SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I11P124

Volume 13 Issue 11, 386-397, November 2026
© 2026 Seventh Sense Research Group®

Original Article

Design and Implementation of a Quantum-Resistant Identity Authentication System using PQC Techniques

Vivek Kumar[1], Madhu Kirola[1], Dev Baloni[2]

[1]*Computer Science & Engineering Department, Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, Uttarakhand, India.*
[2]*Computer Science & Engineering Department, Shivalik University, Uttarakhand, India.*

[1]*Corresponding Author: vivek11krr@gmail.com*

Received: 03 September 2026 Revised: 13 October 2026 Accepted: 19 August 2026 Published: 27 Novmeber 2026

Abstract *- The creation and administration of cryptographic keys, like passwords and pin codes, in modern digital security systems frequently depend on complex mathematical transformations and stochastic random processes. Although these keys provide strong protection, their distribution and storage need expensive and complex systems. Despite being commonly utilized for biometric verification, face recognition technologies have two main issues. First, analyzing big datasets and high-resolution photos takes a lot of processing time. Second, the encryption techniques used to safeguard stored face templates could be compromised by newly developed quantum computers. Unlike passwords, facial features cannot be changed, biometric data will always be at risk since quantum computers will soon be able to decipher existing security solutions. This research proposes a quantum computing-based approach that adds quantum-resistant security and speeds up facial recognition. It uses rotation gates and entanglement to apply quantum feature encoding, then uses AerSimulator to create quantum fingerprints, and finally uses McEcliece, a post-quantum cryptography technique, for signature and verification. Performance is significantly improved by the suggested approach. This paper conducted a security, time, and performance metrics study and discussion of the results. The security metrics findings for accuracy, FAR, FRR, EER, ADR, HAD, FMR, and FNMR are 99.09%, 0.0000, 0.0182, 0.0091, 100%, 2.7, 0.0000, and 0.0182. Enrolment, matching, throughput, feature extraction, encryption, and decryption times are 52.77 ms, 0.19 ms, 77.15 transactions/second, 2.41 ms, 49.78 ms, and 12.77 ms, according to time measurements. According to performance measures, the results for F1-Score, recall, and precision are 99.08%, 98.18%, and 100%, respectively. Accuracy, encryption time, and decryption time are used to compare various cryptographic methods using the suggested model. These findings show that a quantum-resistant system for PQC IA System can address security and speed issues with existing biometric systems, making it feasible for practical implementation as quantum technology develops. The results demonstrate that the integration of quantum-resistant cryptography and cryptographic privacy enforcement is necessary for secure post-quantum identity.*

Keywords *- Feature extraction, Identity authentication, McEcliece Pqc technique, Post-Quantum cryptography, Quantum feature encoding.*

1. Introduction

Secure and effective authentication methods are more important than ever because modern information technology advancements have coincided with an increase in cyberthreats and increased worries about data privacy. The increasing sophistication of cyberattacks and the widespread sharing of private data on internet platforms have exposed flaws in traditional authentication methods. Additionally, a new class of vulnerabilities to current security infrastructures is presented by the possibility of practical QC [1]. With its distinct benefits over conventional password- or token-based methods, biometric authentication has become a key component of contemporary identity verification systems. These days, identity verification and smartphone unlocking are essential for both security and convenience. Biometric characteristics are more resistant to efforts at impersonation than passwords because they are intrinsically linked to individuals [2]. In this research, a quantum-resistant post-quantum cryptography system for identity authentication using an input user image is presented.

For practical implementation, we integrate post-quantum cryptography and quantum feature extraction techniques in this system. The fundamental schematic for the quantum-resistant system for PQC identity and biometric feature extraction from images is the definition of authentication:


This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

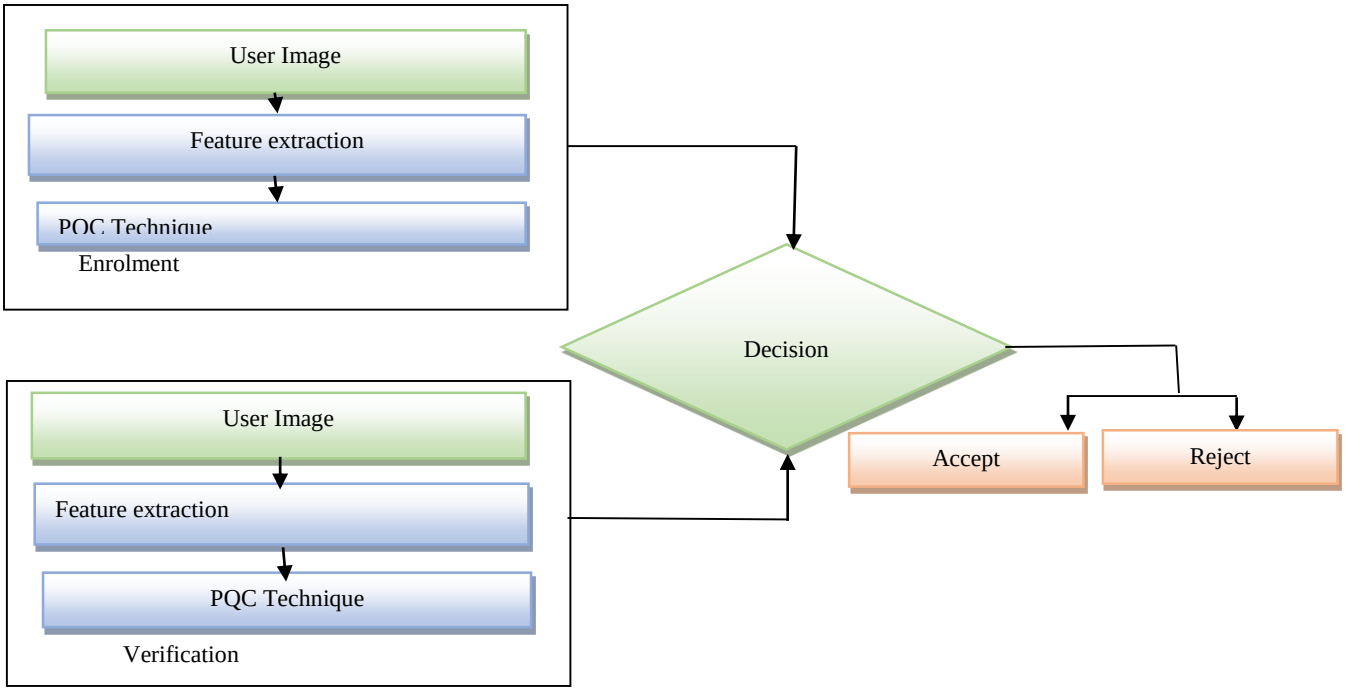

Fig. 1 Quantum-Resistant system for PQC identity authentication

Our model is split into two modules: the enrolment module and the verification module. The user uploads an image to the enrolling module, following which we extract the image's features and apply the PQC approach. Similar to this, in the verification module, the user uploads a picture, from which we extract features before applying the PQC approach. Next, we must determine whether or not they are comparable. The user is authenticated if they are similar, and not authenticated if they are not. The process of confirming a user's identification is called authentication. The user is given access to the security system if the information matches the enrolment information; otherwise, the user is refused or does not receive access to the security system.

Biometric privacy and the use of a single biometric for authentication are the two main issues with biometric systems. Biometric cryptosystems, in which biometrics are encrypted using encryption keys, could address the first issue. Stronger multi-factor biometric authentication could be used to address the second issue. Because of its innate, unwavering security against quantum computers, QC has recently emerged as a potential solution to this issue [3]. We present a comprehensive quantum-resistant post-quantum cryptography identity authentication system in this research. Our proposal's primary benefits are:

- Compared to traditional methods, the suggested approach enables a more effective key size, leading to increased security, speed, and computational efficiency.
- McEcliece post quantum cryptography, which is significantly superior to conventional cryptography, is used during the verification stages.
- No confidential information that could jeopardise the architecture's security is shared between entities.

Instead of offering a complete end-to-end solution, the majority of methods focus on quantum augmentation of particular face verification pipeline components. According to the suggested model, in order to fully realise quantum advantages, all stages of enrolling and verification are required.

This is how the paper is organized. The history and relevant work are described in Section 2. The research methodology utilized to guarantee the success of the entire procedure is presented in Section 3. Section 4, we present a post-quantum computing technique. The performance measures for the results are described in Section 5. The results, analysis, and discussion of the suggested model are shown in Section 6. The outcome is graphically found in Section 7. Lastly, Section 8 discusses the conclusion and future scope.

2. Related Work and Background

In order to inform our quantum-resistant system for post-quantum cryptography Identity Authentication System, this part examines pertinent literature from important disciplines. Biometric systems use facial traits, which cannot be lost or stolen like passwords, to provide safe, practical identity authentication. They are therefore an effective instrument for safeguarding sensitive data, devices, and services. However, significant privacy and data protection issues are brought up by their increasing use [4]. There are two subsections inside it. The development of

facial biometrics technology is covered in the first subsection, and the fundamental ideas of quantum computing that underpin our methodology are covered in the second.

2.1. Evolution of Feature Extraction

In this article, we look at a method that adds quantum-resistant security and speeds up facial recognition using quantum computing. It uses the SWAP test and QPCA to develop lattice-based cryptography, which is unbreakable by quantum computers, and to lower computational complexity. With log(N) complexity for eigenvalue extraction compared to $O(N^3)$ traditionally, the suggested framework significantly improves performance [5]. The Gujjala PKR framework integrates a hybrid authentication technique that combines safe multi-party computation for transaction verification, continuous behavioural pattern recognition using deep learning models, and quantum-resistant cryptographic protocols. Superior performance with 99.7% authentication accuracy while preserving quantum resistance is demonstrated by experimental validation on a synthetic banking dataset [6]. The authors of Kipchirchir BS et al. employ a hybrid quantum-classical approach, utilising Quantum-Enhanced GANs (QGAN) to accelerate the creation of synthetic fingerprints and Quantum Support Vector Machines (QSVM) for feature categorisation. The models were processed by the system far more quickly than their classical equivalents [7]. The authors of Khan F et al. employ a novel hybrid quantum-classical framework that extracts high-dimensional representation using InceptionResnetV1, CNN and a Quantum Inspired Attention Mechanism to choose which features are most crucial to analyse [8]. Some other literature review of feature extraction is shown in Table 1.

Table 1. Literature review

Author (s) & Year	Title	Research Objective	Key Findings
S. Mehta et al. (2024) [12]	Hybrid Deep Learning Approaches for Feature Extraction and Cancelable Template Generation in Iris Recognition	This research provides a deep learning-based model for effective iris detection that blends hybrid Convolutional Neural Network (CNN) architectures with cancelable template generation approaches. To produce discriminative iris characteristics, model integrating MobileNetV3Small, EfficientNetB0, XceptionNet, InceptionNetV3, and DenseNet121 are used.	With an EER of 0.044 and an accuracy of upto 97.78% on the MMU dataset.
V. Thenmozhi et al. (2025) [13]	Cancelable Biometric Template Generation Using Deep Learning-Based Secure Transforms	This work creates a framework for cancelable fingerprint template creation based on deep learning. Several Convolutional Neural Network (CNN) backbones such as VGG16, MobileNetV2, ResNet18, ResNet50, and DenseNet121 are used to extract features.	Revocability of 0.49, True Acceptance Rate of 95.8% at 1% False Acceptance Rate, and Equal Error Rate of 15.9% were all attained using bio-hashing.
Y. Wang et al. (2025) [11]	A Two-Tier Authentication Framework Integrating Post-Quantum Cryptography with AI-Based Emotion Recognition	The authors describe an AI-enhanced post-quantum two-tier authentication architecture that combines adaptive, behaviour-based biometrics with cryptographic robustness. The generated emotion signatures are signed using the CRYSTALS-Dilithium scheme and connected to the credential system using a lattice-based chameleon hash.	Under targeted adversarial attacks, the simulation findings indicate a 2.1% false acceptance rate and a 95.7% true acceptance rate.
S. Singh et al. (2025) [14]	Quantum-Enhanced Facial Biometrics: A Hybrid Framework with Post-Quantum Security	This research proposes a quantum computing-based approach that adds quantum-resistant security and speeds up facial recognition. It uses the SWAP test and QPCA to achieve lattice-based cryptography and lower computational complexity.	The authors' accuracy was 91.2%, they had an equal error rate of 2.7%, true positive rate of 96.8%, and false positive rate of 2.1%.

2.2. Post-Quantum Cryptography

Wang LJ et al. The authors achieved effective and quantum safe QKD authentication by combining the PKI with the post-quantum digital signature method based on lattices, Aigis-Sig. In order to achieve pairwise interconnection, this method requires $C^2_n = n(n-1)/2$ pairs of symmetric keys for an n-user QKD network. On the other hand, every user needs to submit one application to a certificate authority for a digital certificate in order to accomplish effective and safe authentication.

For QKD with the aid of an established PKI and PQC with quantum-resistant security [9]. Yang Y. and others. The current AKA protocol is constantly vulnerable to attacks that the LIAMKA protocol can withstand. Additionally, the computational efficiency of the LIAMKA protocol is comparatively good [10]. A post-quantum two-tier authentication system augmented by AI scheme that combines adaptive, behaviour-based biometrics with cryptographic robustness is presented by Wang Y et al. Tier-1 establishes a baseline identification using traditional factors, such as passwords and static biometrics. Next, Tier-2 uses facial expressions to gather dynamic emotional data. Under targeted adversarial attacks, the results reveal a False Acceptance Ratio of 2.1% and a True Acceptance Ratio of 95.7% [11].

3. Research Methodology

In this research, the reliability of the proposed model was tested based on a face image dataset having 7,000 images CFPW dataset. This dataset is used for testing only. Where appropriate, subject-level data partitioning was used to prevent accidental overlap of testing and enrolling samples. Same image enrolment and verification samples were compared. The point at which an identification was approved or disapproved was determined.

3.1. Requirements

- Processor (CPU): Intel Core i7 for efficient parallel multi-threaded quantum processing.
- Memory (RAM): 16 GB DDR4 to avoid memory overflow errors.
- Operating System: Windows 10/11 or Ubuntu Linux.
- Development Environment: Spyder IDE (v5.5 or v6.0).
- Core Language Runtime: Python 3.13.19
- PQC Framework: pqcrypto
- Cryptographic Primitive: McEliece

The creation of a useful and efficient biometric template protection system is the primary driving force behind the construction of a Quantum-Resistant System for PQC Identity Authentication. The development of the biometric-based PQC Identity Authentication system will be thoroughly described in this part. The two phases of the suggested authentication method are enrolment and verification, as shown in Figure 2 and explained below. The enrolling process was crucial to the proposal since it requires capturing biometric pictures and securely storing an individual's image. Enrolment is the initial step in the suggested authentication method, and the procedures are as follows:

3.2. User Image

When a user registers, they should upload their user image so that we can confirm they are the right person when they log in later.

3.3. Quantum Feature Extraction

It uses the concepts of quantum mechanics to convert unprocessed images into intricate, higher-dimensional representations. In the suggested model, image processing was used, then the quantum-inspired feature generation. First, the image is resized to 4 by 4 pixels. No significant features are derived from this. Equation 1 carries out this operation:

$$r = cv2.resize(image_array, (4,4)) \quad (1)$$

Next, using equation 2, we must get the shrunk image's average brightness or mean pixel intensity. The mean pixel intensity was computed to start the random-number generator.

$$\text{Mean Brightness} = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (2)$$

Where N = 16 pixels and x_i = pixel values. Equation 3 then transforms this retrieved feature/mean brightness into a seed:

$$np.random.seed(int(Mean\ Brightness * 100) \% 2026) \quad (3)$$

Where 100 is used to scale the brightness, 2026 is the divisor used with the modulus operator, which restricts the seed value to the range 0 to 2025, random is used to generate random numbers, and seed is used to initialise the random number generator. Next, we used equation 4 to construct the quantum signature:

$$q = np.random.randint(0, 2, size=16) \quad (4)$$

The brightness of the image determines the seed; comparable bit sequences may be produced by images with similar average brightness. Then, a feature vector of 16-bits was generated. The quantum circuit was configured with 4 qubits. Two qubits were linked linearly by a CNOT quantum gate and a Y-Rotation gate. The quantum circuits were executed with the stabiliser approach using the qiskit and qiskit-aer libraries. The obtained feature represented was secured by the McEliece PQC method.

3.4. McEliece PQC Technique

In order to encrypt a communication, the input plaintext message is encoded using a disguised version of the generating matrix as the public key. Equation (5) can be used to do this:

$$G_{pub} = SGP$$

$$c = mG_{pub} + e \pmod 2 \quad (5)$$

Where S is the invertible scrambling matrix, P is the permutation matrix, G_{pub} is the public generator matrix, e is the random error vector, G is the generating matrix, and m is the message.

The encrypted process encodes the message so that the original message is transformed into a ciphertext. Then the ciphertext is decrypted with the respective private key. First, the received ciphertext is multiplied by the inverse permutation matrix:

$$c' = cP^{-1} \quad (6)$$

The output vector is then processed by the private error-correcting decoding algorithm to correct the errors introduced and recover the scrambled message:

$$m' = mS \quad (7)$$

The original plaintext message is obtained by applying the inverse scrambling matrix:

$$m = m'S^{-1} \quad (8)$$

Beyond the McEliece encryption process, the proposed model performs additional bitwise transformations on the binary feature vector coming out of the quantum process.

Let the extracted quantum feature vector be binary Q. At first, each bit is inverted by:

$$\bar{Q} = Q \oplus 1 \quad (9)$$

Where 1 is an all-one binary vector of the same length as Q. The first bit is flipped by:

$$\bar{Q}' = \bar{Q} \oplus e_1 \quad (10)$$

Where e_1 is a binary vector with 1 in the first position and 0 in all other positions. The additional bitwise transformation is given by:

$$C = \bar{Q} \oplus E \quad (11)$$

Where C is the transformed feature vector, and E is the additional bitwise error vector. These are extra feature processing steps and are different from the random error-vector mechanism used in McEliece operation.

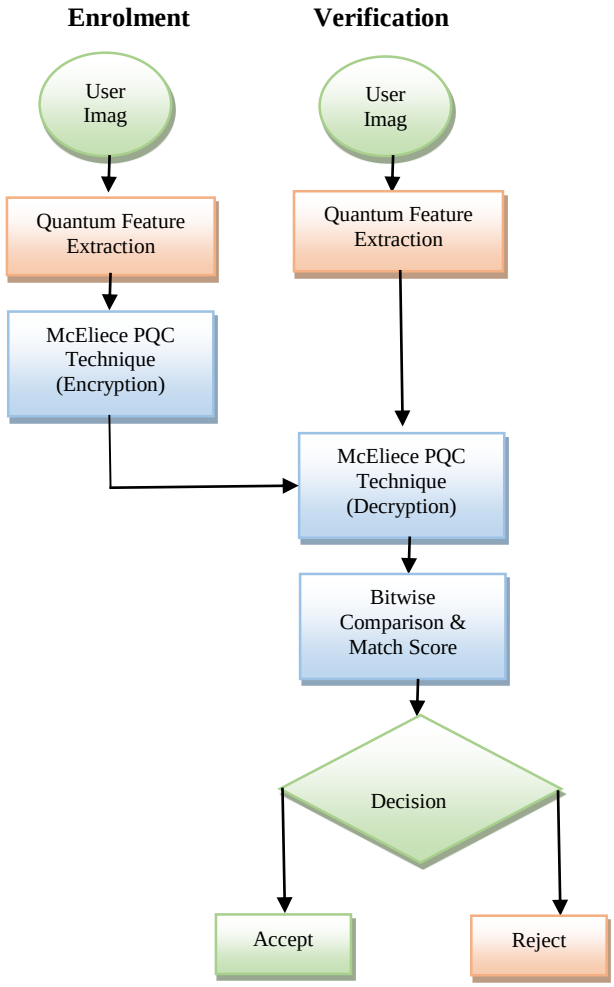

Fig. 2 Proposed model

4. PQC Techniques

Public-Key cryptography, which enables secure key exchange, data confidentiality, and authentication over intrinsically untrusted networks, is the foundation of modern digital networking security. Public-key cryptographic cyphers provide the essential mechanisms that enable secure interaction and communication between billions of devices and people. Critical infrastructure is protected, 5G and Internet of Things-based mobile environments are secure, secure web transactions are made possible, trusted software upgrades are enabled, and sensitive financial and medical records are protected [15]. The potential reality of quantum computing's enormous computing capability has been revealed by recent developments in the field [16]. Before carefully creating an optimisation strategy or choosing a PQC algorithm for encrypting and decrypting in different applications, understanding the effects of using PQC algorithms in different situations is essential. A mechanism for encrypting and decrypting sent data is required to assess

the effects of PQC algorithms on applications [17]. In order to secure our system, we have proposed a PQC model that makes use of the McEliece PQC approach. Figure 3 depicts the McEliece PQC method Cryptosystem.

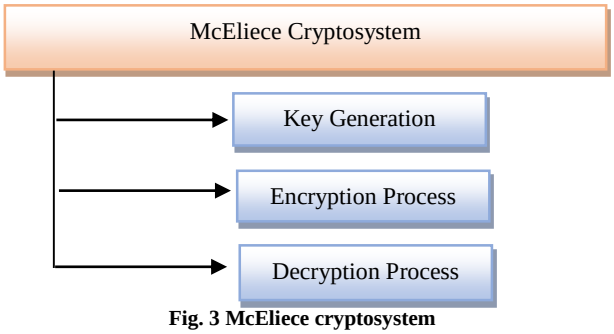

Fig. 3 McEliece cryptosystem

The first public-key cryptosystem based on code. A random binary Goppa code is specified by the public key. A codeword plus a random mistake is called a ciphertext. Effective decoding, codeword extraction from the ciphertext, and error detection and removal are all made possible by the private key [18]. Enhanced McEliece multiplies the ciphertext by the inverse of the sparse matrix, or the private key, in place of syndrome decoding using the Goppa Matrix [19]. A secret key (i.e., $\{K_1, K_2, K_3\}$) is created during key creation. It consists of a scrambler K_1 (dimension $\zeta_1 \times \zeta_1$), a permutation matrix K_3 (dimension $\zeta_2 \times \zeta_2$) and a generator matrix K_2 (dimension $\zeta_1 \times \zeta_2$ encoder matrix). Additionally, the product of these three matrices yields the dimensions of the public key are $\zeta_1 \times \zeta_2$ (i.e., $L = K_1K_2K_3$) [20]. Based on the generator matrix K_2, a decoder matrix K_4 (with dimensions $\zeta_2 \times \zeta_1$) and an error-detector matrix K_5 are created for decoding and error-correcting.

The definition of an encryption function e (m, L) is defined in Equation 12, is employed to carry out encryption. It is used to create ciphertext z by using a random number r and the public key L to encrypt plaintext m.

$$e(m, L) = mL + r = mK_1K_2K_3 + r = z \quad (12)$$

When plaintext z is decrypted using the private key $\{K_1, K_2, K_3\}$, the decryption function d (z, $\{K_1, K_2, K_3\}$) is defined as Equation 13, resulting in plaintext m (with dimensions 1x ζ_1). Furthermore, the random integer r is identified and eliminated using an error-correcting function f (α, K_5) based on the error-detector matrix K_5. The encoded message generated by the encoder matrix K_2 can be decoded using the decoder matrix K_4 (i.e., $xK_2K_4 = x$).

$$\begin{aligned} D(z, \{K_1, K_2, K_3\}) &= f(zK_3^{-1})K_4K_1^{-1} \\ &= f((mL + r)K_3^{-1})K_4K_1^{-1} \\ &= f((mK_1K_2K_3 + r)K_3^{-1})K_4K_1^{-1} \\ &= f((mK_1K_2K_3K_3^{-1} + rK_3^{-1})K_4K_1^{-1} \\ &= mK_1K_2K_4K_1^{-1} \\ &= mK_1K_1^{-1} = m \end{aligned} \quad (13)$$

5. Result Performance Metrics

The experimental evaluation shows that the suggested framework performs better. For the suggested model, a number of performance indicators have been examined. Time-based performance metrics, feature performance, and security metrics have all been covered in this section.

5.1. Security Metrices

This thorough security examination of biometric authentication aids in comprehending its advantages, dangers, and privacy ramifications. The correctness of the suggested model, FAR, FRR, EER, ADR, HDA, and spoof attack resistance were all included in these security metrics:

5.1.1. Accuracy

By evaluating the percentage of corrective choices out of all user authentication attempts, it assesses how accurately a system recognises a user [21]. Equation 14 displays its formula.

$$\text{Accuracy} = \frac{TA+TR}{TA+TR+FA+FR} \times 100 \quad (14)$$

TA stands for True Acceptance (accepted by the system), TR for True Rejection (unauthorised user rejected by the system), FA for False Acceptance (unauthorised user accepted by the system), and FR for False Rejection (user rejected mistakenly).

5.1.2. False Acceptance Rate

Accepting an impostor is what it is [22]. The probability that a system will identify a person who typically should not have been identified is determined by this rate. Equation 15 displays the FAR equation.

$$\text{FAR} = \frac{\text{Number of Imposters Accepted}}{\text{Total Number of Imposters Access}} \quad (15)$$

5.1.3. False Rejection Rate

This rate establishes the probability that a system will fail to identify an individual who ought to be identified. It is calculated by dividing the total number of legitimate individuals being authenticated by the number of lawful individuals who are denied access [23]. Equation 16 displays the formula used for FRR.

$$\text{FRR} = \frac{\text{Number of Rejected "Client"}}{\text{Total Number of "Client" Access}} \quad (16)$$

5.1.4. Equal Error Rate

This rate serves as a point of current performance measurement and is computed using the first two criteria. This point represents the optimal balance between false rejections and false acceptances, or the location where FRR = FAR [24].

5.1.5. Attack Detection Rate

The proportion of fraudulent login attempts that are successfully detected and prevented [25]. Equation 17 displays the ADR equation utilised in the biometric authentication system.

$$ADR = 1 - \frac{\text{No.of Presentation Attack Failed Attempts}}{\text{Total No.of Presentation Attacks}} \quad (17)$$

5.1.6. Hamming Distance Rate

HAD looks for a match between two binary strings. The user is allowed access if they HAD been low, and access is denied if the HAD been high [26]. Equation 18 applies to HDR:

$$HDR = \frac{1}{n} \sum_{i=1}^{n} (X_i \oplus Y_i) \quad (18)$$

Where the total number of bits is denoted by n, $\oplus$ is the XOR operator, and X_i and Y_i are the bits to be compared.

5.1.7. False Match Rate

The likelihood that the system will recognise a fraudster as a legitimate user is known as the FMR.

5.1.8. False Non-Match Rate

The likelihood that the system will reject a legitimate user as an impostor is known as the FNMR [27].

5.2. Time Metrices

Image quality affects the temporal performance of biometric feature extraction from quantum pictures and quantum-resistant systems for PQC identity authentication systems. The metrics depending on feature performance are:

5.2.1. Enrollment Time

It is the amount of time the system takes to scan and save your distinct image [28]. Equation 19 calculates the total time needed for system enrolment.

$$T_{enroll} = T_{capture} + T_{extract\ feature} + T_{temp} + T_{save} \quad (19)$$

T_{enroll} is the user's enrolment time; $T_{capture}$ is the user's image capture time; $T_{extract\ feature}$ is the feature extraction time from an image; T_{temp} is the template generating time; and T_{save} is the template writing time into a database.

5.2.2. Matching Time

It is the amount of time the system takes to verify your identity by comparing your login biometric information with an image that has been saved in the database [29]. Equation 20 determines the matching time.

$$T_{match} = N \times \frac{\text{end time} - \text{start time}}{\text{iterations}} \quad (20)$$

Where N is the total quantity of photos in the system, and T_{match} is the total time the system takes to match one image.

5.2.3. Throughput Time

It is the amount of time needed by the system to complete an authentication procedure, from registration to verification [30]. Equation 21 is used to compute the throughput time.

$$T_{throughput} = T_{capture} + T_{processing} + T_{match} + T_{net} + T_{resp} \quad (21)$$

$T_{capture}$ is the amount of time it takes the system to take a picture of a user, the time needed to match an image with an existing image is represented by T_{net}, whereas the overall time needed to match an image is represented by T_{match} and $T_{processing}$ represents the time required to process an image with an existing picture, and T_{resp} is the amount of time it takes to calculate the score and send the decision.

5.2.4. Feature Extraction Time

The system takes time to transform unprocessed data into quantum states [31]. Equation 22 calculates the feature extraction time.

$$|\psi> = \sum_{j=0}^{63} c_j |j> \quad (22)$$

The image has 16 spatial coordinates because we are transforming it to 4x4. The system maps to a 6-qubit space with 26 possible states because each requires three color pixels.

5.2.5.Encryption Time

It is the amount of time required for the McEcliece PQC technique to multiply and alter the matrices that result from feature extraction utilizing quantum computing [32]. Equation 23 is used to calculate it.

$$T_{enc} = (c.n).t_{op} \quad (23)$$

Where t_{op} is the speed of a single computer operation, c is the size of biometric feature data, n is the size of the security key, and T_{enc} is the encryption time.

5.2.6. Decryption Time

It is the amount of time the system takes for the user to upload an image after random errors have been eliminated. Patterson's algorithm is used in the McEliece PQC approach [33].

Equation 24 is used to calculate it.

$$T_{dec} = (2t.n + t^2).t_{op} \quad (24)$$

Where the size of the post-quantum public key block is n, t is the error-correcting capability, and T_{dec} is the decryption time.

5.3. Performance Metrices

In essence, the suggested model is employed for identification verification. Strong protection against eavesdropping is achieved by this substance. The suggested design security is assessed using the F1-Score, Recall, and Precision metrics.

5.3.1. Precision

It demonstrates the ability of the model to reduce false positives by quantifying the proportion of accurate positive predictions among all positive predictions [34]. Equation 25 is used to calculate it.

$$\text{Precision} = \frac{\text{TP}}{\text{TP+FP}} \quad (25)$$

Where FP stands for False Positives and TP for True Positives.

5.3.2. Recall

The capacity of the model to accurately detect genuine positives among all actual positives is measured by what is known as sensitivity [35]. Equation 26 is used to calculate it.

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \quad (26)$$

Where FN is the false negatives, and TP is the true positives.

5.3.3. F1-Score

It offered a fair evaluation of a model's recall and precision. It functioned as a trustworthy gauge of the model's overall performance [36]. Equation 27 is used to calculate it.

$$\text{F1-Score} = 2 * \frac{\text{Precision} * \text{Recall}}{\text{Precision+Recall}} \quad (27)$$

6. Results/ Analysis and Discussion

Biometric information security can be greatly enhanced by using quantum computing in biometric identity authentication systems. An identity identification system uses the geometric features of the human face as its keys. Personal authentication is carried out by utilising the different traits that are retrieved from the face image. Real-world photos were used to test the suggested model in order to assess its performance and practical efficiency.

This section examines the suggested paradigm using performance, time, and security criteria. The accuracy, FAR, FRR, EER, ADR, HDA, FMR, and FNMR are among the security metrics we assess. We assess enrolment, matching, throughput, feature extraction, encryption, and decryption time in terms of time metrics. We assess performance metrics regarding F1-Score, Recall, and Precision.

6.1. Security Performance

An essential first stage in determining the efficacy and efficiency of the suggested model's solutions is security evaluation.

Table 2. Security based evaluation of the proposed model

Metrices	Results
Accuracy (in %)	99.09
False Acceptance Rate	0.0000
False Rejection Rate	0.0182
Equal Error Rate	0.0091
Attack Detection Rate (in %)	100
Hamming Distance Analysis	2.7
False Match Rate	0.0000
False Non-Match Rate	0.0182

This identifies and evaluates the particular metrics used to gauge the suggested model's security performance. Table 2 illustrates that the suggested model achieves 99.09% accuracy, 0.0000 false acceptance rate, 0.0182 false rejection rate, 0.0091 equal error rate, 100% attack detection rate, 2.7 hamming distance analysis, 0.0000 false match rate, and 0.0182 false non-match rate.

6.2. Time Performance

In the suggested approach, the time factor is the most frequently utilised statistic. Table 3 displays the enrolment time of 52.77 msec, matching time of 0.19 msec, throughput time of 77.15 msec, features extracted time of 2.41 msec, encryption time of 49.78 msec, and decryption time of 12.77 msec based on the suggested model.

Table 3. Time based evaluation of the proposed model

Metrices	Results
Enrolment Time (msec)	52.77
Matching Time (msec)	0.19
Throughput Time (msec)	77.15
Feature Extracted Time (msec)	2.41
Encryption Time (msec)	49.78
Decryption Time (msec)	12.77

6.3. Performance

The third preferred metric for assessing the solutions is performance.

Table 4. Performance based evaluation of the proposed model

Metrices	Results
Precision (in %)	100
Recall	98.18
F1-Score	0.9908

As indicated in Table 4, we have determined the recall, F1-Score, and precision for the suggested model. The values are 98.18%, 99.08%, and 100%.

6.4. Comparison of Cryptographic Technique used in Biometric Security

For biometric security, it is crucial to take into account critical factors like accuracy, encryption time, and decryption time when analysing the suggested job. The suggested model is significantly better in terms of accuracy when compared to other cryptographic techniques utilized in biometric security approaches (Hyperlattice-AES, MCC Hashing, Modified Logistic Map, Probability Confidence Matrix, and TNCB), as shown in Table 5.

Table 5. Comparison of proposed model with different techniques for biometric authentication system [37]

Cryptographic technique for biometric security	Accuracy	Encryption Time (msec)	Decryption Time (msec)
Hyperlattice-AES	96.3	0.054	0.13
MCC Hashing	88.0	0.47	0.44
Modified logistic Map	97.0	1.17	1.25
Probability Confidence Matrix	97.0	1.17	1.25
TNCB	91.1	1.20	0.27
Proposed Model	99.09	49.78	12.77

7. Graphical Representation

We will use a graph to illustrate our findings, analysis, and debate in this section. First, we will display security-based performance results using two graphs: the accuracy and attack detection rate-based graph and the FA, FR, EE, FM, and FNM rates. The suggested model has an accuracy of 99.09% and an attack detection rate of 100%, as shown in Figure 4.

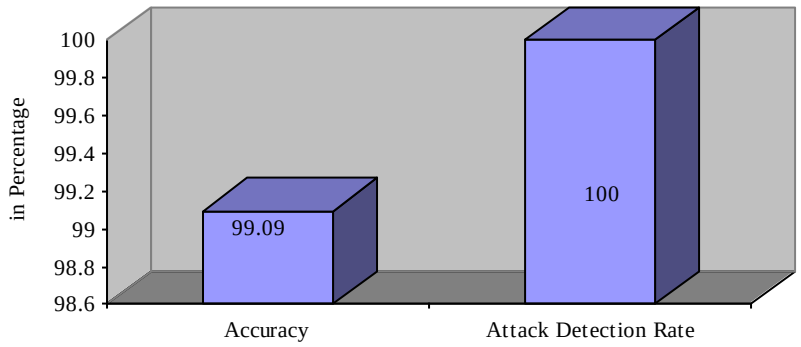

Fig. 4 Accuracy and attack detection rate of the proposed model

The suggested model's FA, FR, EE, FM, and FNM rates are 0.0000, 0.0182, 0.0091, 0.0000, and 0.0182, respectively, as shown in Figure 5.

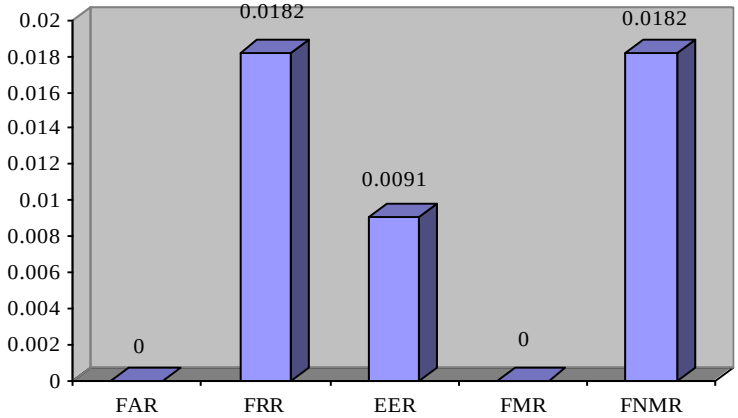

Fig. 5 Security based performance of the proposed model

The suggested model's enrolment, matching, throughput, feature extraction, encryption, and decryption times are 52.77, 0.19, 77.15, 2.41, 49.78, and 12.77, respectively, as shown in Figure 6.

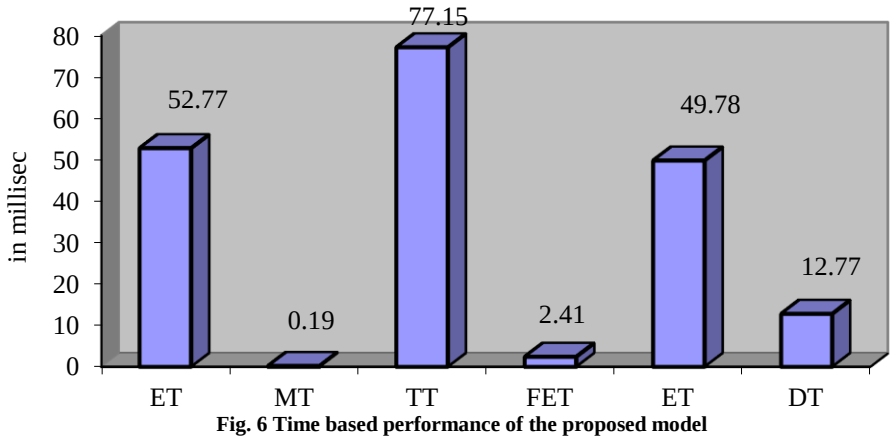

Fig. 6 Time based performance of the proposed model

The suggested design F1-Score, Precision, and Recall are 99.08%, 100% and 98.18%, respectively, as shown in Figure 7.

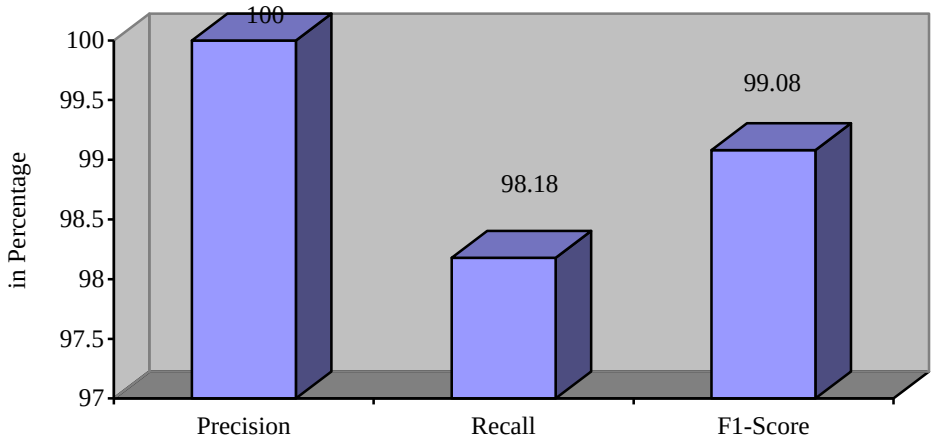

Fig. 7 Performance of the proposed model

8. Conclusion

The security of private or sensitive data was considerably simpler in the past than it is now, or more accurately, in the past 200 years, when even brief but crucial information frequently changed the course of human history and warfare. The fact that only authorised individuals have access to this information and that no one else has the chance to grant access in any other manner is also the primary reason why technology is a major focus nowadays. Everywhere, biometrics are commonly used to verify a person's identity. Performance is significantly improved by the suggested approach. In this research, we have used McEcliece PQC technique for encryption and decryption. The results analysis and discussion we have done based on the accuracy, attack detection rate, false acceptance, false rejection, equal error, false match, and false non-match rates and enrolment, matching, throughput, feature extraction, encryption, and decryption time, and precision, recall, and F1-Score.

References

[1] David Palma, and Pier Luca Montessoro, "A Post-Quantum Cryptography Enabled Feature-Level Fusion Framework for Privacy-Preserving Multimodal Biometric Recognition," *Cryptography*, vol. 9, no. 4, pp. 1-30, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[2] Tooba Qasim et al., "Quantum Secure Biometric Authentication in Decentralised Systems," *2025 IEEE International Joint Conference on Biometrics (IJCB)*, Osaka, Japan, pp. 1-9, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] Roayat Ismail Abdelfatah, "Robust Biometric Identity Authentication Scheme using Quantum Voice Encryption and Quantum Secure Direct Communications for Cybersecurity," *Journal of King Saud University Computer and Information Sciences*, vol. 36, pp. 1-22, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[4] Archana G. Pai et al., "A New Feature Set for Texture-based Classification of Remotely Sensed Images in a Quantum Framework," *Journal of Imaging*, vol. 12, no. 4, pp. 1-30, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[5] Satinder Singh et al., "Quantum-Enhanced Facial Biometrics: A Hybrid Framework with Post-Quantum Security," *Quantum Reports*, vol. 7, no. 4, pp. 1-14, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[6] Praveen Kumar Reddy Gujjala, "Quantum-Enhanced Multi-Factor Authentication Framework for Digital Banking Systems: A Post-Quantum Cryptographic Approach," *International Journal for Multidisciplinary Research*, vol. 5, no. 6, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Birir Kipchirchir Sospeter, Wilfred Odoyo, and Laura Akinyi, "Quantum-Assistant Fingerprint Biometrics: A Novel Approach to Fast and Accurate Feature Extraction and Synthetic Generation," *International Conference on Information Technology and Security*, vol. 5, no. 1, pp. 613-620, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Farhaan Khan et al, "A Quantum-Hybrid Framework for Enhanced Deepfake Detection: Integrating QAOA-based Feature Selection With Quantum-Inspired Attention Mechanisms," *IEEE Access*, vol. 14, pp. 17853-17873, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[9] Liu-Jun Wang et al., "Experimental Authentication of Quantum Key Distribution with Post-Quantum Cryptography," *NPJ Quantum Information*, vol. 7, pp. 1-7, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Yang Yang et al, "Post-Quantum Identity-based Authenticated Multiple Key Agreement Protocol," *ETRI Journal*, vol. 45, no. 6, pp. 1090-1102, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Yong Wang, and Eddie Shahril Ismail, "A Two-Tier Authentication Framework Integrating Post-Quantum Cryptography with AI-based Emotion Recognition," *Contemporary Mathematics*, vol. 6, no. 5, pp. 6081-6106 2025. [CrossRef] [Google Scholar] [Publisher Link]

[12] Shakti Mehta, and Krunal Vaghela, "Hybrid Deep Learning Approaches for Feature Extraction and Cancelable Template Generation in Iris Recognition," *IEEE Communications Standards Magazine*, vol. 6, pp. 1-34, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[13] V. Thenmozhi, S. Veluchamy, and Neeshna Lakshmi H, "Cancelable Biometric Template Generation using Deep Learning-based Secure Transforms," *2025 International Conference on Intelligent Innovations in Engineering and Technology (ICIIET)*, Coimbatore, India, pp. 1-5, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[14] Satinder Singh et al, "Quantum-Enhanced Facial Biometrics: A Hybrid Framework with Post-Quantum Security," *Quantum Reports*, vol. 7, no. 4, pp. 1-14, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sang-Yoon Chang, and Qaiser Khan, "Post-Quantum Cryptography in Networking Protocols: Challenges, Solutions, and Future Directions," *MDPI-Cryptography*, vol. 10, no. 1, pp. 1-24, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[16] Sana Farooq et al., "Analyzing Post-Quantum Cryptography Algorithms Efficiency for Transport Security Layer," *Computers and Electrical Engineering*, vol. 125, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[17] Babatunde Ojetunde et al., "A Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication," *Network*, vol. 5, no. 2, pp. 1-34, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[18] Peter Pekarčík, and Eva Chovancová, "Post-Quantum Encryption Algorithms," *Acta Electrotechnica et Informatica*, vol. 25, no. 3, pp. 16-24, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[19] Veeresh R. Maned et al., "Enhancing Quantum Key Distribution via McEliece-based hybrid PQC-QKD architecture," *EPJ Quantum Technology*, vol. 13, no. 33, pp. 1-20, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abel C.H. Chen, "PQCMC: Post-Quantum Cryptography McEliece-Chen Implicit Certificate Scheme," *arXiv Preprint*, pp. 1-5, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Reena Garg, Pooja Pathak, and Manu Pratap Singh, "A Multimodal Biometric Recognition System based on Fingerprints, Iris and ECG via Swin Transformer and CNN Model," *Systems and Soft Computing*, vol. 7, pp. 1-12, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[22] Noor Basha Shaik Riyaz, and V. Parthipan, "A Novel Prediction Analysing the False Acceptance Rate and False Rejection Rate using CNN Model to Improve the Accuracy for Iris Recognition System for Biometric Security in Clouds Comparing with Traditional Inception Model," *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Greater Noida, India, pp. 690-694, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Fatima Zohra Allam, Latifa Hamami-Mitiche, and Hicham Bousbia-Salah, "Evaluation and Comparison of the Performance of Biometric Recognition," *International Journal of Industrial Engineering & Production Research*, vol. 33, no. 1, pp. 1-12, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Swimpy Pahuja, and Navdeep Goel, "Multimodal Biometric Authentication: A Review," *AI Communications*, vol. 37, no. 4, pp. 525-547, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[25] Pavani Chitrapu, Mahesh Kumar Morampudi, and Hemantha Kumar Kalluri, "A Secure and Explainable Multimodal Biometric System using Trust Adaptive Fusion for Face and Fingerprint," *Scientific Reports*, vol. 16, pp. 1-23, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[26] Smita Khairnar et al., "Advanced Techniques for Biometric Authentication: Leveraging Deep Learning and Explainable AI," *IEEE Access*, vol. 12, pp. 153580-153595, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Jeyalakshmi Vijayarajan, "Multi-Biometric System based on the Fusion of Fingerprint and Finger-Vein," *Electronic Letters on Computer Vision and Image Analysis*, vol. 23, no. 1, pp. 32-46, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] S. Jenifa Sabeena, and S. Balamurugan "Biometrics Real-Time Authentication and Applications," *Journal of Applied Bioanalysis*, vol. 11, no. 13s, pp. 471-474, 2025. [Google Scholar] [Publisher Link]

[29] Ayman Iskandar al., "Biometric Systems for Identification and Verification Scenarios using Spatial Footsteps Components," *Neural Computing and Applications*, vol. 36, pp. 3817-3836, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Diego Aguilar et al, "PPG-based Biometric Authentication: A Review On Architectures, Datasets, Attacks and Security Challenges," *Computational and Structural Biotechnology Journal*, vol. 28, pp. 511-528, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[31] Ruihan Hu, Zhiri Tang, and Rui Yang, "QE-DAL: A Quantum Image Feature Extraction with Dense Distribution-Aware Learning Framework for Object Counting and Localization," *Applied Soft Computing*, vol. 138, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[32] Galiya Yesmagambetova et al., "Applications of Quantum Computing in Biometric Information Security," *Journal of Theoretical and Applied Information Technology*, vol. 103, no. 12, pp. 5213-5226, 2025. [Publisher Link]

[33] Yooan Lee, Taeyun Nam, and Sanghyeok Yune, "Encryption and Decryption Technology for Quantum Computing," *International Journal of Business Studies and Innovation*, vol. 4, no. 3, pp. 8-13, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[34] Nebil Vural Gündoğan, and Baris Celiktas, "Keystroke Dynamics for Authentication: A Systematic Comparative Analysis of Machine Learning, Deep Learning, Hybrid, and Quantum Approaches," *Black Sea Journal of Engineering and Science*, vol. 9, no. 3, pp. 1503-1522, 2026. [CrossRef] [Google Scholar] [Publisher Link]

[35] Akram Al-Rumaim, and Jyoti D. Pawar, "Enhancing User Authentication: An Approach Utilizing Context-Based Fingerprinting with Random Forest Algorithm," *IEEE Access*, vol. 12, pp. 110850-110861, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[36] Ahmed Omar, and Tarek Abd El-Hafeez, "Quantum Computing and Machine Learning for Arabic Language Sentiment Classification in Social Media," *Scientific Reports*, vol. 13, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] Aanjankumar Sureshkumar et al., "A Lattice-Integrated AES Framework for Ultra-Secure Biometric Protection on Resource-Constrained Edge Devices," *Scientific Reports*, vol. 16, pp. 1-22, 2026. [CrossRef] [Google Scholar] [Publisher Link]