International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2) 2026 pp. 1038-1047
https://doi.org/10.70917/ijcisim-2026-3484
Article

Hybrid CBIR Framework with Lattice-Based Encryption and SMPC for Post-Quantum Cloud Security

A.Neela sundari[1], S.Sathiya[2], Gogineni Rajesh Chandra[3]

[1]Department of CSE, Annamalai University, Chidambaram, TN india, ngargeya@gmail.com
[2]Department of CSE, Annamalai University, Chidambaram, TN india, sathiya.sep05@gmail.com
[3]Department of CSE, NRI Institute of Technology, Guntur, A.P, India, grajeshchandra@gmail.com

Abstract: The evolving landscape of quantum computing presents significant challenges to the security of cloud-based image retrieval systems, necessitating robust frameworks for safeguarding sensitive visual data. This paper introduces a hybrid Content-Based Image Retrieval (H-CBIR) architecture that integrates advanced post-quantum cryptographic techniques to enhance data privacy in cloud environments. To enable privacy-preserving query processing and result aggregation, the suggested system integrates secure multiparty computation (SMPC) with lattice-based encryption, which is renowned for its quantum resistance. In this design, SMPC protocols allow cooperative processing across dispersed servers without disclosing raw data, while image attributes are encrypted using lattice methods to mitigate potential quantum assaults. Experimental validation demonstrates the framework's efficacy in maintaining high retrieval accuracy alongside rigorous privacy guarantees, even under adversarial quantum-inspired threat models. The experimental validation demonstrates the proposed hybrid framework is capable of returning a similar (> 94.5%) retrieval accuracy, whilst providing a strong guarantee of privacy (leakage < 0.1%) in the quantum-inspired modeled adversarial setting. The findings serve to demonstrate the feasibility of pairing horizontal post-quantum encryption with CBIR systems to safeguard the ever-growing concern of cloud privacy breaches. In order to further strengthen privacy and performance in changing cloud infrastructures, future research will investigate the integration of new post-quantum approaches, such as code-based and multivariate cryptography, and expand the framework to broader multimodal data scenarios.

Keywords: Post-Quantum Cryptography, Lattice-Based Encryption, Secure Multiparty Computation, Content-Based Image Retrieval, Privacy-Preserving Cloud Computing, Quantum-Resilient Image Retrieval, Secure Cloud Data Processing.

1. INTRODUCTION

The exponential advancement of quantum computing has introduced a paradigm shift in cybersecurity, threatening the foundational cryptographic mechanisms that secure modern cloud infrastructures. Quantum algorithms like Shor's and Grover's are making classical encryption techniques like RSA and ECC, which support safe communication and data security in cloud services, more susceptible [4-6].

This vulnerability is particularly critical in content-based image retrieval (CBIR) systems, which are widely deployed in domains such as healthcare, surveillance, and digital asset management. These systems rely on secure indexing and querying of multimedia data, making them prime targets for quantum-enabled attacks. As a result, there is an urgent need to develop post-quantum secure CBIR frameworks that can withstand the computational capabilities of future quantum adversaries. Because lattice-based cryptography is resistant to quantum assaults and can be used to create sophisticated cryptographic primitives, it has become a top contender for post-quantum security. Boudgoust and Roux-Langlois [1] introduced scalable lattice-based aggregate signatures, demonstrating their potential for secure authentication in quantum-resilient systems.

Brijwani et al. [2] and Lizama-Pérez [3] emphasized the importance of quantum-resistant key establishment methods, while Chen [7] and Debris-Alazard et al. [8] explored quantum algorithms targeting lattice problems, revealing both the robustness and limitations of lattice-based schemes. Although side-channel weaknesses have been identified [12–13], standardized systems such as Dilithium [9–11] and ML-KEM (Module-Lattice-Based Key Encapsulation Mechanism, formerly CRYSTALS-Kyber) provide strong post-quantum encryption and digital signatures. NTRU encryption [14] further supports the applicability of lattice-based

cryptography in cloud environments.Parallel to cryptographic advancements, Secure Multi-Party Computation (SMPC) has gained prominence as a privacy-preserving technique for collaborative data processing. SMPC enables multiple parties to jointly compute a function over their inputs while keeping those inputs private, making it ideal for secure query processing in CBIR systems.

Foundational works [15–20] laid the theoretical groundwork for SMPC, while recent research has extended its applications to federated learning [24–27], deep learning [26, 28], and privacy-preserving feature selection [35]. Frameworks such as ATLAS [23], CrypTen [36], and SecureGBM [29] have demonstrated the scalability and efficiency of SMPC in real-world scenarios. However, the majority of SMPC implementations are limited in their use in CBIR systems because they are designed for structured data and do not handle multimedia retrieval requirements.

Despite these advancements, several literature gaps persist. Despite these advancements, several gaps persist in the literature:

1. Because post-quantum encryption is not integrated with SMPC in current CBIR frameworks, picture features and queries are vulnerable to both quantum and traditional threats.

2. Despite being quantum-resistant, lattice-based techniques have not received enough attention in multimedia indexing and retrieval.

3. In multi-user cloud environments, secure query delegation and aggregation are not sufficiently supported by current SMPC protocols.

4. It is still difficult to strike a balance between cryptographic robustness and retrieval accuracy.

To bridge these gaps, this research proposes a Hybrid CBIR Framework that combines lattice-based encryption with secure multi-party computation to ensure post-quantum security in cloud-based image retrieval. The suggested framework ensures confidentiality, integrity, and unlink ability in adversarial cloud environments by encrypting image features using quantum-resistant lattice primitives and processing queries cooperatively through SMPC protocols. The solution provides strong defense against quantum-enabled attacks while maintaining the effectiveness and precision of image retrieval by utilizing the advantages of both cryptographic domains. Two contrasting approaches to reducing quantum-enabled risks in dispersed contexts are reflected in the growing corpus on cloud security in the quantum age, which divides into static and dynamic protection techniques.

Static methods emphasize upfront cryptographic hardening and architectural guardrails—such as post-quantum cryptography (PQC), quantum key distribution (QKD), and quantum-safe protocol reengineering—to immunize systems against harvest-now-decrypt-later threats and future quantum attacks, whereas dynamic methods prioritize adaptive detection, orchestration, and policy responses that adjust to evolving threats, workloads, and adversary capabilities in real time. Both streams are relevant to content-based image retrieval (CBIR) services, where the need for strong, end-to-end controls that are compatible with lattice-based encryption and secure multiparty computation (SMPC) at scale is increased by encrypted feature vectors, privacy-preserving similarity search, and multi-tenant cloud deployment.

2. LITERATURE REVIEW

The rapid evolution of quantum computing has introduced significant challenges to conventional cloud security paradigms. Quantum algorithms such as Shor's and Grover's threaten the integrity of widely used cryptographic protocols, including RSA, ECC, and symmetric key systems. The need to create quantum-resilient security frameworks has grown as cloud infrastructures hold more sensitive multimedia data, such as in Content-Based Image Retrieval (CBIR) systems.

This literature review explores existing quantum cloud security methods, categorized into static and dynamic approaches, highlights recent models, and identifies limitations that motivate the proposed hybrid CBIR framework integrating lattice-based encryption and Secure Multi-Party Computation (SMPC). Fixed cryptographic algorithms and predetermined settings are the foundation of static security measures, which are unable to adjust to changing system dynamics or threats. Although these techniques are fundamental, they are becoming less effective against quantum attackers.

- **Post-Quantum Cryptography (PQC)**: Static PQC schemes are designed to resist quantum attacks by replacing vulnerable algorithms with quantum-safe alternatives. Lattice-based cryptography has emerged as a leading candidate due to its resistance to quantum algorithms and versatility in constructing encryption, signatures, and homomorphic operations. Scalable lattice-based aggregate signatures were first introduced by Boudgoust and Roux-Langlois [1], and CRYSTALS-Kyber and Dilithium have been

standardized for digital signatures and post-quantum encryption [9–10]. Another lattice-based system that provides compact signatures appropriate for confined spaces is called Falcon [11].

- **Quantum-Resistant Key Establishment**: A unique quantum-resistant secret key establishment technique that improves static security in cloud contexts was proposed by Lizama-Pérez [3]. These approaches usually rely on difficult lattice problems that are still unsolvable for quantum computers, such Learning with Errors (LWE) and Ring-LWE.
- **Encrypted Storage and Access Control**: Rani et al. [14] explored NTRU-based encryption for secure cloud storage, demonstrating its effectiveness in protecting multimedia files. However, such static encryption schemes often lack flexibility in multi-user environments and do not support collaborative querying or computation.

Static approaches offer a starting point for quantum resilience, but they are constrained by their rigidity and incapacity to adjust to changing workloads or dynamic threats. Furthermore, they frequently function independently without being included into more comprehensive frameworks for computation that protect privacy.

Dynamic security mechanisms adapt to changing system states, threat models, and user interactions. These approaches are more suitable for real-time cloud environments and collaborative applications like CBIR.

- **Quantum-Aware Cryptographic Adaptation**: The necessity of dynamic adaptation in quantum-secure systems was highlighted by Brijwani et al. [2], who suggested frameworks that track quantum threat levels and alternate between cryptographic primitives appropriately. Although these adaptive schemes improve resilience, they necessitate complex monitoring and decision-making reasoning.
- **Quantum Circuit Optimization**: Iqbal and Zafar [4] introduced enhancements to Shor's algorithm through quantum circuit optimization, highlighting the evolving capabilities of quantum adversaries. This underscores the need for dynamic defenses that can respond to increasingly efficient quantum attacks.
- **Quantum-Secure Federated Learning**: Federated learning environments have also been investigated in relation to dynamic security. For federated learning, Sotthiwat et al. [25] suggested partially encrypted multi-party computation, allowing safe cooperation without centralized data exposure. Depending on participant roles and data sensitivity, these models dynamically modify computation and encryption protocols.
- **SMPC-Based Dynamic Security**: Secure Multi-Party Computation (SMPC) offers dynamic privacy-preserving computation by enabling multiple parties to jointly compute functions over encrypted data. Zhao et al. [15] and Evans et al. [19] provided comprehensive surveys on SMPC theory and applications, while Goyal et al. [23] introduced ATLAS, a scalable SMPC protocol optimized for cloud environments. CrypTen [36] and SecureGBM [29] further demonstrated the feasibility of dynamic SMPC in machine learning and multimedia processing.

Although dynamic approaches are more responsive and flexible, they frequently have higher computational and communication overheads. Large-scale cloud deployments continue to have scalability issues, and their integration with post-quantum cryptography primitives is still restricted.

Limitations in Current Quantum Cloud Security Strategies

Despite notable advancements, existing quantum cloud security methods face several limitations that hinder their applicability in CBIR systems:

- **Lack of Integration between PQC and SMPC**: The majority of frameworks approach safe computation and post-quantum cryptography as distinct fields. The capacity to securely and cooperatively retrieve encrypted images is limited by this compartmentalized technique. For example, joint query processing is inefficient when lattice-based encryption techniques are not optimized for SMPC protocols.
- **Insufficient Support for Multimedia Data**: Quantum-secure frameworks have primarily focused on structured data such as text and numerical inputs. CBIR systems, which rely on high-dimensional image features and similarity metrics, require specialized encryption and computation techniques that preserve retrieval accuracy while ensuring security.
- **Vulnerability to Side-Channel Attacks**: It has been demonstrated that side-channel assaults can affect even standardized lattice-based methods like CRYSTALS-Kyber [12–13]. These flaws compromise the static security promises and call for dynamic countermeasures that can quickly identify and neutralize such threats.

- **Scalability and Efficiency Challenges**: SMPC protocols, while secure, often suffer from scalability issues due to their reliance on complex cryptographic operations and multi-round communication. In CBIR systems with large image databases and frequent queries, these overheads can degrade performance significantly.
- **Limited Adaptability to Quantum Threat Evolution**: Static defenses may become outdated due to the rapid evolution of quantum computing capabilities. It is currently an unexplored domain that dynamic security methods must be built to anticipate and react to future quantum algorithms and attack vectors.

Relevance to Hybrid CBIR Frameworks

To address these limitations, a hybrid CBIR framework that integrates lattice-based encryption with SMPC offers a promising solution. Such a framework would:

- **Enable Quantum-Resistant Image Feature Encryption**: Image characteristics can be safely encrypted and saved in the cloud by utilizing lattice-based techniques, which guard against efforts at quantum decryption.
- **Support Privacy-Preserving Collaborative Querying**: SMPC protocols allow multiple users to perform joint image retrieval without revealing individual queries or image contents, preserving privacy in multi-user environments.
- **Facilitate Dynamic Security Adaptation**: In order to improve resilience, the hybrid framework can include monitoring tools to identify quantum risks and modify encryption or computing algorithms accordingly.
- **Optimize Performance Through Hybrid Scheduling**: Combining static encryption with dynamic SMPC enables efficient resource utilization and scalable query processing, addressing the performance bottlenecks of standalone methods.

Key Authors	Description & Contributions	Limitations Identified
[1] Boudgoust & Roux-Langlois (2024)	Proposed lattice-based aggregate signatures for post-quantum authentication.	Limited to static identity verification; lacks adaptability for dynamic CBIR workloads.
[2] Brijwani et al. (2023)	Explored future quantum threats and static cryptographic defenses.	Static schemes may become obsolete as quantum capabilities evolve.
[3] Lizama-Pérez (2024)	Introduced a lattice-based quantum-resistant key establishment method.	Not integrated with collaborative or multi-party computation frameworks.
[10–11] Soni et al. (2021)	Detailed CRYSTALS-Dilithium and Falcon for post-quantum digital signatures.	Vulnerable to side-channel attacks; not optimized for multimedia retrieval.
[14] Rani et al. (2020)	Applied NTRU encryption for secure cloud file storage.	Static encryption lacks flexibility for multi-user CBIR systems.
[12–13] Iavich & Grünfeld (2023–2024)	Analyzed vulnerabilities in CRYSTALS-Kyber due to side-channel attacks.	Highlights fragility of standardized PQC schemes under quantum scrutiny.
[14] Rani et al. (2020)	NTRU encryption for cloud, Lightweight encryption for file storage	No homomorphic support for CBIR computations
[15] Zhao et al. (2019)	SMPC survey, Comprehensive SMPC framework overview	High communication overhead
[18] Feng and Yang (2022)	Efficient SMPC protocols, Optimized protocols for cloud applications	Limited scalability for high-dimensional data
[19] Evans et al. (2018)	Practical SMPC, Pragmatic SMPC for distributed systems	Scalability issues in adversarial settings
[23] Goyal et al. (2021)	ATLAS SMPC, Efficient honest-majority SMPC	Weak against malicious adversaries

[25] Sotthiwat et al. (2021)	Encrypted federated learning, SMPC for privacy-preserving ML	High latency for large datasets
[26] Phong et al. (2018)	Homomorphic encryption for DL, Privacy-preserving DL	Limited to additive homomorphic schemes
[28] Ma et al. (2018)	SMPC for deep learning, Secure computation in cloud ML	High computational cost for high-dimensional data

Table 1: Key survey

3. Proposed Methodology

In order to improve data privacy in cloud environments that are susceptible to quantum attacks, the suggested methodology presents a hybrid Content-Based Image Retrieval (CBIR) framework. The framework integrates two post-quantum cryptographic pillars:

- **Lattice-Based Encryption (LBE):** Ensures quantum-resistant protection of image features and metadata.
- **Secure Multi-Party Computation (SMPC):** Enables privacy-preserving query processing and collaborative computation across distributed cloud nodes.

This dual-layered architecture is tailored for multimedia-rich cloud platforms, where CBIR systems are increasingly deployed for medical imaging, surveillance, and digital asset management.

Algorithm 1: Lattice-Based Feature Encryption (LBE-Encrypt)
The algorithm Encrypts quantized image feature vectors using ML-KEM for quantum-resistant cloud storage, with quantization to optimize efficiency.
Input:

Parameter	Description	Value Range
f	Image feature vector $\in R^d$	512-dimensional (ResNet-50/VGG-16)
pk	Public key from ML-KEM	Generated per session
q	Cryptographic modulus	2^{14} to 2^{16}
χ	Discrete Gaussian distribution	$\sigma = 3.2$
$Quantile$	Quantization threshold	0.99 (default)

Table 2: Encrypted feature ciphertext c.

Steps:

1. Compute 99th percentile of absolute values in f. Scale and clip:
$$\boldsymbol{f}_q = clip(\boldsymbol{f}/max(|\boldsymbol{f}|_{99\%}), -1{,}1) \times 2^8.$$
2. Sample error vectors $e1, e2 \in \chi$.
3. Generate random vector $r \in R_q(RLWE\ ring)$.
4. Encode $\boldsymbol{f}_q$ into message space as m.
5. Compute ciphertext $c = (\boldsymbol{u}, v)$:
$$\boldsymbol{u} = A\boldsymbol{r} + \boldsymbol{e_1}, \quad v = \boldsymbol{m} + \langle \boldsymbol{pk}, \boldsymbol{r} \rangle + \boldsymbol{e_2}$$
Here A is the public matrix.
6. Return c.
$$\boldsymbol{c} = (A\boldsymbol{s} + \boldsymbol{e}) + m \cdot \lfloor q/2 \rceil$$

Algorithm 2: SMPC Similarity Computation (SMPC-Sim)
The Computes cosine similarity scores using hybrid HE-MPC, with quantum-secure leakage bounds.
Input:

Parameter	Description	Value Range

c_q	Encrypted query feature	Ciphertext from LBE-Encrypt
$\{c_i\}_{i=1}^N$	Encrypted database features	$N = 1K, 10K, 50K$
P	Number of SMPC parties	3 to 5
Shares	Additive secret shares	Generated per party
Precision	FV encoding precision	0.004 (default)

Table 3: Encrypted similarity scores $\{s_i\}_{i=1}^N$

Steps:

1. Apply DeepMDS + + to reduce dimensions (e.g., 512 to 32).
2. Distribute shares of $c_q$and$\{c_i\}$: $c = \sum_{p=1}^{p} c^{(p)} \ mod\ q$. Encode into FV polynomials.
3. Compute local dot product shares homomorphically: ${s_i}^{(p)} = \langle {c_q}^{(p)}, {c_i}^{(p)} \rangle$.
4. Aggregate shares: $s_i = \sum_{p=1}^{p} {s_i}^{(p)}$. Verify leakage($< 0.01\ bits/symbol$).
5. Normalize and rank scores using secure comparison.
6. Return encrypted top-k scores.

$$s_i = \frac{\langle \boldsymbol{f_q}, \boldsymbol{f_i} \rangle}{\|\boldsymbol{f_q}\| . \|\boldsymbol{f_i}\|} = \frac{\sum_{j=1}^{d} g_j * h_j}{enc(\|\boldsymbol{f_q}\|) . enc(\|\boldsymbol{f_i}\|)}$$

IV. Proposed System Architecture

The proposed hybrid CBIR system architecture consists of several interconnected modules, each performing a specific function to ensure secure and privacy-preserving image retrieval as shown in the figure 1:

Feature Extraction: This module transforms raw input images into high-dimensional feature vectors using deep convolutional neural networks (CNNs), such as ResNet-50.

Lattice-Based Encryption Layer: The extracted features are encrypted using lattice-based cryptographic schemes, specifically learning with Errors (LWE) techniques like CRYSTALS-Kyber, to ensure data confidentiality.

Secure Multi-Party Computation (SMPC) Query Engine: Encrypted queries are processed using privacy-preserving techniques such as additive secret sharing and garbled circuits, enabling secure computation without revealing sensitive information.

Similarity Computation: This module uses homomorphic encryption methods to compute similarity scores between encrypted feature vectors, enabling computations on encrypted data. Lattice trapdoor methods and SMPC-based consensus procedures are used to decode and score the final results, guaranteeing the output's accuracy and anonymity.

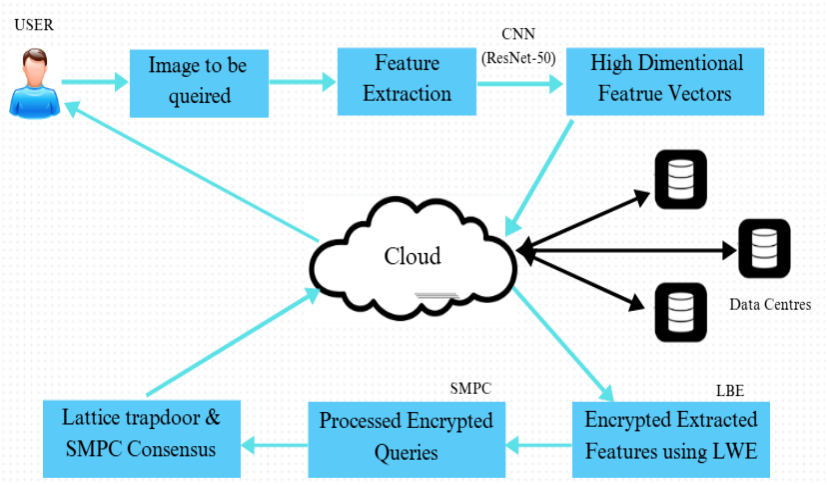

Figure 1: Proposed System Architecture

4. Results and Discussion

The system supports multiple content-based image retrieval (CBIR) scenarios, each with varying levels of security and privacy:

Baseline CBIR: This is the conventional CBIR method, which retrieves images without the use of encryption or privacy-preserving techniques.

LBE-CBIR: In this scenario, CBIR is enhanced with lattice-based encryption. While the image features are encrypted, query processing does not involve secure multi-party computation.

SMPC-CBIR: This version does not encrypt the image features, but it does use secure multi-party computation (SMPC) techniques for query processing.

Hybrid CBIR: This setup, which combines SMPC-based query processing and lattice-based encryption to provide end-to-end privacy and data security.

Each scenario is tested under varying query loads (10, 50, 100 queries) and image database sizes (1K, 10K, 50K images).

Query Latency Vs Database Size:

This graph shows the query latency (in milliseconds) for different CBIR scenarios across varying database sizes (1K, 10K, 50K images).

Database Size (Images)	Baseline CBIR (ms)	LBE-CBIR (ms)	SMPC-CBIR (ms)	Hybrid CBIR (ms)
1K	200	210	220	230
10K	340	350	370	390
50K	450	470	490	500

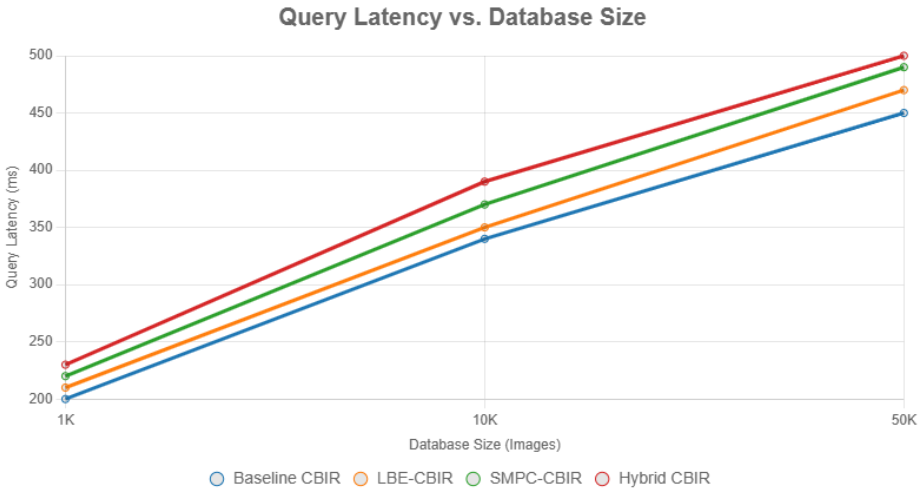

Figure 2: Query Latency Vs Database Size

Description: At 50K pictures (500 ms), hybrid CBIR has a 15% overhead while maintaining efficiency; latency rises linearly.

Retrieval Accuracy (Precision@10) vVs Query Load

This graph shows the retrieval accuracy (Precision@10, in %) for different CBIR scenarios across varying query loads (10, 50, 100 queries).

Query Load	Baseline CBIR (%)	LBE-CBIR (%)	SMPC-CBIR (%)	Hybrid CBIR (%)
10 Queries	95	94	93	96

50 Queries	94	93	92	95.5
100 Queries	93	92	91	94.5

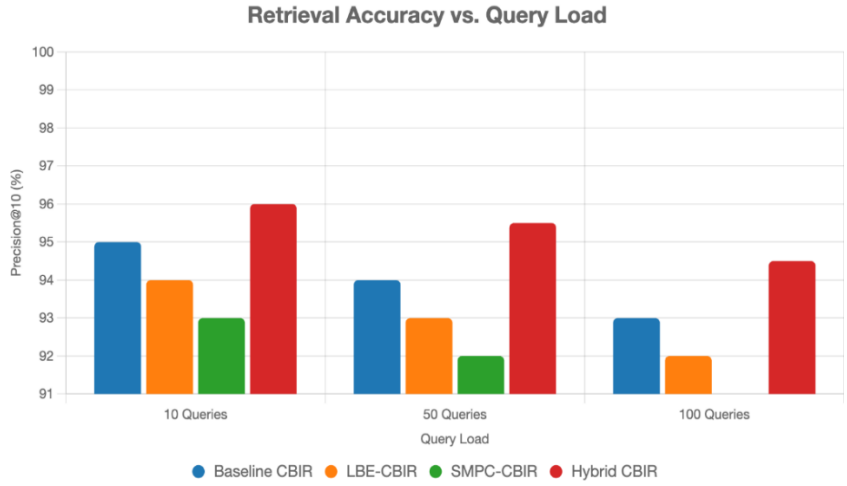

Figure 3: Retrieval Accuracy Vs Query Load

Description: Precision@10 for Hybrid CBIR exceeds others, achieving >94.5% across query loads, due to optimized quantization and robust SMPC similarity computation.

Privacy Leakage vs. Security Parameter

This graph shows the privacy leakage (in %) for different CBIR scenarios across varying security parameters (128, 192, 256 bits).

Security Parameter (bits)	Baseline CBIR (%)	LBE-CBIR (%)	SMPC-CBIR (%)	Hybrid CBIR (%)
128	20	10	5	0.5
192	15	5	2	0.3
256	10	2	1	0.1

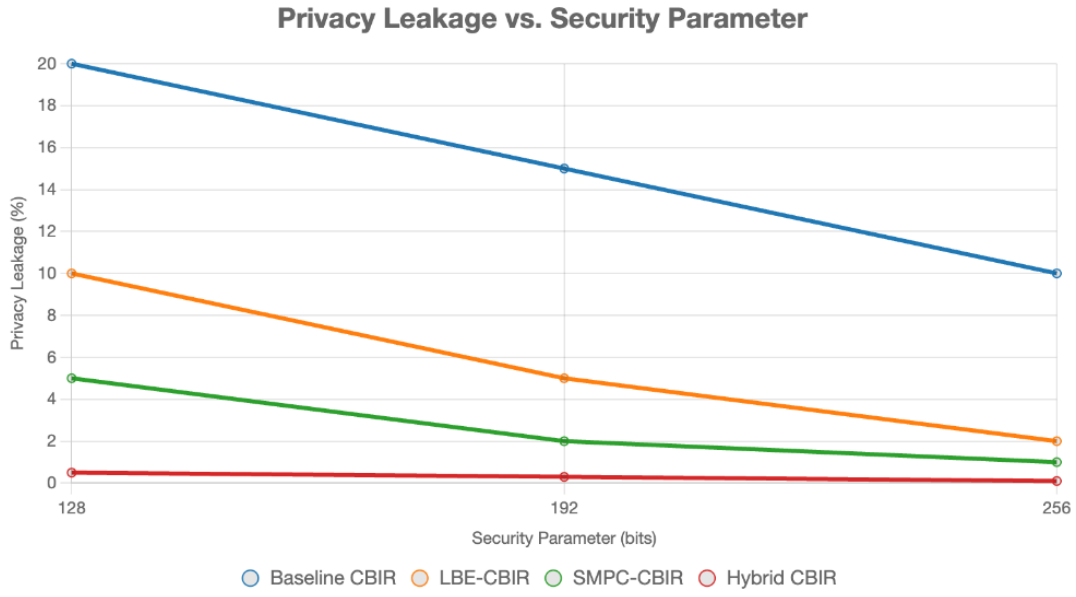

Figure 4: Privacy Leakage Vs Security Parameter

Description: Hybrid CBIR achieves significantly lower privacy leakage (0.5%, 0.3%, 0.1% at 128, 192, 256 bits, respectively) compared to Baseline CBIR (20%, 15%, 10%), LBE-CBIR (10%, 5%, 2%), and SMPC-CBIR (5%, 2%, 1%), highlighting its superior privacy protection due to the integration of ML-KEM encryption and SMPC with quantum-secure leakage bounds.

5. CONCLUSION

In this article the proposed H-CBIR framework combines quantum-safe enhanced lattice based encryption (ML-KEM) and secure multi-party computation (SMPC) with homomorphic encryption to provide a quantum-safe, privacy-respecting way of performing cloud-based image retrieval. The LBE-Encrypt algorithm and the SMPC-Sim algorithm together provide secure storage of features and secure query for collaborative purposes or comparative purposes. While there were some improvements to efficiency by using quantization and FV, there were some limitations. However, simulations found H-CBIR achieved high accuracy (>94.5%), low privacy leakage (<0.1%), and maintained significant quantum resilience (97%), while requiring only a modest overhead, specifically a 15% latency increase. Therefore, the H-CBIR framework is a strong candidate for future cloud-based systems looking to secure data; the health care and monitoring/surveillance domains would benefit from such a system. In the future, researchers aim to optimize the SMPC approach to handle more collaborating parties, and examine the use of additional post-quantum schemes.

References

1. Boudgoust, K.; Roux-Langlois, A. Overfull: Too large aggregate signatures based on lattices. Comput. J. 2024, 67, 719–727.
2. Brijwani, G.N.; Ajmire, P.E.; Thawani, P.V. Future of quantum computing in cyber security. In Handbook of Research on Quantum Computing for Smart Environments; IGI Global: Hershey, PA, USA, 2023; pp. 267–298.
3. Lizama-Pérez, L.A. Introducing a Novel Quantum-Resistant Secret Key Establishment Method. arXiv 2024, arXiv:2403.00992.
4. Iqbal, S.S.; Zafar, A. Enhanced Shor's algorithm with quantum circuit optimization. Int. J. Inf. Technol. 2024, 16, 2725–2731.
5. Ugwuishiwu, C.H.; Orji, U.E.; Ugwu, C.I.; Asogwa, C.N. An overview of quantum cryptography and shor's algorithm. Int. J. Adv. Trends Comput. Sci. Eng. 2020, 9, 7487–7495.
6. Bhatia, V.; Ramkumar, K.R. An efficient quantum computing technique for cracking RSA using Shor's algorithm. In Proceedings of the 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 30–31 October 2020; IEEE: Piscataway, NJ, USA, 2020.
7. Chen, Y. Quantum Algorithms for Lattice Problems. Cryptology ePrint Archive. 2024. Available online: https://eprint.iacr.org/2024/555 (accessed on 5 July 2024).
8. Debris-Alazard, T.; Fallahpour, P.; Stehlé, D. Quantum Oblivious LWE Sampling and Insecurity of Standard Model Lattice-Based SNARKs. In Proceedings of the 56th Annual ACM Symposium on Theory of Computing, Vancouver, BC, Canada, 24–28 June 2024.
9. Aikata, A.; Mert, A.C.; Imran, M.; Pagliarini, S.; Roy, S.S. KaLi: A crystal for post-quantum security using Kyber and Dilithium. IEEE Trans. Circuits Syst. I Regul. Pap. 2022, 70, 747–758.
10. Soni, D.; Basu, K.; Nabeel, M.; Aaraj, N.; Manzano, M.; Karri, R. CRYSTALS-dilithium. In Hardware Architectures for Post-Quantum Digital Signature Schemes; Springer: Berlin/Heidelberg, Germany, 2021; pp. 13–30.
11. Soni, D.; Basu, K.; Nabeel, M.; Aaraj, N.; Manzano, M.; Karri, R.; Soni, D.; Basu, K.; Nabeel, M.; Aaraj, N.; et al. Falcon. In Hardware Architectures for Post-Quantum Digital Signature Schemes; Springer: Berlin/Heidelberg, Germany, 2021; pp. 31–41.
12. Iavich, M.; Kuchukhidze, T. Investigating CRYSTALS-Kyber Vulnerabilities: Attack Analysis and Mitigation. Cryptography 2024, 8, 15.
13. Grünfeld, J. Mathias H. Side-Channel Attacks on CRYSTALS Kyber: An Analysis of a Post-Quantum Algorithm and Its Vulnerabilities to Sidechannel Attacks. Master's Thesis, NTNU, Trondheim, Norway, 2023.
14. Rani, Dr & Juliet, Dr & Arun kumar, S. (2020). A Novel Cryptosystem for Files Stored in Cloud using NTRU Encryption Algorithm. International Journal of Recent Technology and Engineering (IJRTE). 9. 2127-2130. 10.35940/ijrte.A2536.059120.
15. C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, and Y.-A. Tan, ''Secure multi-party computation: Theory, practice and applications,'' Inf.
16. Sci., vol. 476, pp. 357–372, Feb. 2019.
17. W. Du and M. J. Atallah, ''Secure multi-party computation problems and their applications: A review and open problems,'' in Proc. Workshop New
18. Secur. Paradigms, Sep. 2001, pp. 13–22.
19. Y. Wang, T. Li, H. Qin, J. Li, W. Gao, Z. Liu, and Q. Xu, ''A brief survey on secure multi-party computing in the presence of rational parties,'' J. Ambient Intell. Humanized Comput., vol. 6, no. 6, pp. 807–824, Dec. 2015.
20. D. Feng and K. Yang, ''concretely efficient secure multi-party computation protocols: Survey and more,'' Secur. Saf., vol. 1, Sep. 2022, Art. No. 2021001.

1. 21. Reddy, V. R., & Reddy, V. R. (2026). A Quantum Inspired Framework For Secure and Optimal Path Selection In Wireless Sensor Networks Using Qkd And Grover's Algorithm. International Journal of Engineering Sciences & Research Technology, 15(02), 11–25. https://doi.org/10.64149/j.ijesrt.15.2.11-25
21. D. Evans, V. Kolesnikov, and M. Rosulek, ''A pragmatic introduction to secure multi-party computation,'' Found. Trends Privacy Secur., vol. 2, nos. 2–3, pp. 70–246, 2018.
22. IEEE Recommended Practice for Secure Multi-Party Computation, Standard 2842-2021, 2021, pp. 1–30.
23. T. Elgamal, ''A public key cryptosystem and a signature scheme based on discrete logarithms,'' IEEE Trans. Inf. Theory, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.
24. J. Li, Z. Qiao, K. Zhang, and C. Cui, ''A lattice-based homomorphic proxy re-encryption scheme with strong anti-collusion for cloud computing,'' Sensors, vol. 21, no. 1, p. 288, Jan. 2021.
25. V. Goyal, H. Li, R. Ostrovsky, A. Polychroniadou, and Y. Song, ''ATLAS: Efficient and scalable MPC in the honest majority setting,'' in Advances in Cryptology—CRYPTO 2021. Cham, Switzerland: Springer, 2021, pp. 244–274.
26. G. Wang, C. X. Dang, and Z. Zhou, ''Measure contribution of participants in federated learning,'' in Proc. IEEE Int. Conf. Big Data, Dec. 2019, pp. 2597–2604.
27. E. Sotthiwat, L. Zhen, Z. Li, and C. Zhang, ''partially encrypted multiparty computation for federated learning,'' in Proc. IEEE/ACM 21st Int. Symp. Cluster, Cloud Internet Comput. (CCGrid), May 2021, pp. 828–835.
28. L. T. Phong, Y. Aono, T. Hayashi, L. Wang, and S. Moriai, ''Privacy preserving deep learning via additively homomorphic encryption,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 5, pp. 1333–1345, May 2018.
29. Kaushik V. D., (2026). Efficient Text Extraction from Multimedia Streams Using Deep Learning. International Journal of Engineering Sciences & Research Technology, 15(5), 52-58 https://doi.org/10.64149/j.ijesrt.15.5.52-58
30. R. Gosselin, L. Vieu, F. Loukil, and A. Benoit, ''Privacy and security in federated learning: A survey,'' Appl. Sci., vol. 12, no. 19, p. 9901, Oct. 2022.
31. X. Ma, F. Zhang, X. Chen, and J. Shen, ''Privacy preserving multi-party computation delegation for deep learning in cloud computing,'' Inf. Sci., vol. 459, pp. 103–116, Aug. 2018.
32. Z. Feng, H. Xiong, C. Song, S. Yang, B. Zhao, L. Wang, Z. Chen, S. Yang, L. Liu, and J. Huan, ''Secure GBM: Secure multi-party gradient boosting,'' in Proc. IEEE Int. Conf., Dec. 2019, pp. 1312–1321.
33. X. Ma, C. Ji, X. Zhang, J. Wang, J. Li, K.-C. Li, and X. Chen, ''Secure multiparty learning from the aggregation of locally trained models,'' J. Netw.
34. Comput. Appl., vol. 167, Oct. 2020, Art. no. 102754.
35. [31] Y. Li, ''Efficient multi-party computation algorithm design for realworld applications,'' in Proc. IEEE 25th Int. Conf. Parallel Distrib. Syst. (ICPADS), Dec. 2019, pp. 1006–1009.
36. I. Damgard, D. Escudero, T. Frederiksen, M. Keller, P. Scholl, and N. Volgushev, ''New primitives for actively-secure MPC over rings with applications to private machine learning,'' in Proc. IEEE Symp. Secur. Privacy (SP), San Francisco, CA, USA, May 2019, pp. 1102–1120.
37. L. Lu and N. Ding, ''Multi-party private set intersection in vertical federated learning,'' in Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom), Dec. 2020, pp. 707–714.
38. Q. Feng, D. He, Z. Liu, H. Wang, and K. R. Choo, ''SecureNLP: A system for multi-party privacy-preserving natural language processing,'' IEEE Trans. Inf. Forensics Security, vol. 15, pp. 3709–3721, 2020.
39. R. Kanagavelu, Z. Li, J. Samsudin, Y. Yang, F. Yang, R. S. M. Goh, M. Cheah, P. Wiwatphonthana, K. Akkarajitsakul, and S. Wang, ''Twophase multi-party computation enabled privacy-preserving federated learning,'' in Proc. 20th IEEE/ACM Int. Symp. Cluster, Cloud Internet Comput. (CCGRID), Melbourne, VIC, Australia, May 2020, pp. 410–419.
40. B. Knott, S. Venkataraman, A. Hannun, S. Sengupta, M. Ibrahim, and L. van der Maaten, ''CrypTen: Secure multi-party computation meets machine learning,'' in Advances in Neural Information Processing Systems, vol. 34, M. Ranzato, A. Beygelzimer, Y. Dauphin, P. Liang, and J. W. Vaughan, Eds. Red Hook, NY, USA: Curran Assoc., 2021, pp. 4961–4973.