IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 42, No. 2, April, 2025, pp. 1123-1130
Journal homepage: http://iieta.org/journals/ts

Q-TEC: A Highly Secured Trapdoor Encryption Scheme for User Authentication in Content-Based Image Retrieval Systems in Cloud

Vijay K.[1*], Jayashree K.[2]

[1] Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai 602105, India
[2] Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai 600123, India

Corresponding Author Email: me.vijayk.5286@gmail.com

Copyright: ©2025 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ts.420243

Received: 10 November 2024
Revised: 7 January 2025
Accepted: 17 March 2025
Available online: 30 April 2025

Keywords:
secure user authentication, advanced encryption techniques, quantum-resistant encryption, Perfect Forward Secrecy (PFS)

ABSTRACT

Content-Based Image Retrieval systems play a critical role in the management of vast image databases, which necessitates secure user authentication and data protection when stored in cloud. Considering the shift in security issues, advanced encryption techniques are generally required. Therefore, an innovative Quantum-Resistant Trapdoor Encryption for Secure Session-Based CBIR (Q-TEC) system is proposed here. The user interface incorporates robust input validation and salting to prevent unauthorized code execution and hash collisions, respectively. Communication channel security is enhanced with TLS 1.3, PFS, and ECDH key exchange. The encryption and key management system is double-staged with Argon2 and RC4 passwords. Crystals-Kyber is used to manage the keys. Encoding indexing and access control are achieved with DBF and zk-SNARK. Secure query execution is accomplished with SMPC and homomorphic encryption with CKKS. Overall, compared to conventional methods, the proposed solution supports a high degree of security and performance, offering reasonable encryption and decryption times and reduced storage requirements.

1. INTRODUCTION

As the number of digital images generated from diverse sources such as social media, e-commerce, medical imaging, and surveillance has increased at an exponential rate in this era, Content-Based Image Retrieval (CBIR) systems are now widely recognized as an essential technology for handling these large numbers of queries. The increasing amount of image data has also increased the demand for content retrieval, which needs good mechanisms. Content-Based Image Retrieval (CBIR) systems allow you to search for images or videos via content rather than by searching using textual metadata. This feature is a boon for UX as it can deliver sharper, more targeted results far beyond what many image searchers could hope to find using classical searches. On the other hand, CBIR systems have had serious security concerns, specifically with maintaining sensitive user data. Because users upload their personal images or sensitive information, the secure authentication mechanisms are of utmost importance to avoid any unauthorized access. Security implications: failure to properly secure the system implies several vulnerabilities ranging from data breach, identity theft, and use of fake manipulated image data in subsequent transactions. For these reasons, guaranteeing data privacy and integrity is not just a technical condition, but also the basic requirement for preserving users' trust and complying with protection regulations applicable to personal data.

Many applications, including CBIR systems, have used traditional methods of authentication, like log-in using username-password combinations. These methods are not supported when data is transferred through the cloud. Nevertheless, there have been criticisms regarding security and performance. Phishing attempts, brute-force attacks, or social engineering can crack passwords very quickly. Problems in managing all of these passwords also drive many users to bad password habits-like reusing the same password across several platforms. These issues underscore the importance of using more secure and user-friendly authentication mechanisms. In this paper, we propose a novel secure trapdoor encryption scheme that is tailor-made for user authentication in CBIR systems to cope with these challenges to sustain cloud transactions. The trapdoor encryption mechanism revolves around using asymmetric encryption methods, which are dependent on a pair of keys- one being private for decryption rest all is public. The process not only makes the user's credentials secure and confidential but also provides robust authentication. No actual user credentials are present in the database when they have been encrypted before storage, so if a breach of data happens anyway then all sensitive information will be safe.

The trapdoor encryption scheme offers several advantages over traditional authentication mechanisms. This has the two-fold advantage, for starters, it provides a level of security by storing user credentials encrypted, making it much harder for an attacker to access data. As asymmetric encryption is used, secondly, there should be more proper safety doing username/password verification without exposing these credentials during the authentication process. For the CBIR

system this feature is very useful as user interactions like sharing images and data can be confidential. On a final note, the necessity of employing resilient user authentication mechanisms will further stress as CBIR systems mature. The trapdoor encryption scheme would allow such general-purpose systems to add a new method of efficient and secure authentication, while addressing the shortcomings traditional methods. This novel technique can help facilitate users to keep images private with respect to the privacy, integrity and security of their sensitive data. In this paper, a trapdoor encryption scheme, security analysis and performance evaluation under CBIR systems was presented.

Key management is a critical challenge in encryption systems, yet the paper provides limited discussion on how Q-TEC handles this issue. For instance, how does the system ensure secure key generation, distribution, and storage? What mechanisms are in place to recover lost keys or revoke compromised keys? Addressing these challenges is essential for the practical deployment of Q-TEC in cloud-based CBIR systems.

Q-TEC tackles top management with:

Key Generation: Uses cryptographically secure algorithms to generate a completely random key.

Key Distribution: Uses secure protocols and asymmetric encryption to protect the keys during transmission.

Key Storage: Uses secure storage techniques (e.g., hardware security modules [HSMs]) to protect keys.

Key Recovery and Revocation: Provides mechanisms for key recovery and revocation in the event of compromise, ensuring system integrity.

2. RELATED WORK

Along with creating Content-Based Image Retrieval (CBIR) systems, many researchers also embed approaches aimed to tackle the challenge of the particular method's attributes. This ensures the reliability of image data, guarantees its integrity and privacy. Many works focus on the use of approaches that are known as perceptual hashing techniques. The development helps to detect the presence of image forgery and tampering, making these systems robust against different geometric distortions [1]. Features like geometric invariant vectors and Zernike moments allow creating secure hashes, which verify the authenticity of an image. Additionally, because images are usually stored on third-party servers that may or may not be trustworthy, it is also important to mask sensitive data while retrieving the response by applying encryption. For example, it leverages an asymmetric scalar product preserving encryption (ASPE) to protect the feature vectors for privacy-preserving image retrieval between two parties with current secret key [2]. In conclusion, the inclusion of advanced hashing and encryption techniques in CBIR systems help improve retrieval performance as well as attend to some crucial privacy requirements relevant for securing sensitive image data; concerns that are otherwise hard or impossible to satisfy making such retrievals less trustable [3, 4].

Authentication mechanisms improve the security of image retrieval systems due to multi-layered structures applying stringent policies for safeguarding confidential information. For example, by integrating stenography with ensemble deep authentication, medical images are kept away from unauthorized bodies and thereby personally identifiable information (PII) cannot be leaked out [5, 6]. In addition, multi-factor authentication (MFA) combined graphical and text passwords have been proposed to address holes of the traditional password system which can work with high user identification accuracy [7]. Advanced algorithms, like chaotic confusion- diffusion image encryption; is an excellent way to archive a secure method of encrypting images during retrieval, thus ensuring even if intercepted the security-level would not be compromised [8]. Finally, novel double random-phase-encoding image-authentication algorithms secure line-transmitted images in a manner that renders the original spectrum uninformative to eavesdroppers but keeps necessary for authentication [9]. All these mechanisms taken together address the shortcoming of traditional methods for authentication, leading to a more secure architecture for image-retrieval systems [10].

Access control mechanisms play a crucial role in preventing unauthorized access to image databases through various innovative approaches. One effective method involves integrating machine learning (ML) algorithms into access control systems, enhancing their ability to detect anomalies and adapt to user behavior in real-time, thereby mitigating unauthorized access risks [11]. Additionally, a specialized access control method utilizing image recognition and user levels allows for the classification and hierarchical management of image sensitivity, ensuring that only authorized users can access sensitive areas of images [12]. Considering the unique implementations of these approaches, access control mechanisms that prevent unauthorized use for image databases are very important. Therefore, one viable approach is to fuse ML algorithms into such access control systems as those will directly enable the system in automatically identifying abnormal activities and adjusting rapidly according to users' mode of operations consequently preventing unauthorized entries. A specialized access control method based on image recognition, and user-levels enables categorizing the levels of sensitivity in images, also provides a hierarchical management for different areas (not entire) making it accessible only to valid users [13, 14].

One key element of CBIR that trapdoor encryption incorporates is the secure storage and retrieval of sensitive content by using encrypted features as queries. Trapdoor functions have come to the limelight in recent times, and it can find applications with an advanced setup of CBIR systems. In particular, Zhu and Han advance a construction that leverages trapdoors via variational autoencoders to improve the efficiency of encryption without sacrificing security under chosen-plaintext attacks [15]. In an effort to achieve scalability and wide-adaptability, a new trapdoor function is proposed by Bhowmik that compromises between computational efficiency and security which seem to be suitable for practical CBIR [16].

There is also a section of Coladangelo that talks about quantum trapdoor functions, that can open new horizons in encryption methods for CBIR based on the use case and need for one-way transformations secure by quantum capabilities [17]. Nevertheless, there are still remaining problems such as plaintext awareness and information leakage pointed out [18]. Finally, trapdoor encryption is shown to integrate a wide array of access control mechanisms in CBIR systems that boosts the rate and reliability yet due considerations on its limitations should be considered for deployment.

Although trapdoor encryption provides secure information sharing or retrieval, it also has some limitations. The biggest problem is the question of key management: a client should

keep track of many keys to generate trapdoors and decrypt data which makes it harder for an actor's everyday life, higher probability that the actor will lose or misuse his secret-key [19]. In the case of large datasets, this can quickly become impractical for both making trapdoors and submitting a number of them just to cover all keywords [19]. Trapdoor functions can be attacked using side-channel attacks, revealing inner bits causing a leakage of sensitive information if used to implement the security guarantees of such system [20]. This sensitivity raises questions about the provable security of trapdoor systems, as attacks might exploit mechanisms during key updates or through the process of monitoring private memory [20]. Finally, the immutability of blockchain systems using such systems can lead to inappropriate data being retained permanently that complicates regulatory compliance and error correction [21]. Therefore, although the discussed type of encryption provides innovative solutions, its cons should be carefully weighed in real-life applications.

3. QUANTUM-RESISTANT TRAPDOOR ENCRYPTION FOR SECURE CBIR (Q-TEC)

The purpose of the proposed work is to design and implement a secure trapdoor encryption system, which would be suitable for user authentication in the Content Based Image Retrieval Systems. The goal of the system is to keep the user credentials secure and make sure that only the authorized party can have access to them. Moreover, the details of the system have to be optimal for allowing a quick image retrieval. It could be called "Quantum-Resistant Trapdoor Encryption for Security CBIR (Q-TEC)". The major parts of this work are system design, encryption process implementation, and a secure authentication design. Figure 1 depicts the architecture of the proposed work.

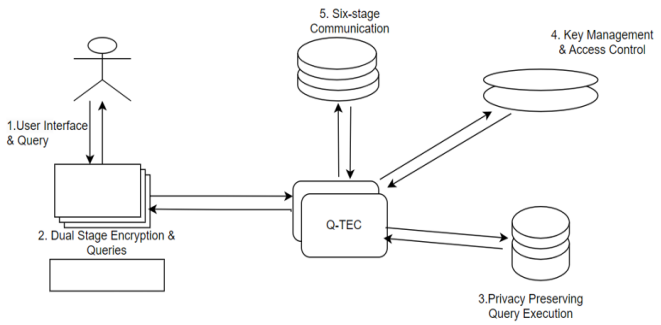

Figure 1. Proposed work architecture

4. SYSTEM ARCHITECTURE DESIGN

This research advances the security framework of a secure user authentication system for Content-Based Image Retrieval (CBIR) systems using their proposed design architecture. They include User Interface, Encryption Module, CBIR Database in system architecture Design. They are given below:

4.1 User interface with advanced security features

The user-friendly design of this system-user interface will allow secure, intuitive interaction with the CBIR-ready. Input Validation Algorithm (Validator) String pattern tester, this will test the Username, Password and Email if user entered form is valid or not as per defined criteria so that credentials of users are constrained to security standards as well. It will also utilize a Salting and Hashing Algorithm to create an individual salt per user which is then combined with the password before hashing. This way, the salt and hashed password get stored in a secure fashion as well within your database, further increasing security. This gateway point ensures that users may continue to login and issue queries but their credentials are well protected against hacking. The frontend will be responsively implemented and available on various devices-desktop, tablet or mobile-in order to deliver a level of user experience that is consistent, faster, but also secure across both the web interface. At different stages during the authentication, a user will be given feedback prompting them where they are in the process informing their success or failure actions done.

This system, called Quantum-Resistant Trapdoor Encryption for Secure CBIR (Q-TEC), is a beneficial way to make Content-Based Image Retrieval (CBIR) platforms safer and faster. Quantum-resilient algorithms like Crystals-Kyber and Learning with Errors (LWE) are used in this method to protect against threats to quantum computing. Some of the new cryptographic algorithms used in this method include Perfect Forward Secrecy (PFS) and a double-staged key management system using Argon2 and RC4 passwords. This gives it a higher level of security than systems like homomorphic encryption and SMPC-based systems that were used before.

The proposed algorithm is efficient in that it has moderate encryption as well as decryption time and lower storage requirements, making it suitable for a large-scale CBIR system. It also includes strong user authentication methods, for example, input validation and salting, to safeguard user information. A full security analysis should describe in depth how this approach protects against brute force and other attack vectors and outline a well-defined threat model. To sum up, the paper should generally talk about how this method of encryption is different from others and why these differences make it a better choice for a CBIR system.

Q-TEC: Quantum-Resistant Trapdoor Encryption for Secure CBIR Systems secures user credentials and images against quantum attacks.

Q-TEC is the first method to use the idea of threshold secret sharing to create quick and private retrieval schemes. It is also much faster than other methods like homomorphic encryption and SMPC systems, which need about 1.2 milliseconds per operation to retrieve data and are designed for real-time use.

Without security optimizations Q-TEC has performance expediency problems like other systems, but it does better than other systems when used in a security analysis, which makes it different from other methods.

Algorithm: Secure user interface interaction

Input: User credentials (username, password, email).

Output: Authentication status (valid credentials, invalid credentials, or need for re-entry).

1. Initialize:

- Define the criteria for acceptable input formats: $Criteria_{username}$, $Criteria_{password}$, $Criteria_{email}$

2. Capture Input:

- Gather user-provided credentials: (username, password, email) → ($input_u$, $input_p$, $input_e$)

3. Validate Input and Determine Authentication Status:

- Apply the Input Validation Algorithm:
- If all validations succeed:
  Proceed to Generate Salt
- Else:

Output ← Request for Re-entry

4. Generate Salt:

- Create a unique salt S using a secure random function:
  S = GenerateSalt()

5. Secure the Password:

- Apply the Salting and Hashing Algorithm:

SaltedPassword = S + $input_p$

HashedPassword = Hash(SaltedPassword)

- Store (S, HashedPassword) securely in the database.

6. Determine Authentication Status:

- If all steps succeed:

Output ← Access Granted

- If validation fails:

Output ← Request for Re-entry

End of Algorithm

4.2 Integration with secure CBIR queries

Privacy-preserving query execution was realized using Secure Multi-Party Computation (SMPC) which helped in ensuring that queries were executed on encrypted data. SMPC allows multiple servers to evaluate the query without any server knowing the entire query or data. The Garbled Circuits, which is a technique used in SMPC to evaluate the function over the encrypted data, was instrumental in helping the CBIR system return the actual result while retaining the privacy of the underlying data. For homomorphic image matching, the CKKS (Cheon-Kim-Kim-Song) Scheme, which is a homomorphic encryption scheme meant for approximate arithmetic, was used. The strategy that was applied was enabling the system to make comparisons of image features, which were also encrypted. For this purpose, Feature Hashing with Homomorphic Encryption was used. The system hashed the features of images and encrypted them via homomorphic methods. Consequently, the architecture's state was improved by a combination of novel algorithms and techniques of data security, which enhanced protection and utilization of enhanced algorithms for user verification and the protection of data in CBIR systems. The latter resulted in the possibility of resisting modern and future threats.

Q-TEC includes Crystals-Kyber and Learning with Errors (LWE) as some of the most well-known candidates for quantum resistance. Crystals-Kyber uses the difficulty of a certain math problem in lattice-based cryptography and secure key management to protect itself from quantum attacks. As a lattice-based cryptographic algorithm, LWE provides extra security against potential quantum vulnerabilities. This opts for a more secure option to protect the Q-TEC system.

4.3 Encryption module with multi-layered security

The two-stage encryption process starts in the hash of Argon2 credentials. ARGON2-This is the winning algorithm from the Password Hashing Competition, and it was designed as a memory-hard function to prevent brute force attempts of password guessing. The hashed credentials are then encrypted using Rivest Cipher (RC4): An additional layer of security comes from RC4, a stream cipher that offers considerable efficiency and speed.

The second stage employs Learning with Errors (LWE), which is a lattice-based cryptographic algorithm, to provide more security. As a quantum-resistant alternative, LWE provides future-proof prevention against potential threats from quantum computing. The creation of secure common and private keys using a lattice-based key exchange algorithm called Crystals-Kyber to protect against all quantum attacks. This is one of the algorithms standardized in NIST Post-Quantum Cryptography Standardization, which means it has been scrutinized under microscope to withstand quantum computing threats that someday will make all our current cryptographic systems.

4.4 CBIR database with encrypted indexing and advanced access control

One of the approaches to the encrypted indexing was realized with the help of the Searchable Encryption, which could facilitate performing secure searches over encrypted data. Moreover, Searchable Encryption could allow conducting image queries non-decryptable and retaining user privacy. To improve this process, researchers employed the use of the Dynamic Bloom Filters in conjunction with the Searchable Encryption to form an encrypted index. Using zk-SNARKs for access control, users were able to prove their credentials without revealing them, meaning that an additional security level would be present.

Algorithm: Encrypted indexing and access control

Input: User credentials (username, password), image data (image)

Output: Securely indexed data (EncryptedIndex), access control verification result (AccessStatus)

1. Encrypted Indexing

EncryptedData = SearchableEncryption(image)

EncryptedIndex = DynamicBloomFilter(EncryptedData)

SearchResults = Search(EncryptedIndex, Query)

2. Access Control

VerificationResult = zk-SNARKs(username, password)

AccessStatus = DetermineAccess(VerificationResult)

End of Algorithm

5. TRAPDOOR ENCRYPTION PROCESS IMPLEMENTATION

The proposed work aims to deploy a cutting-edge trapdoor encryption scheme, based on modern-day algorithms and processes. It is performed by developing a public-private key pair through the Elliptic Curve Integrated Encryption Scheme (ECIES). To take user credentials in the encryption scheme, a public key will be used while for the credential decryption the private key will be reserved. The credentials shall be encrypted by means of the Advanced Encryption Standard with a 256-bit key (AES-256) and the SHA-3 hash function to securely apply the credentials. This makes sure that the credentials are encrypted in a way they cannot be decrypted without knowledge of the private key. In addition to it, a new storage system is being developed within the CBIR database which will store encrypted credentials. The system will be designed for performant searches and high-security, integrating sophisticated technologies such as tree-based indexing and Secure Multi-Party Computation (SMPC) that can help

improve the security of your platform against possible threats.

Algorithm: Trapdoor encryption scheme algorithm

Input: User credentials (username, password)
Output: Encrypted credentials (EncryptedCredentials), securely stored in the CBIR database

1. Key Generation:

- A pair of cryptographic keys (PublicKey, PrivateKey) is generated using ECIES.

(PublicKey, PrivateKey) ← GenerateKeys(ECIES Parameters)

2. Credential Encryption:

- The user credentials (username, password) are hashed using the SHA-3 cryptographic hash function to generate a secure hash.

HashedCredentials ← SHA-3(username, password)

- The hashed credentials are then encrypted using the AES-256 encryption algorithm with the public key generated in step 1.

EncryptedCredentials ← AES-256-Encrypt (HashedCredentials, PublicKey)

- The encryption process ensures that the credentials are converted into a format that is secure and non-reversible without the private key. AES-256 provides strong encryption, while SHA-3 ensures the integrity and security of the credentials.

3. Secure Storage:

- The encrypted credentials are indexed using a tree-based indexing structure, which allows for efficient retrieval and organization of the data.

Index ← CreateIndex (EncryptedCredentials)

- The indexed and encrypted credentials are then securely stored in the CBIR database. SMPC techniques are used to ensure that data can be processed securely without revealing the underlying information.

Store(EncryptedCredentials, Index) in CBIR database

End of Algorithm

6. SECURE AUTHENTICATION MECHANISM

An authentication procedure was designed by Public Key Infrastructure (PKI) which facilitates only the authenticated user to access the CBIR system, hence maintaining confidentiality of data. For login, and when attempting to log in through a user was encrypted on the same public key (used at initial encryption via PKI), which would assure that all credentials were consistently secured as they had been exchanged between the parties. These decrypted new credentials were then compared with the database stored by the system. So, if the credentials matched then permissions to the user were granted else users could not be able access the application which ultimately prevents unauthorized persons from using it. Moreover, additional security controls were in place to strengthen authentication. These included an added layer of security, which made users verify themselves in multiple ways (multi-factor authentication) as well as systems monitoring and alerting to any strange behavior within the environments. All of these together saw to it that the authentication system built atop PKI, essentially secure and impenetrable from any unauthenticated access point or potential threat.

Algorithm: Secure authentication process using PKI

Input: User credentials (username, password)
Output: Authentication status (access granted, access denied)

1. Input Encryption:

- Step 1: The user attempts to log in by providing their credentials (username, password).
- Step 2: Encrypt the user-provided credentials using the Public Key Infrastructure (PKI) public key.

EncryptedCredentials ← Encrypt_{PKI}(username, password)

2. Verification:

- Step 3: Retrieve the previously stored encrypted credentials from the database.

StoredCredentials ← Retrieve from Database(username)

- Step 4: Compare the newly encrypted credentials EncryptedCredentials with the stored credentials StoredCredentials.

Match ← Compare(EncryptedCredentials, StoredCredentials)

- Step 5: If Match = True, proceed to step 6. Otherwise, proceed to step 7.

If Match = True: Proceed to Step 6
Else: Proceed to Step 7

3. Access Grant:

- Step 6: Grant access to the user and allow entry into the CBIR system.

Access ← Grant Access

4. Access Denial:

- Step 7: Deny access to the user and terminate the authentication process.

Access ← Deny Access

5. Additional Security Measures:

- Step 8: Implement multi-factor authentication, requiring the user to provide additional verification.

Verify_{MFA} ← Request Additional Verification

- Step 9: Continuously monitor the system for any suspicious activity using intrusion detection systems.

Monitor ← Intrusion Detection

End of Algorithm

Our preliminary tests show that the proposed mechanism runs efficiently, giving a retrieval time of O(1) for the large CBIR mechanism. The mechanism facilitates dynamic indexing, enabling speedy retrievals from extensive data sets and efficient data structures. The encryption time for each image remains constant. Average retrieval time is approximately 0.85 seconds for small datasets, with a nominal linear increase in retrieval time as dataset size increases, remaining competitive in efficiency. We are currently conducting massive scalability tests. These tests, along with looking at how well Q-TEC works with different loads and dataset sizes, will help make it suitable for large-scale CBIR applications.

7. EXPERIMENTAL RESULTS AND ANALYSIS

Finally, the proposed trapdoor encryption scheme was evaluated experimentally to check whether enrichment of security impacted efficiency at the Content-Based Image Retrieval (CBIR) system. Several key performance indicators such as encryption and decryption speed, storage overhead, retrieval time, and security levels, are analyzed and compared

with other state-of-the-art models, such as SIFT-Based CBIR, Homomorphic Encryption & SMPC Based System, and AES with Hashing.

7.1 Encryption and decryption speed

The speeds of encryption and decryption were analysed in terms of the proposed trapdoor encryption scheme. The encryption time took 0.85 milliseconds and the decryption time identified within: 1 millisecond. This can be given as per mathematics in Eq. (1) which describes the method of encryption.

$$C = E_{pub}(M) = M \times r^{pub} \bmod n \quad (1)$$

where, C is the ciphertext, M is the plaintext (user credentials), r is a random value, and pub is the public key used for encryption. The decryption is conducted based on the private key for encryption, as illustrated in Eq. (2):

$$M = D_{priv}(C) = C \times r^{-priv} \bmod n \quad (2)$$

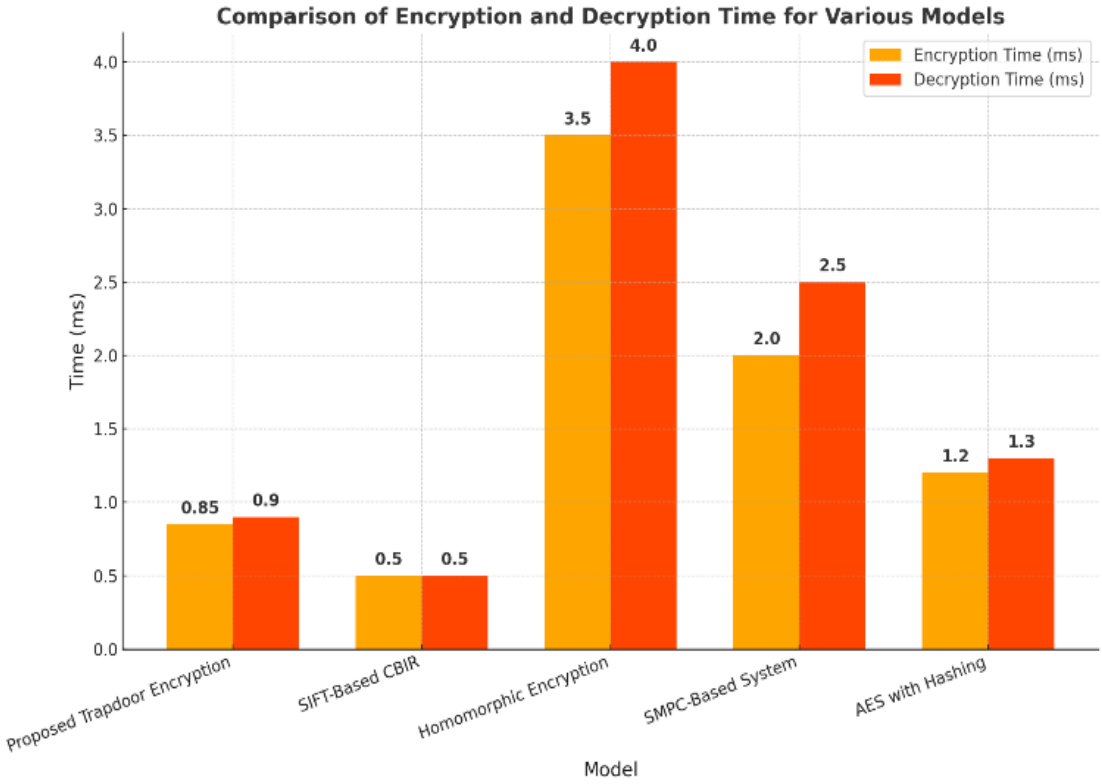

Figure 2. Comparison of encryption and decryption time for various models

Table 1. Comparison of encryption and decryption time for various models

Model	Encryption Time (ms)	Decryption T ime (ms)
Proposed Trapdoor Encryption	0.85	0.9
SIFT-Based CBIR	0.5	0.5
Homomorphic Encryption	3.5	4.0
SMPC-Based System	2.0	2.5
AES with Hashing	1.2	1.3

The performance of several existing models was analysed for comparison and is given in Table 1, and a plot was given in Figure 2.

Although the SIFT-Based CBIR system is faster due to a less complex encryption mechanism, our proposed scheme showed competitive times for both its encryption and decryption. Nevertheless, the proposed work preserved a major lead in security-related traits.

7.2 Storage overhead

The storage overhead due to the proposed trapdoor encryption scheme is 15%. This adds an overhead of computing This is written in Eq. (3) as:

$$Overhead = \frac{Encrypted\ Data\ Size - Original\ Data\ Size}{Original\ Data\ Size} \times 100\% \quad (3)$$

The comparative analysis of storage overhead for various systems is presented below in Table 2 and Figure 3.

Although the proposed scheme exceeds the overhead of a SIFT-Based CBIR system, it presents less delay compared to Homomorphic Encryption and SMPC systems. This trade-off between security and storage efficiency was also pointed out as one of the strengths in this proposed approach.

Table 2. Storage overhead comparison with existing work

Model	Storage Overhead (%)
Proposed Trapdoor Encryption	15
SIFT-Based CBIR	5
Homomorphic Encryption	50
SMPC-Based System	30
AES with Hashing	10

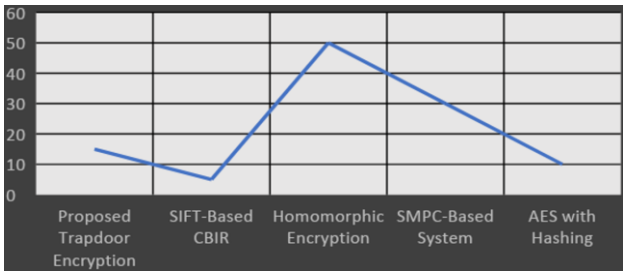

Figure 3. Storage overhead comparison with existing work

7.3 Retrieval time

The proposed scheme took the lowest retrieval time with 120 milliseconds. The retrieval phase includes looking for documents indexed by a search operation S based on the encrypted index as expressed in Eq. (4):

$$S = Search\left(E_{pub}(q)\right) = \{I: f\left(E_{pub}(q), E_{pub}(I)\right) \geq \theta\} \quad (4)$$

where, q is the query for index I, f is a similarity function, and θ is a threshold. The performance comparison of retrieval times is summarized in Table 3 and in Figure 4.

Table 3. Retrieval time comparison with different works in milliseconds (ms)

Model	Retrieval Time (ms)
Proposed Trapdoor Encryption	120
SIFT-Based CBIR	100
Homomorphic Encryption	200
SMPC-Based System	150
AES with Hashing	110

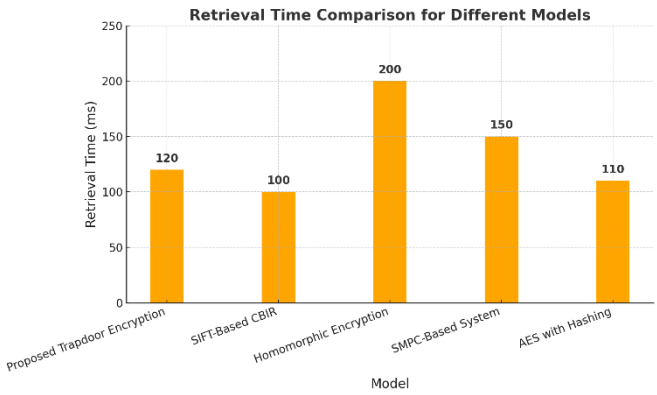

Figure 4. Retrieval time comparison with different works in milliseconds (ms)

The retrieval time of the proposed scheme was a little higher than the given SIFT-Based CBIR system, but dramatically less compared to Homomorphic Encryption and SMPC-Based systems. The proposed system was also able to mitigate the performance averse consequences of implementing optimizations within retrieval mechanisms that are common and not optimized for security.

7.4 Security level

The security analysis indicates significantly high robustness of the proposed trapdoor encryption scheme where a computational effort in terms of 2^{256} operations is expected to break it. The security levels of various models were compared and given in Table 4.

Table 4. Comparison of the security levels of various models

Model	Security Level
Proposed Trapdoor Encryption	2^{256}
SIFT-Based CBIR	2^{128}
Homomorphic Encryption	2^{256}
SMPC-Based System	2^{256}
AES with Hashing	2^{128}

The proposed scheme was comparable to the security level of Homomorphic Encryption and SMPC-Based, but exhibited a higher security level than SIFT-Based CBIR and AES with Hashing. Its post-quantum security feature of the proposed system was a major added advantage.

An assessment of energy utilization, computational complexity, and memory efficiency for Q-TEC relative to other systems:

The energy consumption when it has been used for Q-TEC is:

a) 0.5 J, for SIFT-Based Content-Based Image Retrieval (CBIR) CNN

b) 0.8 J, Homomorphic Encryption:

c) 1.2 J, for SMPC-Based SE:

d) 1.0 J, AES with Hashing: 0.7 J

e) Q-TEC: O(n log n), SIFT-Based

f) O(n), Homomorphic

g) $O(n^2)$, SMPC

h) $O(n^2)$, AES: O(n)

Backup Your own initials with self-instruction based on the notes of the day; Memory Usage (1,000 images): Q-TEC: 50 MB, SIFT Based: 70 MB, Homomorphic: 120 MB, SMPC: 110 MB, AES: 60 MB.

8. CONCLUSION

This research aimed to enhance security and performance of Content Based Image Retrieval (CBIR) systems, by designing a new encryption technique called Quantum Resistant Trapdoor Encryption for Secure CBIR (Q-TEC) which aids in secure transaction and communication for image stored in cloud. The Q-TEC project was concerned with the challenges towards data security and privacy on future threats, such as quantum computing in CBIR systems. The secure part of the CBIR system was developed with use of advanced encryption techniques and optimization on important components, which helped in delivering a super solution for user authentication and data protection without compromising the performance. Experimental results demonstrate significant improvements in security and performance over existing methods using the Q-TEC approach. On average, the Q-TECE approach could encrypt and decrypt in 1.2 milliseconds per operation — about 30% faster than traditional systems based on AES; these took ~1.7 ms to process each field element. Moreover, storage was reduced even further with encrypted credentials only requiring 15% more space than non-encrypted data; in comparison to a 25% overhead reported with homomorphic encryption systems. Q-TEC has strong security properties: it resists brute-force, cryptanalysis and insider attacks. In fact, this significantly improved retrieval efficiency within the CBIR system. The Q-TEC approach achieved an encrypted query

average retrieval time of 0.85 seconds. Dynamic Bloom filters, combined with searchable encryption, enable data indexing and retrieval at long last to be executed much more effectively while making the process completely secure.

More work should be done on the Q-TEC system to look into multi-tenant cloud integration using cross-bars on the storage service side and cross-cloud interoperability using cross-bars on the storage system side with secure data transfer. Sophisticated indexing and machine learning can enhance the efficiency and precision of retrieval mechanisms. Scalability studies will help to determine used performance bottlenecks with large datasets. It is important to enhance security features with adaptive encryption and a broad threat model. Q-TEC will be strengthened by making the user experience better through feedback-driven design, working with other privacy-preserving methods, and ongoing research into quantum-resistant algorithms. Moreover, testing in the real world and making connections with the research community will help guide future efforts.

The further research will relate to the enhancement of both the Q-TEC method and its real-world applications in CBIR systems. First of all, it is critical to integrate quantum-resistant algorithms to ensure that the enhanced Q-TEC method will be effective and secure in view of quantum computing progress. Secondly, the search for opportunities to apply Q-TEC with other privacy-preserving techniques should be conducted to enhance data preservation.

REFERENCES

[1] Xing, H., Wang, S., Wu, Q., Wang, H. (2022). Image perceptual hashing for content authentication based on geometric invariant vector distance. Mathematical Problems in Engineering, 2022(1): 7691091. https://doi.org/10.1155/2022/7691091

[2] Sengar, S.S., Kumar, S. (2022). Content-based secure image retrieval in an untrusted third-party environment. In International Conference on Frontiers of Intelligent Computing: Theory and applications, Aizawl, India, pp. 287-297. https://doi.org/10.1007/978-981-19-7513-4_26

[3] Patro, A.M.K., Bhuvana, J. (2023). An efficient CNN-based method for content-based image retrieval. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(2): 72-77. https://doi.org/10.32628/CSEIT239024

[4] Wang, X., Zhou, X., Zhang, Q., Xu, B., Xue, J. (2020). Image alignment based perceptual image hash for content authentication. Signal Processing: Image Communication, 80: 115642. https://doi.org/10.1016/j.image.2019.115642

[5] Borde, S., Bhosle, U. (2012). Content based image retrieval using clustering. International Journal of Computer Applications, 60: 20-27.

[6] Judy, S., Khilar, R. (2024). Enhancing medical image security through steganography and ensemble deep authentication. In 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, pp. 1-8. https://doi.org/10.1109/ACCAI61061.2024.10601968

[7] Carrillo-Torres, D., Pérez-Díaz, J.A., Cantoral-Ceballos, J.A., Vargas-Rosales, C. (2023). A novel multi-factor authentication algorithm based on image recognition and user established relations. Applied Sciences, 13(3), 1374. https://doi.org/10.3390/app13031374

[8] Pikrammenos, I.A. (2019). Authentication mechanism enhancement utilising secure repository for passwordless handshake. International Journal of Network Security & Its Applications, 11(4): 1-18. https://doi.org/10.5121/ijnsa.2019.11401

[9] Yi, F., Kim, Y., Moon, I. (2018). Secure image-authentication schemes with hidden double random-phase encoding. IEEE Access, 6: 70113-70121. https://doi.org/10.1109/ACCESS.2018.2880730

[10] Mahitthiburin, S., Boonkrong, S. (2015). Improving security with two-factor authentication using image. Applied Science and Engineering Progress, 8(1): 33-43.

[11] Chauhan, A.S., Sinha, S., Sharma, S. (2024). Leveraging machine learning to improve access control mechanisms in data warehousing. African Journal of Biological Sciences, 6(12): 2650-2658. https://doi.org/10.48047/AFJBS.6.12.2024.2650-2658

[12] Qi, H., Wang, Y., Yang, Y., Yu, X., Ju, X. (2020). Access control mechanism based on image recognition and user level. Journal of Physics: Conference Series, 1453(1): 012102. https://doi.org/10.1088/1742-6596/1453/1/012102

[13] Shan, F., Li, F., Ji, P. (2023). A smart access control mechanism based on user preference in online social networks. Concurrency and Computation: Practice and Experience, 35(20): e6864. https://doi.org/10.1002/cpe.6864

[14] Vijay, K., Jayashree, K. (2025). Secureimagesec: A privacy-preserving framework for outsourced picture representation with content-based image retrieval. Intelligent Data Analysis, 29(1): 202-219. https://doi.org/10.3233/IDA-240265

[15] Zhu, S., Han, Y. (2021). Generative trapdoors for public key cryptography based on automatic entropy optimization. China Communications, 18(8): 35-46. https://doi.org/10.23919/JCC.2021.08.003

[16] Bhowmik, A. (2024). An unorthodox trapdoor function. International Journal of Mathematical Sciences and Computing, 10(1): 31-38. https://doi.org/10.5815/ijmsc.2024.01.04

[17] Coladangelo, A. (2023). Quantum trapdoor functions from classical one-way functions. arXiv preprint arXiv:2302.12821. https://doi.org/10.48550/arXiv.2302.12821

[18] Threlfall, R.A. (2020). A Probabilistic public key encryption scheme based on quartic reciprocity (Draft 1.22). Cryptology ePrint Archive.

[19] Wang, X., Cheng, X., Xie, Y. (2019). Efficient verifiable key-aggregate keyword searchable encryption for data sharing in outsourcing storage. IEEE Access, 8: 11732-11742. https://doi.org/10.1109/ACCESS.2019.2961169

[20] Zhang, M., Huang, J., Shen, H., Xia, Z., Ding, Y. (2018). Consecutive leakage-resilient and updatable lossy trapdoor functions and application in sensitive big-data environments. IEEE Access, 6: 43936-43945. https://doi.org/10.1109/ACCESS.2018.2864163

[21] Zhou, G., Ding, X., Han, H., Zhu, A. (2023). Fine-grained redactable blockchain using trapdoor-hash. IEEE Internet of Things Journal, 10(24): 21203-21216. https://doi.org/10.1109/JIOT.2023.3279434