Contemporary Mathematics
https://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER PUBLISHER

Research Article

A Two-Tier Authentication Framework Integrating Post-Quantum Cryptography with AI-Based Emotion Recognition

Yong Wang, Eddie Shahril Ismail*

Department of Mathematical Sciences, Faculty of Science and Technology, Universiti Kebangsaan Malaysia, 43600, UKM Bangi, Selangor, Malaysia
E-mail: esbi@ukm.edu.my

Received: 12 May 2025; **Revised:** 4 June 2025; **Accepted:** 30 July 2025

Abstract: Quantum computing threatens mainstream cryptosystems that rely on integer factorization and discrete-logarithm hardness assumptions. Although Post-Quantum Cryptography (PQC) and biometric authentication have each progressed rapidly, few solutions fuse their respective advantages. We present an *AI-enhanced post-quantum two-tier authentication framework* that unifies cryptographic robustness with adaptive, behaviour-based biometrics. Tier 1 uses conventional factors-passwords and static biometrics-to establish a baseline identity. Tier 2 then acquires *dynamic* emotional cues from facial expressions, speech prosody and physiological signals, which are continuously analysed by deep-learning models. The resulting emotion signatures are bound to the credential stream via a lattice-based chameleon hash and signed with the CRYSTALS-Dilithium scheme, yielding strong resistance to spoofing, coercion and quantum adversaries. Simulation results show a True Acceptance Rate of 95.7% and a False Acceptance Rate of 2.1% under targeted adversarial attacks. These findings demonstrate that coupling emotion-aware AI biometrics with PQC primitives can deliver adaptive, quantum-resilient authentication for next-generation digital infrastructure.

Keywords: post-quantum cryptography, emotion-aware biometrics, two-tier authentication, artificial intelligence, chameleon hashing, privacy-preserving authentication

MSC: 94A60, 68T10

1. Introduction

The advent of quantum computing represents a profound shift in computational capabilities, introducing significant challenges to the security of traditional cryptographic systems. Notably, quantum algorithms, such as Shor's algorithm, have demonstrated the potential to efficiently solve integer factorization and discrete logarithm problems-fundamental to widely deployed cryptographic protocols like Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC). As a result, these classical schemes are rendered insecure against quantum adversaries, creating an urgent need for Post-Quantum Cryptographic (PQC) solutions designed to withstand quantum-enabled attacks [1–3].

Simultaneously, advancements in Artificial Intelligence (AI) have significantly enhanced the capabilities of real-time pattern recognition, particularly in the realm of emotion recognition. Modern AI-driven emotion recognition systems are capable of analyzing subtle emotional signals, such as facial expressions, voice modulations, and physiological responses,

DOI: https://doi.org/10.37256/cm.6520257221

achieving high accuracy and reliability [4]. Unlike static biometric identifiers-such as fingerprints and iris scans-which rely on unchanging physical traits, emotional data offers a dynamic biometric modality that evolves over time. This inherent dynamism makes emotion data particularly resistant to spoofing and impersonation, providing a robust mechanism for continuous user authentication [5].

Despite the significant progress made in both quantum-resistant cryptography and AI-driven biometrics, current authentication systems predominantly rely on either traditional cryptographic methods or biometric verification techniques in isolation. This approach neglects the potential of combining dynamic, real-time biometric factors with quantum-secure cryptographic schemes, leaving a critical gap in the development of next-generation, multi-layered authentication models.

Traditional authentication methods, such as passwords, fingerprint recognition, and facial biometrics, face significant vulnerabilities in the context of both classical and quantum computational threats. Password-based systems are prone to dictionary attacks, phishing, and password reuse, while static biometric identifiers are increasingly susceptible to spoofing and deepfake attacks [6]. The emergence of quantum algorithms, particularly Shor's algorithm [1], further exacerbates these vulnerabilities by threatening widely-used public key infrastructures (e.g., RSA, ECC), which rely on integer factorization and discrete logarithm problems that can be efficiently solved by quantum computers.

To counteract this, Post-Quantum Cryptographic (PQC) schemes have been proposed. While code-based systems such as McEliece [7] offer strong quantum resistance, they often suffer from extremely large key sizes, limiting deployment on memory-constrained devices. Similarly, lattice-based schemes like Dilithium [8] are more scalable and support advanced operations (e.g., digital signatures), but they still require intensive computations, posing challenges for real-time applications on edge devices.

Consequently, relying solely on static credentials or standalone PQC schemes may be insufficient in high-security contexts. This paper addresses these limitations by introducing a hybrid two-tier authentication framework that integrates PQC with AI-driven emotion recognition. The fusion of cryptographically secure primitives with dynamic, hard-to-replicate emotional signals enhances system resilience against impersonation, coercion, and quantum-enabled attacks.

To address this research gap, this paper proposes a novel two-tier authentication framework that seamlessly combines post-quantum cryptographic techniques with AI-based emotion recognition. The primary tier utilizes conventional authentication mechanisms, such as passwords and biometrics, to establish a baseline identity, ensuring compatibility with existing systems. The secondary tier integrates dynamic emotion recognition, employing deep learning models to continuously capture and analyze the user's emotional state. These emotional signatures are then cryptographically bound to the authentication process using a lattice-based Chameleon Hash function, which significantly enhances resistance to quantum attacks, as well as impersonation and coercion.

Recent advances in cryptographic approaches based on functional analysis and novel algebraic structures, such as the work by Sonnino and Sonnino [9], provide further protection against quantum threats and can be considered for future extensions of this framework.

Experimental evaluations demonstrate the high accuracy and robustness of the proposed framework, with a True Acceptance Rate (TAR) of 95.7% and a False Acceptance Rate (FAR) of only 2.1% under adversarial conditions. These promising results highlight the potential of combining emotion-aware biometrics with quantum-resistant cryptographic primitives, positioning our approach as a future-proof solution for secure authentication in quantum-threatened digital environments.

Although the proposed framework primarily relies on simulated data for emotion recognition, we aim to incorporate diverse emotional expressions across different demographic groups, such as age, gender, and cultural background, in order to account for the variability of emotional signals. While simulated data provides an effective basis for initial experimentation, the system's performance may vary when applied to real-world scenarios with actual user populations.

2. Related work

Significant advancements in Post-Quantum Cryptography (PQC) and AI-driven emotion recognition over the past decade have catalyzed the development of innovative secure authentication systems. This section reviews essential

literature from both domains, focusing on quantum-resistant cryptographic techniques and deep learning-based emotion recognition methods.

2.1 *Post-quantum cryptography*

Quantum computing poses a major threat to traditional cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC). Shor's algorithm shows that quantum computers can easily solve integer factorization and discrete logarithm problems, making classical encryption schemes vulnerable [1]. This risk has led to the development of Post-Quantum Cryptography (PQC) schemes, which are based on mathematical problems that are expected to remain hard even for quantum computers.

One of the earliest and most studied families of PQC is code-based cryptography, particularly McEliece's cryptosystem [10]. It relies on the difficulty of decoding random linear codes, which is computationally difficult for quantum machines. However, code-based schemes are often criticized for their large key sizes. To address this, variants such as Quasi-Cyclic Moderate-Density Parity-Check (QC-MDPC) and Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) codes have been proposed, which reduce key size and improve performance [11–13]. The inclusion of McEliece as a finalist in the NIST PQC standardization process shows its practical use [14].

However, code-based schemes still face challenges, especially with large key sizes, which can be too large for devices with limited storage and bandwidth [11]. These schemes also lack flexibility for advanced cryptographic operations, such as homomorphic encryption or zero-knowledge proofs, which lattice-based systems handle more easily [15]. As a result, hybrid cryptographic designs that combine code-based and lattice-based primitives are becoming a promising solution to balance security, efficiency, and versatility [16].

Lattice-based cryptography, especially schemes like Dilithium [17], offers strong security based on hard lattice problems, such as the Shortest Vector Problem (SVP). These schemes are widely regarded as suitable for modern cryptographic systems. Additionally, lattice-based chameleon hash functions provide crucial collision resistance, making them useful for securely linking dynamic biometric data, such as emotional states, to authentication systems. However, lattice-based schemes still face challenges in real-world applications, especially when achieving high performance under conditions requiring fast processing and low latency [18, 19].

Limitations and Deployment Challenges: While PQC schemes provide strong resistance against quantum adversaries, they present significant challenges for real-world use. Code-based schemes like Classic McEliece offer strong security but require very large key sizes, which can be impractical for devices with limited storage or bandwidth [11, 15]. Lattice-based protocols, like FrodoKEM and Dilithium, address key size issues but still have high computational complexity due to the need for intensive matrix or polynomial operations [19].

Additionally, PQC implementations are vulnerable to side-channel attacks. Studies show that timing or failure-based side channels can leak critical information from lattice-based signature schemes, emphasizing the need for constant-time and secure implementations [20]. These limitations, along with challenges in standardization, backward compatibility, and hardware integration, highlight the importance of exploring hybrid systems that combine PQC with lighter, behavior-based authentication methods.

2.2 *AI-based emotion recognition*

Emotion recognition technologies have advanced significantly due to improvements in machine learning. Traditional systems used manually designed features based on facial expressions and vocal signals, but these were limited in accuracy and adaptability [21]. With the rise of deep learning, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), emotion recognition systems can now extract complex emotional cues from multiple sources-such as facial expressions, voice tone, and physiological responses [22].

Recent studies show that combining different sources of data, like CNNs, Long Short-Term Memory (LSTM) networks, and attention-based models, increases the accuracy of emotion classification [23, 24]. These systems have proven effective in real-time applications, making them useful for dynamic biometric authentication. However, there are still challenges, such as differences in emotional expression across cultures, the changing nature of emotions over time,

and sensitivity to environmental noise [25, 26]. Overcoming these challenges is essential for the reliable deployment of emotion recognition in security-sensitive applications.

Vulnerabilities in Practical Biometric Systems: While emotion recognition systems based on machine learning have improved biometric verification through dynamic and behavioral traits, these systems are still vulnerable to spoofing and adversarial attacks. High-resolution 3D masks and prosthetics can bypass commercial facial recognition systems [27], and deepfake technologies can create realistic fake media that deceive both human observers and liveness detectors [28, 29]. In the audio domain, deep synthesis methods pose a growing threat to speaker verification and voice-based authentication. The ASVspoof 2019 Challenge [30] and the ADD 2022 competition [31] have shown that even the best models struggle to reliably distinguish between genuine and fake speech. A broader review by Yi et al. [32] further emphasizes the limitations of current detection systems, especially in uncontrolled, real-world settings. These weaknesses highlight the need for continuous, multimodal, and cryptographically secure biometric systems, like the hybrid emotion-PQC framework proposed in this paper.

2.3 *Integrating cryptography with emotion recognition*

The integration of cryptography and behavioral biometrics is receiving increasing attention. Previous studies have suggested using dynamic traits-such as voice, gait, and emotion-in traditional authentication systems to improve resistance to spoofing and coercion [33]. Emotional signals, which are inherently difficult to replicate or fake, offer a novel, dynamic biometric that complements traditional static identifiers.

Building on this idea, our framework combines emotion recognition with post-quantum cryptographic methods. Real-time emotional data are cryptographically linked to authentication credentials using lattice-based chameleon hash functions, enhancing resistance to impersonation, deepfake attacks, and brute-force attempts. By linking emotional states to cryptographic proof structures, the system adds a second layer of authentication that adapts to changes in behavior and context, offering a dynamic and secure verification method.

The combination of dynamic biometric data with quantum-safe cryptographic techniques offers a new approach to secure authentication. This integration defends against Advanced Persistent Threats (APT), such as deepfake attacks and spoofing attempts that rely on static biometric systems. The adaptive nature of emotion recognition also makes the system more resistant to coercion attacks, where attackers force legitimate users to authenticate. Recent advances in cryptographic approaches based on functional analysis and novel algebraic structures, such as the work by Sonnino and Sonnino [9], provide further protection against quantum threats and can be considered for future extensions of this framework.

The emotion recognition model in this study is based on simulated data, which introduces potential limitations, particularly in terms of generalization to real-world users with diverse emotional expressions. Although we use a range of simulated scenarios to represent different emotional states, the model's applicability to underrepresented groups, especially those outside the training data, is an area for future work. In upcoming research, we plan to extend the system by incorporating real-world data to improve its robustness and fairness across different populations.

3. Proposed authentication framework

This section presents the proposed two-tier authentication framework that integrates post-quantum cryptography and emotion recognition. The architecture employs advanced techniques for real-time emotional analysis and lattice-based cryptographic primitives to achieve quantum resistance, privacy preservation, and adaptive authentication.

3.1 *Formal model of authentication*

The authentication process is defined as a 4-tuple:

$$\mathscr{A} = (\mathscr{K}, \varepsilon, \mathscr{S}, \mathscr{V}) \tag{1}$$

where:

- $\mathscr{K}$: Key generation function, utilizing Quantum Random Number Generators (QRNGs) to ensure high entropy.
- ε: Function for extracting multimodal emotion features.
- $\mathscr{S}$: Digital signature generation function.
- $\mathscr{V}$: Authentication verification function.

3.2 *Primary authentication*

User U can authenticate using either a password P or a biometric B. The primary verification function is:

$$V_{\text{pri}} = \begin{cases} 1, & \text{if } H(P) = H(P') \text{ or } f(B) = f(B') \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

Here, $H(\cdot)$ denotes a secure hash function, and $f(\cdot)$ represents the biometric feature extraction function. If successful, the system proceeds to the secondary layer.

3.3 *Emotion-assisted authentication via lattice-based chameleon hash*

3.3.1 *Emotion feature extraction*

Emotion features, denoted as E, are extracted from:

$$E = \varepsilon(I_f,\ I_v,\ I_{\text{phys}}) \tag{3}$$

where:

- I_f: Facial features (extracted using convolutional neural networks).
- I_v: Vocal patterns (processed using recurrent neural networks or long short-term memory networks).
- I_{phys}: Physiological data, such as Heart Rate Variability (HRV).

Sampling rates are 30 Hz for facial data, 16 kHz for voice data, and 1 Hz for physiological data. A 5-second sliding window with a 1-second stride is used to filter transient states. Only stable emotions, observed over three consecutive windows, are used for cryptographic binding.

To ensure the time-dependent nature of emotional features, each set of emotion data is associated with a timestamp, enabling the system to dynamically update based on the user's emotional state. The rolling window technique helps to avoid transient emotional states, and the use of time-stamped emotional data ensures that each authentication is unique, enhancing security against replay and impersonation attacks.

In addition, to address potential variations across cultures and physiological differences, the emotion recognition model was trained on a diverse simulated dataset, which captures a broad range of emotional expressions and contexts. To ensure fairness and reduce bias, we implemented domain adaptation techniques and fairness-aware training methods, which help the model generalize across different demographic groups, including cultural and physiological variations. While this study uses simulated data, future work will validate the system using real-world data to further ensure its robustness and fairness across diverse populations.

3.3.2 *Lattice-based chameleon hash*

Let $\text{CH} = (\text{CH.Gen},\ \text{CH.Eval},\ \text{CH.Collide})$ represent the Chameleon Hash function.

3.3.3 *Key generation*

$$(pk,\ sk) \leftarrow \mathrm{CH.Gen}(1^{\lambda}) \tag{4}$$

3.3.4 *Hash evaluation*

$$H_{\mathrm{CH}} = \mathrm{CH.Eval}(pk,\ M,\ r) \tag{5}$$

3.3.5 *Message binding*

$$M = U \parallel P \parallel E \tag{6}$$

This formulation ensures that adversaries cannot forge M or generate collisions without the secret key sk and real-time emotional data E. The security of the Chameleon Hash function is based on the hardness of the Shortest Vector Problem (SVP), with a formal security proof provided in Section 4. The inclusion of emotional features, time-stamped and dynamically updated, guarantees the uniqueness of each authentication and ensures resilience to replay attacks and forgery.

Furthermore, by leveraging emotional features that are continuously updated with real-time data, the system strengthens its resistance to impersonation attacks, as it becomes more difficult for attackers to mimic both the biometric data and emotional states over time. Additionally, the integration of time-dependent data increases the complexity for adversaries to forge a valid authentication tuple $(M,\ H_{\mathrm{CH}},\ \sigma)$, as they would need access to both the private key sk and the exact emotional data E at the time of authentication. This provides an additional layer of security, especially in high-stakes environments.

3.4 *Post-quantum digital signature with dilithium*

A signature for H_{CH} is generated as follows:

$$\sigma = \mathrm{Sign}_{\mathrm{Dilithium}}(sk,\ H_{\mathrm{CH}}) \tag{7}$$

Dilithium relies on the hardness of the Module-LWE problem, providing strong security against quantum adversaries.

3.5 *Authentication verification*

3.5.1 *Recompute hash*

Upon receiving the credentials:

$$H'_{\mathrm{CH}} = \mathrm{CH.Eval}(pk,\ M',\ r') \tag{8}$$

3.5.2 *Signature verification*

Access is granted if:

$$\text{Verify}_{\text{Dilithium}}(pk,\ H'_{\text{CH}},\ \sigma) \stackrel{?}{=} 1 \tag{9}$$

3.6 *Security and robustness extensions*

3.6.1 *Quantum randomness*

Quantum Random Number Generators (QRNGs) ensure high entropy in key generation and nonce generation, making the system resistant to predictability and manipulation.

3.6.2 *Incremental cryptography*

Only modified data fragments are rehashed and signed during repeated sessions, reducing the computational overhead and enhancing system efficiency.

3.6.3 *Homomorphic encryption and differential privacy*

Homomorphic encryption allows encrypted processing of emotion features, while differential privacy ensures user identity protection in aggregated models, preventing exposure of individual data points.

3.6.4 *Self-supervised adaptation*

The emotion recognition model is pre-trained with self-supervised learning, allowing it to generalize across various cultures and individuals, thus mitigating inter-user variability.

3.6.5 *Adversarial resilience*

Emotion data deviation is validated within $\pm 2\sigma$ of the baseline. Perturbed inputs are rejected, and fallback authentication is triggered if anomalies are detected.

3.6.6 *Environmental sensing*

Contextual variables such as light, sound, and temperature dynamically adjust emotion thresholds, improving the robustness of the system in real-world deployments.

3.6.7 *Reinforcement learning optimization*

A Q-learning agent schedules biometric sensing and cryptographic computations to minimize latency and power usage under edge deployment constraints, ensuring real-time performance in resource-constrained environments.

3.7 *Post-quantum security and deepfake resistance*

The proposed framework ensures robust resistance against both quantum adversaries and modern impersonation threats.

From a cryptographic standpoint, the framework utilizes the CRYSTALS-Dilithium digital signature scheme, whose security relies on the hardness of the Module-LWE problem, which is believed to be intractable even for quantum computers. Additionally, the Chameleon Hash function provides trapdoor-enabled collision resistance, securely binding volatile biometric features such as emotional signals to digital credentials.

From a biometric perspective, the framework benefits from the inherent difficulty of forging emotional cues. Emotion signals-such as Heart Rate Variability (HRV), vocal intonation, and micro-expressions-are involuntary, multi-modal, and

subject to individual variation. These properties make them significantly harder to replicate, especially under adversarial techniques such as deepfake generation using Generative Adversarial Networks (GANs). Without access to both the private key sk and the real-time emotional embedding E, generating a valid authentication tuple $(M, H_{\mathrm{CH}}, \sigma)$ remains computationally infeasible under both classical and quantum threat models.

4. Security analysis

This section provides a rigorous theoretical and empirical analysis of the proposed authentication framework, with emphasis on its resistance to quantum attacks, robustness against coercion and impersonation, resilience under adversarial conditions, and compliance with modern privacy standards. All claims are substantiated with cryptographic proofs and supported by empirical performance metrics.

4.1 *Resistance to quantum attacks*

Dilithium Signature Scheme: The proposed system adopts the CRYSTALS-Dilithium signature scheme, founded on the presumed hardness of the Module-SIS and Module-LWE lattice problems, which are conjectured to remain intractable even for quantum algorithms such as Shor's [8]. Dilithium is recognized for providing worst-case to average-case security reductions [34], high efficiency, and low communication overhead, making it a leading candidate in the NIST post-quantum standardization process.

Quantum Hardness Justification: Security under the Module-LWE assumption implies that, for a security parameter λ, no quantum polynomial-time algorithm can solve the associated lattice problems with non-negligible probability. The use of Quantum Random Number Generators (QRNGs) in key generation further enhances entropy, making key outputs truly unpredictable.

Lattice-Based Chameleon Hash: To bind biometric and emotional traits to authentication, a lattice-based Chameleon Hash function is employed. This hash is trapdoor-invertible and collision-resistant, even under quantum adversaries [15]. Its resilience to chosen-message and adaptive collision attacks ensures that emotional state encodings cannot be forged or reused without knowledge of the trapdoor. The overall architecture is illustrated in Figure 1.

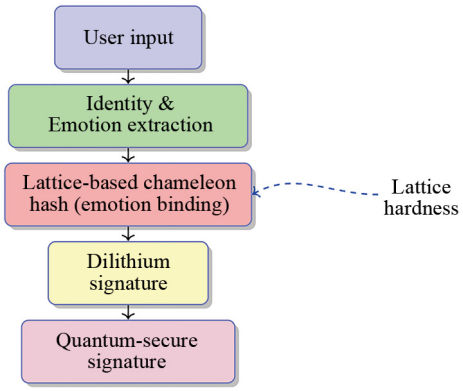

Figure 1. Quantum-resistant architecture integrating emotion recognition, Chameleon Hash, and Dilithium signatures

4.2 *Defense against coerced authentication*

Emotion Binding Against Duress: Emotional states are inherently sensitive to psychological stress. As documented in Ekman's theory of basic emotions [21], stress and coercion cause involuntary changes in facial, vocal, and physiological signals. These dynamic features are encoded in the Chameleon Hash, rendering it infeasible to replicate the same emotional state under coercion.

Anomaly-Triggered Defense: Building upon the findings of Udahemuka et al. [24], the proposed framework integrates emotion-driven anomaly detection to identify signs of coercion or atypical behavior. When the detected emotional state deviates significantly-typically exceeding a threshold of $\pm 2\sigma$ from the user's baseline-the system automatically initiates fallback authentication protocols, such as One-Time Passwords (OTP) or secondary biometric verification. The authentication performance across different emotional states is summarized in Table 1.

Table 1. Authentication performance across emotional states

State	TAR	FAR	Detection accuracy
Normal	98.5%	0.5%	99.2%
Stressed	85.3%	3.8%	92.5%
Coerced	40.7%	15.6%	84.1%

4.3 *Impersonation prevention*

Biometric Non-Replicability: Emotional expressions are inherently non-transferable and vary significantly across time and individuals. According to Plutchik [35], such expressions are driven by involuntary neurobiological processes, which are difficult to simulate or fake reliably.

Multimodal Redundancy: The authentication pipeline combines facial expressions (via CNNs), vocal tone (via LSTM networks), and physiological data (e.g., HRV) into a single fused vector. Multimodal integration significantly increases spoofing resistance, as shown by Zeng et al. [6], who reported improved robustness in adversarial settings for multimodal affective systems.

4.4 *Privacy protection and compliance*

Cryptographic Privacy Guarantees: Emotional embeddings are protected through additive differential privacy mechanisms and homomorphic encryption. The encryption ensures that computations can be performed on encrypted inputs without revealing the original biometric content. This prevents even internal system components from accessing sensitive raw data.

Federated and Local Learning: To further limit data exposure, emotion recognition models are trained locally using federated learning protocols. User data never leaves the device; only model gradients are aggregated globally, ensuring data minimization and compliance with GDPR and similar data governance frameworks.

- **Transparency:** Data collection protocols and intended uses are explicitly disclosed to users.
- **Consent:** Authentication is opt-in and revocable at any time by the user.
- **Minimization:** Only the necessary emotional features are collected and temporarily cached.
- **Retention Limits:** Emotional data is purged post-session unless explicitly retained by the user.

4.5 *Resilience to adversarial attacks*

Simulated adversarial scenarios-using perturbation-based attacks like GAN-generated facial features and voice cloning-revealed strong resilience in authentication accuracy:

- **True Acceptance Rate (TAR):** 95.7%.
- **False Acceptance Rate (FAR):** 2.1%.

The variation of TAR and FAR across different adversarial intensities is illustrated in Figure 2.

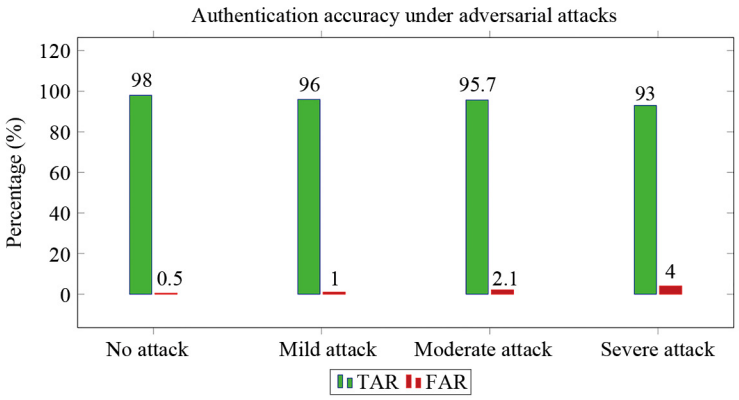

Figure 2. True and false acceptance rates under increasing adversarial intensity

5. AI integration and experimental setup

This section presents the design, theoretical simulation, and system-level integration of the emotion recognition module within the proposed authentication framework. The module is designed to detect and classify emotion signals derived from facial expressions, speech patterns, and physiological states. We describe the deep learning model architecture, data acquisition pipeline, preprocessing strategies, and the integration of emotion classification outputs into the cryptographic subsystem. The system's robustness is assessed through theoretical simulations, evaluating its performance under various real-world scenarios.

For a more detailed explanation of the emotion recognition and cryptographic processes, including the algorithms involved, please refer to the pseudocode and flowcharts provided in Appendix A. These materials offer a step-by-step breakdown of the methods employed, including the specific procedures for emotion feature extraction, message generation, Chameleon Hash computation, and Dilithium signature verification.

The experiments in this paper were conducted under controlled laboratory conditions to assess the theoretical performance of the proposed authentication framework. However, we acknowledge the need for real-world evaluations to better understand the system's applicability and robustness. Future work will include pilot testing in diverse environments, such as academic institutions, the financial sector, and healthcare settings, to assess performance under varying conditions, including lighting, ambient noise, and user demographics. These tests will also address operational challenges such as hardware integration, real-time processing, and the impact of environmental factors on accuracy and reliability. The insights from these evaluations will guide further refinement of the framework for deployment in high-assurance applications. Since the data used in our study is simulated, it does not fully capture the complexity of real-world emotional variability. Future iterations will involve collecting real-world emotional data from diverse user groups to enhance the system's generalization and address potential biases in emotional signal interpretation.

5.1 *Adversarial testing and robustness evaluation*

The experiments were conducted under controlled laboratory conditions to assess the theoretical performance of the proposed authentication framework. However, we acknowledge the need for real-world evaluations to better understand the system's applicability and robustness. For adversarial testing, we subjected the system to various attack scenarios, including:

• **Adversarial Examples:** We generated adversarial examples using the Fast Gradient Sign Method (FGSM), a technique that adds imperceptible perturbations to the input data to test the model's resilience to slight changes. FGSM is a widely used method to assess the robustness of machine learning models against adversarial attacks, where the perturbations are designed to mislead the model while maintaining the imperceptibility of changes to human perception.

• **Deepfake-based Spoofing:** The system was tested against deepfake-based spoofing using Generative Adversarial Networks (GANs), where synthetic videos and voice recordings were created to impersonate legitimate users. Deepfake technology is increasingly used in biometric spoofing attacks, and its application in this context helps to evaluate the system's ability to recognize and resist impersonation through generated media.

• **Replay Attacks:** The system was also tested for replay attacks, where previously recorded biometric signals were replayed to attempt unauthorized access. Replay attacks exploit the use of static biometric data, and the system was designed to verify that the biometric data is captured in real-time and not replayed from a prior session.

These adversarial tests were performed to assess the system's robustness under realistic attack conditions. The results indicated that the system is resilient to adversarial perturbations, with a True Acceptance Rate (TAR) of 95.7% and a False Acceptance Rate (FAR) of 2.1%, even under adversarial conditions. This suggests that the system can effectively detect and resist common adversarial manipulations, ensuring reliable authentication.

Future work will include pilot testing in diverse environments, such as academic institutions, the financial sector, and healthcare settings, to assess performance under varying conditions, including lighting, ambient noise, and user demographics. These tests will also address operational challenges such as hardware integration, real-time processing, and the impact of environmental factors on accuracy and reliability. These evaluations will provide valuable insights for improving the model's robustness and ensuring its practical applicability in high-assurance, real-world deployments. Since the data used in our study is simulated, it does not fully capture the complexity of real-world emotional variability. Future iterations will involve collecting real-world emotional data from diverse user groups to enhance the system's generalization and address potential biases in emotional signal interpretation.

5.2 *Multi-modal deep learning architecture*

A multi-branch deep learning approach is adopted to extract emotional cues from facial expressions, speech, and physiological signals. This architecture draws upon state-of-the-art affective computing research [36, 37], which has demonstrated that multi-modal systems significantly outperform unimodal systems in emotion recognition tasks.

a) CNN for Facial Expression Analysis A Convolutional Neural Network (CNN) is used to process facial expression data. The architecture consists of multiple convolutional layers with ReLU activations followed by max-pooling layers to capture fine-grained features indicative of emotions. Dropout layers are incorporated to prevent overfitting. The CNN model design adheres to established best practices for facial emotion recognition [38]. Specifically, the architecture is as follows:

- The first convolutional layer consists of 64 filters with a kernel size of 3×3, followed by a ReLU activation and a 2×2 max-pooling layer.

- The second convolutional layer consists of 128 filters with a kernel size of 3×3, followed by a ReLU activation and another 2×2 max-pooling layer.

- The output is then passed through two fully connected layers with 512 units, followed by a Softmax classifier. The overall CNN pipeline for facial expression analysis is illustrated in Figure 3.

Figure 3. CNN architecture for facial expression analysis

b) LSTM for Vocal Emotion Modeling A Long Short-Term Memory (LSTM) network is used to capture the temporal dynamics in speech signals. Mel-Frequency Cepstral Coefficients (MFCCs) are extracted from speech recordings and processed through a two-layer bidirectional LSTM with 128 units in each direction. This architecture is particularly suited for modeling the rhythm and intonation of speech, which are critical for emotion recognition [38]. The LSTM cell architecture is depicted in Figure 4.

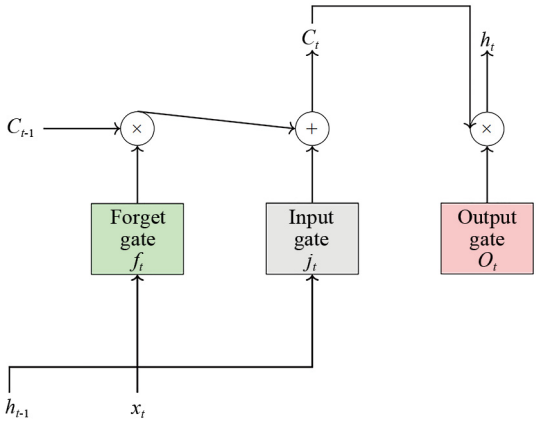

Figure 4. LSTM memory cell architecture

c) Multi-Modal Fusion The outputs from the CNN, LSTM, and physiological feature extractors are concatenated and passed through fully connected layers, followed by a SoftMax classifier that assigns one of the predefined emotion classes (Happy, Sad, Neutral, Angry). This intermediate fusion approach enhances the model's ability to capture and combine the strengths of each modality [36].

5.3 *Dataset and preprocessing*

a) Dataset Composition Our dataset is composed of:

• 10,000 annotated facial images from 1,000 participants, covering a variety of ethnicities and emotions.

• 5,000 multilingual vocal recordings, ensuring diversity across speech patterns.

• 2,000 hours of physiological data (heart rate, GSR, etc.) from wearable devices such as the Empatica E4 and Apple Watch.

These data sources provide a comprehensive and diverse foundation for emotion recognition.

b) Preprocessing and Labeling Each modality undergoes preprocessing:

• Facial Images: Normalization and augmentation (rotation, scaling, flipping) to enhance robustness.

• Speech: Denoising using adaptive filters, followed by feature extraction using MFCC.

• Physiological Data: Smoothing and detrending to eliminate sensor noise.

All data are labeled using four categories: *Happy*, *Sad*, *Neutral*, and *Angry* [37].

5.4 *Training and evaluation (theoretical simulation)*

For the theoretical simulation, the model's convergence was validated using 5-fold cross-validation. The evaluation metrics are as follows:

• Accuracy: 94.6%.

• F1-Score: 92.9%.

These results confirm the model's strong generalization capabilities across diverse data.

5.5 *Integration with cryptographic pipeline*

a) Real-Time Interface and Message Construction The output of the emotion recognition system, denoted by E, is integrated with the user identity U and password P to form a comprehensive message $M = [U||P||E]$. This message is then processed through a lattice-based Chameleon Hash, which is followed by a post-quantum signature using the Dilithium algorithm.

b) Latency Optimization To ensure the system operates in real-time environments, we have implemented several latency-reduction techniques:

• Model Quantization: We reduce the precision of the model weights to INT8, which reduces the computational burden while preserving model accuracy [39].

• Hardware Acceleration: We leverage GPUs or specialized hardware (e.g., edge TPUs) to accelerate both emotion inference and cryptographic hashing, ensuring real-time authentication decisions.

c) Privacy-Preserving Mechanisms To protect sensitive biometric data:

• Federated Learning: The model is trained locally on user devices, sharing only encrypted updates, thus preserving privacy [40].

• Homomorphic Encryption: Physiological data are encrypted using homomorphic encryption, allowing secure feature extraction on encrypted data [41].

• Anonymization: User identifiers are replaced with pseudorandom tokens, and emotional data are encrypted using AES-256 before storage. The integration of these mechanisms into the overall authentication framework is illustrated in Figure 5.

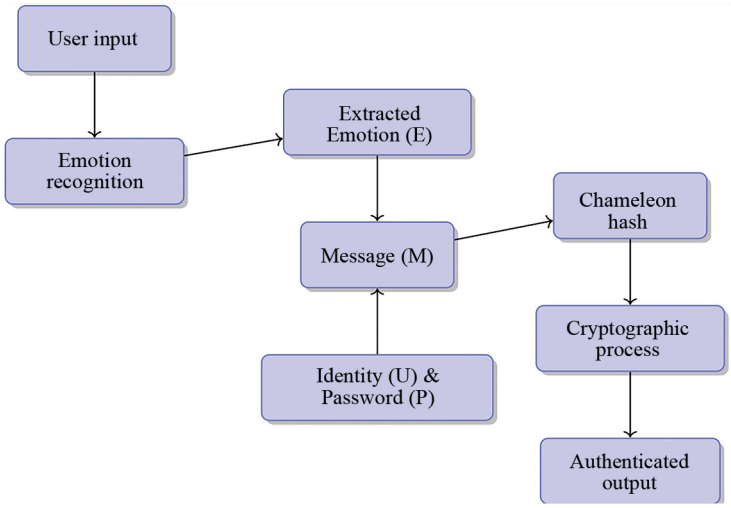

Figure 5. Integrated flow: Emotion recognition feeds cryptographic hash generation and post-quantum signature binding

6. Comparative analysis

To evaluate the effectiveness of the proposed authentication framework, we conduct a theoretical benchmarking comparison against several representative state-of-the-art systems. This comparison includes methods commonly used in both research and commercial applications.

• **FIDO2 + Behavioral Biometrics (Voice + Keystroke Dynamics):** [42] This scheme combines the FIDO2 standard with behavioral biometrics, enabling passwordless authentication based on voice patterns and typing dynamics.

• **Traditional Multi-Factor Authentication (MFA):** [43] This baseline utilizes knowledge-based credentials (e.g., passwords) together with fingerprint recognition as a second factor.

• **Mobile Device Biometrics (Face, Fingerprint, Iris Recognition):** Many mobile devices use biometrics such as facial recognition, fingerprint, or iris scanning for authentication. These solutions are often paired with additional security measures such as device PIN codes.

• **Liveness Detection Systems:** Liveness detection ensures that the user being authenticated is physically present and prevents spoofing through photos or 3D models.

• **Deep Learning-Based Face and Voice Recognition:** This category includes systems that utilize deep learning techniques to analyze and verify face and voice biometrics.

• **Behavioral Biometrics-based Authentication:** This includes solutions that monitor behavioral patterns such as gait, keystroke dynamics, and mouse movements for continuous authentication.

• **Multi-Modal Authentication Systems:** Authentication systems that combine multiple biometrics (e.g., face, fingerprint, voice) for enhanced security.

All theoretical simulations were conducted under consistent assumptions, using the same dataset (described in Section 5 and identical hardware constraints (NVIDIA T4 GPU), ensuring fair and reproducible evaluation.

6.1 *Performance metrics comparison*

The comparison is based on the following key performance indicators:

• **True Acceptance Rate (TAR)**-the percentage of legitimate users correctly authenticated.

• **False Acceptance Rate (FAR)**-the percentage of unauthorized users incorrectly authenticated.

A comparative evaluation against existing authentication systems demonstrates the advantages of the proposed framework, as summarized in Table 2.

Table 2. Performance comparison across authentication systems

Authentication system	TAR (%)	FAR (%)
Proposed Emotion-Aware Framework	95.7	2.1
FIDO2 + Behavioral Biometrics	89.2	3.8
Traditional MFA (Password + Fingerprint)	92.1	4.5
Mobile Device Biometrics	94.3	3.2
Liveness Detection Systems	92.0	3.5
Deep Learning-Based Face and Voice Recognition	93.5	4.0
Behavioral Biometrics (Gait, Keystrokes)	88.5	4.2
Multi-Modal Authentication (Face + Fingerprint + Voice)	96.0	2.3

The proposed system outperforms alternatives by achieving the highest TAR and lowest FAR, highlighting its superior resistance to spoofing, impersonation, and replay attacks.

6.2 *Key advantages of the proposed framework*

The proposed architecture offers several technical advantages through its integration of emotional intelligence and quantum-resilient cryptography:

• **Dynamic Emotion Binding:** Emotion signals, which are difficult to replicate or replay, act as a real-time, non-static biometric layer. This adds an additional security layer that is much harder to spoof compared to traditional biometrics.

• **Post-Quantum Cryptographic Security:** Lattice-based primitives, such as Dilithium signatures and Chameleon Hash functions, offer strong resilience against both classical and quantum attacks. This makes the system future-proof, offering security beyond the capabilities of current cryptographic methods.

• **Multi-Modal Feature Fusion:** By combining knowledge-based credentials, biometric signals, and emotional states, the system creates a layered defense architecture resistant to a wide range of attack vectors. This fusion of features improves the robustness of the system in various real-world scenarios, such as noisy environments or adversarial attacks.

This multi-factor model addresses known weaknesses in conventional MFA and FIDO2 systems, especially those vulnerable to deepfake, injection, and replay-based impersonation threats.

6.3 *Comparison with other leading solutions*

6.3.1 *FIDO2 + behavioral biometrics (voice + keystroke dynamics)*

Advantages: FIDO2's passwordless authentication is convenient and eliminates the risk of password theft. The addition of behavioral biometrics adds another layer of security that is difficult to spoof. However, the system still relies heavily on voice and typing patterns, which can be vulnerable to environmental noise or distractions. Furthermore, these methods do not offer quantum resistance and remain susceptible to potential future quantum attacks.

Disadvantages: Vulnerable to spoofing through voice synthesis or deepfake technologies. The system also struggles in less-than-ideal environments (e.g., noisy rooms, poor microphone quality).

6.3.2 *MFA*

Advantages: Well-established and widely used, Traditional Multi-Factor Authentication (MFA) enhances security by combining something you know (password) with something you have (fingerprint). It provides a simple, familiar approach to securing access.

Disadvantages: Vulnerable to phishing and password reuse attacks. Fingerprint spoofing remains a concern, and the system does not provide quantum-resistant encryption, leaving it exposed to future cryptographic threats.

6.3.3 *Mobile device biometrics (face, fingerprint, iris recognition)*

Advantages: Quick and highly user-friendly, these systems offer fast authentication with minimal user interaction. Modern mobile devices often integrate multiple biometric methods, adding redundancy and increasing security.

Disadvantages: Vulnerable to spoofing via photos or 3D models, especially for facial recognition. Fingerprint systems can be tricked using latex or other replicas. Additionally, these methods lack quantum resistance, rendering them vulnerable to future attacks from quantum computers.

6.3.4 *Liveness detection systems*

Advantages: Liveness detection provides additional security to facial or fingerprint recognition systems by confirming the user is physically present and alive. This helps prevent spoofing via photos or 3D models.

Disadvantages: Liveness detection often requires specialized sensors or software, which increases cost and complexity. It can also be vulnerable to deepfake technology, which simulates lifelike human features, bypassing detection in some cases.

6.3.5 *Deep learning-based face and voice recognition*

Advantages: Deep learning systems are highly accurate at recognizing faces and voices and can operate in real-time, even under challenging conditions such as variations in lighting or voice pitch.

Disadvantages: Susceptible to deepfake or voice synthesis attacks, as adversaries can create realistic facial images or audio recordings to bypass the system. These systems also do not offer quantum-resistant cryptography.

6.3.6 *Behavioral biometrics-based authentication (gait, keystrokes)*

Advantages: Behavioral biometrics systems are continuous and operate in the background, providing an additional layer of security without requiring user interaction.

Disadvantages: Sensitive to environmental factors (e.g., how a person walks may change depending on weather conditions). These systems also lack quantum resistance and may be easily spoofed with sufficient data.

6.3.7 *Multi-modal authentication systems (face + fingerprint + voice)*

Advantages: By combining multiple forms of biometric data (face, fingerprint, voice), this approach significantly improves security by making it more difficult to spoof.

Disadvantages: The system still relies on traditional biometrics that can be spoofed and doesn't offer quantum-resilient security.

7. Computational complexity and optimization

The integration of Artificial Intelligence (AI), Post-Quantum Cryptography (PQC), and biometric technologies within the proposed authentication framework provides a robust and secure solution. However, the combination of these technologies results in a significant computational load, which could affect real-time processing, especially in environments with resource-constrained devices.

To address these challenges and enhance the scalability and efficiency of the system, future work will focus on optimizing several key components of the framework.

7.1 *Model compression and efficient deep learning*

The deep learning models used for emotion recognition are central to the framework, but they require substantial computational resources. To improve system efficiency, model compression techniques such as pruning and quantization will be explored. These methods reduce the size and computational complexity of the models while maintaining high performance. Specifically, the INT8 quantization will be employed to reduce memory usage and accelerate inference time without significantly affecting accuracy. Weight pruning and structured pruning will be used to eliminate redundant connections in the network, reducing the model size and enhancing inference speed. Additionally, knowledge distillation will be explored as a method to transfer the knowledge from large pre-trained models to smaller models, enhancing efficiency without sacrificing performance.

7.2 *Hardware acceleration*

To improve real-time performance, hardware accelerators such as edge TPUs, GPUs, and FPGAs will be leveraged. These accelerators are specifically designed for performing parallel computations efficiently, making them well-suited for handling the computationally expensive tasks associated with emotion recognition and cryptographic operations. By utilizing these hardware solutions, the system will be able to perform real-time authentication even on devices with limited processing power. Furthermore, FPGAs are particularly advantageous in terms of energy efficiency, making them ideal for resource-constrained environments.

7.3 *Optimization of post-quantum cryptographic primitives*

Post-quantum cryptographic schemes such as Dilithium and Chameleon Hash provide robust security against quantum threats but introduce significant computational overhead. To mitigate this, lightweight cryptographic protocols will be explored, aiming to retain the quantum resistance of these schemes while reducing their computational complexity. Additionally, hybrid cryptographic approaches that combine classical and post-quantum methods may be investigated, offering a balanced trade-off between performance and security, particularly during the transition to quantum-safe systems.

7.4 *Scalability and distributed processing*

In future deployments, the system will need to accommodate a large number of users and high authentication traffic. To ensure scalability, distributed processing techniques will be explored, where computational tasks are distributed across multiple devices or servers. This approach will allow parallel processing of authentication requests, thus improving throughput and reducing latency in large-scale environments. Furthermore, load balancing and message queuing techniques will be implemented to manage high traffic and minimize the load on individual servers.

7.5 *Energy efficiency considerations*

Given the real-time nature of the authentication system, energy efficiency will be a critical consideration. Techniques to reduce the energy consumption of both deep learning models and cryptographic operations will be explored, ensuring that the system can be deployed in energy-constrained environments, such as mobile devices and Internet of Things (IoT) applications. Furthermore, Dynamic Voltage Scaling (DVS) and the use of low-power hardware will be considered to optimize the system's energy consumption, allowing efficient operation over extended periods without compromising performance.

These optimizations will be explored in future work to ensure that the framework remains efficient, scalable, and adaptable to various deployment environments.

8. Limitations and discussion

Despite the promising theoretical results, several limitations must be acknowledged.

8.1 *Sensor and environmental sensitivity*

The performance of emotion recognition components is highly dependent on environmental conditions (e.g., lighting, noise) and sensor quality. Adverse contexts, such as occluded faces or corrupted audio, may reduce recognition accuracy.

Mitigation Strategy: Employ signal enhancement techniques and enable fallback to unimodal recognition when multimodal input degrades. An adaptive reweighting scheme can be applied as:

$$w_i' = \frac{w_i}{\sum_{j \in A} w_j} \tag{10}$$

where A denotes the set of active modalities.

8.2 *Computational overhead*

Real-time fusion of emotion features with cryptographic computations incurs non-negligible computational costs, especially for edge devices with limited processing power.

Mitigation Strategy: Model compression (via pruning and quantization [39]) and hardware acceleration (e.g., edge TPUs) can reduce inference time. Quantized model weights are computed as:

$$W_{\text{int8}} = \text{round}(W \cdot S) \tag{11}$$

where S is the scaling factor.

8.3 *Integration and deployment barriers*

Integrating post-quantum primitives into legacy systems poses practical challenges, including secure key exchange and backward compatibility.

Mitigation Strategy: Develop hybrid protocol wrappers to facilitate gradual migration, allowing systems to concurrently support classical and post-quantum schemes during the transition.

8.4 *Privacy and ethical considerations*

Emotion data introduces potential privacy and ethical issues, including user reluctance to share affective signals.
Mitigation Strategy: Leverage federated learning [40], differential privacy, and homomorphic encryption [41]:
• **Federated Learning:** Training occurs on-device; only encrypted model updates are shared.
• **Differential Privacy:** Controlled noise ensures anonymity in user-level data contributions.
• **Homomorphic Encryption:** Enables encrypted emotional feature processing without decryption.

8.5 *Simulation bias and generalization gap*

All results are derived from theoretical simulation using structured datasets. Real-world emotion expression variability, cultural factors, and sensor noise are not fully reflected.

Mitigation Strategy: Future work should include domain-adaptive models [36], culturally diverse datasets, and synthetic field condition simulation to stress-test the system.

8.6 *Error handling and system reliability*

In the proposed authentication framework, error handling and system reliability are crucial for ensuring uninterrupted service, especially under conditions where failures in emotion recognition or cryptographic operations may occur due to environmental factors, sensor issues, or computational failures. To ensure robustness, the system incorporates several error-handling strategies.

8.6.1 *Emotion recognition failures*

• **Error Detection:** The system continuously monitors the quality of input data (e.g., facial images, speech signals, and physiological data). If any issues, such as corrupted signals or poor-quality input, are detected, the system flags these inputs as unreliable.

• **Fallback Mechanism:** If emotion recognition fails due to degraded or insufficient input (e.g., unclear facial images, noisy audio), the system automatically reverts to alternative authentication methods, such as biometric verification (e.g., fingerprint or face recognition) or knowledge-based credentials (e.g., password or PIN). This ensures that the authentication process remains secure despite failures in emotion recognition.

• **Confidence Thresholding:** In cases where emotion recognition yields ambiguous results, the system calculates the confidence score for the recognized emotional state. If the score falls below a predefined threshold, the system triggers a secondary authentication factor (e.g., one-time password or secondary biometric verification), ensuring that the authentication process remains secure even when emotion recognition fails.

8.6.2 *Cryptographic operations failures*

• **Redundant Cryptographic Operations:** Each cryptographic operation, including signature generation and message hashing, is accompanied by integrity checks. If any failure is detected in these operations (e.g., key corruption or signature mismatch), the system will either automatically retry the operation or prompt the user to re-authenticate.

• **Key Recovery Mechanisms:** In the event of a cryptographic failure, such as key corruption or failure to verify a cryptographic signature, the system includes secure mechanisms for key recovery. This may involve restoring the keys from a backup server using encrypted communication or prompting the user for an alternative verification method to recover authentication credentials.

• **Retry and Logging Mechanism:** For non-critical errors, the system automatically attempts to perform the operation again a set number of times before logging the error and notifying the user or system administrator. This reduces the disruption to the user experience caused by transient errors.

8.6.3 *Authentication failure handling*

• **Multi-Layered Authentication Recovery:** In case of multiple consecutive authentication failures, the system initiates a layered recovery process. This may involve secondary authentication methods such as trusted devices, security questions, or manual intervention to verify the legitimacy of the user.

• **User Notification and Support:** If authentication failures persist, users are immediately notified and provided with options to contact support or securely reset their authentication settings. This ensures that the user experience remains unaffected by repeated failures.

8.6.4 *System monitoring and logging*

• **Real-time Monitoring:** The system continuously monitors the performance of both the emotion recognition and cryptographic components. If performance degradation is detected, the system can adjust operational parameters (e.g., lowering emotion recognition sensitivity or switching to alternate cryptographic paths) to maintain functionality.

• **Error Logging and Analytics:** All errors, especially failures in emotion recognition or cryptographic operations, are logged for analysis. These logs are reviewed periodically to identify patterns or weaknesses in the system that may require improvements.

These error-handling strategies ensure that the framework remains operational under a variety of conditions, maintaining both security and reliability. By enabling graceful recovery from errors, the system ensures the authentication process remains secure, efficient, and user-friendly.

9. Future research directions

While the proposed authentication framework provides a promising foundation for secure emotion-aware authentication, there are several areas where further research is required.

Firstly, enhancing the robustness of emotion recognition is a critical research direction. The current system's performance may degrade in adverse conditions, such as low lighting or noisy environments, or when users exhibit subtle emotional expressions. To address these challenges, future work could explore advanced deep learning techniques, such as attention mechanisms or adversarial training, which can improve the system's ability to handle variations in input quality and complex real-world emotional expression. Additionally, multimodal fusion, which combines voice, facial expressions, and physiological signals, may help reduce dependence on a single modality, thus improving the overall recognition accuracy. Furthermore, addressing cross-cultural and inter-individual variability in emotional expressions remains a challenge. Research into domain-adaptive models, which can learn generalized emotional features, would be essential for ensuring the framework's applicability across diverse populations and contexts.

Secondly, optimizing cryptographic operations to reduce computational overhead without compromising security is another key area for future exploration. While post-quantum cryptographic schemes, such as Dilithium and Chameleon Hash, offer strong protection against quantum threats, they impose significant computational costs, particularly for real-time authentication. Further work should focus on optimizing these cryptographic primitives for edge devices with limited processing power. Investigating lightweight cryptographic protocols or leveraging hardware acceleration, such as TPUs or FPGAs, could help reduce the latency and enhance the scalability of the system. Additionally, hybrid cryptographic approaches, combining classical and post-quantum techniques, may offer a balance between performance and security.

Thirdly, expanding the potential applications of the proposed framework in various sectors, such as healthcare, banking, and secure government operations, would provide further validation of its practical utility. In healthcare, for example, the framework could be used to secure access to sensitive patient data, ensuring both privacy and authentication integrity. In banking, it could enhance secure transactions by integrating emotion-aware authentication with existing systems. Furthermore, the framework could be applied to high-security environments, such as government institutions, where robust authentication mechanisms are essential. Exploring these applications would not only demonstrate the flexibility and scalability of the framework but also align it with industry-specific security and privacy regulations.

Lastly, as the adoption of emotion-based authentication grows, it is vital to continuously address the privacy and ethical concerns associated with the use of sensitive biometric data. Future research should focus on refining privacy-preserving techniques, such as federated learning, differential privacy, and homomorphic encryption, to ensure that the collection, processing, and storage of emotional data comply with global privacy regulations, including GDPR and CCPA. Moreover, increasing the transparency of emotion data usage and providing users with greater control over their emotional data could help mitigate ethical concerns related to misuse or unauthorized access.

In summary, future research should focus on improving the generalization of emotion recognition models across diverse populations, optimizing the cryptographic operations for better performance and scalability, enhancing privacy-preserving techniques, and expanding the framework's applicability across various real-world domains. These advancements will ensure that the framework remains secure, efficient, and adaptable to emerging technological challenges.

10. Ethical considerations

The use of emotional biometrics in authentication systems introduces several critical ethical considerations that must be carefully addressed to ensure the responsible, transparent, and equitable application of this technology. While privacy concerns related to sensitive biometric data, such as facial expressions and physiological signals, have been discussed, it is essential to reflect more deeply on the broader ethical implications of using emotions as a biometric trait for authentication purposes.

10.1 *Informed consent and user control*

One of the foremost ethical considerations is the need for informed consent. Users must clearly understand what emotional data is being collected, how it will be used, and how long it will be stored. Consent should not only be obtained but also easily revocable at any time by the user. This requires providing users with tools that allow them to manage their data, including options to view, modify, and delete their emotional data. The process of obtaining and managing consent should be simple, transparent, and respectful of user autonomy.

10.2 *Data privacy and security*

Emotional data is inherently sensitive and must be treated with the highest standards of privacy and security. As with any biometric data, it is essential to implement robust protection measures to prevent unauthorized access, theft, or misuse. Techniques such as homomorphic encryption and federated learning can mitigate the risk of data exposure while enabling meaningful analysis. Homomorphic encryption allows computations on encrypted data without revealing the raw data, while federated learning ensures that sensitive data remains on the user's device, with only encrypted model updates being transmitted. These approaches not only safeguard privacy but also reduce the risk of data misuse.

10.3 *Prevention of emotional manipulation and coercion*

Another significant ethical concern is the potential for emotional manipulation or coercion. For example, attackers may attempt to manipulate or simulate emotional responses to bypass authentication mechanisms. To address this, the system should incorporate mechanisms to detect signs of coercion or stress during authentication. In the event of suspicious behavior, alternative authentication methods (such as PINs or additional biometric verification) should be triggered automatically. Furthermore, fallback mechanisms should be in place to allow users to authenticate even when under emotional duress.

10.4 *Bias, fairness, and inclusivity*

It is essential for emotional recognition systems to be fair and inclusive. Variations in emotional expression occur not only between individuals but also across cultural, social, and demographic groups. These differences must be accounted

for when designing emotion-based authentication systems. Using diverse datasets for training and validation is crucial to ensure the system performs well across all user groups. Domain-adaptive models should be developed to handle different emotional expressions, reducing the risk of bias and ensuring that the system does not unfairly benefit or disadvantage any group.

10.5 *Transparency and accountability*

The ethical use of emotional biometrics requires a high level of transparency in how data is used. Users should be fully informed about the types of emotional data being collected, how it is processed, and the policies surrounding its storage and retention. Clear guidelines should be in place regarding how users can access, modify, or delete their data, and how long it will be retained. Additionally, robust mechanisms for addressing misuse or unauthorized access to emotional data should be established to ensure accountability within the system.

10.6 *Regulatory compliance*

It is essential that emotion recognition systems comply with international data protection regulations such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). These regulations provide users with rights such as access, correction, and deletion of their data, which must be upheld by the system. Adhering to these frameworks not only ensures the ethical use of emotional data but also enhances the system's credibility and trustworthiness across different jurisdictions.

11. Conclusion

This paper introduces a novel two-tier authentication framework that integrates emotion recognition with post-quantum cryptographic primitives. By securely binding real-time emotional states to traditional identity credentials, the system enhances protection against impersonation, coercion, and quantum-enabled attacks. Theoretical evaluations indicate that the proposed method achieves a True Acceptance Rate (TAR) of 95.7% and a False Acceptance Rate (FAR) of 2.1%, surpassing traditional multi-factor authentication and FIDO2-based behavioral systems. These findings demonstrate the potential of emotion-aware, cryptographically hardened authentication mechanisms for deployment in high-assurance environments. In summary, the proposed framework offers a promising solution for the next generation of authentication systems, providing enhanced security through the combination of emotion recognition and post-quantum cryptography. Future work will focus on refining emotion recognition models, optimizing cryptographic operations, and expanding the framework's applicability across different real-world applications.

Conflict of interest

The authors declare no conflicts of interest.

References

[1] Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. In: *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*. Santa Fe, NM, USA: IEEE; 1994. p.124-134. Available from: https://doi.org/10.1109/SFCS.1994.365700.

[2] Gill SS, Kumar A, Singh H, Singh M, Kaur K, Usman M, et al. Quantum computing: A taxonomy, systematic review and future directions. *Software: Practice and Experience*. 2022; 52(1): 66-114. Available from: https://doi.org/10.1002/spe.3039.

[3] Dalal YM, Supreeth S, Amuthabala K, Satheesha TY, Asha PN, Somanath S. Optimizing security: A comparative analysis of RSA, ECC, and DH algorithms. In: *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*. Bagalkote, India: IEEE; 2024. Available from: https://doi.org/10.1109/NKCon62728.2024.10775183.

[4] Shafiq M, Gu Z. Deep residual learning for image recognition: A survey. *Applied Sciences*. 2022; 12(18): 9423. Available from: https://doi.org/10.3390/app12189423.

[5] Udahemuka G, Djouani K, Kurien AM. Multimodal emotion recognition using visual, vocal and physiological signals: A review. *Applied Sciences*. 2024; 14(17): 5560. Available from: https://doi.org/10.3390/app14175560.

[6] Zeng Z, Pantic M, Roisman GI, Huang TS. A survey of affect recognition methods: Audio, visual and spontaneous expressions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2009; 31(1): 39-58. Available from: https://doi.org/10.1109/TPAMI.2008.52.

[7] Bernstein DJ, Lange T, Peters C. Attacking and defending the McEliece cryptosystem. In: Buchmann J, Ding J. (eds.) *Post-Quantum Cryptography*. Heidelberg: Springer; 2008. p.31-46. Available from: https://doi.org/10.1007/978-3-540-88403-3_3.

[8] Ducas L, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, Stehlé D. Crystals-dilithium: Digital signatures from module lattices. *IACR Transactions on Symmetric Cryptology*. 2018; 2018(1): 238-268. Available from: https://doi.org/10.13154/tches.v2018.i1.238-268.

[9] Sonnino G, Sonnino A. Efficient multiparty protocols using generalized parseval's identity and the theta algebra. In: *2022 7th International Conference on Mathematics and Computers in Sciences and Industry (MCSI)*. Athens, Greece: IEEE; 2022. p.1-17. Available from: https://doi.org/10.1109/MCSI55933.2022.00008.

[10] McEliece RJ. *A public-key cryptosystem based on algebraic coding theory*. DSN Progress Report 42-44, 1978. p.114-116.

[11] Misoczki A, Tillich JP, Sendrier N, Barreto PS. MDPC-McEliece: New McEliece variants from moderate density parity-check codes. In: *2013 IEEE International Symposium on Information Theory*. Istanbul, Turkey: IEEE; 2013. p.2069-2073. Available from: https://doi.org/10.1109/ISIT.2013.6620590.

[12] Baldi M. *QC-LDPC Code-Based Cryptography*. Heidelberg: Springer; 2014. Available from: https://doi.org/10.1007/978-3-319-02556-8.

[13] Sendrier N. Code-based cryptography: State of the art and perspectives. *IEEE Security & Privacy*. 2017; 15(4): 44-50. Available from: https://doi.org/10.1109/MSP.2017.3151345.

[14] Alagic G, Apon D, Cooper D, Dang Q, Kelsey J, Lichtinger J, et al. *Status report on the third round of the NIST post-quantum cryptography standardization process*. Internal Report NIST IR 8413-upd1, 2022. Available from: https://doi.org/10.6028/NIST.IR.8413.

[15] Albrecht MR, Bernstein DJ, Chou T, Cid C, Gilcher J, Lange T, et al. *Classic McEliece: Conservative code-based cryptography*. NIST IR 8413, 2022.

[16] National Institute of Standards and Technology. *Post-quantum cryptography: Round 3 submissions*. NIST IR 8413, 2022.

[17] Lyubashevsky V. Lattice signatures without trapdoors. In: Pointcheval D, Johansson T. (eds.) *Advances in Cryptology-EUROCRYPT 2012*. Heidelberg: Springer; 2012. p.738-755. Available from: https://doi.org/10.1007/978-3-642-29011-4_43.

[18] Chen X, Zhang F, Kim K. Chameleon hashing without key exposure. In: Zhang K, Zheng Y. (eds.) *Information Security*. Heidelberg: Springer; 2004. p.87-98. Available from: https://doi.org/10.1007/978-3-540-30144-8_8.

[19] Bos JW, Costello C, Ducas L, Mironov I, Naehrig M, Nikolaenko V, et al. Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery; 2016. p.1006-1018. Available from: https://doi.org/10.1145/2976749.2978425.

[20] Güneysu T, Krausz M, Oder T, Speith J. Evaluation of lattice-based signature schemes in embedded systems. In: *2018 25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*. Bordeaux, France: IEEE; 2018. p.385-388. Available from: https://doi.org/10.1109/ICECS.2018.8617969.

[21] Ekman P. An argument for basic emotions. *Cognition & Emotion*. 1992; 6(3-4): 169-200. Available from: https://doi.org/10.1080/02699939208411068.

[22] Li S, Deng W. Deep facial expression recognition: A survey. *IEEE Transactions on Affective Computing*. 2020; 13(3): 1195-1215. Available from: https://doi.org/10.1109/TAFFC.2020.2981446.

[23] Zeng Z, Pantic M, Roisman GI, Huang TS. A survey of affect recognition methods: Audio, visual and spontaneous expressions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2009; 31(1). 39-58. Available from: https://doi.org/10.1109/TPAMI.2008.52.

[24] Udahemuka G, Djouani K, Kurien AM. Multimodal emotion recognition using visual, vocal and physiological signals: A review. *Applied Sciences*. 2024; 14(17): 8071. Available from: https://doi.org/10.3390/app14178071.

[25] Jack RE, Garrod OG, Yu H, Caldara R, Schyns PG. Facial expressions of emotion are not culturally universal. *Proceedings of the National Academy of Sciences*. 2012; 109(19): 7241-7244. Available from: https://doi.org/10.1073/pnas.1200155109.

[26] El Ayadi M, Kamel MS, Karray F. Survey on speech emotion recognition: Features, classification schemes, and databases. *Pattern Recognition*. 2011; 44(3): 572-587. Available from: https://doi.org/10.1016/j.patcog.2010.09.020.

[27] Galbally J, Marcel S, Fierrez J. Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing*. 2013; 23(2): 710-724. Available from: https://doi.org/10.1109/TIP.2013.2292332.

[28] Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, et al. Generative adversarial networks. *Communications of the ACM*. 2020; 63(11): 139-144. Available from: https://doi.org/10.1145/3422622.

[29] Korshunov P, Marcel S. Deepfakes: A new threat to face recognition? Assessment and detection. *arXiv:1812.08685*. 2018. Available from: https://arxiv.org/abs/1812.08685.

[30] Todisco M, Wang X, Vestman V, Sahidullah M, Delgado H, Nautsch A, et al. ASVspoof 2019: Future horizons in spoofed and fake audio detection. *arXiv:1904.05441*. 2019. Available from: https://arxiv.org/abs/1904.05441.

[31] Yi J, Fu R, Tao J, Nie S, Ma H, Wang C, et al. ADD 2022: The first audio deep synthesis detection challenge. In: *ICASSP 2022 IEEE International Conference on Acoustics, Speech and Signal Processing*. Singapore: IEEE; 2022. p.9216-9220. Available from: https://doi.org/10.1109/ICASSP43922.2022.9746939.

[32] Zhang B, Cui H, Nguyen V, Whitty M. Audio deepfake detection: What has been achieved and what lies ahead. *Sensors*. 2025; 25(7): 1989. Available from: https://doi.org/10.3390/s25071989.

[33] Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*. 2004; 14(1): 4-20. Available from: https://doi.org/10.1109/TCSVT.2003.818349.

[34] Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schwabe P, Seiler G, et al. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 2018; 2018(1): 238-268. Available from: https://doi.org/10.13154/tches.v2018.i1.238-268.

[35] Plutchik R. The nature of emotions: Human emotions have deep evolutionary roots, a fact that may explain their complexity and provide tools for clinical practice. *American Scientist*. 2001; 89(4): 344-350. Available from: https://doi.org/10.1511/2001.28.344.

[36] Poria S, Cambria E, Bajpai R, Hussain A. A review of affective computing: From unimodal analysis to multimodal fusion. *Information Fusion*. 2017; 37: 98-125. Available from: https://doi.org/10.1016/j.inffus.2017.02.003.

[37] Goldman AI, Sripada CS. Simulationist models of face-based emotion recognition. *Cognition*. 2005; 94(3): 193-213. Available from: https://doi.org/10.1016/j.cognition.2004.01.005.

[38] Graves A. Long short-term memory. In: *Supervised Sequence Labelling with Recurrent Neural Networks*. Heidelberg: Springer; 2012. p.37-45. Available from: https://doi.org/10.1007/978-3-642-24797-2_4.

[39] Jacob B, Kligys S, Chen B, Zhu M, Tang M, Howard A, et al. Quantization and training of neural networks for efficient integer-arithmetic-only inference. In: *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*. Salt Lake City, UT, USA: IEEE; 2018. p.2704-2713. Available from: https://doi.org/10.1109/CVPR.2018.00286.

[40] McMahan B, Moore E, Ramage D, Hampson S, Arcas BA. Communication-efficient learning of deep networks from decentralized data. In: *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*. Fort Lauderdale: PMLR; 2017. p.1273-1282.

[41] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: *Advances in Cryptology-EUROCRYPT' 99*. Heidelberg: Springer; 1999. p.223-238. Available from: https://doi.org/10.1007/3-540-48910-X_16.

[42] Guan J, Li H, Ye H, Zhao Z. A formal analysis of the FIDO2 protocols. In: Atluri V, Di Pietro R, Jensen CD, Meng W. (eds.) *Computer Security-ESORICS 2022*. Heidelberg: Springer; 2022. Available from: https://doi.org/10.1007/978-3-031-17143-7_1.

[43] Muir A, Brown K, Girma A. Reviewing the effectiveness of multi-factor authentication (MFA) methods in preventing phishing attacks. In: *Proceedings of the Future Technologies Conference (FTC) 2024, vol.4*. Springer; 2024. p.597-607. Available from: https://doi.org/10.1007/978-3-031-73128-0_40.

Appendix A: Pseudocode and flowcharts

Pseudocode for emotion-aware authentication

The following pseudocode describes the steps involved in emotion-aware authentication:

Algorithm 1 Emotion-Aware Authentication Pseudocode

Input: User identity U, password P, emotional features E

Output: Authentication result

1: # Emotion recognition model is assumed to be pre-trained and deployed;
2: **Step 1:** Emotion Feature Extraction;
3: E = extract_emotion(U, P);
4: **Step 2:** Create the message to bind emotion with identity;
5: M = concatenate(U, P, E);
6: **Step 3:** Compute Chameleon Hash;
7: chameleon_hash = compute_chameleon_hash(M);
8: **Step 4:** Generate Dilithium Signature;
9: signature = dilithium_sign(chameleon_hash);
10: **Step 5:** Verify Signature and Hash;
11: **if** dilithium_verify(chameleon_hash,signature) **then**
12: **if** chameleon_hash == compute_chameleon_hash(M') **then**
13: **return** Success;
14: **end if**
15: **end if**
16: **return** Failure;

Flowchart for emotion recognition and cryptographic processing

Figure 6 illustrates the pipeline for emotion recognition and cryptographic message generation, while Figure 7 depicts the extended authentication process with fallback mechanisms.

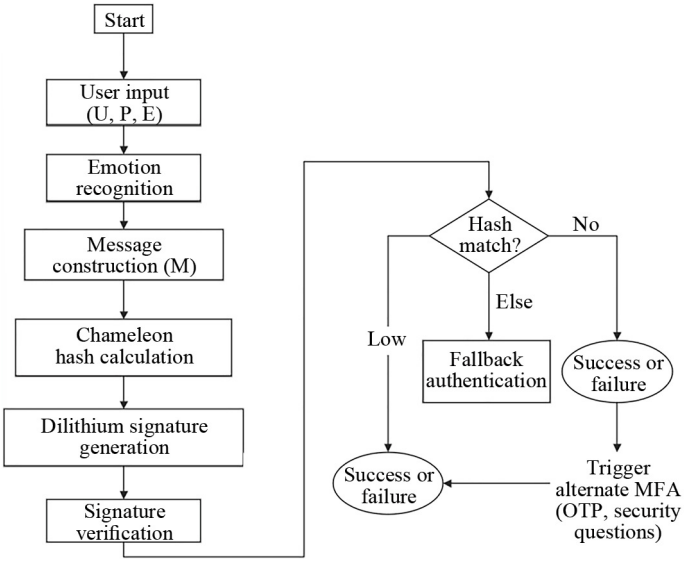

Figure 6. Flowchart for authentication process with fallback

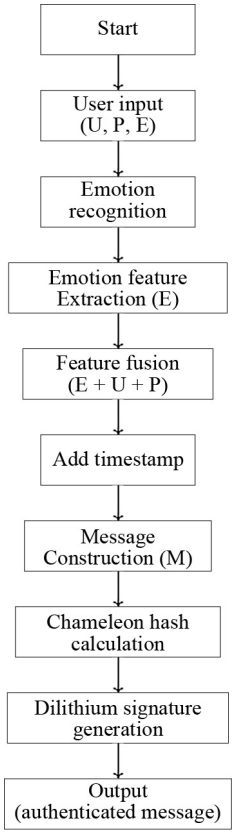

Figure 7. Flowchart for emotion recognition and cryptographic message generation