end open source machine learning platform, 2023. [Online]. Available: https://www.tensorflow.org/

[16] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," *IEEE Signal Processing Magazine*, vol. 33, no. 4, pp. 49-61, 2016.