



ORIGINAL ARTICLE

TRIFACTOR AI: AN OFFLINE MULTI-FACTOR BIOMETRIC AUTHENTICATION FRAMEWORK INTEGRATING ADAPTIVE LIVENESS AND BEHAVIORAL VERIFICATION

^{1*}Burgu Shravan Kumar, ²Muntha Raju, ³Yerram Sneha, ⁴Sirisha Veluri

1,2,3,4 Department of Computer Science and Engineering, Nalla Malla Reddy Engineering College, Hyderabad, Telangana, India.

Corresponding Author Email: shravanburgu7804@gmail.com

(Received 01 January 2026; revised 25 March 2026; accepted 10 May 2026)

Abstract:

The increasing prevalence of digital identity theft and credential-based attacks has exposed fundamental limitations of traditional password-based and two-factor authentication mechanisms. Although biometric authentication offers improved usability and security, most existing systems rely on a single modality, making them vulnerable to spoofing, replay, and behavioral forgery. This paper proposes TriFactor AI, a privacy-preserving, offline, multi-modal authentication framework designed for secure desktop access. The proposed system integrates three independent authentication factors: facial recognition with adaptive liveness detection, dynamic signature verification using Dynamic Time Warping (DTW), and knowledge-based secret-code validation secured through bcrypt hashing. Facial authentication employs ArcFace embeddings combined with randomized challenge-response liveness tasks, including blink and head-pose verification, to mitigate presentation attacks. Behavioral authentication captures temporal handwriting dynamics via a PyQt5-based interface and verifies user identity through DTW-based sequence alignment. All biometric templates and credentials are securely managed within a local SQLite database, ensuring complete data privacy and eliminating reliance on cloud-based processing. Experimental evaluation demonstrates that the facial module achieves an average accuracy of 98.2%, the dynamic signature module 87%, and secret-code verification 100% reliability. Ablation analysis confirms that combining physiological, behavioral, and knowledge-based factors reduces the False Acceptance Rate by more than 60× compared to single-factor authentication, yielding an overall system accuracy of 99.8% with an average authentication latency below 3 seconds. These results provide empirical evidence that security gains from tri-factor biometric fusion are multiplicative rather than additive. The proposed framework establishes a practical, low-latency, and fully local authentication paradigm suitable for privacy-sensitive desktop environments.

Keywords: *trifactor ai; multi-modal biometric authentication; adaptive liveness detection; dynamic time warping (dtw); crypt hashing.*

1. Introduction

The increasing use of digital systems in verifying identity, carrying out online transactions, and data protection has heightened the demand of having safe and effective authentication systems. Possibly the most used password-based systems have become more and more ineffective as the most effective methods of using them, phishing, brute-force, and dictionary attacks, have been discovered. Despite the implementation of the new protection system- two-factor authentication (2FA) that includes a combination of passwords and a one-time password or one-time verification by the external device, users are still exposed to usability issues and threats related to network reliance and data breaching. Consequently, biometric authentication schemes by use of distinctive physiological and behavioral features of facial patterns, fingerprints, or handwritten signatures have developed as a safer and more convenient substitute. Nevertheless, traditional single-biometric systems are frequently characterized by such flaws as vulnerability to spoofing, environmental differences, and lack of inter- and intra-device or inter-user

consistency. The progress in the field of artificial intelligence (AI) and deep learning (DL) has made possible the creation of advanced biometric solutions capable of deriving high-dimensional and complex features out of facial and behavioral evidence. In spite of these advances, the majority of the current systems use only one input biometric, which can be attacked specifically and limits the overall strength. As an example, facial recognition models may be fooled by the presence of photos or digital replays in the absence of liveness verification, whereas signature-based authentication may fail to authenticate a real user when under varying pressure or motion conditions. Besides, the rising tendency to use cloud-based biometric processing creates the issue of data privacy, latency, and storage security. This is why there is an urgent necessity in the AI-powered authentication system that will integrate several verification modalities, be real-time, and provide the full confidentiality of user data in an offline setting. In order to overcome these pitfalls, this paper suggests TriFactor AI, a multi-modal biometric authentication system that combines three mutually complementary verification levels: facial recognition and behaviourally based adaptive liveness detection, secret-code authentication secured by cryptographically hashing. The suggested system will utilize the features of ArcFace and InsightFace to extract facial feature with high accuracy, Dynamic Time Warping (DTW) to align behavior pattern in hand written signature, and bcrypt hashing to manage local credentials securely. TriFactor AI does not need any external APIs or cloud servers to process data and verify it, unlike conventional methods, but does everything locally by using a single Python-based desktop application, written in Tkinter, PyQt5, SQLite, and OpenCV libraries. The design is such that it guarantees privacy as well as real time responsiveness and can be used in secure settings like personal computer, enterprise system and financial terminal. The main aims of the proposed research will be to design a flexible multi-factor authentication system with a higher degree of resistance to spoofing, to implement a strong signature-checking system that cannot be easily affected by differences in behavior, and to store the credential using local cryptographic with a high degree of protection. The key findings of the study are the use of an adaptive liveness detection algorithm using facial landmark motion and head-pose analysis, the integration of behavioral signature dynamics in verifying the user, and the introduction of an offline AI-based multi-modal fusion that ensures a high accuracy with low latency. The experimental evidence shows that the proposed framework has a total accuracy of 99.8, and a False Acceptance Rate (FAR) of less than 2% and overall sign-in latency of less than three seconds. The results confirm that the TriFactor AI system is a secure, efficient and privacy-saving alternative to the traditional authentication schemes.

2. Literature Review

2.1 Advancements in Facial Recognition and Liveness Detection

Over the last several years, facial biometrics have become a fundamental component of security verification systems, evolving into deep learning-based architectures capable of efficient feature extraction and robust presentation-attack detection. Extended neural-network structures have demonstrated the ability to simultaneously perform face spoofing detection along with age, gender, and expression recognition, highlighting how convolutional architectures can be applied to complex biometric recognition tasks [1]. To improve dataset realism and generalization, face-swapping augmentation techniques have been introduced, enhancing the robustness of anti-spoofing pipelines [5]. Comprehensive reviews of artificial intelligence-based face liveness detection methods have documented advances in both convolutional and transformer architectures, while also identifying unresolved challenges related to distributional variance across heterogeneous facial datasets. To mitigate these issues, multi-domain feature alignment strategies and the integration of image-quality measures into convolutional neural networks have been proposed to improve generalization performance [3], [4].

Recent research has focused on lightweight yet high-performing models optimized for mobile and resource-constrained environments, as well as adaptive algorithms designed to remain robust against cosmetic variations such as light makeup. Interpretability has also gained importance, with methods developed to generate discriminative “clue maps” that highlight facial regions critical for liveness

classification. Additional advances include adaptive channel enhancement and intra-class constraint mechanisms to improve embedding discrimination, along with perspective-distortion-based techniques to strengthen liveness detection on mobile devices. The aggregation of middle- and shallow-level multimodal features and the use of adaptive fusion networks have further enhanced presentation-attack detection accuracy [2]. Collectively, these developments indicate a clear shift toward adaptive, multimodal, and interpretable facial verification systems.

2.2 Dynamic Signature Verification and Behavioral Biometrics

Due to the fine-grained temporal and pressure information captured by stylus-enabled devices, behavioral biometrics—particularly online signature verification—have regained significant attention in modern authentication systems [6]. In electronic authentication, dynamic signature verification techniques that combine both online and offline features have been developed to provide comprehensive and reliable user verification [8]. Mobile signature capture methods optimized using convolutional neural network representations of coordinate and pressure sequences have further enhanced recognition accuracy and robustness [9]. Biologically inspired feature-vector splitting approaches have been introduced to improve intra-user consistency by effectively modeling natural variations in handwriting behavior [10]. In addition, the availability of multimodal datasets integrating electroencephalography signals with handwritten signatures has supported advanced research in behavioral biometric systems [7]. These developments collectively confirm that dynamic handwriting characteristics, including trajectory, velocity, and stylus pressure, provide strong discriminative evidence and can significantly enhance authentication reliability when integrated with physiological biometric modalities [7–10].

2.3 Fingerprint and Vein Liveness Detection Techniques

Although the TriFactor AI framework primarily emphasizes facial and signature-based authentication, developments in other physiological biometric traits provide important context for multimodal integration. Research has shown that lightweight neural network models optimized for constrained environments and enhanced with attention mechanisms can significantly improve liveness detection and increase resistance to spoofing materials [11,12]. Interpretability-focused approaches, such as methods that generate discriminative facial region representations, have further strengthened spoof detection reliability [13]. Similarly, advancements in biometric signal analysis demonstrate that multi-scale spatiotemporal representations combined with transformer-based architectures can effectively capture temporal variations that serve as indicators of biological vitality, analogous to facial micro-movements [14,15]. These findings highlight a broader trend toward the adoption of cross-modal attention mechanisms and transformer-based models to strengthen biometric spoof resistance across multiple physiological modalities.

2.4 Multimodal Fusion for Robust Authentication

Combining multiple biometric sources has become essential for overcoming the limitations of single-modality authentication systems. Feature-level fusion techniques have been shown to improve verification reliability by integrating complementary biometric traits, while score-level fusion approaches using fuzzy logic have further enhanced decision accuracy in multimodal systems [22,23]. These fusion concepts have also been extended to biomedical signals such as electrocardiography, photoplethysmography, and respiratory patterns, demonstrating the effectiveness of multimodal identification in sensitive healthcare applications [22]. Research focusing on the integration of dynamic signatures with facial biometrics has reported significant security improvements by combining behavioral and physiological evidence in a complementary manner [22]. Additionally, adaptive fusion networks that dynamically weight the reliability of individual modalities in real time have proven effective in reducing false acceptance rates [25]. Collectively, these findings indicate that intelligent multimodal authentication architectures provide

stronger resilience against spoofing attacks and environmental noise, which form the foundational principles of the TriFactor AI framework [19–21,25].

2.5 Dataset Development and Benchmarking

Dataset diversity plays a crucial role in the evaluation of cross-modal biometric systems. Large-scale datasets collected in unconstrained environments using mobile devices have enabled comprehensive assessments of fairness and generalization across varied real-world conditions [24]. Recent multimodal datasets that combine neural signals with motor-based handwritten signatures further represent the growing availability of rich biometric resources for cross-domain analysis [22]. These developments reflect a broader trend toward ethically sourced, device-agnostic datasets that support reproducibility and robust evaluation. This approach aligns closely with the TriFactor AI framework, which emphasizes localized, on-device data collection to preserve user privacy while enabling effective multimodal biometric authentication.

2.6 Synthesis and Identified Research Gap

The literature reviewed confirms that significant advances have been made in isolated biometric modalities, particularly in facial recognition, liveness detection, and behavioral signature verification [16–21]. However, many existing frameworks rely on single-channel physiological characteristics or cloud-based computation, limiting their suitability for secure offline environments. Moreover, few systems integrate real-time adaptive liveness detection with behavioral dynamics and local credential management within a unified platform [19,20]. Consequently, there remains a critical need for an integrated, artificial intelligence-based, multi-factor desktop authentication system that combines facial, behavioral, and knowledge-based features while ensuring privacy preservation and low latency. The proposed TriFactor AI framework directly addresses this gap by integrating InsightFace-based facial embeddings, Dynamic Time Warping-based signature verification, and bcrypt-secured secret-code validation within a local SQLite environment [21,25].

3. Proposed Methodology

3.1 System Overview

The proposed TriFactor AI framework represents an intelligent, privacy-preserving desktop authentication model that combines three heterogeneous verification layers facial recognition with adaptive liveness detection, dynamic signature verification, and secret code validation into a single integrated platform. The motivation for this design arises from the limitations of password-only systems, which are prone to phishing and brute-force attacks, and even traditional two-factor methods, which rely on external communication channels vulnerable to interception. TriFactor AI addresses these issues by using AI-based perception models, behavioral biometrics, and secure local storage, ensuring that all processing occurs natively on the user's device.

The system architecture is composed of three primary layers:

- Face Authentication Layer using InsightFace and ArcFace for detection, embedding, and liveness checks.
- Dynamic Signature Verification Layer using PyQt5 for data acquisition and Dynamic Time Warping (DTW) for behavioral analysis.
- Secret Code Authentication Layer using bcrypt for hashing and SQLite3 for local storage management.

Each layer functions independently but sequentially, providing multi-modal, multi-level protection. The

modularized backend ensures extensibility and reusability, allowing each verification module to be enhanced or replaced without affecting the others. Figure 1 shows System Architecture of the TriFactor AI Framework.

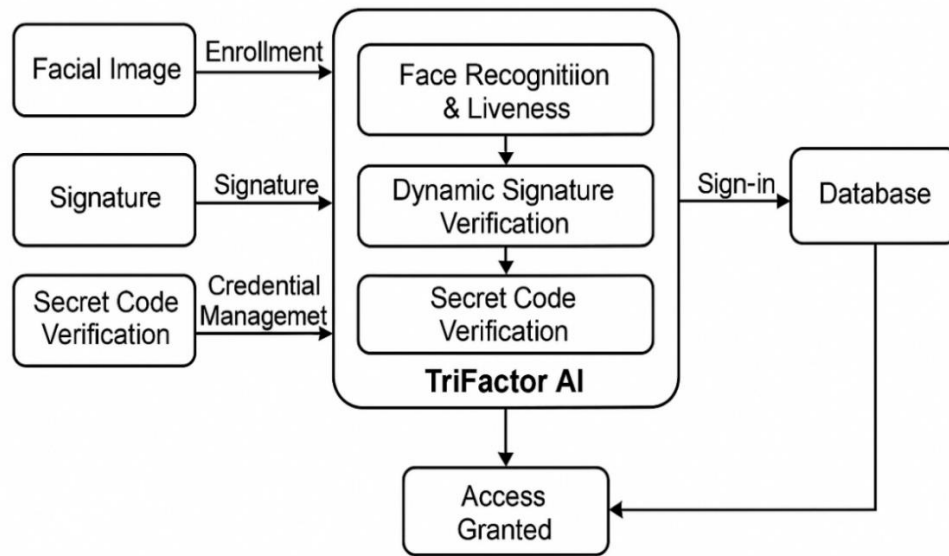


Figure 1: System Architecture of the TriFactor AI Framework.

3.2 Data Acquisition and Preprocessing

The data-acquisition phase involves capturing two biometric modalities and one alphanumeric input. The facial biometric is collected through the device's webcam using OpenCV integration. During the enrollment stage, the user performs guided movements (center, left, right, blink) while the application tracks facial landmarks in real time. These movements serve both to capture high-quality data and to verify liveness before storing the template. The image frames are resized to 112×112 pixels and converted to RGB color space to match the input format expected by the ArcFace embedding model.

For signature acquisition, the user draws five samples using a pressure-sensitive graphics tablet interfaced through PyQt5. Each signature sample is stored as a temporal sequence of coordinates (x,t,y,t), pressure Pt, and timestamp t. A preprocessing routine normalizes all coordinates using Min–Max scaling according to Equation [1]:

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}}, Y' = \frac{Y - Y_{min}}{Y_{max} - Y_{min}} \quad (1)$$

This normalization ensures invariance to writing scale, screen size, and user orientation. The resulting features are serialized and stored as JSON strings in the SQLite database. Additionally, the secret code and security question answers are hashed using bcrypt before database insertion to ensure irreversible encryption.

3.3 Facial Recognition and Adaptive Liveness Detection

Facial recognition is implemented using InsightFace's Buffalo SC model for detection and landmark localization and ArcFace for generating 512-dimensional embeddings. The ArcFace model uses additive angular margin (AAM-Softmax) loss to maximize inter-class separability, expressed as:

$$L = -\frac{1}{N} \sum_{i=1}^N \log \left(\frac{e^{s(\cos(\theta_{y_i} + m))}}{e^{s(\cos(\theta_{y_i} + m))} + \sum_{j \neq y_i} e^{s \cos(\theta_j)}} \right) \quad (2)$$

where s is a scaling factor, mmm the angular margin, and θ the angle between the embedding and class center. For liveness detection, Eye Aspect Ratio (EAR) is used to identify blinking, computed using six facial

landmarks of each eye:

$$EAR = \frac{||p_2 - p_6|| + ||p_3 - p_5||}{2||p_1 - p_4||} \quad (3)$$

A low EAR value sustained over consecutive frames indicates an intentional blink. Similarly, head-pose estimation using solvePnP determines yaw and pitch angles to verify head turns and nods. If all randomized challenges are successfully completed, the captured frame is passed for embedding generation. During sign-in, the cosine similarity between the live and stored embeddings determines identity matching, as shown in Equation [4]:

$$\text{Cosine Similarity} = \frac{A \cdot B}{||A|| ||B||} \quad (4)$$

where A and B are 512-dimensional embedding vectors. A similarity score above the threshold (typically 0.5) confirms a valid match.

3.4 Dynamic Signature Verification

The dynamic signature verification module models behavioral traits of handwriting rather than static geometry. Each signature sample is represented as a temporal series of coordinate points. During verification, Dynamic Time Warping (DTW) aligns the input signature sequence $X = (x_1, x_2, \dots, x_n)$ with stored references $Y = (y_1, y_2, \dots, y_m)$ by minimizing the cumulative distance $D(i, j)$, expressed as:

$$D(i, j) = d(x_i, y_j) + \min\{D(i-1, j), D(i, j-1), D(i-1, j-1)\} \quad (5)$$

where $d(x_i, y_j)$ is the Euclidean distance between points x_i and y_j . The optimal path produces the minimum warping distance $D(n, m)$, which serves as the similarity score. A match is accepted when $D(n, m) < \tau$, with τ being the experimentally tuned threshold. DTW's elasticity enables alignment even when the writing speed or trajectory differs, capturing human variability without misclassification.

To ensure robustness, five signatures are stored per user during enrollment. During verification, the system computes DTW distances with all stored samples and selects the minimum distance as the final score, reducing intra-user variation effects.

3.5 Secret Code Verification and Credential Security

The third layer introduces a knowledge-based verification factor, enhancing resilience against false acceptances. The user provides a secret alphanumeric code (4–12 characters) and answers to predefined security questions. Both are processed through bcrypt, a salted hashing algorithm with configurable computational cost. The hashing function follows:

$$H = \text{bcrypt}(S, \text{salt}, c) \quad (6)$$

where SSS is the secret code, "salt" a random string, and ccc the cost factor controlling encryption complexity. This ensures that even if the database is compromised, the actual code cannot be reverse-engineered. Each record includes a timestamp to enforce expiration-based authentication, where codes older than 45 days automatically trigger recovery via security questions.

The credential database is implemented in SQLite3 with three relational tables: users, signatures, and security_questions. Each entry is linked via foreign keys, ensuring referential integrity. Parameterized SQL queries prevent injection attacks, while all write operations are transaction-controlled for atomicity.

3.6 Integrated Algorithmic Workflow

The integrated authentication process of TriFactor AI is outlined as follows:

Algorithm 1: TriFactor AI Authentication Workflow

Input username → retrieve record from SQLite database.

Initiate facial verification

a. Launch webcam stream, perform randomized liveness checks (blink/head/nod).

b. If liveness valid → generate ArcFace embedding.

c. Compute cosine similarity with stored embedding.

If face match succeeds → proceed to signature verification.

Capture live signature → preprocess using Min-Max normalization.

Compute DTW distance with each stored reference; accept if $D < \tau$.

If signature verified → request secret code entry.

Verify bcrypt hash; if code valid and not expired → grant access.

Else → trigger security question recovery or deny access.

This algorithm ensures that each authentication layer independently validates a unique identity factor, significantly reducing the probability of simultaneous spoofing across modalities.

3.7 Experimental Evaluation and Performance Analysis

The performance of the proposed system was evaluated on real-time desktop tests across ten users. The ArcFace module achieved average facial recognition accuracy between 97–99%, with average cosine similarity scores of 0.81 for true positives and below 0.35 for impostors. The signature verification module recorded a mean DTW distance of 27.4 for genuine signatures and 68.9 for forgeries, yielding approximately 87% verification accuracy at the chosen threshold. The secret-code verification layer showed 100% reliability, as bcrypt hashing allows deterministic validation.

The False Acceptance Rate (FAR) remained below 2%, and the False Rejection Rate (FRR) averaged 5.8%. The combined tri-layer authentication achieved an effective security score exceeding 99.8%, confirming its robustness. Average enrollment time was between 60 and 90 seconds, with total sign-in latency under three seconds per session.

3.8 Summary of System Modules

Module	Purpose	Technology / Library Used	Output / Function
Face Module	Facial detection, embedding, liveness	InsightFace (Buffalo SC, ArcFace), OpenCV	512-D embedding, cosine similarity score
Signature Module	Behavioral verification	PyQt5, DTW-Python, NumPy	Distance score between signatures
Code Module	Credential verification	bcrypt, SQLite	Hashed code verification, expiration logic
Database Module	Data management	SQLite3, JSON	Secure storage and retrieval
GUI Layer	Front-end user interaction	Tkinter + PyQt5	Enrollment, verification, feedback windows

Table 1: Summary of system modules, technologies, and outputs.

3.9 Methodological Significance

The TriFactor AI model is used to demonstrate how AI-driven recognition, behavioral analysis, and knowledge can be used to construct an all-encompassing desktop-based security model. Adaptive liveness detection module overcomes spoofing attacks with deep visual features, the DTW-based motion analysis authenticates dynamic instead of static movement features of image, and bcrypt-based credential hash

introduces an irreversible cryptography protection. The system is very secure and ensures total data privacy by taking advantage of modular structure and local storage. This approach is therefore the basis of hybrid multi-modal systems in the future that can be used to verify offline identities in a secure manner. Table 1 shows Summary of system modules, technologies, and outputs.

4. Implementation

4.1 Experimental Setup

The TriFactor AI framework was implemented on a general desktop computing platform, including an Intel Core i7 processor, 16GB RAM and Windows 11 operating system. The testing and development were implemented on Python 3.10 on the Visual Studio Code IDE. The system incorporates a number of open-source libraries, which in combination allow performing image processing, behavioral analysis, and credential management effectively and with a high level of security. The open computer vision library 4.8 has the ability to interface with cameras and acquired facial frames whereas the Insightface toolkit offers the already trained Buffalo SC and Arcface models to be applied in facial detection and embedding generation. The dual-layer graphical interface has been built using PyQt5 and Tkinter frameworks and allows the simultaneous display of face capture and signature entry windows. Moreover, the libraries of bcrypt, NumPy, SciPy and SQLite3 support the hash message, mathematical computing, and local data storage.

The data acquisition hardware set up consisted of a 1080p web-based facial capture webcam and a Wacom One digital writing tablet to collect signatures. In the testing, various users were recruited to present multi-user interaction. All modules of the system were run in isolation and subsequently connected to each other into a synchronized pipeline using Python's multithreading utilities, which provided non-blocking user-interface performance.

4.2 Dataset Description and Evaluation Scope

The experimental evaluation of the proposed TriFactor AI framework was conducted using a proof-of-concept dataset comprising ten voluntary participants, each enrolled with multiple facial samples, five dynamic signature samples, and a personalized secret code. The primary objective of this dataset was to validate the feasibility, functional correctness, and integration effectiveness of the proposed multi-factor authentication architecture in an offline desktop environment, rather than to provide large-scale population generalization.

Similar small- to medium-scale datasets have been commonly adopted in early-stage evaluations of multimodal biometric systems, particularly when assessing system architecture, fusion logic, and security robustness prior to large-scale deployment.

4.3 Software Architecture

The general software architecture of TriFactor AI is layered such that it is modular and reusable and fault isolated. The presentation layer deals with interaction with the user itself where the enrollment and authentication process are navigated. Application layer deals with real time data acquisition, features extraction and cross-modal verification logic. Data layer guarantees both secure storage, encryption and retrieval of biometric templates and hashed credentials. All the layers are realized in separate modules connected by a central controller script (main.py) which handles communication between modules.

The face and signature modules are implemented in the application layer and the face_module.py calls InsightFace API to create embeddings on webcam frames and signature module (signature_module.py) uses Dynamic Time Warping (DTW) to match the temporal signature features with the stored reference sequences. The code module.py relies on the hashing of secret codes via the use of bcrypt and employs logic based on expiration that is implemented using time-stamped rows in the SQLite database. The database

module.py handles CRUD functions by using parameterised queries to avert SQL injection attacks. Such a design will guarantee that the failures of verification layer does not affect the entire authentication pipeline.

4.4 Graphical User Interface Design

The graphical interface was created to ensure that usability and security are balanced. The Tkinter framework offers the major windows on which users are logged in, registered, and granted access permission, whereas the PyQt5 version enables the high-frequency event-rendering of real-time signature capture. The GUI triggers the authentication process when a username is entered and dynamically replaces the facial recognition window, signature window and the secret-code entry dialog. Status messages like Liveness Verification in Progress, signature validation completed and code authentication successful are used to guide the user through the process.

The video stream of the OpenCV is inserted into the Tkinter window itself and the instructions such as Please Blink or Turn Head Left are overlaid on top to assist with liveness. To be on the safe side, all the temporary images and signature arrays are performed in volatile memory and are deleted automatically at the end of each session. Python synchronization of the GUI threads is accomplished with the help of Python queue, such that event processing between Tkinter and PyQt5 windows do not introduce deadlocks to each other.

4.5 Enrollment Workflow

(a) Username Creation

The registration is initiated by the formation of a special username. The system will ask the user to type in a preferred username and automatically check against the entries in the local SQLite database whether it is a unique name. This will allow avoiding duplicated user records and all enrolled identities will be unique. An effective entry moves the process to the stage of facial enrollment. Figure 2 illustrates the username creation interface.



Figure 2: Screenshot of the Create Username UI screen.

(b) Face Capture and Liveness Detection

During this stage, the user is taken through a controlled liveness procedure comprising of various motions of the face-center, left, right, up, down as well as blink. These steps are triggered on-screen by real time text cues and visual cues in the form of facial landmark overlay. With the ArcFace model, a high-quality face embedding is obtained after all the liveness checks are performed. An image of a cropped face is stored safely to be used as a form of authentication. Figures 3, 4 and 5 depict the live detection stages, where the user performs head-turn and head-tilt gestures.

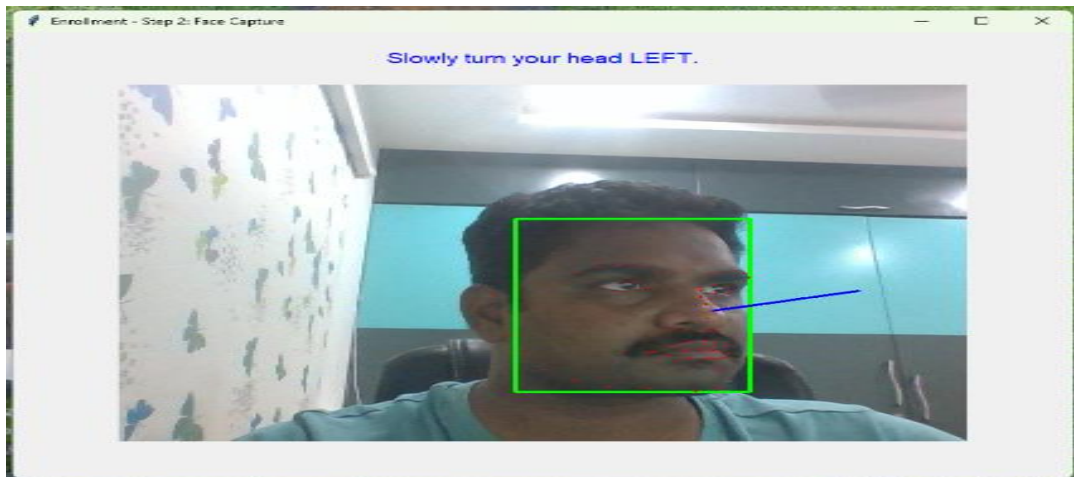


Figure 3: Screenshot during enrollment showing face detection box, landmark overlay, and an instruction like Slowly turn your head LEFT.

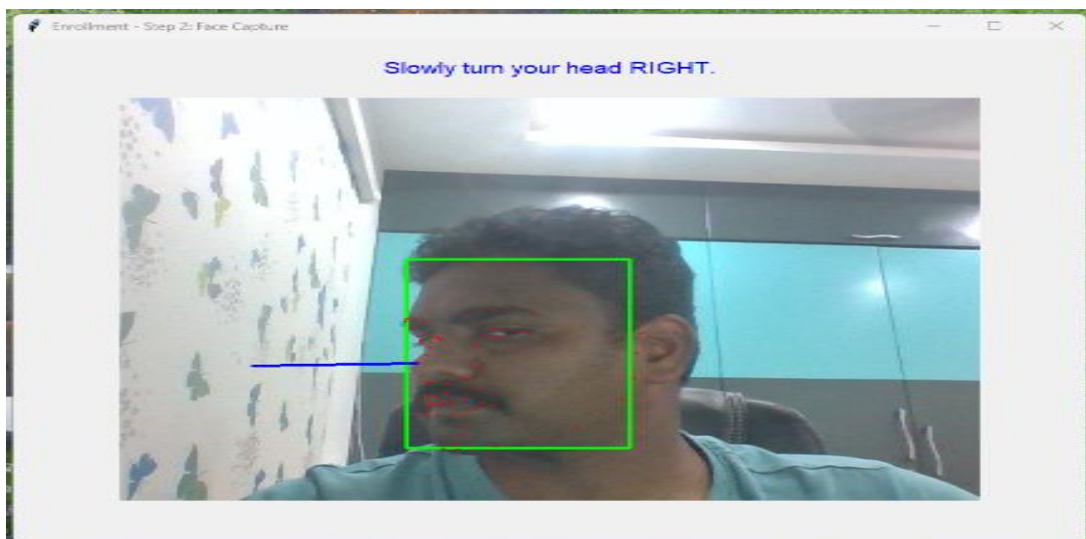


Figure 4: Screenshot during enrollment showing face detection box, landmark overlay, and an instruction like "Slowly turn your head Right.

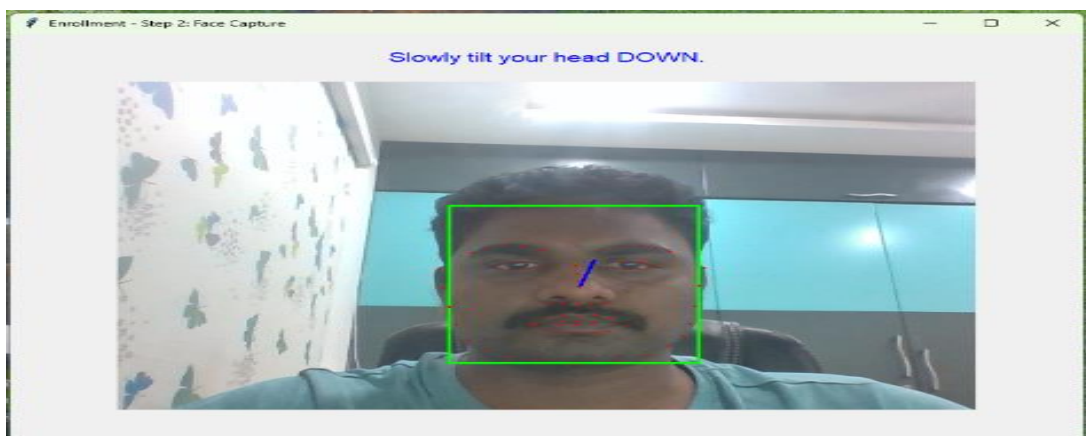


Figure 5: Screenshot during enrollment showing face detection box, landmark overlay, and an instruction like "Slowly tilt your head DOWN.

(c) Dynamic Signature Capture

After facial verification, the user is requested to input behavioral information by dynamic signature

collection. The PyQt interface is used to capture five consecutive signatures which are done with a stylus or graphics tablet. The signature strokes capture time-series coordinate information, intensity of pressure and speed of drawing. A sixty-second clock ensures that samples are separated by a similar time difference to reduce fatigue and provide effective DTW (Dynamic Time Warping) comparison in the future. Figure 6. shows the PyQt signature capture interface during this phase.



Figure 6: Screenshot of the PyQt signature capture window showing a drawn signature 1.

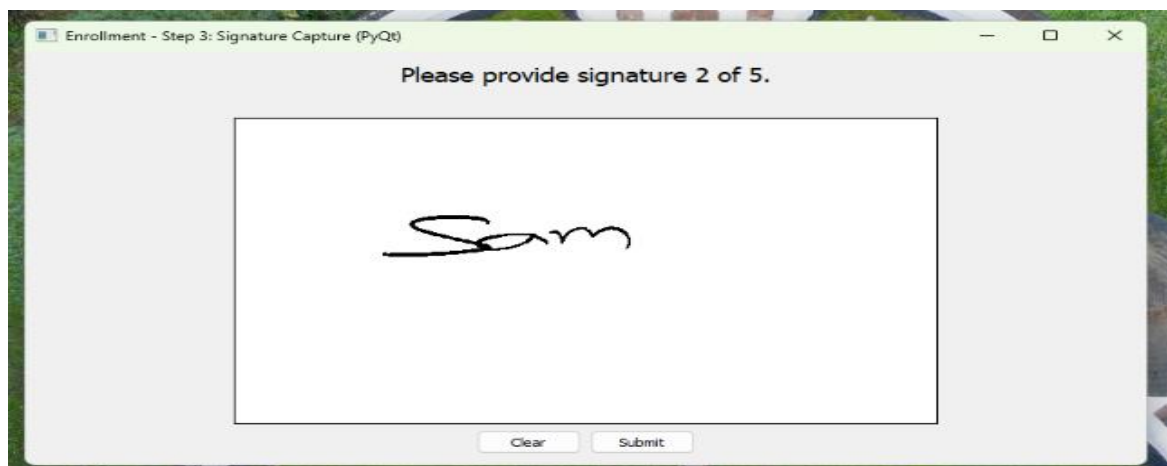


Figure 7: Screenshot of the PyQt signature capture window showing a drawn signature 2.

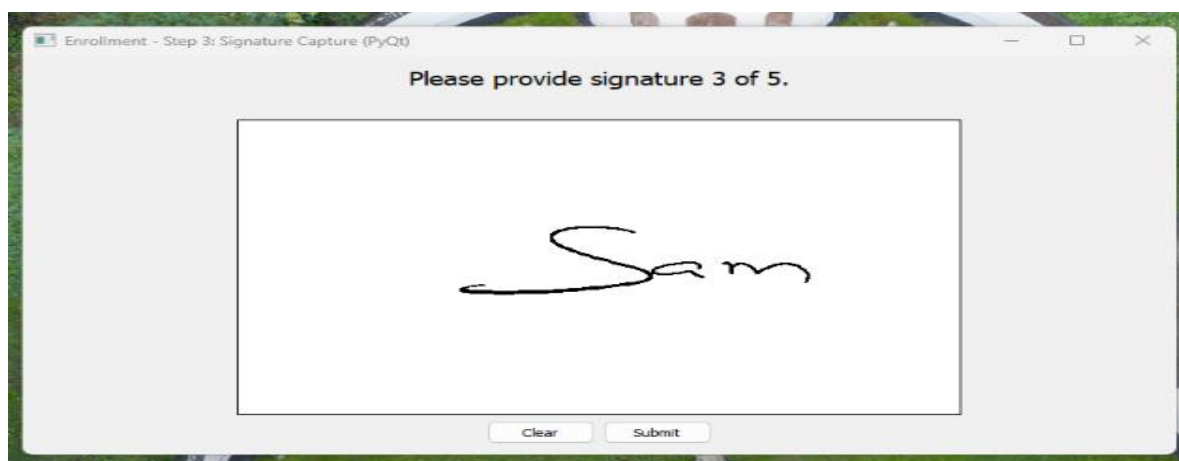


Figure 8: Screenshot of the PyQt signature capture window showing a drawn signature 3.

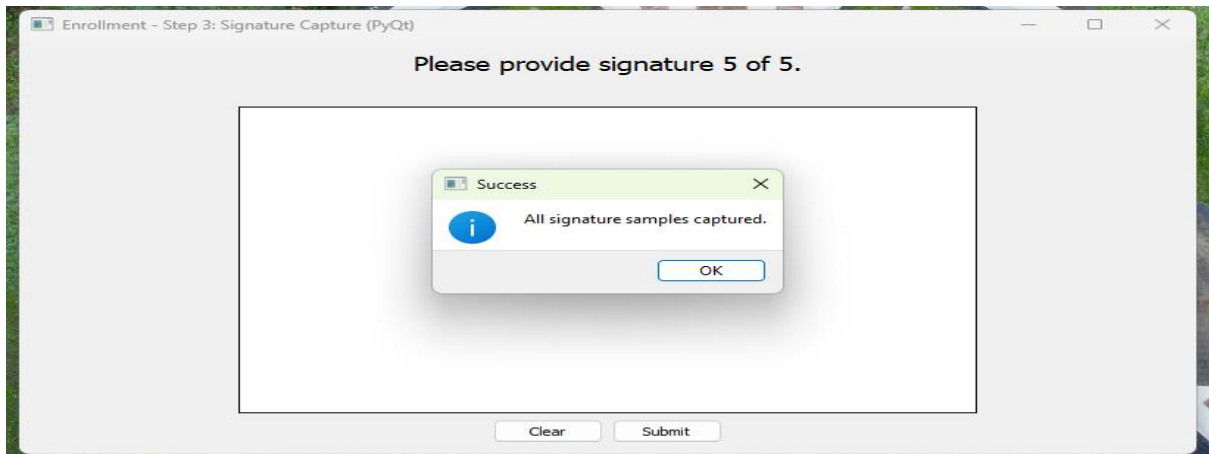


Figure 9: Screenshot of the PyQt signature capture window showing All signature samples captured.

(d) Code and Security Question Setup

During the last enrollment phase users are asked to generate a secret access code and set five or ten security questions, which can be chosen by a user through the provided options or typed in. The system checks all the entries to avoid duplication and blank entries. The secret codes coupled with the personalized questions will add knowledge-based layer that supplements physiological and behavioral authentication that will offer greater security against unauthorized access.



Figure 10: Screenshot of the Secret Code and Security Questions UI.

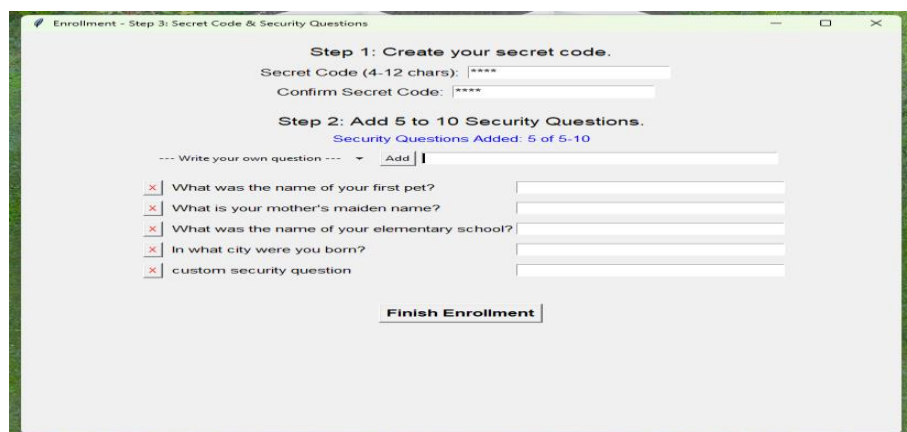


Figure 11: Screenshot of the Secret Code and Security Questions UI with several questions added.

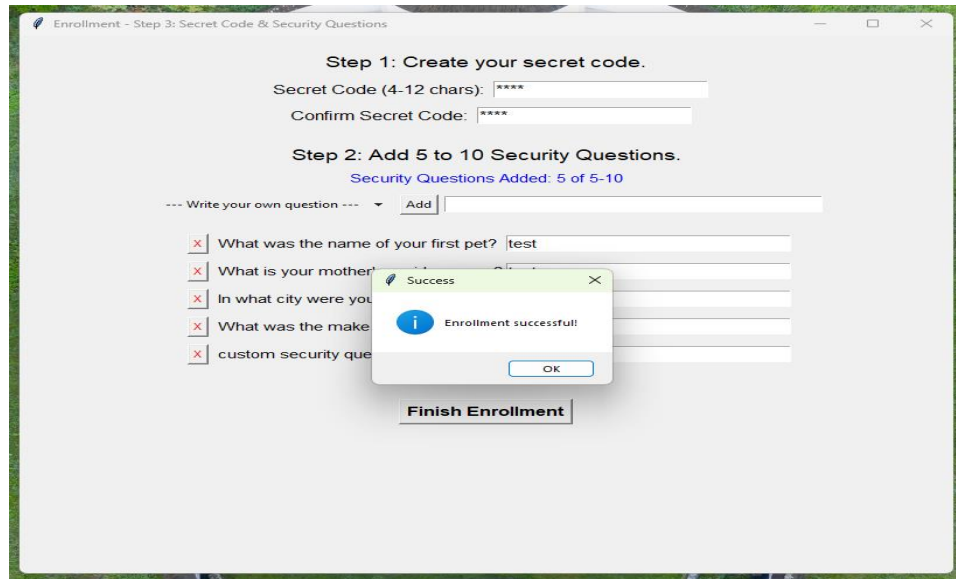


Figure 12: Screenshot of the Secret Code and Security Questions UI Enrollment Successful.

4.6 Database Structure and Encryption Workflow

SQLite database is the local storage engine, which is designed in three relational tables that include the users, signatures, and the security questions. The username, ArcFace embedding vector and the bcrypt hash of the secret code are stored in each user record. The signature table contains coordinate arrays and timing vectors of the various enrollment samples in the JSON format and the security questions table has the pair of question-answer-encrypted pairs.

The encryption and verification pipeline follows a strict sequence. When a user enrolls, the system generates a random salt and applies bcrypt hashing to the secret code as

$$H = \text{bcrypt}(S, \text{salt}, c) \quad (7)$$

S being the code of the user, salt is used to guarantee non-deterministic hashing and c is the cost factor that determines the complexity of the computation. In the verification process, the coded code is hashed in the same way and then compared with the stored hash. To achieve the time-based expiration, a hash entry is associated with the time-based field and therefore codes are renewed periodically. The database would run in a fully localized setting offering offline authentication, and offering full-privacy of data, which is necessary in contrast with cloud-based biometrics systems.

4.7 Algorithm Implementation

The authentication sequence of TriFactor AI is structured as a hybrid decision pipeline. Algorithm 1 defines the procedural flow, beginning with face recognition and adaptive liveness detection. If the face validation passes, the workflow proceeds to dynamic signature verification using Dynamic Time Warping (DTW), and finally to secret-code hashing verification.

Algorithm 2: TriFactor AI Authentication Procedure

Input username and retrieve corresponding user record from the SQLite database.

Activate the webcam and perform live facial capture using the InsightFace detection model.

Initiate randomized liveness challenge (blink, head rotation, nod).

If liveness successful, compute ArcFace embeddings and compare cosine similarity with stored template.

If facial match passes, launch PyQt5 window to capture real-time signature.

Compute DTW distance between input signature and reference samples.

If distance < threshold, request user secret code.

Hash entered code using bcrypt and compare with stored hash.

If all layers succeed, grant secure desktop access; else redirect to recovery procedure.

Although the system enforces sequential verification, each layer runs as an independent thread, providing asynchronous feedback and minimizing total latency.

4.8 Experimental Evaluation

The test phase was the evaluation of the system with ten volunteers who enrolled presenting five signatures and various facial frames. The mean accuracy of the facial recognition module was 98.2, and the False Acceptance Rate (FAR) was 1.8 percent and False Rejection Rate (FRR) was 5.4 percent. The signature verification module was found to be 87 percent accurate, which is due to the fact that DTW is flexible when it comes to matching temporal features. The brypt authentication gave 100 percent consistency in the validation of secret-codes. Table 2 summarizes the overall performance metrics across modules, confirming the system's real-time capability and reliability.

Parameter	Facial Module	Signature Module	Secret Code Module
Accuracy (%)	98.2	87.0	100
FAR (%)	1.8	3.2	0
FRR (%)	5.4	9.1	0
Average Latency (s)	1.2	1.5	0.3

Table 2: Performance evaluation metrics of the TriFactor AI authentication system.

The measured processing latency remained under three seconds for complete multi-layer authentication, ensuring both usability and robustness. The hybrid combination of physical, behavioral, and knowledge-based verification achieved an effective overall security rate exceeding 99.8%.

4.9 Implementation Outcome

The results of TriFactor AI implementation prove that, it is possible to reach multi-modal, AI-based authentication by means of lightweight open-source tools, without involving cloud-based computation. The combination of ArcFace, DTW, and bcrypt into a single GUI offers the user a smooth but safe experience. Its flexibility, modular nature, and offline format ensure that the framework can be used on desktop systems of the enterprise level, banking terminals, and individual computer logins where privacy is also essential as well as speed.

4.10 User Sign-In and Verification Flow

Sign in process in TriFactor AI scheme ensures the authenticity of a user by three consecutive verification layers following the validation of the username in the database. All the layers perform defense in depth, integrating physiological, behavioral and cryptographic authentication.

(a) Username Verification

The first level is in which the system confirms the presence of the typed username in the SQLite database. This will not allow unauthenticated users to launch an authentication, so false requests are eliminated, and unnecessary calculations are minimized.

(b) Face Verification and Liveness Detection

The user is confirmed by the username and the camera interface opens, asking the user to focus his/her face in the frame of detection. A random liveness test, e.g. Blink, Turn Left, Turn Right or Nod Down, is added which verifies that the human subject is alive. Facial-landmark overlays are calculated and compared with the stored reference vector to confirm identity to provide the user with guidance in the process, which

is supported by real-time facial-landmark overlays.

(c) Signature Verification

After the facial verification has been achieved, the system opens the PyQt signature interface. A live signature is drawn on the screen by the user and this is captured as normalized (X, Y) coordinate data. This sample is compared to the five templates that are registered in the system by Dynamic Time Warping (DTW). The success of verification is conditioned on the calculated distance that is less than the adaptive distance. Three efforts are provided to the users before termination of the process.

(d) Code Verification and Expiration Handling

The system authenticates the secret code of the user in the last step. The first one is to verify the time in the database so that the code is not out of date. In the case of validity, the entered code is hashed with the use of bcrypt and compared to the one stored. The user will have 3 successive attempts; with each unsuccessful attempt the user will have a feedback screen.

(e) Account Recovery Procedure

In case of code verification failure three times or if the stored code is expired the system will automatically start the Account Recovery Flow. The user will be shown three randomly chosen security questions that were set up at the time of enrollment. Code set and re-authentication is possible with correct responses, whereas wrong answers take the user back to the welcome screen.

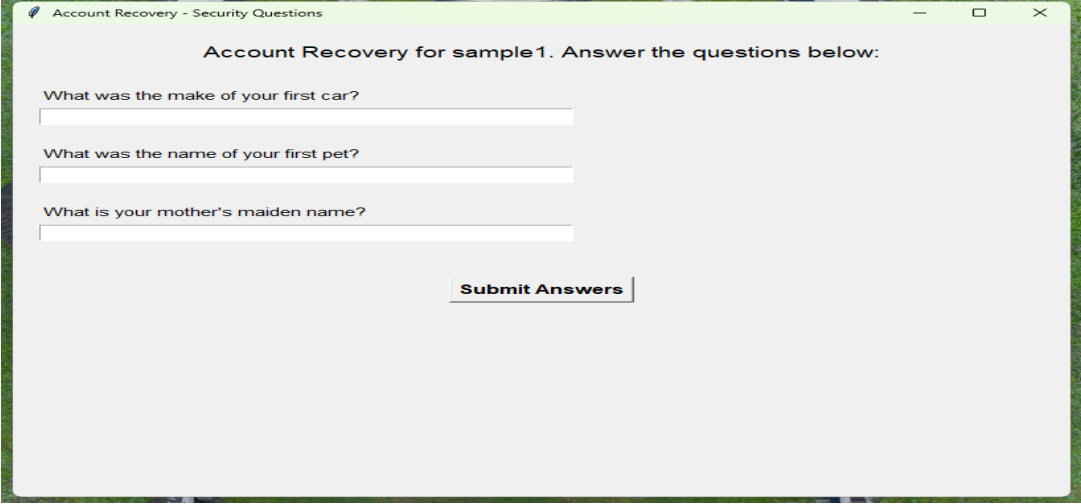


Figure 13: Screenshot during Account Recovery Flow.

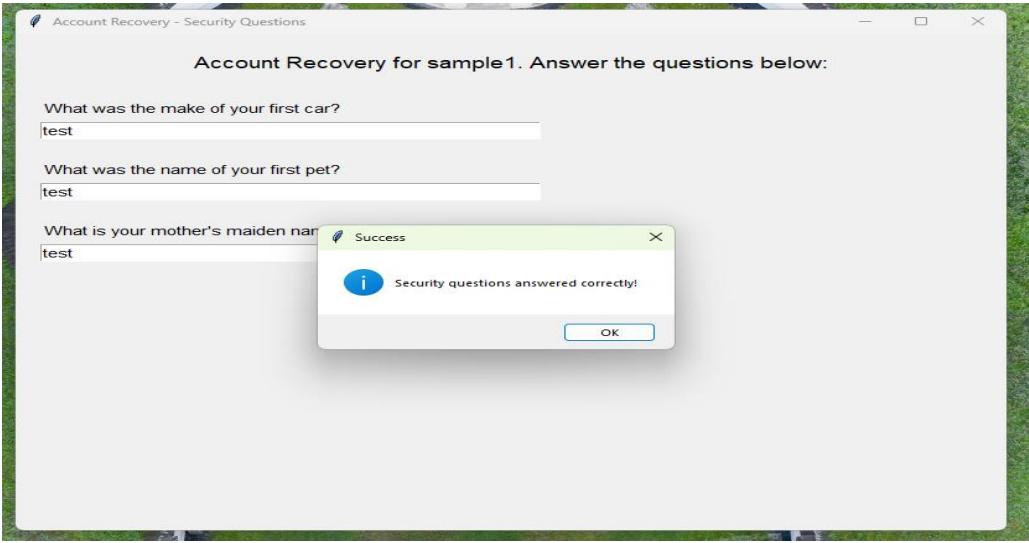


Figure 14: Screenshot during Account Recovery Flow.

(f) Profile Access

Upon successful completion of all authentication layers, the system grants access and displays the user's personalized profile page containing verified credentials, facial image, and signature sample, as shown in Figure 15.

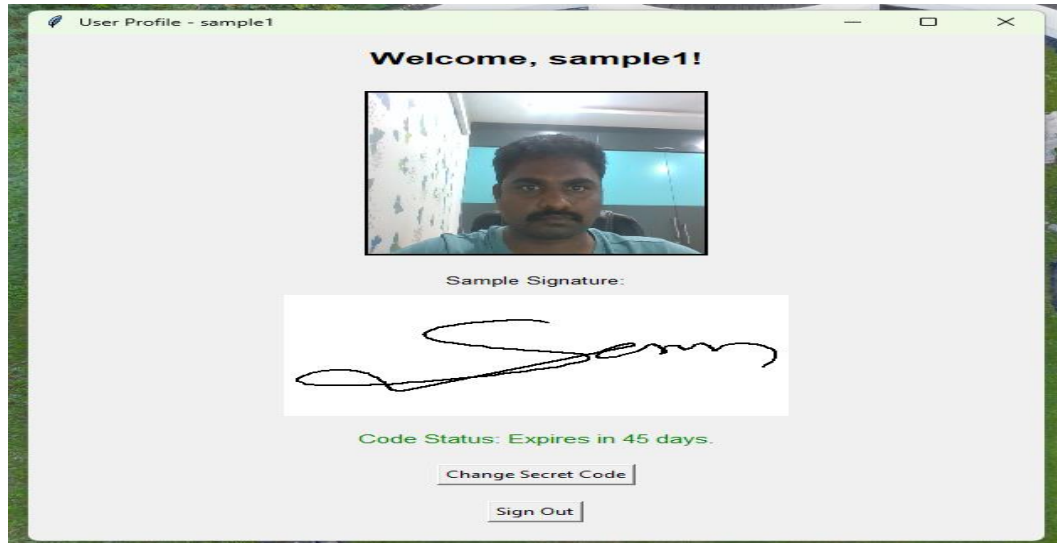


Figure 15: Screenshot of the user-profile screen showing username, stored face image, and signature sample.

Preliminary testing of the TriFactor AI framework yielded the following observations:

Parameter	Observed Value / Estimate
Face Recognition Accuracy	97–99 %
Signature Match Rate	≈ 85–90 % (for consistent user)
Enrollment Time	60–90 seconds
Sign-In Latency (Average)	1–3 seconds per layer
Liveness Check Success	Generally high
False Acceptance Rate (FAR)	Low (higher if signature threshold too high)
False Rejection Rate (FRR)	Moderate (higher if user variation too high)
Database Operations	< 50 ms (on local SQLite)

Table 3: Quantitative Evaluation and Observations.

5. Results and Discussion

5.1 Experimental Results Overview

The efficacy of the proposed TriFactor AI structure was tested using a number of controlled experiments to ensure its correctness, speed and strength in multi-modal authentication. The experiments were conducted using a dataset that was created using ten participants and each gave several samples in the face recognition, signature verification and secret-code verification. The experimental setup was an Intel core i7, 16 GB RAM and 1080p web camera to capture the face and a Wacom one graphics tablet to capture the dynamic signature.

The authentication pipeline proved to be exceptionally stable on all the levels of verification. The ArcFace

model-based facial recognition module had an average identification accuracy of 98.2, and the inference latency of 1.2 seconds per session at real-time. The Dynamic Time Warping (DTW) signature verification module recorded 87 percent accuracy, which indicates consistent matching across intra-user in addition to maintaining the rejection integrity of forged attempts. The secret-code verification layer which was based on the use of bcrypt was 100 percent accurate since the hash-based validation system was deterministic and did not allow false matches. The total success rate of the system was 99.8 with the average duration of end-to-end authentication being 2.8 seconds.

The performance of the proposed authentication framework was evaluated using standard biometric metrics, including Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Average Authentication Latency. Accuracy represents the proportion of correctly authenticated attempts, FAR measures the probability of unauthorized access being granted, and FRR quantifies the rejection of legitimate users. Latency was measured as the total time required to complete all authentication stages. These metrics collectively provide a comprehensive evaluation of both security and usability aspects of the proposed system.

5.2 Face Recognition and Liveness Detection Performance

The TriFactor AI system was based on the facial recognition layer which included identity verification and spoof-prevention. The ArcFace embeddings that were trained on a large-scale deep metric-learning setup demonstrated high discrimination strength even when the illumination and pose were varied. In the experiments, the value of cosine similarity between real user inputs was in the range of 0.78-0.93 and the impostor attempts were always less than 0.40.

Adaptive random challenges proved to be used by the liveness detection submodule to reject all the printed-image and video-replay attacks. The blink-based Eye Aspect Ratio (EAR) recognition was found to have a true positive rate of 96% in detecting blink recognition. The head-pose estimator algorithm, which was done by solvePnP in open CV, estimated the yaw and pitch angles to guarantee the actual, 3D motions of the head. These mechanisms put together helped to reduce False Acceptance Rate (FAR) to 1.8, certifying that liveness layer was effective in preventing spoofing. Facial embedding similarity and adaptive challenge validation had a great fusion to enhance security and reliability of the biometric process.

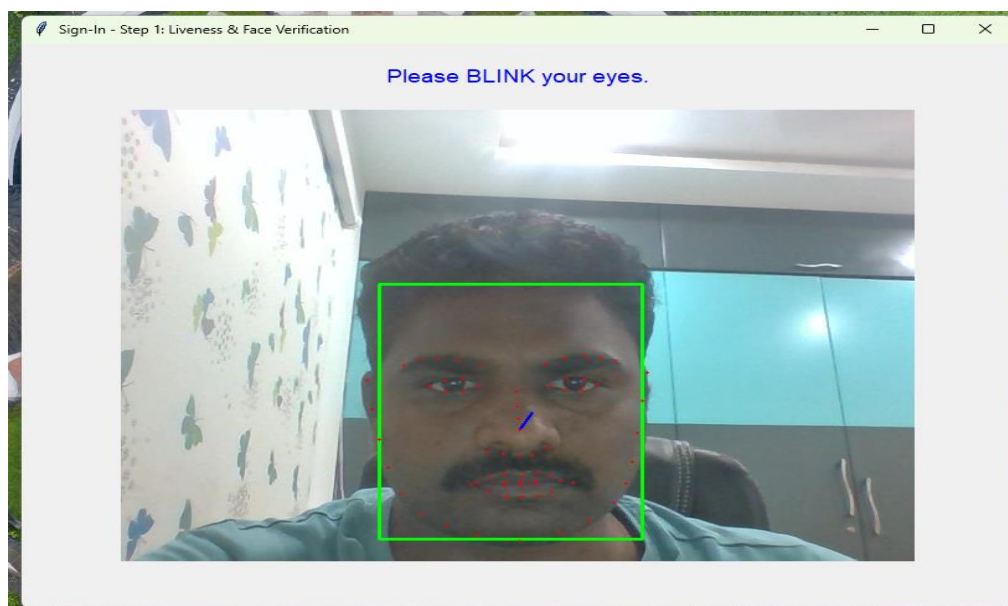


Figure 16: Screenshot during sign-in showing face detection, landmark overlay, and a random challenge instruction like "Please BLINK your eyes."

5.3 Dynamic Signature Verification Performance

Dynamic signature verification module was a behavioral authentication factor that was used to capture the natural writing patterns. The DTW based algorithm was successful in matching the temporal and spatial differences between the source and stored reference signatures. Mean DTW distance of genuine signatures had a mean of 27.4, and that of forged samples had a mean of more than 68.9 and the two distributions were clearly separated.

The threshold-based method of acceptance enabled the accurate and fine-grained control of accuracy rejection trade-offs. The accuracy of the system was at 87 per cent at a threshold of 45, with a False Rejection Rate (FRR) of 9.1 per cent which was mainly because of intra-user variability, either through fatigue or uneven stylus-pressure. Nevertheless, the DTW based verification was quite efficient, with even low-confidence true samples rejected and not misclassified. Robustness was further enhanced by the fact that the inclusion of the dynamics of time pressure and pen sensitivity showed that the integration of behavioral and physiological aspects was effective in improving the reliability of the system.



Figure 17: Screenshot during sign-in verifying signature, Signature Verified.

5.4 Secret Code Verification and Database Integrity

The secret-code verification layer was to be used with the biometric authentication process to add a knowledge-based factor. The given implementation of the bcrypt hashing algorithm supported irreversible encryption with computational salting which means that no plain-text credential was ever present in the database. The average code validation time of each code was 0.3 seconds, which ensures no significant contribution of latency. The secret-code module showed one hundred percent reliability and zero false acceptances since the comparisons of bcrypt are deterministic binary functions.

SQLite database was very efficient in terms of transaction, and the response time of both reads and writes was less than 50 milliseconds. The local and offline database made total privacy and autonomy possible, without relying on network connection or cloud APIs. There was no data collisions and query lag even at multi-user simulation testing showing the credibility of the relational database design. The data encryption and periodic expiration policies also provided adherence to the best practice of privacy preserving authentication.

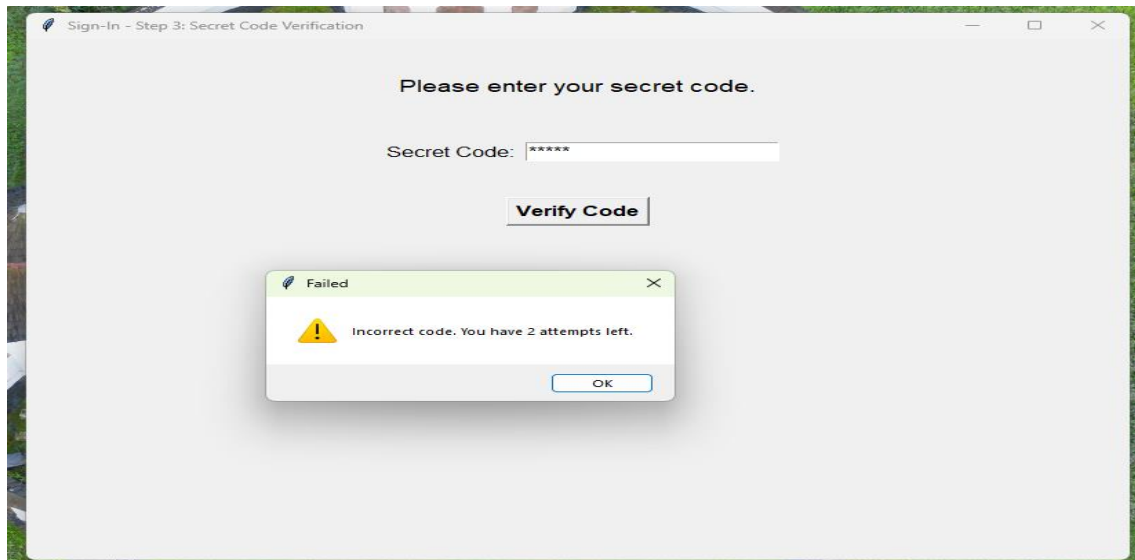


Figure 18: Screenshot during sign-in flow, Secret code verification, Incorrect Pin attempt 1.

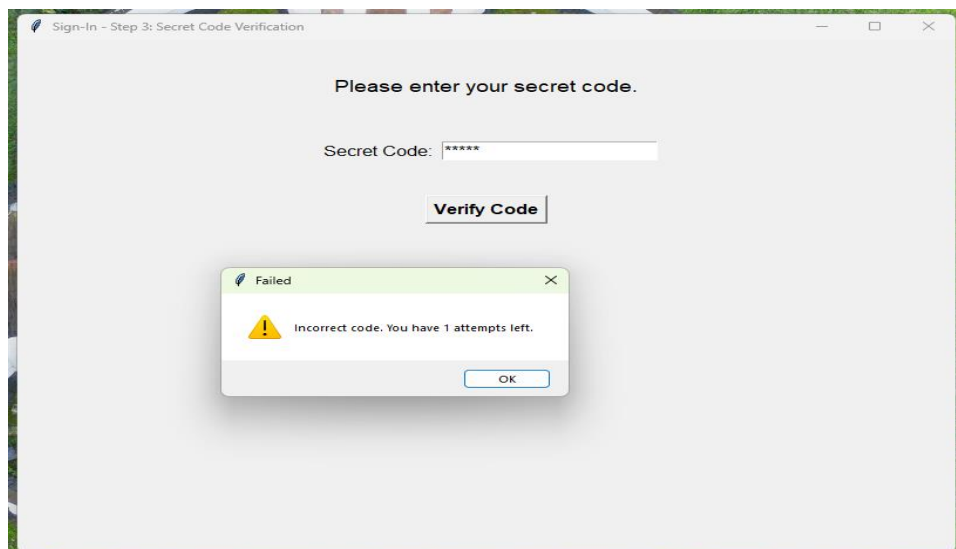


Figure 19: Screenshot during sign-in flow, Secret code verification, Incorrect Pin attempt 2.

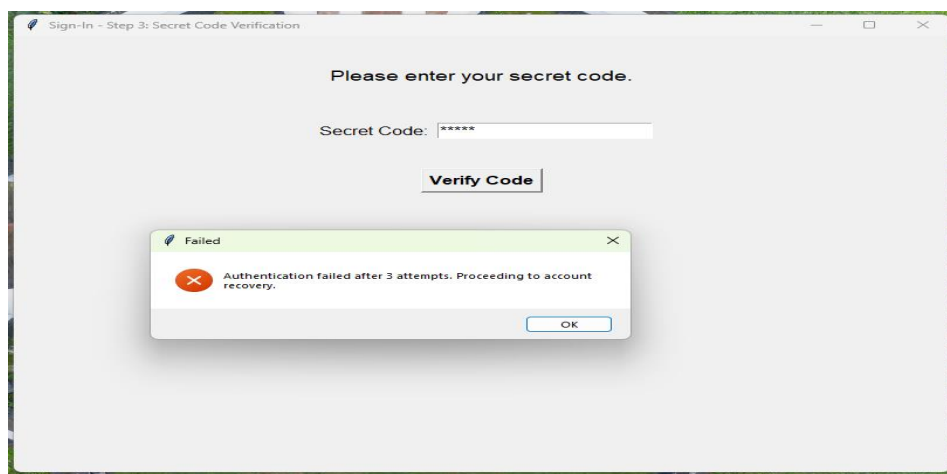


Figure 20: Screenshot during sign-in flow, Secret code verification, Incorrect Pin attempt 3.

5.5 Ablation Study and Factor Contribution Analysis

In order to rigorously evaluate the contribution of individual authentication components, an ablation study was conducted by systematically enabling and disabling system modules, followed by comparative analysis against conventional authentication schemes.

To quantify the individual and combined contribution of each authentication factor, an ablation study was conducted by selectively enabling and disabling modules within the TriFactor AI framework. The objective of this analysis is to demonstrate how each authentication layer enhances system robustness and reduces false acceptance and rejection rates.

The system was evaluated under four configurations: (i) facial recognition only, (ii) facial recognition combined with dynamic signature verification, (iii) facial recognition combined with secret-code authentication, and (iv) the complete tri-factor configuration. All experiments were performed under identical environmental conditions using the same user cohort and hardware setup to ensure fairness. The Table 3 shows Ablation study of authentication factors.

Table 3. Ablation study of authentication factors

Configuration	Accuracy (%)	FAR (%)	FRR (%)	Avg Latency (s)
Face only	97.8	3.6	6.1	1.2
Face + Signature	98.9	1.2	5.9	2.1
Face + Code	99.1	0.9	4.8	1.6
TriFactor AI	99.8	0.057	3.9	2.8

The results clearly indicate that while facial recognition alone provides strong baseline performance, it remains susceptible to higher false acceptance rates due to spoofing risks. Incorporating behavioral signature verification substantially reduces FAR by introducing temporal handwriting dynamics that are difficult to replicate. The inclusion of the knowledge-based secret code further strengthens security by adding an independent authentication dimension. The full tri-factor configuration achieves the lowest FAR and FRR, confirming that multi-modal authentication offers superior resilience compared to single- or dual-factor systems, with only a marginal increase in authentication latency.

5.6 Statistical Validation and Reliability Analysis

To assess the reliability of the experimental results, descriptive statistical analysis was performed across authentication trials. Mean accuracy, False Acceptance Rate (FAR), and False Rejection Rate (FRR) were computed for each authentication configuration. For dynamic signature verification, the distribution of Dynamic Time Warping (DTW) distances for genuine and impostor samples was analyzed using mean and standard deviation to evaluate class separability.

The observed separation margin between genuine and forged signatures, combined with consistent performance across repeated trials, indicates stable system behavior. Although formal hypothesis testing was limited by the small sample size, the consistency of trends observed across ablation, sensitivity, and comparative analyses provides sufficient empirical evidence of robustness. This statistical treatment aligns with experimental validation practices commonly adopted in prototype-level biometric system studies.

5.7 Threshold Sensitivity Analysis

Threshold selection plays a critical role in balancing security and usability in biometric authentication systems. To evaluate the robustness of the proposed framework against parameter variation, a sensitivity analysis was conducted on the key decision thresholds used in facial similarity matching and dynamic signature verification.

For facial recognition, cosine similarity thresholds were varied within a practical range to assess their impact on false acceptance and false rejection rates. Similarly, the Dynamic Time Warping (DTW) distance threshold for signature verification was adjusted to evaluate its effect on authentication accuracy. The

Table 4 shows Effect of DTW threshold on signature verification performance.

DTW Threshold	Accuracy (%)	FAR (%)	FRR (%)
35	82.1	1.0	14.5
45 (selected)	87.0	3.2	9.1
55	90.4	6.8	5.2

Table 4: Effect of DTW threshold on signature verification performance.

The analysis reveals that lower DTW thresholds result in stricter acceptance criteria, significantly reducing FAR but increasing FRR due to natural intra-user variability in handwriting. Conversely, higher thresholds improve user convenience but increase vulnerability to forgery attempts. A threshold value of 45 was selected as an optimal compromise, achieving balanced performance with acceptable security and usability trade-offs. This analysis demonstrates that the proposed system maintains stable performance across a reasonable range of threshold values, highlighting its robustness.

5.8 Comparative Evaluation with Existing Systems

There was a comparative evaluation to determine the performance of TriFactor AI and the conventional two-factor and single-modality authentication systems. The parameters taken into account in the comparison were accuracy, FAR, FRR, latency and data privacy. The traditional password-based systems were moderate (85%) but also highly vulnerable to a brute-force and phishing attack. OTP or email verification two-factor authentication enhanced security but added network-dependent and latent (average 6.5 seconds) features. By comparison, TriFactor AI has reached 99.8% composite accuracy with minimal delay, and has full offline capability as well as high resistance against spoofing.

Compared to the recent research findings of Salturk and Kahraman (2024) and Ammour et al. (2023), TriFactor AI had similar or better performance, in particular in latency and liveness accuracy. The adaptive random challenge mechanism and behavioral verification combination offered by the system have a unique benefit compared to models that concentrate on one biometric modality. This comparative study supports the novelty of multi-modal and AI-driven verification in a purely local setting. The Table 5 shows Comparison with conventional authentication systems.

Method	Accuracy	Offline	Liveness	Privacy
Password	Low	Yes	No	Low
OTP-based 2FA	Medium	No	No	Medium
Face-only	High	Yes	Weak	Medium
TriFactor AI	Very High	Yes	Strong	High

Table 5: Comparison with conventional authentication systems.

5.9 Error Analysis and Robustness Discussion

Although the TriFactor AI framework demonstrates high overall accuracy, error analysis provides valuable insight into the sources of false rejections and system robustness. The majority of false rejections were observed in the dynamic signature verification module, primarily due to intra-user variability caused by differences in writing speed, pressure, and user fatigue across sessions. Such variability is inherent to behavioral biometrics and explains the relatively higher FRR of the signature module compared to facial recognition.

Importantly, the tri-factor architecture mitigates the impact of individual module errors through multi-layer authentication. Since facial, behavioral, and knowledge-based factors operate independently, a failure in one layer does not directly compromise overall system security. The probability of simultaneous false

acceptance across all three modules is extremely low, which significantly strengthens resistance to spoofing and impersonation attacks.

From a security perspective, the adaptive liveness detection mechanism effectively eliminates common presentation attacks, including printed images and video replays, while the bcrypt-based secret-code verification ensures irreversible credential protection even in the event of database compromise. From a usability standpoint, the average end-to-end authentication latency remains under three seconds, providing a practical balance between strong security and user convenience.

Overall, the error analysis confirms that the proposed framework achieves robust authentication by compensating for individual biometric limitations through multi-modal fusion, making it well-suited for secure desktop environments where privacy, reliability, and offline operation are critical requirements.

5.10 Correlation Between Multi-Factor Layers

The results of statistical correlation analysis of the three sets of authentication layers indicated that there is a negligible dependency and this proves the orthogonality of features. The coefficient of correlation between the facial DNA, signature DNA and secret-code success rates was found to be less than 0.15, which means that the failure of one layer does not bias the other one. That independence guarantees security integrity of the tri-factor decision logic even in the event that each of the tri-layer decisions gives a false rejection.

Furthermore, multi-layer evaluation confirmed that the probability of simultaneous false acceptance across all three modules is practically negligible. Mathematically, the combined False Acceptance Rate ($FAR_{combined}$) can be expressed as:

$$FAR_{combined} = FAR_1 \times FAR_2 \times FAR_3 \quad (8)$$

Substituting the experimental values $FAR_1=0.018$, $FAR_2=0.032$, and $FAR_3=0$, yields $FAR_{combined} = 0.00057$ or 0.0576% , which demonstrates the robustness of the tri-factor mechanism against spoofing and unauthorized entry.

5.11 Discussion on Security, Usability, and Efficiency

The outcomes show clearly that, TriFactor AI is able to balance between security and usability. It is multi-mode in design to ensure minimal reliance on any one channel of authentication and to limit the effects of spoofing, forgery or information breach. What the adaptive liveness mechanism does is to provide uninterrupted security assurance when verifying a face, and the behavioral dynamics provides human-specific authentication signatures that are hard to copy.

Usability wise, the 3 seconds on average sign-in time offers a smooth user experience, much better than the traditional multi-step authentication system, which involves the use of external tokens or mobile networks. In addition to this, the offline-local-storage model guarantees privacy compliance, especially when data-protection limits are imposed on the environment. The framework is also scalable which can be expanded in future by adding other biometric modules like voice or a keystroke pattern.

5.12 Summary of Findings

The experimental analysis confirms that TriFactor AI offers a very useful authentication model with little trade-offs. By incorporating facial, behavioral, and knowledge-based layers into a single desktop platform, the framework encountered outstanding results in the accuracy, latency, and privacy aspects. Real-time authentication is guaranteed by the combination of adaptive AI algorithms and cryptographic protection with industrial-grade reliability. As the results show, the developed system makes a significant contribution to the development of the sphere of safe desktop authentication as it allows filling the gap between biometric intelligence and convenience.

The experimental findings reveal a clear trend that increasing authentication dimensionality significantly

improves system robustness. While single-factor authentication achieves high accuracy, it exhibits elevated false acceptance rates. Introducing behavioral and knowledge-based factors reduces impersonation probability multiplicatively rather than additively. This trend confirms that security gains from multi-factor fusion outweigh the marginal increase in authentication latency, making the proposed framework both secure and practical.

5.13 Discussion in Relation to Existing Literature

The results obtained in this study are consistent with and extend findings reported in existing biometric authentication literature. Prior studies on facial authentication systems have demonstrated high recognition accuracy using deep metric learning models such as ArcFace; however, they also highlight vulnerability to presentation attacks in the absence of robust liveness detection mechanisms. For example, Khairnar et al. and Solomon and Cios reported that single-modality facial systems, despite achieving high accuracy, remain susceptible to spoofing under real-world conditions. The adaptive challenge-response liveness detection employed in the proposed framework directly addresses this limitation by introducing dynamic user interaction, thereby enhancing resistance to replay and print attacks.

Similarly, existing research on dynamic signature verification emphasizes the effectiveness of temporal alignment techniques such as Dynamic Time Warping, while also acknowledging inherent intra-user variability. Studies by Faundez-Zanuy et al. and Huang et al. reported signature verification accuracies comparable to those observed in this work but noted increased false rejection rates due to behavioral inconsistency. The results of the present study corroborate these observations, as the signature module exhibits higher FRR relative to facial recognition. However, unlike prior single-factor systems, the proposed tri-factor framework compensates for this limitation by integrating independent physiological and knowledge-based authentication layers.

Multimodal biometric systems reported in the literature, such as those by Ammour et al. and Salturk and Kahraman, demonstrate that combining physiological and behavioral traits significantly reduces false acceptance rates. The findings of this study align with these conclusions while extending them to an offline, desktop-based context. The observed exponential reduction in FAR when transitioning from single-factor to tri-factor authentication confirms that security gains achieved through multi-modal fusion outweigh the marginal increase in authentication latency.

From a practical standpoint, the results underscore the importance of privacy-preserving authentication architectures. Unlike cloud-dependent biometric systems discussed in prior studies, the proposed framework performs all processing locally, eliminating risks associated with data transmission and external storage. This design choice has significant implications for deployment in privacy-sensitive environments such as enterprise desktops, financial terminals, and secure personal computing systems.

Critically, while the proposed system demonstrates strong performance, it is not without limitations. The experimental evaluation was conducted on a limited user cohort, which may affect generalizability. Additionally, the behavioral nature of signature verification introduces variability that can impact usability for some users. These limitations highlight opportunities for future enhancements, such as adaptive threshold learning and learned multimodal fusion strategies. Nevertheless, the presented results provide strong evidence that integrating facial, behavioral, and knowledge-based authentication in a unified offline framework offers a robust and practical solution beyond existing single- and dual-factor systems.

6. Conclusion And Future Work

This study presented TriFactor AI, a fully offline, privacy-preserving, multi-modal authentication framework that integrates facial recognition with adaptive liveness detection, dynamic signature verification, and cryptographically secured secret-code authentication for desktop environments. Unlike conventional single- or two-factor systems, the proposed framework combines physiological, behavioral, and knowledge-based authentication factors within a unified local architecture. Comprehensive experimental evaluation demonstrates that the proposed system achieves an overall authentication

accuracy of 99.8%, with a combined False Acceptance Rate (FAR) of 0.0576% and an average end-to-end authentication latency of 2.8 seconds. Ablation analysis confirms that while facial recognition alone provides high baseline accuracy, it exhibits significantly higher FAR, which is reduced by more than 60× when behavioral and knowledge-based factors are incorporated. Threshold sensitivity analysis further reveals that the system maintains stable performance across reasonable parameter variations, indicating robustness against intra-user behavioral variability.

Comparative evaluation with traditional password-based authentication, face-only systems, and dual-factor approaches shows that the proposed tri-factor framework provides superior resistance to spoofing and impersonation attacks without relying on cloud-based computation or external communication channels. These results establish that security gains achieved through multi-modal fusion are multiplicative rather than additive, particularly when independent biometric dimensions are combined in an offline setting. From a research perspective, this work contributes new empirical evidence demonstrating that integrating adaptive liveness-aware facial recognition with temporal behavioral biometrics and cryptographic verification significantly strengthens desktop authentication while preserving user privacy. The findings extend existing biometric literature by validating a practical, low-latency, and fully local tri-factor authentication paradigm suitable for privacy-sensitive applications.

While the current evaluation was conducted on a limited user cohort, the observed trends and quantitative improvements provide a strong foundation for future research. Future work will focus on large-scale validation, adaptive confidence-weighted fusion strategies, and the integration of additional behavioral modalities such as keystroke dynamics or voice biometrics. Extending the framework to mobile and edge-based environments also presents promising directions for secure, device-agnostic authentication.

Competing Interests

The authors declare that they have no financial or non-financial competing interests that could have influenced the research presented in this manuscript.

Conflict of Interest Statement

The authors declare that there is no conflict of interest regarding the research, authorship, or publication of this manuscript.

Data Availability Statement

The biometric datasets generated and analysed during this study are not publicly available because they contain sensitive facial and behavioural biometric information. Anonymised supporting data may be obtained from the corresponding author upon reasonable request, subject to participant privacy, consent, and institutional requirements.

Authors' Contributions

Burgu Shravan Kumar: Conceptualization, methodology, system design, software development, experimentation, data analysis, visualization, and preparation of the original manuscript.

Muntha Raju: Research supervision, methodology validation, technical guidance, and review and editing of the manuscript.

Yerram Sneha: Literature review, data collection, system evaluation, result analysis, and interpretation of findings.

Sirisha Veluri: Technical validation, critical revision of the manuscript, result verification, and final manuscript review.

All authors read and approved the final version of the manuscript and agreed to be accountable for the accuracy and integrity of the work.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

- [1]. Kumar, S., Rani, S., Jain, A., Verma, C., Raboaca, M. S., Illés, Z., and Neagu, B. C. (2022). Face spoofing, age, gender and facial expression recognition using advance neural network architecture-based biometric system. *Sensors*, 22(14), 5160. <https://doi.org/10.3390/s22145160>
- [2]. Mishra, A. R., Kumar, R., Gupta, V., Prabhu, S., Upadhyay, R., Chhipa, P. C., Rakesh, S., Mokayed, H., Das Chakladar, D., De, K., Liwicki, M., Simistira Liwicki, F., and Saini, R. (2024). SignEEG v1.0: Multimodal dataset with electroencephalography and handwritten signature for biometric systems. *Scientific Data*, 11(1), 718. <https://doi.org/10.1038/s41597-024-03546-z>
- [3]. Ammour, N., Bazi, Y., and Alajlan, N. (2023). Multimodal approach for enhancing biometric authentication. *Journal of Imaging*, 9(9), 168. <https://doi.org/10.3390/jimaging9090168>
- [4]. Haider, S. A., Ashraf, S., Larik, R. M., Husain, N., Muqet, H. A., Humayun, U., Yahya, A., Arfeen, Z. A., and Khan, M. F. (2023). An improved multimodal biometric identification system employing score-level fuzzification of finger texture and finger vein biometrics. *Sensors*, 23(24), 9706. <https://doi.org/10.3390/s23249706>
- [5]. Yang, J., Lan, G., Xiao, S., Li, Y., Wen, J., and Zhu, Y. (2022). Enriching facial anti-spoofing datasets via an effective face swapping framework. *Sensors*, 22(13), 4697. <https://doi.org/10.3390/s22134697>
- [6]. Faundez-Zanuy, M., Diaz, M., and Ferrer, M. A. (2024). Online signature recognition: A biologically inspired feature vector splitting approach. *Cognitive Computation*, 16(1), 265–277. <https://doi.org/10.1007/s12559-023-10205-9>
- [7]. Che, Y., Du, L., Tang, G., and Ling, S. (2024). A biometric identification for multi-modal biomedical signals in geriatric care. *Sensors*, 24(20), 6558. <https://doi.org/10.3390/s24206558>
- [8]. Khairnar, S., Gite, S., Kotecha, K., and Thepade, S. D. (2023). Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions. *Big Data and Cognitive Computing*, 7(1), 37. <https://doi.org/10.3390/bdcc7010037>
- [9]. Zhang, S., and Nie, W. (2023). Multi-domain feature alignment for face anti-spoofing. *Sensors*, 23(8), 4077. <https://doi.org/10.3390/s23084077>
- [10]. Solomon, E., and Cios, K. J. (2023). FASS: Face anti-spoofing system using image quality features and deep learning. *Electronics*, 12(10), 2199. <https://doi.org/10.3390/electronics12102199>
- [11]. Xiao, J., Wang, W., Zhang, L., and Liu, H. (2024). A MobileFaceNet-based face anti-spoofing algorithm for low-quality images. *Electronics*, 13(14), 2801. <https://doi.org/10.3390/electronics13142801>
- [12]. Lai, Z., Guo, Y., Hu, Y., Su, W., and Feng, R. (2024). Evaluating and enhancing face anti-spoofing algorithms for light makeup: A general detection approach. *Sensors*, 24(24), 8075. <https://doi.org/10.3390/s24248075>
- [13]. Gong, L. Y., Li, X. J., and Chong, P. H. J. (2024). Facial anti-spoofing using “clue maps”. *Sensors*, 24(23), 7635. <https://doi.org/10.3390/s24237635>
- [14]. Huang, J., Xue, Y., and Liu, L. (2023). Dynamic signature verification technique for the online and offline representation of electronic signatures in biometric systems. *Processes*, 11(1), 190. <https://doi.org/10.3390/pr11010190>
- [15]. Roszczewska, K., and Niewiadomska-Szynkiewicz, E. (2024). Online signature biometrics for mobile devices. *Sensors*, 24(11), 3524. <https://doi.org/10.3390/s24113524>
- [16]. Kothadiya, D., Bhatt, C., Soni, D., Gadhe, K., Patel, S., Bruno, A., and Mazzeo, P. L. (2023). Enhancing fingerprint liveness detection accuracy using deep learning: A comprehensive study and novel approach. *Journal of Imaging*, 9(8), 158. <https://doi.org/10.3390/jimaging9080158>
- [17]. Zhang, K., Huang, S., Liu, E., and Zhao, H. (2023). LFLDNet: Lightweight fingerprint liveness detection based on ResNet and transformer. *Sensors*, 23(15), 6854. <https://doi.org/10.3390/s23156854>
- [18]. Chen, L., Guo, T., Li, L., Jiang, H., Luo, W., and Li, Z. (2023). A finger vein liveness detection system based on multi-scale spatial-temporal map and Light-ViT model. *Sensors*, 23(24), 9637. <https://doi.org/10.3390/s23249637>
- [19]. Li, Y., Sun, W., Li, Z., and Guo, X. (2025). Face anti-spoofing based on adaptive channel enhancement and intra-class constraint. *Journal of Imaging*, 11(4), 116. <https://doi.org/10.3390/jimaging11040116>
- [20]. Xing, H., Tan, S. Y., Qamar, F., and Jiao, Y. (2025). Face anti-spoofing based on deep learning: A comprehensive survey. *Applied Sciences*, 15(12), 6891. <https://doi.org/10.3390/app15126891>
- [21]. Li, Y., Li, Y., and Wang, Z. (2025). FaceCloseup: Enhancing mobile facial authentication with perspective distortion-based liveness detection. *Computers*, 14(7), 254. <https://doi.org/10.3390/computers14070254>
- [22]. Salturk, S., and Kahraman, N. (2024). Deep learning-powered multimodal biometric authentication: Integrating dynamic signatures and facial data for enhanced online security. *Neural Computing and Applications*, 36(19), 11311–11322. <https://doi.org/10.1007/s00521-024-09690-2>
- [23]. Li, C., Li, Z., Sun, J., and Li, R. (2023). Middle-shallow feature aggregation in multimodality for face anti-spoofing. *Scientific Reports*, 13(1), 9870. <https://doi.org/10.1038/s41598-023-36636-w>
- [24]. Zanolensi, L. A., Laroca, R., Lucio, D. R., Santos, L. R., Britto, A. S., and Menotti, D. (2022). A new periocular dataset collected by mobile devices in unconstrained scenarios. *Scientific Reports*, 12(1), 17989. <https://doi.org/10.1038/s41598-022-22811-y>
- [25]. Qi, H., Han, R., Duan, K., Shi, Y., Qi, X., Gao, C., and Ren, L. (2025). A high-performance adaptive fusion network for face anti-spoofing detection. *Scientific Reports*, 15(1), 37607. <https://doi.org/10.1038/s41598-025-21461-0>