

Privacy or Performance? Towards Secure and Scalable Medical Image Storage and Retrieval Management in the Cloud

Arun Amaithi Rajan*
Department of Computer Science and Engineering
College of Engineering Guindy, Anna University
Chennai, Tamil Nadu, India
arunamaithirajan@gmail.com

Vetriselvi V
Department of Computer Science and Engineering
College of Engineering Guindy, Anna University
Chennai, Tamil Nadu, India
kalvivetri@gmail.com

Abstract

Medical images play an important role in diagnosis in digitalized healthcare and carry essential and sensitive information regarding effective patient care. Given the increasing volume of medical imaging data, the healthcare sector has become more reliant on cloud-based third-party storage for the purposes of effective storage and retrieval. Content-Based Medical Image Retrieval (CBMIR) has become important. However, privacy and security concerns are inherent to cloud-based solutions. This thesis has laid out a series of frameworks from different points of view to provide secure, efficient, and scalable storage and retrieval of medical images. An integrity-centric image encryption technique has been developed to ensure better security along with searchable encrypted hashcodes that can help with CBMIR. Nevertheless, achieving a balance between retrieval performance and security remains a challenge. Targeted encryption is employed to achieve this balance by focusing on sensitive regions in the images, thus exploiting fusion-based hashcodes to assist with image retrieval. For scaling purposes, a distributed storage scheme is presented, where the encrypted images are broken down into shadow segments to ensure data integrity and resilience. Edge computing is used to achieve better latency with security and scalability. The presented solutions for secure storage and retrieval of medical images provide novel frameworks to support the healthcare industry's demands in a cloud environment, making these solutions relevant for improving security, performance, and scale in digital healthcare applications.

CCS Concepts

• **Security and Privacy** → **Multimedia Security**.

Keywords

Medical Images, Cloud Computing, Secure Storage, Efficient CBIR, Scalability

ACM Reference Format:
Arun Amaithi Rajan and Vetriselvi V. 2025. Privacy or Performance? Towards Secure and Scalable Medical Image Storage and Retrieval Management in the Cloud. In *18th Innovations in Software Engineering Conference (ISEC 2025), February 20–22, 2025, Kurukshetra, India.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3717383.3717398



This work is licensed under a Creative Commons Attribution International 4.0 License.

ISEC 2025, Kurukshetra, India
© 2025 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1424-5/25/02
https://doi.org/10.1145/3717383.3717398

1 Introduction

In this era of massive technological advancement, multimedia files such as videos, images, and audio represent some of the most common forms of conveying information, with a huge volume of data transferring on data networks. According to the latest statistics, 1.72 trillion images are taken every year, mostly by smartphones, and it is estimated that this number will grow by 10-14% annually. By 2030, the figure will stand at an astonishing 28.6 trillion [4]. Therefore, this expansion in numerical value gives weight to the concept of how important images are for life. Nowadays, images are indispensable in remote sensing and healthcare. More with regard to the medical profession, medical imaging has been one of the most important elements of assuring enhancement in accuracy upon growing difficult diagnoses [11].

Increasing medical imaging data often prompts facilities to utilize cloud storage, typically short for cost, scalability, and accessibility [7]. By eliminating disadvantages plaguing local storage, cloud solutions assist in data-sharing, collaborations, and remote access to medical imaging. On the contrary, however, cloud storage comes with security challenges, including potential data loss, insider threats, and data breaches [9]. Heady methods like data loss prevention, granular access controls such as role-based permissions and multi-factor authentication, and encryption of images both in transit and at rest will enhance the security of medical images. Healthcare organizations may maintain the availability, confidentiality, and integrity of medical images stored on cloud servers if given a complete security framework. Besides secure storage, efficient retrieval plays an important role in healthcare applications, especially in CBIR [5]. Earlier, manual annotation techniques such as Text-based Image Retrieval (TBIR) [13] were used for retrieving images in the healthcare domain. Content-based Image Retrieval was developed due to its tedious nature and mainly uses inherent properties of images to improve search efficiency, particularly for medical images [10]. The retrieval turns overly complex while images are encrypted for decryption, meeting both latency and computation complexity. Since retrieving healthcare images for diagnosis and treatment is usually time-sensitive, secure and efficient retrieval mechanisms are needed to balance data confidentiality and accessibility [8]. As a consequence, secure and efficient retrieval frameworks must be developed. Today, most of the storage and retrieval systems are centralized storage, which prevents scalability. The rising data volume proves this approach to be challenging [6].

Hence, the investigation into strategies built on distributed storage forms for maintaining performance and capacity is a top priority in providing security and efficiency at scales. Figure 1 shows the generalized framework of secure storage and retrieval for medical images in cloud-based systems.

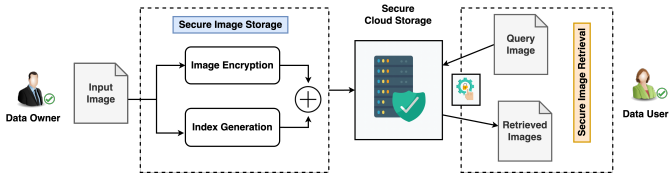


Figure 1: Framework for Secure Medical Image Storage and Retrieval

The objective of this thesis is to find the solution to the major problems of security, retrieval performance, and scalability, so as to propose secure alternatives for CBMIR. The intention is to design dependable systems for scalability, retrieval speed-up, and medical data protection against insecure access in response to an ever-growing volume of medical images.

The contents of this article are as follows: the research questions and objectives leading toward this research are discussed in Section 2, and principal issues posed under potential developments. In Section 3, very wide discussions are conducted with respect to the proposed methodologies for achieving the stated objectives and also the techniques and frameworks employed for the designs. In Section 4, the status quo of the research project is expressed, centering on the common developments made thus far. In Section 5, the results are summarized, and recommendations for further research are made.

2 Research Questions and Objectives

This dissertation aims to address issues concerning security, scalability, and efficiency in cloud-assisted medical image storage and retrieval. The problem statement is articulated through the first research question, which pursues the security of medical image storage and retrieval in the cloud. **RQ1: How could researchers develop a secure and privacy-preserving retrieval system for medical images stored in the cloud?** To handle that, the first work proposes a fully encryption-based solution that keeps sensitive medical images secure while allowing retrieval by means of CBMIR methods. The proposed method encrypts images and indexes to offer both integrity and searchability. However, performance is adversely affected by the encryption, resulting in high storage requirements and computational complexity.

Achieving the ”balance between security and retrieval performance” in the secure CBMIR is the second research question. **RQ2: How could the researchers improve the efficiency of medical image storage and retrieval while also maintaining high levels of security?** To reduce computation overhead and reduce the high requirement for storage, targeted encryption has been proposed. Instead of extracting features from the whole image, authors hash both global and local features into an indexing technique. This proposed approach aims to provide confidentiality with a reasonable retrieval performance to meet requirements for real-world applications in healthcare.

The third question involves an analysis of scalability within distributed storage. **RQ3: How can available solutions be improved to support the secure storage and retrieval of large medical datasets in distributed environments?** Given the massive anticipated amount of medical imaging data, an efficient and scalable system to manage huge collections of medical image data is needed. The method developed generates encrypted image shadows, hashcodes and uses edge computing-based storage for improving scalability and resilience against attacks.

The thesis is thus organized as follows: The Introduction is an overview of the need and the obstacles faced in securely archiving medical images in the healthcare sector. The Related Work chapter then examines the current approaches and the gaps in need of improvement. Work 1 deals with secure retrieval (Chapter 3), Work 2 balances security and efficiency (Chapter 4), and Work 3 presents a scalability solution (Chapter 5). Each of these major chapters elaborates on a particular framework. Contributions, limitations, and directions forward are elaborated in the Conclusion. Figure 2 depicts the structure of this thesis.

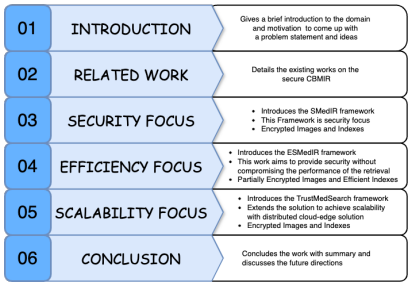


Figure 2: Thesis Plan

3 Research Methodologies

The three solutions proposed aim to address security, efficiency, and scalability issues. Furthermore, as discussed in the following subsections, complete solutions for medical image storage and retrieval will be taken to address the different aspects of each research question.

3.1 SMedIR Framework: From the security viewpoint

In this work, a framework named SMedIR (Secure Medical Image Retrieval) was proposed to ensure secure retrieval of medical images [1]. The method for secure lossless retrieval from encrypted images, which are stored in third-party clouds, is discussed here. The method utilizes a symmetric, integrity-centric image encryption scheme that exploits chaotic maps and cryptographic hash mechanisms. A deep learning-based hashing technique with the ConvNeXt network as a backbone generates hash codes that are

encrypted and searchable for privacy. The method has been evaluated on standard medical datasets and guarantees good security and performance, hence increasing retrieval accuracy by about 5-20% compared to existing models. This shows that SMedIR is a better framework for the secure and efficient handling of encrypted medical image data. Its architecture is illustrated in Figure 3.

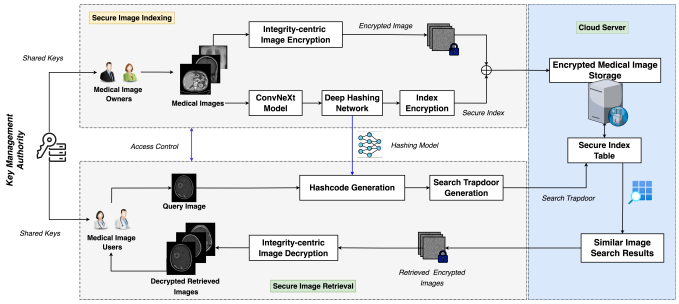


Figure 3: Architecture of SMedIR Framework

3.2 ESMedIR Framework: From an efficiency perspective

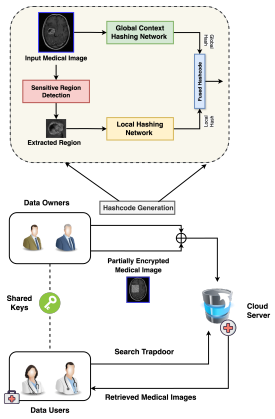


Figure 4: Block Diagram of ESMedIR Framework

The solution proposes a security with the ESMedIR (Efficient and Secure Medical Image Retrieval) Framework, which is efficient in storing and retrieving medical images. Instead of directly encrypting the full image, sensitive regions within the image were kept secret through a hyperchaos-based image encryption scheme [3], reducing both space and computational complexity. In a Dual-level hashing operation, global and local hash codes of both full and sensitive regions are established for fast retrieval. By this fusion, accuracy is improved. The encryption of privacy regions protects their sensitive information: this enhances storage efficiency by 30%, speeds up processing, and increases retrieval speed. Figure 4 shows an overall block diagram of the ESMedIR framework.

3.3 S^2MedIR Framework: From a scalability standpoint

Such extreme protective and other latency-afflicted limitations are addressed via S^2MedIR (Secure and Scalable Medical Image Retrieval), as a very effective framework for secure retrieval of medical images through the specified use of edge computing. Medical images are encrypted through a quantum chaos-based approach [2]. Using homomorphic encryption, locally created similarity-preserving hash codes are encrypted and then securely stored on a master edge server. The encrypted images are divided into shares, which are distributed among edge devices by the server using a Learning With Errors (LWE)-based image-sharing strategy. Security against retrieval during attacks is ensured through the design of a threshold technique for image reconstruction. It has been shown experimentally and theoretically that the suggested framework outperforms the others in efficiency and security for scalability enhancement. This is shown in Figure 5, which represents the overall framework design.

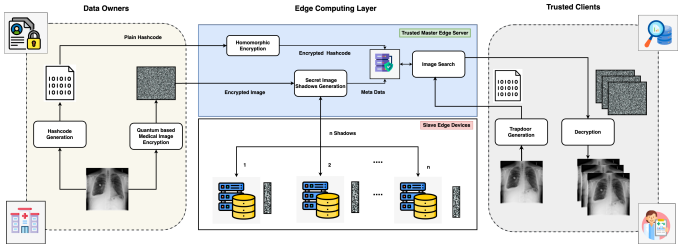


Figure 5: S^2MedIR Framework Design

Though all three frameworks, SMedIR, ESMedIR, and S^2MedIR, are individual, they are more or less connected with each other logically, with each capable of addressing an important aspect of secure medical image storage and retrieval. SMedIR is the starting point, wherein searchable hash codes are combined to securely and privately retrieve encrypted medical images. In addition to this, ESMedIR employs a dual-level hashing procedure that provides efficient storage access and retrieval mechanisms by means of regional encryption. Last, S^2MedIR confers scalability with respect to distributed storage practices of cloud offload and edge computing to assure the system's capability in meeting the growing needs of a voluminous medical image dataset. Although these act as separate modules, these frameworks, however, together provide an evolutionary path to a totally organized response that strikes a balance between security, efficiency, and scalability.

4 Research Progress

While the research progresses, secure indexing for effective retrieval and encryption mechanisms for image storage is being developed. The SMedIR and S²MedIR frameworks are developed and validated. Still, the ESMedIR framework is being developed onwards. Three articles have been published: a hyperchaos-based image encryption scheme published in a series of International Conferences on Computational Intelligence in Data Science, Springer [3]; the SMedIR framework in the Journal of Cloud Computing [1]; and the quantum chaos-based image encryption scheme has been published in the

Journal of Modern Optics [2]. The S²MedIR work has been published in IEEEXplore conference proceedings [12] in addition to being presented at an international conference in Dubai. ESMedIR is directed toward Elsevier with medical image processing-based journals.

5 Conclusion and Future Work

Each framework tackles a unique challenge in itself regarding medical image storage and retrieval. While combined, these solutions offer a comprehensive approach to security, optimization, and scalability of medical image management systems in cloud environments; SMedIR focuses on privacy-preserving retrieval; ESMedIR enhances and balances storage security and retrieval performance; S²MedIR ensures scalability through edge computing and decentralized shadow image storage. Keeping security, performance, and scalability into consideration, the multi-directional approach builds up new frameworks for secure medical image management.

Future research will focus on addressing issues concerning the design of such systems. Ample work will be directed towards the optimization of encryption techniques assuaging the concerns of effective retrieval without adversely affecting security. The second-most prominent domain is real-time threat detection models, effective protection against adversarial attacks and data leaks which are still of greater concern. Also of great importance will be the modification of the frameworks to adapt to different platforms, be they public clouds or hybrid clouds, with different demands on security and latency. The ways outlined formulate a conceptual basis for further enhancing the strong, versatile, secure medical image storage and retrieval systems.

Acknowledgments

The author would like to specially acknowledge their supervisor, Dr. V. Vetriselvi, for directing and conducting the research. Special thanks must also go to one and all: Aruna Gladys A, Dr. Mayank Raikwar, Reshma Balaraman, Aishwarya R and Thirunavukkarasu V for reviewing the designs of frameworks and articles. Finally, the author extends his gratitude to Mohamed Fuzail H, Praveen Kumar R and Ajitesh M for their support in developing the frameworks.

References

[1] Arun Amaithi Rajan, Vetriselvi V, Mayank Raikwar, and Reshma Balaraman. 2024. SMedIR: secure medical image retrieval framework with ConvNeXt-based indexing and searchable encryption in the cloud. *Journal of Cloud Computing* 13, 1 (Sept. 2024). https://doi.org/10.1186/s13677-024-00702-z

[2] Arun Amaithi Rajan and Vetriselvi Vetrian. 2024. QMedShield: a novel quantum chaos-based image encryption scheme for secure medical image storage in the cloud. *J. Mod. Opt.* (Dec. 2024), 1–19. https://doi.org/10.1080/09500340.2024.2436521

[3] Arun Amaithi Rajan, Vetriselvi Vetrian, and Aruna Gladys. 2023. Secure Image Encryption Model for Cloud-Based Healthcare Storage Using Hyperchaos and DNA Encoding. 89–103. https://doi.org/10.1007/978-3-031-38296-3_8

[4] Matic Broz. 2024. How many pictures are there (2024): Statistics, trends, and forecasts. https://photutorial.com/photos-statistics/

[5] Yi-Hui Chen and Min-Chun Huang. 2023. Fine-Grained Encrypted Image Retrieval in Cloud Environment. *Mathematics* 12, 1 (12 2023), 114. https://doi.org/10.3390/math12010114

[6] Yating Duan, Yanping Li, Laifeng Lu, and Yong Ding. 2022. A faster outsourced medical image retrieval scheme with privacy preservation. *Journal of Systems Architecture* 122 (1 2022). https://doi.org/10.1016/j.sysarc.2021.102356

[7] Sahar Ebadinezhad and Temitope Emmanuel Mobolade. 2024. A Novel Cloud-Based IoT Framework for Secure Health Monitoring. *Sustainability* 16, 3 (2024). https://doi.org/10.3390/su16031349

[8] Sumit Kumar, Sunil Kumar Agarwal, and Sayed Sayeed Ahmad. 2022. A Secure Medical Image Retrieval Technique using Encrypted Query Image. In *2022 2nd International Conference on Emerging Frontiers in Electrical and Electronic Technologies, ICEFEET 2022*. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICEFEET51821.2022.9847826

[9] D Lakshmi and Amit Kumar Tyagi. 2024. Emerging technologies and security in cloud computing. https://doi.org/10.4018/979-8-3693-2081-5

[10] Vishwanath S. Mahalle, Narendra M. Kandoi, and Santosh B. Patil. 2023. A powerful method for interactive content-based image retrieval by variable compressed convolutional info neural networks. *Visual Computer* (2023). https://doi.org/10.1007/s00371-023-03104-5

[11] V. R. Nitha and S. S. Vinod Chandra. 2023. ExtRanFS: An Automated Lung Cancer Malignancy Detection System Using Extremely Randomized Feature Selector. *Diagnostics* 13, 13 (7 2023). https://doi.org/10.3390/diagnostics13132206

[12] Arun Amaithi Rajan, Vetriselvi V, Aishwarya R, and Anitha Amaithi Rajan. 2024. Efficient and Lightweight Framework for Confidential Medical Image Search using Edge Computing. In *2024 International Conference on Computational Intelligence and Network Systems (CINS)*. 1–7. https://doi.org/10.1109/CINS63881.2024.10864435

[13] AliAsghar Safaei. 2021. Text-based multi-dimensional medical images retrieval according to the features-usage correlation. *Medical & Biological Engineering & Computing* 59, 10 (01 Oct 2021), 1993–2017. https://doi.org/10.1007/s11517-021-02392-0