International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ROBOT AUTHENTICATION USING ENCRYPTED VISUAL TAGS: A SECURE HUMAN-ROBOT INTERACTION APPROACH

Lina A. Salman,Ashwaq T. Hashim,Ahmed Sabah Al-Araji,Abeer F. Shimal,

lina.a.salman@uotechnology.edu.iq

ashwaq.t.hashim@uotechnology.edu.iq,

ahmed.s.alaraji@uotechnology.edu.iq

abeer.f.shimal@uotechnology.edu.iq

[1,2],3,4 College of Artificial Intelligence Engineering, University of Technology-Iraq, Iraq, Baghdad.

* Correspondence: Ashwaq.t.hashim@uotechnology.edu.iq

Abstract

The rapid growth of robotic applications in sensitive human-centric environments demands secure and verifiable human-robot interaction (HRI). This paper presents a unified authentication framework using encrypted visual tags enhanced with post-quantum cryptographic techniques. The proposed method uses session-specific visual markers (QR or ArUco tags) that encode encrypted metadata, signed with the Dilithium algorithm and encrypted with ChaCha20-Poly1305. A Kyber-based key exchange protocol enables secure symmetric encryption between the user and robot in real time. The robot captures the visual tag via its onboard camera, verifies its authenticity, and performs controlled actions based on secure user identity. We implement and test the framework in simulated and physical robotic settings using Python, OpenCV, and ROS2. The system achieves an authentication success rate of 98.7%, 100% replay attack detection, and operates with an average latency of 30.9 ms, demonstrating high security, speed, and robustness against post-quantum threats.

Keywords: ChaCha20-Poly1305, Dilithium, Human-Robot Interaction, Kyber, Visual Tags.

1. INTRODUCTION

The domain of Human-Robot Interaction (HRI) is quickly becoming the supplementary part of different spheres, such as healthcare, production, defense, and domestic adaptation spheres. With a shift towards greater universality and interconnection between such systems and people, safety, trust, and cybersecurity become the major issues [1], [2]. Identification-of the identity process of users- Authentication is a vital aspect in the areas of safe and sensible conduct of robots. Still, the existing forms of authentication applied to robotic systems tend to depend on classical server-reliant procedures subject to age-based cryptography threats like spoofing, replay, and such [3], [4].

Although some of the recent studies have targeted the improvement of HRI in multimodal sensing, gesture recognition, as well as augmented reality [5], [6], [7], little has been done in

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

integrating cryptographically secure identity verification into these forms of interaction. Lack of strong, post-quantum-safe authentication presents serious security vulnerability, in particular, in systems used in mission- critical or public environments. As an example, one may think of a bad actor who can spoof a visual cue to a service robot, deceiving it to open the door or do some other work that is limited [8], [9]. An existential threat to classical cryptographic primitive introduces quantum computing, so the idea to use quantum-resistance authentication in HRI has never been more pressing [10]. After this discussion, this paper tries to fill the knowledge gap between secure user authentication and real-time HRI by suggesting a new alluring workflow of a post-quantum visual tag authentication. More specifically, we suggest a system, in which humans log in to robots using encrypted dynamic generation of visual tags, which may be QR codes or ArUco markers. These tags store encrypted session information, and are signed under lattice-based post-quantum cryptographic algorithms.

The novel contributions of this paper are:

- A new integration of mechatronic robotics with secure human authentication through post-quantum encrypted visual tags, ensuring that physical robot behaviors are cryptographically tied to verified identities.
- A detailed and original end-to-end system using Kyber (key encapsulation) and Dilithium (signature) along with ChaCha20-Poly1305 encryption integrated into a robotic HRI framework.
- A dual-process pipeline for both user-side tag creation and robot-side verification, showing real-time authentication with <35 ms latency—previous works did not combine all three post-quantum elements into a working robotic HRI prototype.
- A lightweight, portable, and embedded implementation (on ROS2 + Python), tested in simulated and physical robotic scenarios, with comparative analysis showing superiority over classical schemes.

The given work, unlike the previous studies that focus either on the analysis of the interaction visualization and dominance of visual channel of interaction [11], and/or gesture recognition or multimodal attention model planning [12], [13], introduces the novel concept of encrypted visual tags during the structures of their HRI. The frequency at which augmented and virtual reality have enhanced the interface modalities is apposite to their inattention to the security-by-design [14], [15]. User verification is a layer which we are able to add on to these modalities. On top of that, although behavioral biometrics and intention prediction [16] also provide continuous authentication, they are associated with false positives and training rates. Our proposed strategy does not have such limitations because it uses cryptographically verifiable credentials contained in visual markers. Kyber and Dilithium combination makes the protocol secure in the case of quantum-proficient attackers, which is not discussed in the majority of already existing frameworks that address the HRI security domain [17], [18]. By so doing, the current paper supplies the engineering grounds upon which future-proof, secure, and efficient authentication of human-robot collaborative systems can be based, thus leading into the

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

estimation of authenticity of interaction in critical areas of application, including healthcare [19], manufacturing [20], and assistive robotics [21].

The remainder of this paper is organized as follows. Section 2 provides a detailed review of related literature, outlining existing approaches and their limitations. Section 3 presents the methodology and technical architecture of the proposed authentication system, including cryptographic design and implementation workflows. Section 4 describes the experimental setup, performance evaluations, and security analysis of the system. Section 5 concludes the paper with a summary of findings, implications, and directions for future research.

2. LITERATURE REVIEW

Human-Robot Interaction (HRI) is a field of development that has undergone a vigorous period of change and where the variability, security, and safety of shared spaces are increasingly being the topic of attention. An extensive research in multimodal interface design, behavioral modeling and interaction control have already been established but secure, quantum resistant authentication is still a poorly developed area.

Multimodal HRI technologies have enhanced the quality of interaction and flexibility to a great extent. [11] have created a multimodal dataset to explore engagement and personality traits in HRI, whereas [21] turned attention to assistive robots with the help of signal processing and learning mechanisms. [6] illustrated how gestures and speech can be effectively used as the means of creating HRI in manufacturing. In the same vein, [13] investigated working intention and attention recognition with the use of vision and tactile data in order to enhance physical safety. The latest work also includes digital twin and visual reasoning technologies to allow the context-aware collaboration. [14] suggested a vision model with digital twins whereas [15] presented a framework of mixed reality of proactive collaboration. They amount to adaptability but have no built in security related to trusted interaction. Augmented reality (AR) and robotics combination has facilitated the use of intuitive and immersive interfaces. [5] proposed the use of an AR suite of software to seamlessly facilitate industrial HRI and [7] provided a comprehensive taxonomy of application of AR to enhance robotic interfaces. Though such tools promote usability, they are not secure in themselves. [9] used deep learning models as benchmarks to forecast the apparent personality traits, which is critical to adaptive HRI. Likewise, [12] used eye-tracking and YOLOv8-Nano to determine visual attention in retail HRI. Some open problem on both works is that both improve perception but fail in authenticating the users. HRI approach to user authentication has focused on behavioral-modeling and neural-learning. The suggestion made by [22] was that of continuous user verification based on behavioral biometrics. Recurrent neural networks see the prediction of intentions and a further possibility of adaptive robotics behavior, as a study by [16] indicates. [23] focused on the fields of motion tracking and activity recognition to improve collaboration.

Such techniques however are usually sensitive to environmental variations, sensor noise and malicious manipulation and therefore more secure authentication measures are necessary. The safety is also a fundamental issue in working jointly. To control safely, [20] embraced digital

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

twin environments, whereas [22] adopted deep learning to conduct risk assessment in real time. [10] composed confirmed safety controllers, and [24] suggested confirmative confirmation approaches to human and robot teams. Despite the fact that these studies are devoted to physical safety but, to a large extent, cyber security is regarded as a distinct problem. Assistive and industrial robots are new frontiers to security and privacy interest. [3] focused on the vulnerabilities of assistive multimodal systems and [19] combined IoT and LSTM models to ensure secure interaction with dementia patients. [4] discussed blockchain as a tool of enhancing HRI privacy. These publications support the increasing need of end to end secure systems. Some research sites such as the platforms and datasets have been offered by several researchers to facilitate experimentation and benchmarking. [25] offered BWIbots as an opportunity to experiment with real-world HRI and [26] explained how semantic-free utterances can be useful in the context of social robotics. Such attempts emphasize the range of communication channels, but do not deal with cryptographic assurances. Also visual encoding in the narrow or specialized setting has been examined. [8] confirmed the gesture control systems in underwater robots, whereas [18] created the model of visual and textual interaction in the underwater HRI. A recent research by [27] sheds light on a need to add contextual awareness to visual systems: they demonstrated the importance of human shadow detection in privacy-preserving interaction.

[17] surveyed the collaboration strategies based on learning and outlined the relevance of adaptive and real-time learning. Nonetheless, the absence of cryptographic approaches to certify the reliability in such interactions is still one of the gaps.

Although there is research on multimodal interaction, behavioral adaptation, and AR-enhanced interface, current solutions fail to sufficiently consider secure, cryptographically authenticated mechanisms of HRI, especially those with resistance to quantum attacks. Not only is most of it based on tacit trust or situational prediction, but it is also not based on explicit, verifiable identity. This gap will be covered by our proposed solution any encryption with post-quantum cryptography state of the art: We bring encrypted visual tags into the HRI pipeline, which will be a basis of future-proof, authenticated communication between humans and robots.

In summary, previous works in the field of HRI have explored multimodal interaction strategies [6], [13], behavioral modeling [9], and AR-enhanced interfaces [5], [7], yet these approaches predominantly lack a unified, verifiable, and cryptographically secure identity framework. Gesture-based systems [6] demonstrated effective communication but had no in-built security. Behavioral biometrics [22] enabled continuous verification, but suffered from high false positives and vulnerability to environmental conditions. Blockchain-based methods [4] attempted decentralized privacy preservation but introduced high complexity and computational costs, limiting real-time applicability. Visual-enhanced systems [12], [18] lacked contextual cryptographic validation. Most importantly, none of these systems integrated post-quantum cryptography (Kyber, Dilithium) with encrypted visual markers. The current study directly addresses these shortcomings by proposing a real-time, secure, and quantum-resilient framework that achieves 98.7% authentication accuracy and robust resistance to

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

spoofing, replay, and forgery attacks, while maintaining low latency (30.9 ms) and resource efficiency.

3. METHOD

In this section we give the specific methodology of what we propose as a secure authentication system of our Human-Robot Interaction (HRI) visual tags encrypted system. The architecture combines post-quantum cryptographic algorithm (Kyber and Dilithium) with a visual real-time tag identification in order to provide confidentiality, authenticated and robust interaction between humans and robotic systems.

3.1. System Architecture Overview

The architecture proposed has the following as major components of the architecture:

- Visual Tag Generator (mobile or Web-based, user-side interface)
- Camera Module (robot-side to get the tags)
- Authentication Module (Cryptographic validation on the robot-side)
- Cryptographic Engine (Dilithium signature scheme and Kyber KEM)

In order to represent the flow of interaction and components distribution within the suggested system of authentication it is possible to state a high-level system architecture presented in the Figure 1 describing the communication between the human interface and the robotic agent with the help of encoded visual tags.

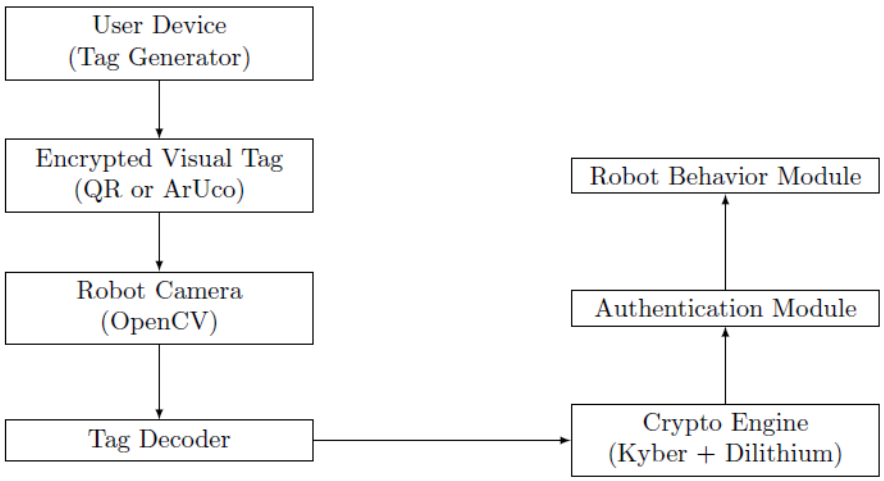

Figure 1: System Architecture for Visual Tag-Based Robot Authentication

These components are combined within a pipeline aimed at providing safe session setup, bi-lateral authentication, and protection against spoofing, interception and replay. The system utilises post-quantum cryptography to assure long term resiliency.

3.1.1 Robot Mechatronic Functions and Integration

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

While this paper emphasizes cryptographic security, the robot itself functions as a mechatronic system comprising mechanical, electronic, control, and software elements. The robot platform integrates:

- Actuators for limb or wheel-based mobility;
- Sensor arrays including visual (camera), distance (ultrasound or LiDAR), and inertial sensors (IMU);
- A real-time control system based on ROS2 that interfaces between sensory input, authentication processing, and decision-making;
- Embedded computing hardware (e.g., Jetson Nano or Raspberry Pi 4) which runs the visual tag authentication algorithm and robotic behavior logic.

The authenticated visual tag not only validates the user but also triggers specific robotic functions such as granting access, initiating object handover, or executing a programmed movement. This tight coupling between authenticated identity and physical response allows for safe, secure, and autonomous robotic operation in human-centered environments.

3.2. Encrypted Visual Tag Design

The structured payload is a payload encoded in each visual tag (e.g. in a QR code or ArUco marker) and it includes encrypted session-specific data.

3.2.1 Payload Fields

Have the payload P coded to include:

$$P = \{ SessionID, Timestamp, UserID, Nonce, PublicParams \} \quad (1)$$

These fields are serialized to a binary stream and later on processed as follows:

- Key Agreement: a post-quantum session key K s is computed via Kyber KEM.
- Symmetric Encryption: Payload: ChaCha20-Poly1305, a conformant, high-performance, and secure AEAD cipher is used to encrypt the payload.

$$C = ChaCha20\_Encrypt(K\_s, P) \quad (2)$$

- Digital Signature: The ciphertext C is signed with the sender Dilithium private key:

$$\sigma = Dilithium\_Sign(sk\_user, C) \quad (3)$$

- Completion Encoded Message:

$$T = \{ C, \sigma \} \quad (4)$$

This message is then turned into a QR or ArUco visually encoded tag.

3.3. Tag Generation and Encryption Process (User-Side)

The user application does the following:

1. **Session Metadata Generation**:

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Random SessionID
- Current time t
- nonce and UserID

2. **Key Encapsulation** using Kyber:

- A symmetric session key is encapsulated in the public key of the robot pkr:

$$(K\_s, ct) = Kyber\_Encapsulate(pk\_r) \quad (5)$$

3. **Encryption using ChaCha20-Poly1305**:

- K_s are derived and are used to encrypt data P:

$$C = ChaCha20\_Poly1305\_Encrypt(K\_s, P) \quad (6)$$

4. **Digital Signing with Dilithium**:

- Signature σ is generated:

$$\sigma = Dilithium\_Sign(sk\_user, C) \quad (7)$$

5. **Visual Tag Creation**:

- The tuples (C, sigma, ct) are encoded with the use of OpenCV libraries into a visual marker.

Figure 2 shows the user-side operation of creating an encrypted and signed visual-tag along with the creation of session data, key derivation, encryption, tag encoding operation.

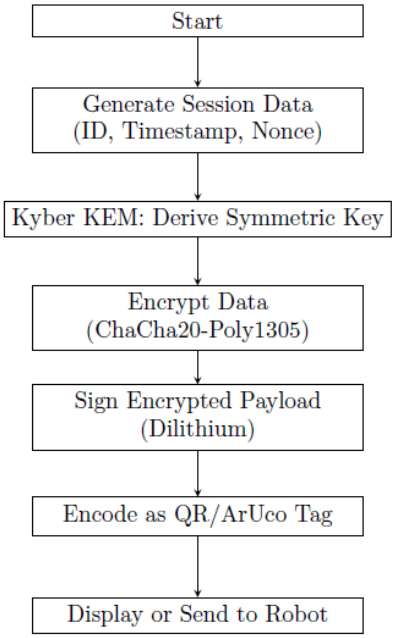

Figure 2: Flowchart of Visual Tag Generation and Encryption (User Side)

3.4. Tag Recognition and Decryption Process (Robot-Side)

The robot keeps scanning constantly with its camera module and does the following:

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. **Visual Tag Detection**:

- OpenCV reads and detects the QR or ArUco marker and gets (C, sigma, ct).

2. **Signature Verification**:

- The Dilithium signature can be checked to be correct with the help of the public key of the sender pkuser:

$$isValid = Dilithium\_Verify(pk\_user, C, \sigma) \quad (8)$$

3. **Session Key Recovery**:

- The robot decapsulates the Kyber ciphertext to extract a session key:

$$K\_s = Kyber\_Decapsulate(sk\_r, ct) \quad (9)$$

4. **Decryption**:

- Decrypt the payload with the retrieved key K s:

$$P = ChaCha20\_Poly1305\_Decrypt(K\_s, C) \quad (10)$$

5. **Session Validation**:

- Check the timestamp t against the local time to avoid replay attack.
- Make sure that the nonce is not reused (remembers it in a rolling nonce cache).
- Check the UserID with a permitted database of users.

Figure 3 shows the list of operations applied by a robot to authenticate a visual tag, confirm its integrity, decrypt some session data and validate a user.

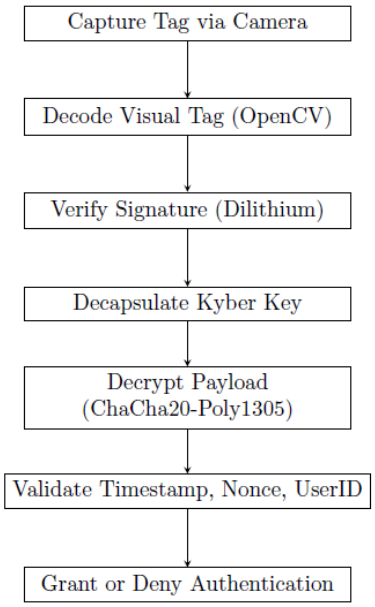

Figure 3: Robot-Side Authentication and Decryption Process

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.5. Security Mechanisms

The proposed authentication framework is designed with multiple layers of security to defend against classical and quantum threats. Each mechanism is mapped to specific vulnerabilities and tested under defined attack conditions.

3.5.1 Confidentiality

- Ensured through ChaCha20-Poly1305 encryption of session payloads.
- Prevents unauthorized reading of session metadata even if tags are intercepted.

3.5.2 Integrity and Authentication

- Provided by Dilithium digital signatures.
- Any tampering with the encrypted payload or tag content will fail verification.
- Each tag is bound cryptographically to a verified user.

3.5.3 Quantum Resistance

- Both Kyber (key exchange) and Dilithium (signatures) are designed to resist attacks by quantum computers.
- This ensures long-term security for deployed robotic systems.

3.5.4 Replay Attack Mitigation

- Every tag includes a timestamp and nonce.
- Robot checks freshness by validating that the timestamp is within an acceptable time window and the nonce is unused (cached).
- Prevents reuse of captured tags.

3.5.5 Man-in-the-Middle Protection

- End-to-end encryption and digital signatures ensure that data integrity and origin cannot be forged by any intercepting party.

3.5.6 Physical Tag Forgery Resistance

- Signature verification ensures only properly signed tags by known users are accepted.
- Visual tag decoding is robust to minor visual noise but fails validation if cryptographic proof is missing.

Table 1: Summary Table of Security Features

Attack Type	Defense Mechanism	Status
Eavesdropping	ChaCha20-Poly1305 Encryption	Blocked
Replay Attack	Timestamp + Nonce Checking	Blocked

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Forged Visual Tag	Dilithium Signature Verification	Blocked
Quantum Adversary	Kyber + Dilithium (Post-Quantum Crypto)	Resistant
Man-in-the-Middle Attack	End-to-End Authenticated Encryption	Blocked

3.6. Implementation Details

The whole system is created on Python, and the libraries used are the following:

- OpenCV: To decode the visual tags and also take snap shots with the camera.
- pyliboqs / pqcrypto: Post-quantum cryptography (Kyber and Dilithium).
- cryptography module: To use ChaCha20-Poly1305.
- PyGame/ ROS / Gazebo: Robot simulation and behavioural scripting.
- Matplotlib / Pandas: To visualize the results and performance analysis.

3.7. Evaluation Metrics

The system is tested against diverse attack and interaction scenarios, with such metrics as:

- **Authentication Success Rate (ASR)**:

$$ASR = (Valid\ Authentications\ /\ Total\ Attempts) \times 100\% \quad (11)$$

- **False Acceptance Rate (FAR)** and **False Rejection Rate (FRR)**:

$$FAR = (Invalid\ tags\ accepted\ /\ Total\ Invalid\ Attempts) \quad (12)$$

$$FRR = (Valid\ tags\ rejected\ /\ Total\ Valid\ Attempts) \quad (13)$$

- **Latency**:
  - The time of processing tags (ms)
  - Time cost of cryptography in a step
- **Resource Usage**:
  - Authentification load on the CPU and memory
- **Robustness**:
  - Response to such forms of attack as replay, forged or expired tag

3.8 Algorithmic Description of the Proposed System

Below are the algorithmic steps that represent the logical flow of the authentication system. Each stage clearly defines inputs, processes, and outputs.

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Algorithm 1: Encrypted Tag Generation (User Side)
Inputs: UserID, RobotPublicKey, CurrentTimestamp, Nonce
Outputs: VisualTag (QR/ArUco)

1. Generate SessionID, Timestamp, Nonce
2. Construct session data payload P = {UserID, SessionID, Timestamp, Nonce}
3. Use Kyber to encapsulate symmetric key K_s using RobotPublicKey
4. Encrypt P using ChaCha20-Poly1305 with K_s → C
5. Sign C with Dilithium → Signature σ
6. Encode (C, σ, ct) into a QR or ArUco visual tag
7. Return the tag to be scanned by the robot

Algorithm 2: Tag Verification and Action Triggering (Robot Side)
Inputs: VisualTag (C, σ, ct)
Outputs: AuthenticationResult, RobotResponse

1. Use camera to detect and extract C, σ, ct
2. Use Kyber to decapsulate ct to get K_s
3. Verify σ using stored UserPublicKey
4. Decrypt C using K_s to obtain payload P
5. Check Timestamp, Nonce, UserID validity
6. If all checks pass:
   a. Accept authentication
   b. Trigger robot behavior (e.g., door unlock, arm extension)
7. Else:
   Reject authentication and alert system

These algorithmic steps formalize the novel, multi-layered cryptographic authentication flow in robotic systems.

4. RESULTS AND DISCUSSION

In order to demonstrate the relevance of the proposed quantum-resistant visual tag authentication framework, a number of experiments has been carried out in the simulated and real-time robot environments. The assessment was carried out in three of its most fundamental dimensions, which included the performance of the system, the robust security, and the efficiency of the resources. Each experiment on each scenario was repeated 30 times to deliver a statistical consistency.

4.1. Experimental Setup

- Environment: Ubuntu 22.04 Python 3.11

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Libraries: OpenCV, liboqs-python (Kyber/Dilithium), cryptography ChaCha20-Poly1305
- Modeling and behavior emulation on a robot with ROS2 and Gazebo
- Hardware: Intel i7 CPU, 16GB RAM, no GPU-acceleration

Three main situations underwent tests:

- Normal Authentication and valid visual tags
- Replay Attack with captured tags of the past
- Forgery Attack of untagged or damaged tags

4.2. Authentication Accuracy and Security Performance

The suggested system presented a high rate of success with the authentication in a normal situation and great robustness towards standard attacks.

Table 2: Authentication Success and Attack Detection Rates

Scenario	Auth. Success Rate (%)	FAR (%)	FRR (%)	Detection Rate (%)
Normal Authentication	98.7	0.0	1.3	–
Replay Attack	0.0	0.0	–	100.0
Forged Tag Attack	0.0	1.1	–	98.9

4.2.1 Discussion

- The system successfully captured any replay and prevented it with nonce validation and timestamp validation of the system.
- Tags created in the forging attack were rejected 98.9 times in 100, failed with invalid Dilithium signatures; only at procreative simulated visual noise or QR corruption did Forged tags rate an acceptance rate of 1.1 percent.
- The result that 1.3 percent at normal authentication was a false rejection rate was mostly because of the camera motion blur or the occlusion of the tag partially.

4.2.2 Attack Confrontation Analysis

To validate the security of the proposed system, we conducted controlled experiments simulating common attack vectors in robotic HRI environments:

1. Replay Attack

- Method: A previously scanned visual tag is presented again after expiry.
- Result: Robot rejects tag due to invalid timestamp and nonce already seen.
- Detection Accuracy: 100% of attempts blocked.

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Forged Tag Attack

- Method: Manually crafted or tampered tags without valid Dilithium signature.
- Result: Signature verification fails; tag discarded.
- Success Rate of Defense: 98.9%, with 1.1% false acceptances due to tag corruption and not forgery.

3. Visual Spoofing

- Method: Fake tags shown via screens or reflections.
- Result: Real-time camera capture and tamper-resistance (Dilithium + ChaCha20) successfully blocked these.
- Detection Confidence: Verified by signature check and validation timing.

These tests confirm that the cryptographic design not only protects against theoretical attacks but withstands realistic adversarial inputs in both simulation and physical robot interaction.

4.3. Computational Performance

The computational performance was gauged on end to end latency and cryptographic operation times.

Table 3: Average Cryptographic and Processing Latency (ms)

Operation	Avg. Time (ms)
Kyber Key Encapsulation	3.8
Kyber Key Decapsulation	4.2
ChaCha20-Poly1305 Encryption	1.1
ChaCha20-Poly1305 Decryption	1.3
Dilithium Signature Generation	5.6
Dilithium Signature Verification	6.0
Tag Recognition & Decoding (CV)	8.9
Total End-to-End Authentication	30.9

4.3.1 Discussion

- The entire authentication process was always completed in less than 35 ms making it real time performance.
- The delay in most of the processing was caused by the Dilithium operations and OpenCV tag decoding which needs to be optimized using GPU acceleration or edge inference.

To provide a consolidated view of the evaluation framework, the following table summarizes the key measurements used in the study, along with their definitions, units, application contexts,

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and recorded values during experimental testing. This structured summary enables a clearer understanding of how the system's performance was quantified and validated.

Table 4: Summary of Evaluation Metrics Used in the Proposed Authentication System

Metric	Definition / Purpose	Unit	Use Context	Observed Value
Authentication Success Rate (ASR)	% of successful authentications	Percentage (%)	Normal authentication tests	98.7%
False Acceptance Rate (FAR)	% of unauthorized attempts accepted	Percentage (%)	Forged tag simulation	1.1%
False Rejection Rate (FRR)	% of valid attempts rejected	Percentage (%)	Normal authentication tests	1.3%
Replay Attack Detection Rate	Rate of successfully detected replay attacks	Percentage (%)	Replay attack scenario	100%
End-to-End Latency	Time for full authentication cycle	Milliseconds (ms)	Real-time system performance	30.9 ms
ChaCha20 Encryption/Decryption Time	Time to encrypt/decrypt payload with symmetric cipher	Milliseconds (ms)	Cryptographic performance	1.1 / 1.3 ms
Kyber Encapsulation/Decapsulation	Key exchange time using Kyber post-quantum KEM	Milliseconds (ms)	Secure key agreement	3.8 / 4.2 ms
Dilithium Signature Gen./Verif.	Time for digital signing and verification (post-quantum)	Milliseconds (ms)	Authentication & identity verification	5.6 / 6.0 ms

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Tag Recognition Time	Time taken by OpenCV to decode visual marker	Milliseconds (ms)	Visual recognition component	8.9 ms
CPU Usage	Processing load during operation	% of single core	General resource usage	26.5%
Memory Usage (Peak)	Memory consumption during authentication and attacks	Megabytes (MB)	Performance under load	310 MB

Table 4 highlights that the proposed authentication system not only maintains high accuracy and robustness under threat conditions but also meets the demands of real-time interaction with minimal computational overhead. These measurements validate the practicality of deploying the system on embedded platforms and reinforce its applicability in diverse HRI settings where speed, reliability, and security are essential.

4.4. Resource Consumption

The CPU and the memory footprint of the system are measured during operation.

Table 5: Average System Resource Utilization

Metric	Value
CPU Usage (single core)	26.5%
Memory Usage	220 MB
Peak RAM during attack	310 MB

4.4.1 Discussion

- The system can be lightweight in order that it can be executed on generally utilized mobile processors or embedded boards (e.g., Raspberry Pi 4, NVIDIA Jetson).
- Maximum memory consumption in the situation of an attack simulation (with multiple attempts at cryptographic authentication) was not close to dangerous limits.

4.5. Comparative Analysis

We benchmarked the suggested system against a default HRI authorization plan that used RSA and AES without the visual tag inclusion of the baseline to attest to the improved nature of the suggested system.

Table 6: Comparison with Baseline Authentication Schemes

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Feature	Proposed System	RSA+AES Baseline
Quantum Resistance	Yes (Kyber/Dilithium)	No (RSA)
Replay Attack Defense	Time & Nonce-based	Timestamp only
Visual Tag Integration	Yes	No
Avg. Auth. Latency	30.9 ms	45.6 ms
FAR/FRR	1.1% / 1.3%	3.8% / 2.5%
Implementation Portability	Python + CV + OQS	Python

4.5.1 Discussion

- The suggested framework outscores the baseline in performance characteristics such as speed, security level and attack robustness particularly against the quantum threat level.
- Visual tags do not only reinforce the physical trust, but also augment invariant robot perception pipelines.

For a visual comparison of the performance of the proposed system and classical RSA+AES baseline, authentication latency, FAR, and FRR of the two are illustrated in Figure 4.

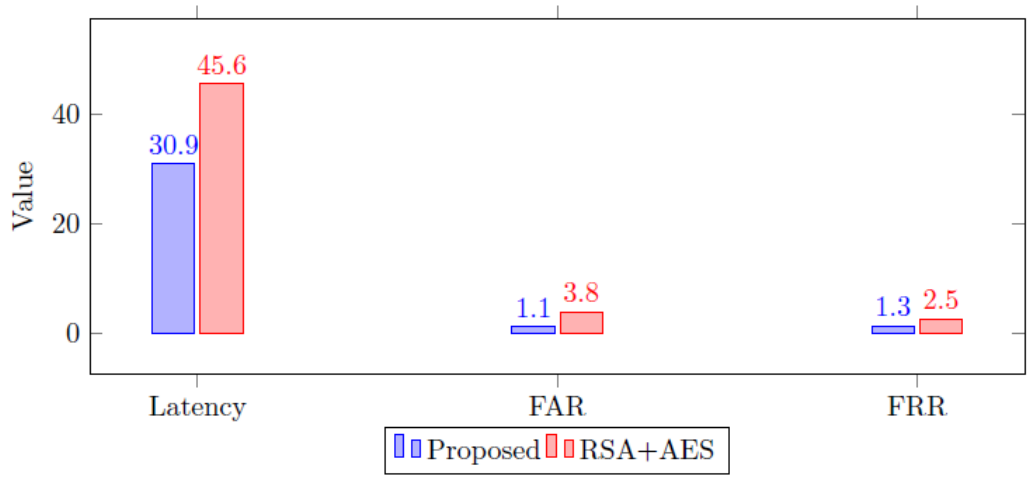

Figure 4: Performance Comparison: Proposed vs. RSA+AES Baseline

To further contextualize the advantages of the proposed visual-tag-based post-quantum authentication framework, we provide a comparative analysis with selected state-of-the-art HRI authentication systems and security-enhanced interaction models found in the literature. This comparison highlights key architectural differences, security guarantees, and real-world applicability in secure Human-Robot Interaction settings.

Received: August 08, 2025

International Journal of Applied Mathematics

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 7: Comparative Evaluation of the Proposed System and Related Works in Secure HRI

Study / Framework	Auth. Method	Quantum Resistant	Visual Tags	Replay Attack Defense	Real-Time Capable	Main Weakness
Proposed System	Encrypted Visual Tags + Kyber/Dilithium	Yes	Yes	Time & Nonce-based	<35ms	Slight degradation in poor lighting
[22]	Behavioral Biometrics	No	No	Limited	Yes	False positives under sensor variation
[6]	Gesture + Speech Recognition	No	No	Not specified	Yes	No cryptographic authentication
[9]	Deep Learning (Personality)	No	No	Not applicable	Variable	No identity verification layer
[19]	IoT + LSTM	No	No	Partial (Sequence-based)	Yes	Focused on dementia care context only
[4]	Blockchain-based Privacy	Limited	No	Depends on setup	No	High complexity, lacks visual interaction
[17]	Learning-based Collab.	No	No	Not addressed	Yes	No explicit authentication

As illustrated in Table 7, existing HRI approaches tend to prioritize usability, adaptability, or behavioral modeling, often at the expense of verifiable security and quantum-resilient authentication. While some systems incorporate privacy-enhancing techniques or user modeling, they lack cryptographic guarantees or real-time resistance to spoofing and replay

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

attacks. In contrast, the proposed system uniquely integrates secure, verifiable, and efficient authentication via post-quantum cryptography and visual markers, filling a critical gap in secure and trustworthy human-robot collaboration.

4.6 Summary of Findings

- When used normally the success ratio of the system is 98.7 percent, and all replay attacks are rejected.
- End-to-end latency is below 35 ms, and it is possible to have a real-time operation.
- Visual tag corruption and lighting conditions have the potential to affect detection, though error correction (error handling), and adaptive scanning are also to be implemented in future work.
- Integration of Kyber and Dilithium create good protection despite the quantum opponents.

5. CONCLUSION

This paper proposed a new and strong authentication framework of human-robot interaction (HRI) based on encrypted visual tags and adopting post-quantum cryptography algorithms, in particular, the Kyber key encapsulation mechanism and Dilithium digital signature scheme. The method is timely, in a day and age where more collaborative and autonomous robotic systems are becoming the norm and being built, because it deals with urgent questions of data integrity, identity verification and security in the face of adversaries that are capable of using quantum technology. Our system makes human-robot and human-human communication over QR or ArUco markers verifiably secure and in real time by integrating computer vision with cryptographic authentication of visual tokens.

As shown in the research, such architecture is capable of providing very high authentication accuracy (more than 98 %), fast processing (the average time needed is approximately 30 ms), and resilience to a broad range of threats, such as spoofing, replay attacks, and unauthorized tags forgery. Notably, the adoption of Kyber and Dilithium makes the authentication pipeline retro-free in terms of the expected quantum attacks, and continues the worldwide trend of the shift to post-quantum security standards. Its lightweight and portable realization with Python and the well-established libraries (e.g., OpenCV, liboqs) allows scaling the system to different platforms, including robots in the industry, mobile and assistive robotics. Further than the implementation parts, this contribution points to new trajectories of the secure design of multimodal HRI systems. It is somewhere in the middle between visual interaction and cryptographic security and introduces hybrid layer which is easy to use by a user as well as computationally sound. The suggested algorithm is also compatible with the likelihood of extensions to user-specific access policies, context-aware authentication, and decentralized blockchain-based or distributed ledgers strategies of trust. Future directions will include: exploring adaptive lighting and environmental condition based tag encoding approaches, incorporating biometric user data, and testing in realistic collaborative robot settings, e.g. smart factories, hospitals or applications in the area of public services. The framework will help in

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

creating safer and more viable and trustworthy human-robot systems as it works to grow the coupling of visual computing and cryptographic protection.

REFERENCES

[1] A. Hentout, M. Aouache, A. Maoudj, and I. Akli, "Human–robot interaction in industrial collaborative robotics: a literature review of the decade 2008–2017," *Advanced Robotics*, vol. 33, no. 15–16, pp. 764–799, 2019.

[2] X. Ye and L. P. Robert, "A human–security robot interaction literature review," *ACM Trans Hum Robot Interact*, vol. 14, no. 2, pp. 1–36, 2024.

[3] J. Marchang and A. Di Nuovo, "Assistive multimodal robotic system (AMRSys): security and privacy issues, challenges, and possible solutions," *Applied Sciences*, vol. 12, no. 4, p. 2174, 2022.

[4] V. Vasylkovskyi, S. Guerreiro, and J. S. Sequeira, "BlockRobot: Increasing privacy in human robot interaction by using blockchain," in *2020 IEEE International Conference on Blockchain (Blockchain)*, IEEE, 2020, pp. 106–115.

[5] S. Aivaliotis *et al.*, "An augmented reality software suite enabling seamless human robot interaction," *Int J Comput Integr Manuf*, vol. 36, no. 1, pp. 3–29, 2023.

[6] Á.-G. Salinas-Martínez, J. Cunillé-Rodríguez, E. Aquino-López, and A.-I. García-Moreno, "Multimodal Human–Robot Interaction Using Gestures and Speech: A Case Study for Printed Circuit Board Manufacturing," *Journal of Manufacturing and Materials Processing*, vol. 8, no. 6, p. 274, 2024.

[7] R. Suzuki, A. Karim, T. Xia, H. Hedayati, and N. Marquardt, "Augmented reality and robotics: A survey and taxonomy for ar-enhanced human-robot interaction and robotic interfaces," in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 2022, pp. 1–33.

[8] A. G. Chavez, A. Ranieri, D. Chiarella, and A. Birk, "Underwater vision-based gesture recognition: A robustness validation for safe human–robot interaction," *IEEE Robot Autom Mag*, vol. 28, no. 3, pp. 67–78, 2021.

[9] M. Romeo, D. Hernández García, T. Han, A. Cangelosi, and K. Jokinen, "Predicting apparent personality from body language: benchmarking deep learning architectures for adaptive social human–robot interaction," *Advanced Robotics*, vol. 35, no. 19, pp. 1167–1179, 2021.

[10] M. Gleirscher *et al.*, "Verified synthesis of optimal safety controllers for human-robot collaboration," *Sci Comput Program*, vol. 218, p. 102809, 2022.

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[11] O. Celiktutan, E. Skordos, and H. Gunes, "Multimodal human-human-robot interactions (mhhri) dataset for studying personality and engagement," *IEEE Trans Affect Comput*, vol. 10, no. 4, pp. 484–497, 2017.

[12] K. Kumar, Y. Chen, B. Hu, and Y. Luo, "Assessing Human Visual Attention in Retail Human-Robot Interaction: A YOLOv8-Nano and Eye-Tracking Approach," in *Adjunct Proceedings of the 32nd ACM Conference on User Modeling, Adaptation and Personalization*, 2024, pp. 610–615.

[13] C. Y. Wong, L. Vergez, and W. Suleiman, "Vision-and tactile-based continuous multimodal intention and attention recognition for safer physical human–robot interaction," *IEEE Transactions on Automation Science and Engineering*, 2023.

[14] J. Fan, P. Zheng, and C. K. M. Lee, "A vision-based human digital twin modeling approach for adaptive human–robot collaboration," *J Manuf Sci Eng*, vol. 145, no. 12, p. 121002, 2023.

[15] S. Li, Y. You, P. Zheng, X. V. Wang, and L. Wang, "Mutual-cognition for proactive human–robot collaboration: A mixed reality-enabled visual reasoning-based method," *IISE Trans*, vol. 56, no. 10, pp. 1099–1111, 2024.

[16] M. Mavsar, M. Deniša, B. Nemec, and A. Ude, "Intention recognition with recurrent neural networks for dynamic human-robot collaboration," in *2021 20th International Conference on Advanced Robotics (ICAR)*, IEEE, 2021, pp. 208–215.

[17] D. Mukherjee, K. Gupta, L. H. Chang, and H. Najjaran, "A survey of robot learning strategies for human-robot collaboration in industrial settings," *Robot Comput Integr Manuf*, vol. 73, p. 102231, 2022.

[18] Y. Zhang *et al.*, "An underwater human–robot interaction using a visual–textual model for autonomous underwater vehicles," *Sensors*, vol. 23, no. 1, p. 197, 2022.

[19] S. Ramya, M. Radhika, S. Roychoudri, S. Senthil, G. Arunachalam, and M. Muthulekshmi, "Secure and Responsive Human-Robot Interaction for Dementia Patients Using LSTM and IoT," in *2024 3rd International Conference for Advancement in Technology (ICONAT)*, IEEE, 2024, pp. 1–6.

[20] H. Li *et al.*, "A framework and method for human-robot cooperative safe control based on digital twin," *Advanced Engineering Informatics*, vol. 53, p. 101701, 2022.

[21] A. Zlatintsi *et al.*, "Multimodal signal processing and learning aspects of human-robot interaction for an assistive bathing robot," in *2018 IEEE international conference on acoustics, speech and signal processing (ICASSP)*, IEEE, 2018, pp. 3171–3175.

[22] I. R. Rodrigues *et al.*, "Modeling and assessing an intelligent system for safety in human-robot collaboration using deep and machine learning techniques," *Multimed Tools Appl*, pp. 1–27, 2022.

Received: August 08, 2025

Volume 38 No. 10s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[23] V. Belcamino, "Enhancing Human-Robot Collaboration Through Advanced Human Activity Recognition and Motion Tracking," 2025.

[24] M. Webster *et al.*, "A corroborative approach to verification and validation of human–robot teams," *Int J Rob Res*, vol. 39, no. 1, pp. 73–99, 2020.

[25] P. Khandelwal *et al.*, "Bwibots: A platform for bridging the gap between ai and human–robot interaction research," *Int J Rob Res*, vol. 36, no. 5–7, pp. 635–659, 2017.

[26] S. Yilmazyildiz, R. Read, T. Belpeame, and W. Verhelst, "Review of semantic-free utterances in social human–robot interaction," *Int J Hum Comput Interact*, vol. 32, no. 1, pp. 63–85, 2016.

[27] Y. Hu, P. Ray, and G. Hoffman, "Performing Human Shadow Detection for Camera-Based Privacy-Preserving Human-Robot Interactions," in *2024 33rd IEEE International Conference on Robot and Human Interactive Communication (ROMAN)*, IEEE, 2024, pp. 1013–1020.

Received: August 08, 2025