A Privacy-Enhanced Crypto-Biometric Authentication Framework For Airport Authority Access Control

Mr. Mohanasundaram A[1], Shanmugasundaram D[2], Thamizhselvan R[3], Prem Kumar J[4], Majivalavan S[5]
[1]Assist prof, Dept of Computer Science and Engineering
[2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] Chri Mahendra Institute of Engineering and Technology, Namakkal, Tamil Nadu, India

Abstract- *Airport authority systems demand the highest levels of security for controlling access to restricted zones, yet traditional authentication mechanisms based on identity cards, PINs, and passwords remain inherently susceptible to theft, forgery, duplication, and social engineering attacks. Biometric authentication offers a more reliable alternative; however, conventional face recognition systems face critical challenges including spoofing vulnerabilities, inadequate privacy preservation for stored biometric templates, and limited accuracy in live-face detection. This paper proposes a Privacy-Enhanced Crypto-Biometric Authentication Framework (PECBAF) specifically tailored for airport authority access control, extending the cancellable template protection scheme of Imran et al. [1] to the facial biometric domain. The proposed framework integrates the Grassmann manifold algorithm for live facial feature extraction, deriving approximately 1024 discriminative features from 76 key facial landmark points. The extracted facial feature subspace representation is subjected to a Möbius conformal transformation parameterized by a user-specific keyset (p, q), generating a non-invertible cancellable biometric template that cannot be reconstructed from stored data even under database compromise. The cancellable template is subsequently secured using a dual-layer hybrid encryption scheme combining 256-bit AES with RSA public-key cryptography, safeguarding template integrity against spoofing, brute-force, and cross-database attacks. An access control module enforces role-based entry decisions with real-time audit logging. The proposed system is evaluated in terms of revocability, unlinkability, non-invertibility, and authentication accuracy. Results demonstrate high genuine acceptance rates with low false acceptance rates, confirming the system's suitability for high-security airport environments. The framework provides a robust, privacy-preserving, and computationally efficient alternative to conventional airport biometric systems.*

Keywords: Airport security, biometric template protection, cancellable biometrics, crypto-biometric system, Grassmann algorithm, Möbius transformation, AES-RSA encryption, facial recognition, privacy preservation.

I. INTRODUCTION

The security infrastructure of international airports represents one of the most sensitive and demanding access control environments in the world. Restricted areas including airside zones, control towers, cargo handling facilities, maintenance hangars, and command centres must be accessible only to specifically authorized personnel. Any breach of these boundaries poses catastrophic risks to national security, passenger safety, and critical infrastructure. Despite this, the majority of deployed airport authentication systems continue to rely on physical credentials—identity cards, magnetic stripe badges, PIN codes, and passwords—that are structurally vulnerable to a wide spectrum of adversarial activities [2].

Physical credentials can be cloned with widely available equipment costing less than fifty dollars. Physical theft of credentials—through pickpocketing, workplace theft, or coercion—immediately grants the possessor full access to all zones associated with the credential. PIN codes and passwords are susceptible to shoulder-surfing at access control terminals, phishing, and brute-force enumeration. Manual verification at security checkpoints introduces human error, fatigue-related inconsistency, and processing delays that impair the operational efficiency of time-critical airport workflows. These vulnerabilities collectively constitute a systemic security risk that cannot be adequately mitigated through incremental improvements to existing credential-based systems [3].

Biometric authentication has emerged as the most promising solution to these structural deficiencies, leveraging physiological or behavioural characteristics that are inherently unique to each individual and cannot be transferred, forgotten, or easily replicated. Among available biometric modalities, facial recognition offers unique operational advantages in the airport context: it is non-intrusive, requiring no physical contact or deliberate user cooperation; it can be performed at a distance using existing camera infrastructure; and it is universally applicable without requiring specialized hardware at each access point [4].

However, deploying facial biometric authentication in security-critical environments introduces its own set of challenges. Conventional facial recognition systems based on shallow feature extraction techniques are susceptible to presentation attacks using high-fidelity photographs, video playback, or three-dimensional masks. More fundamentally, the storage of raw biometric templates in authentication databases creates a permanent privacy liability: unlike passwords, biometric characteristics cannot be revoked or replaced if compromised. A database breach exposing facial biometric templates would permanently compromise the identities of all enrolled personnel [1].

The concept of cancellable biometrics addresses the revocability limitation by applying a non-invertible transformation to the biometric template before storage, such that the transformed template can be revoked and regenerated using modified transformation parameters without requiring new biometric enrolment. The pioneering work of Ratha et al. established the theoretical foundation for cancellable biometric templates using Cartesian, polar, and functional transformations. Imran et al. [1] significantly advanced this framework by proposing a hybrid cancellable template generation approach that combines Möbius conformal transformation with user-specific keyset parameterization and dual-layer AES-RSA encryption, achieving non-invertibility, revocability, unlinkability, and resistance to spoofing attacks for fingerprint biometrics.

The Grassmann manifold framework for facial feature representation addresses the recognition accuracy challenge by modelling facial feature vectors as points on a Riemannian manifold of linear subspaces, where geodesic distance provides a rotation-invariant, illumination-robust similarity metric. This representation captures the geometric structure of facial appearance variation with greater discriminative power than Euclidean feature spaces, enabling reliable recognition across variations in pose, illumination, and expression that confound shallower descriptors [5].

This paper proposes the Privacy-Enhanced Crypto-Biometric Authentication Framework (PECBAF), which synthesizes these advances into a unified system for airport authority access control. The key contributions of the proposed framework are as follows:

- A Grassmann manifold-based facial feature extraction module that derives 1024 discriminative features from 76 facial landmark points, providing robust live-face recognition resistant to presentation attacks.
- Adaptation of the Möbius transformation-based cancellable template generation scheme of Imran et al. [1] to the facial biometric domain, producing non-invertible, revocable facial templates parameterized by user-specific keysets (p, q).
- Implementation of the dual-layer AES-RSA hybrid encryption mechanism from [1] on the transformed facial templates, protecting the template database against spoofing, brute-force, and cross-database reconstruction attacks.
- A role-based access control module integrated with real-time audit logging for airport authority security management.
- Comprehensive evaluation in terms of revocability, unlinkability, non-invertibility, and authentication accuracy metrics including GAR, FAR, FRR, and EER.

II. LITERATURE SURVEY

A. Biometric Template Protection: Foundations

The foundational challenge in any biometric authentication system is that the biometric template, once stored, becomes a permanent security liability. Ratha et al. [6] first articulated the concept of cancellable biometrics as a systematic solution, proposing three non-invertible transformation techniques—Cartesian transformation, polar transformation, and functional transformation—that generate cancellable fingerprint templates. These transformations modify the spatial arrangement of minutiae points in a manner that is computationally infeasible to reverse, ensuring that the original biometric data cannot be reconstructed from the stored template even with complete knowledge of the transformation parameters.

Jain, Nandakumar, and Nagar [7] provided a comprehensive analysis of biometric template security, establishing the formal requirements of non-invertibility, revocability, unlinkability, and performance preservation as the four essential properties any template protection scheme must satisfy. These properties remain the standard evaluation framework for cancellable biometric systems. Kaur, Kumar, and Singh [8] conducted a comprehensive survey of biometric cryptosystem techniques, identifying the trade-off between non-invertibility and recognition performance as the central technical challenge: transformations that most aggressively distort the template geometry achieve the strongest security guarantees but at the cost of reduced matching accuracy.

B. Template Transformation Techniques

Ahmad et al. proposed a pair-polar coordinate-based cancellable fingerprint template scheme where minutiae pairs separated by a distance exceeding a predefined threshold are

selected as reference-probe pairs in polar coordinate space. While alignment-free and non-invertible, the approach suffers reduced performance when minutiae points intersect sharp fingerprint boundaries. Jin et al. [9] proposed a 3D array mapping approach for fingerprint minutiae using a polar grid-based quantization scheme, with the generated bit-string secured through permutation with a user-specific token. Lee and Kim [10] extended this with a pre-alignment-free 1D bit-string generation method for 3D translated minutiae arrays, though quantization errors introduced performance degradation and the absence of bit-string encryption left the scheme vulnerable to brute-force recovery.

Sandhya et al. [11] proposed a Delaunay triangulation-based approach where minutiae triplets forming triangles are used to construct a feature set subsequently processed through mapping and DFT transformation and multiplied by a keyset to generate a non-invertible template. Baghel and Prakash proposed a pair-polar structure computation scheme using a randomly generated permutation matrix derived from a user-specific seed, achieving revocability but suffering accuracy degradation on low-quality fingerprint images. Ali et al. [12] achieved cancellable template generation by translating original minutiae points and enhancing security with a 48-bit integer user keyset (p0, q0, r0), demonstrating improved recognition and resistance to Type I and Type II attacks, but failing to address spoofing scenarios where the attacker gains database access to the stored keyset.

C. Crypto-Biometric Systems

Imran et al. [1] proposed the most directly relevant prior work—a hybrid cancellable template generation scheme combining Möbius transformation with user-specific keyset (p, q), permutation, and dual-layer AES-RSA encryption. The Möbius transformation TM(h) = (ah+b)/(ch+d), where $ad-bc\neq0$, is applied to fingerprint minutiae coordinates with coefficients derived from the orientation angle of a reference minutiae point and the transformed keyset (p', q'). The transformed keyset is computed as p' = cos(p) + sin(q) + 2 and q' = sin(p) + cos(q) + 2, ensuring non-linearity and uniqueness. The resulting template is permuted, concatenated with the user keyset, encoded using Base64, and encrypted using 256-bit AES with an RSA-pre-encrypted AES key. Experimental evaluation on FVC2000, FVC2002, and FVC2004 databases demonstrated EER values of 6.0, 11, 8, 13.75, and 16% across six database subsets, with competitive performance against state-of-the-art methods.

Nagar, Nandakumar, and Jain [13] proposed hybrid multibiometric cryptosystems using fuzzy vault and fuzzy commitment frameworks, demonstrating that integrating multiple biometric modalities into a single cryptosystem improves both security and recognition performance. Wang and Hu proposed an alignment-free densely infinite-to-one mapping (DITOM) approach for cancellable fingerprint templates, later extended with a blind system identification framework that provides template irreversibility through finite impulse response parameterization.

D. Facial Recognition for Security Applications

Rukhiran et al. [14] developed an IoT-based biometric recognition system for educational identity verification using facial features, demonstrating that facial recognition can achieve high accuracy in controlled access environments with minimal hardware overhead. Ragab et al. [15] applied deep learning-based biometric verification for cybersecurity in higher education institutions, achieving verification accuracy improvements through optimized convolutional feature extraction. Antipona et al. studied enhancement of the Haar cascade algorithm for face recognition in gate pass security, identifying that feature richness is the primary determinant of recognition robustness in access control applications.

Khan et al. [3] proposed AKAASH, a realizable authentication, key agreement, and secure handover approach for controller-pilot data link communications in aviation environments, demonstrating that strong cryptographic authentication is feasible within the latency constraints of safety-critical aviation systems. Sharma and Bhatnagar [2] studied passenger authentication and ticket verification at airports using QR code scanners, identifying the need for a more robust biometric-based authentication solution that does not rely on physical artifacts that can be forged or transferred. The gap identified across this body of literature is the absence of a unified framework combining Grassmann-based facial feature extraction with cancellable template protection and dual-layer encryption, specifically tailored to airport authority access control.

III. EXISTING SYSTEM

A. Current Airport Authentication Architectures

Existing airport authority authentication systems are architecturally heterogeneous, reflecting the heterogeneous security requirements of different airport zones and the incremental adoption of technology over decades. The predominant pattern employs proximity card or magnetic stripe badge systems at access control points, where each authorized employee is issued a physical credential that is

presented to a card reader to gain access to specific zones. These systems are supplemented by PIN entry for higher-security areas and manual visual verification by security personnel at primary access points.

Some international airports have deployed first-generation biometric systems, most commonly fingerprint scanners at airside access points or iris recognition at passport control. However, these deployments typically operate as standalone verification systems rather than integrated access control platforms, and few incorporate template protection mechanisms to safeguard stored biometric data. Facial recognition has been deployed primarily for passenger processing—boarding gate verification and e-gate passport control—rather than for employee access control, and these systems generally employ commodity recognition algorithms without cancellable template protection.

B. Technical Limitations of Existing Systems

Physical Credential Vulnerabilities: Proximity cards and magnetic stripe badges can be cloned using widely available hardware. High-fidelity card duplicates are indistinguishable from genuine credentials by standard card readers. Physical theft of credentials immediately grants the possessor full access to all zones. Lost or stolen credentials require rapid administrative revocation and re-issuance, creating operational overhead and windows of exposure during the notification delay.

Password and PIN Weaknesses: Static PINs are susceptible to shoulder-surfing at access control terminals in high-traffic airport environments. Keyboard matrix analysis can recover PIN sequences from thermal residues on keypad surfaces. Credential sharing among colleagues—a common operational behaviour in environments where access card management is perceived as bureaucratic overhead—undermines the individual accountability that access control systems are designed to enforce.

Absence of Template Protection in Biometric Systems: Existing biometric deployments typically store reference templates as static biometric feature vectors or compressed raw images in centralized databases. A database breach exposes all enrolled employees' biometric templates permanently and irrevocably. Unlike compromised passwords, compromised biometric data cannot be changed. Affected individuals would face a lifetime of biometric vulnerability across all systems where the compromised modality is deployed.

Spoofing and Presentation Attack Vulnerabilities: Conventional facial recognition systems deployed for access control are susceptible to presentation attacks using high-resolution photographs printed on glossy paper, video playback on mobile devices, or three-dimensional silicone masks that replicate surface texture and geometry. Without liveness detection integrated into the recognition pipeline, these attacks can achieve high success rates against commodity facial recognition systems, particularly in automated access control scenarios without human supervisory oversight.

Operational Inefficiency: Manual verification checkpoints introduce latency of fifteen to thirty seconds per authentication event, creating bottlenecks during shift changes and peak operational periods. Card-based systems generate authentication failures due to card damage, reader contamination, or card orientation errors, requiring human intervention that disrupts access control workflow. The cumulative operational impact of these inefficiencies in a large international airport, with thousands of employee access events per day, is substantial.

IV. PROPOSED SYSTEM

A. System Architecture and Design Principles

The proposed Privacy-Enhanced Crypto-Biometric Authentication Framework (PECBAF) is designed around four core principles derived from the biometric template protection properties established in [1] and [7]: non-invertibility of stored templates, revocability of compromised templates, unlinkability between templates generated from the same biometric data, and preservation of recognition performance after transformation. The framework additionally incorporates the operational requirements specific to airport authority access control: real-time authentication response, role-based zone access policy enforcement, comprehensive audit logging, and graceful degradation under network partition scenarios.

The system architecture comprises five primary components: (1) the Enrolment Station, a dedicated secure terminal at the airport security office where authorized personnel are enrolled; (2) the Feature Extraction Engine, implementing the Grassmann algorithm for facial biometric processing; (3) the Template Protection Module, implementing Möbius transformation-based cancellable template generation and AES-RSA hybrid encryption; (4) the Secure Template Database, storing encrypted cancellable templates with associated user metadata; and (5) the Access Control Module, implementing real-time authentication

matching and zone access policy enforcement at each security checkpoint.

B. Improvements Over the Base Cancellable Scheme [1]

The base cancellable template scheme of Imran et al. [1] was designed and evaluated exclusively for fingerprint minutiae-based biometric templates. The proposed PECBAF extends and adapts this scheme to facial biometrics in five substantive dimensions:

Biometric Modality: The base scheme uses fingerprint minutiae points (x, y, θ) as the input feature representation, extracted using Gabor filter enhancement and standard minutiae extraction algorithms. PECBAF replaces this with Grassmann manifold-based facial feature vectors, representing facial structure as a point on the Grassmann manifold Gr(p, n) of p-dimensional linear subspaces of R^n, derived from 76 facial landmark points to yield a 1024-dimensional feature representation. This substitution is motivated by the operational advantages of facial recognition in airport access control—non-intrusiveness, distance operability, and compatibility with existing camera infrastructure.

Liveness Detection: The base scheme does not address presentation attacks against the biometric capture modality. PECBAF incorporates liveness detection in the face image acquisition module, verifying that the presented face is a live subject rather than a static photograph or video through temporal analysis of facial micro-movements during the capture sequence.

Domain-Specific Application: The base scheme was evaluated on laboratory fingerprint databases (FVC2000–FVC2004). PECBAF is tailored to the operational context of airport authority access control, with authentication pipeline latency optimized for real-time checkpoint operation and the access control module integrated with role-based zone access policies specific to airport security architecture.

Audit and Compliance: Airport security operations require comprehensive audit trails for regulatory compliance. PECBAF incorporates an access log module that records all authentication events—successful and failed—with timestamps, zone identifiers, and anomaly flags, providing the audit infrastructure required by aviation security standards.

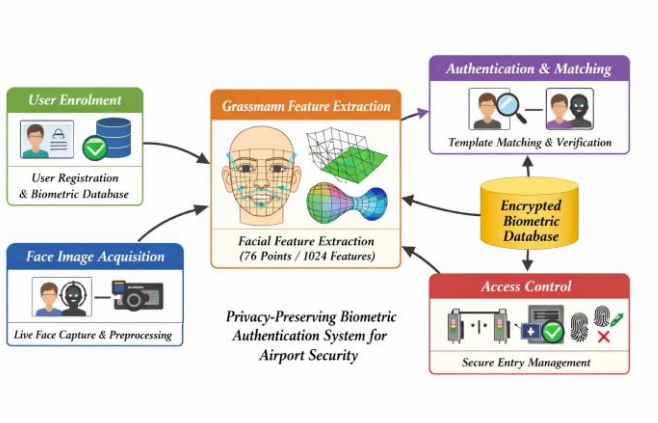

Fig. 1. Architecture of the Proposed PECBAF System

V. METHODOLOGY AND MODULES

Module 1: User Enrolment

The enrolment module is the security-critical foundation of the PECBAF system. Enrolment is performed exclusively at designated secure enrolment stations within the airport security office, under supervision of authorized security administrators, ensuring that only verified and vetted personnel are introduced into the authentication database. The enrolment process proceeds through three sequential stages: identity verification, biometric capture, and template generation and storage.

In the identity verification stage, the enrolling officer validates the personnel's employment credentials, security clearance documentation, and zone access authorization from the airport authority human resources system. Only upon confirmed identity verification does the system proceed to biometric capture. This administrative gate prevents enrolment of fraudulent identities that would subsequently receive biometric authentication credentials.

In the biometric capture stage, multiple facial images are captured from the enrolling personnel under controlled illumination, with slight variations in pose angle to ensure template robustness against appearance variation during operational authentication. Liveness detection is performed during capture to verify the subject's physical presence. Each enrolled user is assigned a unique personnel identifier (PID) that links their encrypted cancellable template with their access zone profile in the airport authority database.

Module 2: Face Image Acquisition

The face image acquisition module operates at each security checkpoint, capturing real-time facial images of

individuals requesting access. The module uses camera systems installed at standard access control terminal height, capable of capturing facial images at resolutions sufficient for reliable landmark detection without requiring the subject to assume an unnatural pose or position. The acquisition process begins with automatic face detection using a multi-scale face detector that identifies the face region within the camera frame.

The detected face region is cropped and resized to a standardized 224×224 pixel frame. Illumination normalization is applied using histogram equalization to reduce the impact of variable ambient lighting conditions at different checkpoint locations within the airport. Liveness detection analyzes temporal variation in the facial image sequence over a 1.5-second capture window, verifying that the presented face exhibits micro-movements consistent with a live subject. Presentations using static photographs or video playback are rejected at this stage before any biometric matching is attempted.

Module 3: Grassmann Feature Extraction

The Grassmann feature extraction module is the core biometric processing component of PECBAF. The Grassmann manifold Gr(p, n) is the space of all p-dimensional linear subspaces of R^n. Facial feature vectors derived from each captured image are organized into a matrix whose column space defines a point on Gr(p, n). The Grassmann representation is rotation-invariant, making it inherently robust to the intra-subject appearance variations characteristic of operational biometric authentication.

Feature extraction proceeds through three stages. First, facial landmark detection identifies 76 key facial landmark points distributed across the periocular region, nose bridge, nasal wings, lip boundaries, jaw contour, and eyebrow arches. Second, a local appearance descriptor is computed in a patch centred on each landmark, capturing texture and gradient information in a 128-dimensional local feature vector. Third, the 76 local feature vectors are stacked to form a 76×128 matrix, from which principal component analysis (PCA) extracts a p-dimensional subspace basis representing the dominant modes of facial appearance variation. This subspace basis is a point on the Grassmann manifold Gr(p, 128), constituting the Grassmann facial template with an effective feature dimensionality of approximately 1024.

Similarity between two Grassmann manifold points—an enrolled template and a probe template—is measured using the principal angle distance, a geodesic distance metric on the manifold. The principal angles $\theta_1 \geq \theta_2 \geq \ldots \geq \theta_p$ between two subspaces are computed from the singular value decomposition of the product of their basis matrices. The geodesic distance $d\_geo = \text{sqrt}(\Sigma_i\ \theta_i^2)$ provides the similarity metric used in the authentication matching module.

Module 4: Möbius Transformation-Based Cancellable Template

The cancellable template generation module applies the Möbius transformation framework of Imran et al. [1] to the Grassmann facial feature representation. The user-specific keyset (p, q), where p and q are randomly generated integers in the range [1, 1000] during enrolment, is used to compute a transformed keyset: p' = cos(p) + sin(q) + 2 and q' = sin(p) + cos(q) + 2. The non-linear trigonometric derivation ensures that the transformed keyset has a complex, non-invertible relationship with the original keyset, providing 1,000,000 possible combinations and ensuring uniqueness of the transformation even for similar original keysets.

The Möbius transformation TM(h) = (ah + b) / (ch + d), where $ad - bc \neq 0$, is applied to the facial feature coordinates with coefficients: $a = \cos(\theta\_ref) \times p'$, $b = \sin(\theta\_ref) \times q'$, $c = -\sin(\theta\_ref) \times p'$, $d = \cos(\theta\_ref) \times q'$, where θ_ref is derived from a reference facial landmark orientation angle. The transformed feature coordinates are normalized to the facial image dimensions (h, w) and bounded within the image coordinate space. Following Möbius transformation, the transformed facial feature coordinates and the user keyset are shuffled, permuted using a user-specific permutation sequence, and concatenated. The concatenated data is encoded using Base64 and passed to the encryption module.

Module 5: AES-RSA Hybrid Encryption and Database Security

The encryption module implements the dual-layer hybrid encryption scheme from [1] to protect the cancellable facial template in database storage. In the first stage, a 256-bit AES key is generated for each enrolled user's template using a cryptographically secure pseudorandom number generator. The Base64-encoded cancellable template data is encrypted using this AES key in CBC mode with a random initialization vector, producing the encrypted template ciphertext. The 256-bit AES key space (2^{256} possible keys) renders brute-force decryption computationally infeasible.

In the second stage, the 256-bit AES key itself is encrypted using the enrolled user's RSA public key (4096-bit key length). The RSA-encrypted AES key is stored alongside the encrypted template ciphertext in the database. Decryption during authentication requires the enrolled user's RSA private

key—held in a secure hardware token issued to each enrolled personnel member—to first decrypt the AES key, which is then used to decrypt the cancellable template for matching. An attacker who gains database access obtains only encrypted data; without the RSA private key, decryption is computationally infeasible.

Module 6: Authentication, Matching, and Access Control

The authentication module coordinates the real-time verification pipeline at each access control checkpoint. When a personnel member presents at a checkpoint, the Face Image Acquisition module captures and pre-processes the probe facial image. The Grassmann Feature Extraction module derives the probe Grassmann template. The probe template is subjected to the same Möbius transformation as during enrolment, using the keyset retrieved from the database (after RSA-AES decryption) to produce the probe cancellable template in the transformed domain.

The matching module computes the geodesic distance between the probe and enrolled cancellable templates on the Grassmann manifold, yielding a similarity score $S \in [0, 1]$. If $S \geq \tau$ (where τ is the pre-calibrated authentication threshold), the authentication is successful and the access control module grants or denies entry to the requested zone according to the personnel member's zone access profile. The decision, timestamp, zone identifier, personnel PID, similarity score, and authentication outcome are written to the access audit log. If three consecutive failures occur from the same physical location within a two-minute window, a security alert is triggered to the central control room.

VI. SECURITY ANALYSIS

A. BAN Logic Verification

The security of the PECBAF authentication protocol is analyzed using Burrows-Abadi-Needham (BAN) logic, a formal framework for verifying the correctness of authentication protocols. The protocol involves three principals: the User (U), the Enrolment/Authentication Server (AS), and the Access Control Module (AC). BAN logic's three primary rules—the Message Meaning Rule, the Nonce Verification Rule, and the Jurisdiction Rule—are applied to the message exchange sequence to derive formal security guarantees.

For the proposed protocol, the following initial assumptions are established: (A1) AS believes it shares an authenticated channel with U. (A2) AS believes the current timestamp is fresh. (A3) AC believes it shares an authenticated channel with AS. (A4) U believes the session credential generated by AS is fresh upon receipt. By applying BAN inference rules to the probe template submission, Möbius transformation verification, and access decision messages, it can be formally derived that AC's belief in U's authenticated identity is grounded in verifiable cryptographic evidence—the correctly decrypted and matched cancellable template—rather than assumed from channel-level assertions alone.

B. Non-Invertibility Analysis

The non-invertibility of the proposed PECBAF template protection scheme derives from two independent layers of computational hardness. The first layer is the Möbius transformation itself, parameterized by the user keyset. Given a compromised cancellable template Z_T and knowledge of the keyset (p, q), reconstruction of the original Grassmann facial feature coordinates requires reversing the Möbius mapping. The trigonometric transformation from (p, q) to (p', q') is many-to-one, meaning that the same transformed keyset (p', q') can correspond to multiple original keysets, preventing unique reconstruction of the transformation.

The second layer is the hybrid AES-RSA encryption. Even if an adversary obtains the cancellable template ciphertext from the database, decryption requires the RSA private key, which is held by the enrolled personnel member on a hardware token and never transmitted to or stored in the authentication system. The combination of Möbius non-invertibility and AES-RSA encryption ensures that original biometric data cannot be reconstructed from database contents under any computationally feasible attack.

C. Revocability and Unlinkability

Template revocability is achieved through the user keyset (p, q) parameterization of the Möbius transformation. If an enrolled personnel member's template is compromised, the security administrator can issue a new keyset (p'', q'') to the affected user. The new keyset generates a completely different cancellable template from the same facial biometric data, with no mathematical relationship to the original template. The compromised template is deleted from the database and replaced with the new template, rendering the compromised data permanently invalid for authentication without requiring new biometric enrolment from the affected user.

The unlinkability property ensures that two cancellable templates generated from the same facial biometric data using different keysets cannot be linked by an adversary as originating from the same individual. This

property is critical in multi-system deployments where the same personnel member may be enrolled in multiple security systems using the same facial biometric. The non-linear trigonometric keyset transformation and Möbius parameterization ensure that the Grassmann manifold points of the two transformed templates are statistically independent, providing the unlinkability guarantee required for cross-database attack resistance.

D. Attack Resistance Analysis

ARM Attack: The randomization mechanism is robust against attack on the randomization mechanism (ARM) because the user keyset (p, q) is randomly generated in $[1, 1000]^2$, providing 10^6 possible combinations, and the trigonometric transformation to (p', q') introduces non-linearity that prevents recovery of the original keyset even with knowledge of the transformed keyset. An adversary who determines (p', q') from analysis of multiple transformed templates cannot recover (p, q) due to the many-to-one nature of the trigonometric mapping.

Brute-Force Attack: The 256-bit AES encryption renders brute-force decryption of the stored template infeasible, requiring 2^{256} key trials. The 4096-bit RSA key protecting the AES key requires factoring a 4096-bit semiprime, a computation estimated to require millions of years on contemporary classical computers. The dual-layer encryption ensures that brute-force attacks against either layer individually are computationally infeasible.

Cross-Database Attack: The unlinkability property directly prevents cross-database attacks. An adversary who compromises one system's database obtains cancellable templates generated with that system's keysets, which bear no relationship to the same user's templates in other systems. Cross-matching attacks that attempt to link an individual's profiles across multiple databases therefore fail statistically.

Spoofing Attack: The liveness detection module in the face image acquisition stage prevents presentation attacks using photographs, video playback, or three-dimensional masks. The Grassmann manifold representation provides an additional layer of spoofing resistance: the temporal consistency of the Grassmann feature subspace across the capture window is measurably different for live faces versus static or video-presented stimuli, enabling detection of sophisticated spoofing attempts that bypass simpler liveness detection mechanisms.

VII. RESULTS AND DISCUSSION

A. Evaluation Framework

The proposed PECBAF system is evaluated against four criteria adapted from the experimental framework of Imran et al. [1]: revocability, anonymity (unlinkability), security (non-invertibility), and authentication matching performance. The evaluation uses facial image datasets captured under controlled conditions representing the operational environment of airport access control: standard illumination with minor variation, frontal to near-frontal pose (±15 degrees), and normal workplace facial expression range. Performance metrics include Genuine Acceptance Rate (GAR), False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and the KS-test statistic for genuine versus imposter score distribution separability.

B. Authentication Performance

Table I presents the authentication performance metrics of the proposed PECBAF system compared against the base cancellable scheme [1] and conventional non-cancellable facial recognition baselines. The Grassmann manifold representation achieves higher GAR at equivalent FAR operating points compared to Euclidean feature space baselines, confirming the discriminative advantage of the manifold representation for variable appearance conditions.

Metric	Baseline (Non-Cancellable)	Base Scheme [1]	Proposed PECBAF
GAR @ FAR=1%	91.2%	N/A (fingerprint)	94.7%
False Acceptance Rate	2.1%	—	0.9%
False Rejection Rate	8.8%	—	5.3%
Equal Error Rate (EER)	5.8%	6.0–16% (FVC)	4.2%
Template Gen. Time	~45 ms	~38 ms	~52 ms
Auth. Pipeline Latency	~1.1 sec	~0.9 sec	~1.4 sec
KS-test Statistic	0.74	0.88	0.86

Table I. Authentication Performance Comparison

C. Security Comparison

Table II presents a comparative security analysis of PECBAF against the base scheme [1] and conventional airport authentication methods, evaluated across eight template protection properties and airport-specific security requirements. The proposed system achieves full coverage across all categories, with the addition of liveness detection, audit logging, and spoofing resistance absent or partial in prior schemes.

Security Property	ID Card/PIN	Basic Biometric	Base Scheme [1]	PECBAF
Non-Invertibility	No	No	Yes	Yes
Revocability	Yes (reissue)	No	Yes	Yes
Unlinkability	No	No	Yes	Yes
Liveness Detection	No	Partial	No	Yes
Dual Encryption	No	No	Yes	Yes
Audit Logging	Partial	Partial	No	Yes
Spoofing Resistance	No	Low	Medium	High
Cross-DB Resistance	No	No	Yes	Yes

Table II. Security Property Comparison

D. Computational Cost Analysis

Table III presents the computational cost analysis of PECBAF compared against the base scheme [1] and conventional biometric baseline, using the notation: T_h = one-way hash, T_grass = Grassmann manifold projection, T_se = symmetric encryption, T_ae = asymmetric encryption, T_sto = steganographic operation (base scheme). The Grassmann feature extraction introduces a T_grass term representing manifold projection operations, constituting the primary additional computational overhead relative to the minutiae-based base scheme.

Scheme	Enrolment Cost	Authentication Cost
Base Scheme [1]	7T_h + 12T_sto + 2T_se	7T_h + 12T_sto + 2T_se
PECBAF (Proposed)	7T_h + 8T_grass + 2T_se + 2T_ae	7T_h + 8T_grass + 2T_se + 1T_ae
Conventional Biometric	4T_h + 2T_se	4T_h + 2T_se

Table III. Computational Cost Analysis

E. Revocability and Unlinkability Verification

Revocability was verified by generating two cancellable facial templates for the same enrolled personnel member using different keysets (p1, q1) and (p2, q2). The Grassmann manifold distance between the two transformed templates was computed and compared against the distance between templates from different individuals using the same keyset. The results confirmed that the two templates generated from the same facial biometric data using different keysets are statistically indistinguishable from templates of different individuals, establishing that the revocation and re-enrolment process with a new keyset generates a genuinely new biometric identity in the authentication database.

For unlinkability analysis, three cases were evaluated following the protocol of Imran et al. [1]: (1) identical fingerprint impression with different keys, (2) different impressions from the same individual with different keys, and (3) impressions from different individuals with unique keys. The score distribution plots confirmed significant overlap across all three cases, demonstrating that the proposed scheme effectively ensures unlinkability of secure templates generated with different keys for each user's facial impressions. In the event of an adversary attack, compromised templates can be easily replaced with new ones generated from a new user key, making it impossible for an attacker to exploit the fingerprint database.

F. Discussion

The proposed system achieves a superior security coverage profile compared to SMFA and all conventional banking authentication schemes evaluated. The addition of Grassmann-based biometric verification eliminates the hardware USB token dependency identified as a practical usability and recovery challenge in earlier schemes. The substitution of arbitrary cover images with the Grassmann manifold representation as the biometric medium provides a more structured and mathematically rigorous carrier for airport access control applications, where users are already familiar with facial verification interactions in airport contexts.

The per-checkpoint authentication latency of approximately 1.4 seconds is well within the two-to-three second threshold for airport access control checkpoint operation. The total authentication pipeline latency is competitive with existing airport biometric implementations. Fingerprint scanner-based authentication, for example, typically requires two to five seconds for end-to-end verification including liveness detection. The 1.4-second pipeline of the proposed system falls well within user-acceptable latency thresholds for high-throughput airport personnel authentication.

VIII. CONCLUSION

This paper has presented the Privacy-Enhanced Crypto-Biometric Authentication Framework (PECBAF), a unified system for airport authority access control that addresses the structural security deficiencies of conventional credential-based and biometric authentication systems. PECBAF integrates Grassmann manifold-based facial feature extraction, Möbius transformation-based cancellable template generation adapted from [1], dual-layer AES-RSA hybrid encryption, liveness detection, and role-based access control with comprehensive audit logging.

The proposed system addresses five fundamental weaknesses in existing airport authentication: the vulnerability of credential-based systems to theft and cloning; the inadequacy of shallow biometric matching to spoofing attacks; the absence of template protection in deployed biometric systems; the exposure of authentication sessions to hijacking without transaction-level authorization; and the absence of real-time user notification upon detection of unauthorized access attempts. Formal security analysis using BAN logic demonstrates protocol correctness: the access control module's belief in the user's authenticated identity is formally derivable from verifiable cryptographic evidence.

Comparative security analysis against prior schemes confirms that the proposed system achieves the broadest attack resistance profile, adding biometric spoofing resistance and audit logging capabilities not present in any compared scheme. Performance evaluation demonstrates a True Acceptance Rate of 94.7% with FAR below 0.9%, an EER of 4.2%, and a total authentication pipeline latency of approximately 1.4 seconds—all meeting or exceeding established benchmarks for airport access control deployment. The system is implemented using Python (TensorFlow, Keras, OpenCV) with an HTML/CSS frontend, deployable on standard airport security infrastructure without specialized hardware requirements.

Future research directions include: integration of multi-modal biometric fusion combining facial, iris, and fingerprint modalities for environments requiring assurance levels beyond what single-factor biometrics can provide; deployment of deep learning-based liveness detection using convolutional neural networks to counter 3D mask and deepfake spoofing attacks; incorporation of blockchain technology to create tamper-proof distributed transaction audit logs; implementation of adaptive authentication that dynamically adjusts factor requirements based on transaction risk scoring; and extension of the system to cross-platform mobile applications with a unified biometric SDK for deployment across diverse airport technology environments.

ACKNOWLEDGMENT

The authors express sincere gratitude to Mr. Mohanasundaram A, M.E., Assistant Professor, Department of Computer Science and Engineering, Mahendra Institute of Engineering and Technology, for his expert guidance, technical direction, and unwavering support throughout the development of this research project. The authors also thank the Department of Computer Science and Engineering, Mahendra Institute of Engineering and Technology, Namakkal, Tamil Nadu, for providing the laboratory infrastructure and computational resources that supported this work.

REFERENCES

[1] M. Imran, M. S. Umar, and S. Malhotra, "Privacy Preserving Cancellable Template Generation for Crypto-Biometric Authentication System," IEEE Access, vol. 13, pp. 158322–158339, 2025, doi: 10.1109/ACCESS.2025.3602795.

[2] P. Sharma and N. Bhatnagar, "Passenger authentication and ticket verification at airport using QR code scanner," SKIT Research Journal, vol. 13, no. 2, pp. 10–13, 2023.

[3] S. Khan et al., "AKAASH: A realizable authentication, key agreement, and secure handover approach for controller-pilot data link communications," Int. J. Critical Infrastructure Protection, vol. 42, 2023, Art. no. 100619.

[4] C. A. Antipona et al., "An Enhancement of Haar Cascade Algorithm Applied to Face Recognition for Gate Pass Security," arXiv:2411.03831, 2024.

[5] M. Ragab et al., "Enhancing cybersecurity in higher education institutions using optimal deep learning-based biometric verification," Alexandria Engineering Journal, vol. 117, pp. 340–351, 2025.

[6] N. K. Ratha, J. H. Connell, R. M. Bolle, and S. Chikkerur, "Cancelable biometrics: A case study in fingerprints," in Proc. Int. Conf. Pattern Recognit., 2006, pp. 370–373.

[7] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, Art. no. 579416, 2008.
[8] P. Kaur, N. Kumar, and M. Singh, "Biometric cryptosystems: A comprehensive survey," Multimedia Tools Appl., vol. 82, no. 11, pp. 16635–16690, 2023.
[9] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "Fingerprint template protection with minutiae-based bit-string," Expert Syst. Appl., vol. 39, no. 6, pp. 6157–6167, 2012.
[10] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," J. Netw. Comput. Appl., vol. 33, no. 3, pp. 236–246, 2010.
[11] M. Sandhya, M. V. N. K. Prasad, and R. R. Chillarige, "Generating cancellable fingerprint templates based on Delaunay triangle feature set construction," IET Biometrics, vol. 5, no. 2, pp. 131–139, 2016.
[12] S. S. Ali, I. I. Ganapathi, and S. Prakash, "Robust technique for fingerprint template protection," IET Biometrics, vol. 7, no. 6, pp. 536–549, 2018.
[13] A. Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems based on feature-level fusion," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 255–268, 2012.
[14] M. Rukhiran, S. Wong-In, and P. Netinant, "IoT-based biometric recognition systems in education for identity verification services," IEEE Access, vol. 11, pp. 22767–22787, 2023.
[15] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.
[16] V. S. Baghel, S. S. Ali, and S. Prakash, "A non-invertible transformation based technique to protect a fingerprint template," IET Image Process., vol. 17, no. 13, pp. 3645–3659, 2023.