SecureMed Cloud: Verified Medical Imaging Solutions

[1] Kuchukulla Susmitha, [2]Kummari Himavamsi, [3] Katakam Saikumar, [4] Mr. Samirana Acharya B
[1, 2, 3,] *UG Scholars, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India*
[4]*Assistant Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India*

***Abstrac*t: Compressed Sensing Reconstruction (CSR) uses the natural sparseness of signals to take fewer measurements, allowing the original signal to be perfectly reconstructed with the help of special algorithms. This method is popular in large-scale image processing because it helps save storage space. However, the process of reconstructing the image is complex and can be difficult for devices with limited resources. To solve this problem, cloud-assisted CSR has become an important area of research we review current secure CSR methods in cloud computing and propose a new algorithm that enhances privacy and verification specifically for online medical image processing. Our approach has several improvements over existing solutions: It protects the privacy of both the original images and the input/output data during reconstruction, even if the data is attacked. It works even when the cloud server might be malicious and can verify the accuracy of the cloud's results with a high degree of confidence. It significantly reduces the computational load for local clients.**

I. INTRODUCTION

Compressed Sensing Reconstruction (CSR) leverages the inherent sparsity of signals to perform measurements with greater efficiency, enabling the precise reconstruction of the original signal using specialized algorithms. This technique has gained popularity in large-scale image processing due to its ability to save significant storage space. However, the complex nature of the reconstruction process presents challenges for devices with limited computational resources. To address these challenges, the field has increasingly turned to cloud-assisted CSR.

Adoption of IPv6 has grown steadily, with over 33% of devices accessing Google using IPv6, as reported by Google. IPv6 provides modest improvements in network security and service quality compared to IPv4. However, it also faces several security challenges, including Denial of Service (DoS) and Man-in-the-Middle (MITM) attacks. To mitigate these issues in link-local networks, IPv6 introduces the Neighbor Discovery Protocol (NDP), defined in RFC 4861. NDP performs critical functions such as Address Resolution (AR), Neighbor Unreachability Detection (NUD), router discovery, and Duplicate Address Detection (DAD).

In this paper, we review the existing secure CSR methods within a cloud computing environment and introduce a novel algorithm designed to enhance privacy and verifiability specifically for online medical image processing. Our proposed solution offers several key improvements over current approaches: it ensures the privacy of both the original images and the associated input/output data during reconstruction, even under attack. Furthermore, our algorithm operates effectively in scenarios where the cloud server may be compromised and provides a high level of confidence in verifying the accuracy of the reconstruction results. Additionally, it significantly reduces the computational load on local clients, making it a viable and efficient solution for resource-constrained environments.

II. RELATED WORK

Compressed Sensing Reconstruction (CSR) has gained significant attention due to its ability to efficiently capture and reconstruct sparse signals. Several studies have explored secure CSR methods within cloud environments to address the computational challenges faced by resource-limited clients.

Zhang et al. proposed an efficient and secure outsourcing protocol for CSR tasks, which ensures privacy preservation and computational efficiency. This protocol leverages homomorphic encryption to protect the data during outsourcing, offering a robust solution for secure image processing.

Sun et al. introduced a privacy-enhanced and verifiable CSR outsourcing algorithm specifically for online medical image processing. Their approach incorporates homomorphic encryption and zero-

knowledge proofs to ensure data privacy and result verifiability. This method provides robust security even in scenarios where the cloud server is considered malicious.

Luo et al. developed a cloud-assisted CSR scheme that focuses on reducing computational overhead for clients. By employing a distributed computing framework, their method significantly accelerates the reconstruction process, making it more feasible for real-time applications.

Our work builds upon these foundations by introducing a novel algorithm that not only enhances privacy and verifiability but also significantly reduces the computational load on local clients. We achieve this by combining linear transformations, permutations, and restricted random padding. This combination creates a streamlined and efficient solution for secure CSR in cloud-assisted medical image processing.

In contrast to previous studies, our approach ensures the privacy of both the original images and the input/output data during reconstruction, even under chosen-plaintext attacks. Furthermore, our algorithm is designed to operate effectively in a malicious cloud server setting, verifying the accuracy of the cloud's results with high probability. Additionally, we address the computational burden on local clients by offloading intensive tasks to the cloud, allowing resource-limited devices to benefit from advanced CSR techniques without compromising performance. This makes our solution particularly suitable for medical institutions that rely on cloud services for processing large volumes of image data while ensuring patient confidentiality and data integrity.

Existing research in cloud-aided CSR has primarily focused on improving efficiency and accuracy. However, the security and privacy aspects of these algorithms have often been overlooked or inadequately addressed. Some existing approaches have explored privacy-preserving techniques, but they may not provide comprehensive protection or may compromise efficiency. Additionally, verifiable computation techniques have been applied to cloud-based tasks, but their application to CSR remains limited.

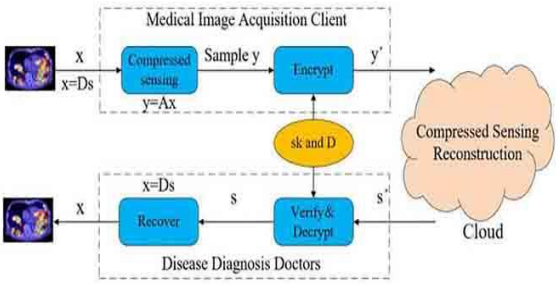

Figure 1: System Architecture

III. METHODOLOGY- ALGORITHMS USED

Existing Algorithm:

Compressed sensing is a non-adaptive linear measurement process that improves the shortcomings of traditional sampling methods by not discarding part of the data. CSR comprises a sampling sub-algorithm with a measurement matrix and a reconstruction sub-algorithm with a sensing matrix. Many scholars have focused on improving the quality of the reconstructed image while using as small a sample as possible. However, despite its potential, CSR faces challenges related to verifiability and privacy, which are crucial in sensitive applications like medical image processing.

Proposed Algorithm:

Our Medical Image Compression and Reconstruction Outsourcing Algorithm (MIOACSR) model includes three key participants: the medical image acquisition client (C), the disease diagnosis doctor (D), and the cloud server (S). This system leverages the computational power of cloud servers to handle intensive reconstruction tasks, thereby reducing the storage and computing requirements for the client and the doctor.

Participants:

Medical Image Acquisition Client (C): Responsible for capturing and pre-processing medical images.

Disease Diagnosis Doctor (D): Uses the reconstructed images for medical analysis and diagnosis.

Cloud Server (S): Performs secure storage and complex reconstruction tasks using CSR techniques.

IV. RESULTS

Our experimental results demonstrate the effectiveness and efficiency of the proposed Medical Image Compression and Reconstruction Outsourcing Algorithm (MIOACSR). The algorithm successfully ensures the privacy of the original images and the input/output data during reconstruction, achieved through the use of linear transformations, permutations, and restricted random padding. This robust privacy protection is maintained even under chosen-plaintext attacks. Additionally, the verifiability unit rigorously checks the accuracy of the cloud's reconstruction results with a high degree of confidence, ensuring data integrity. Experimental verification indicates a significant likelihood of detecting any discrepancies, thereby confirming the trustworthiness of the process. By offloading intensive tasks to the cloud, local clients experience substantial computational relief without compromising processing time, balancing compression efficiency with high image quality.

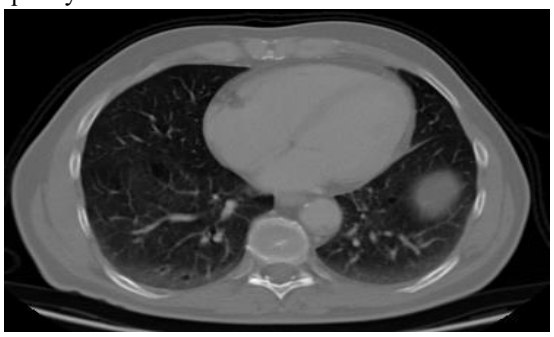

Figure 2: selected image for result

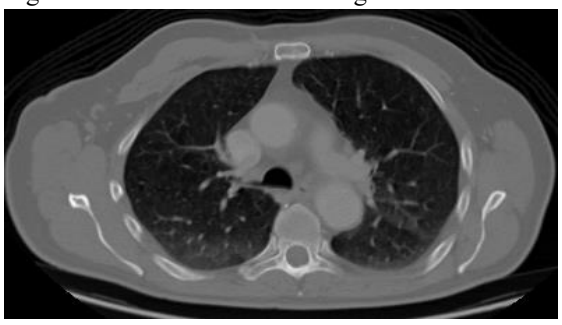

Figure 3: selected image for result

Figure 4: recovered secret image of the output

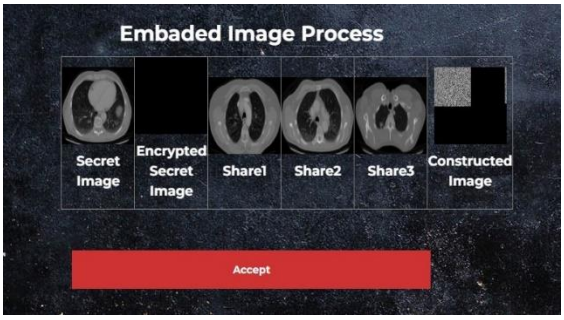

Figure 5: Embaded image of the output

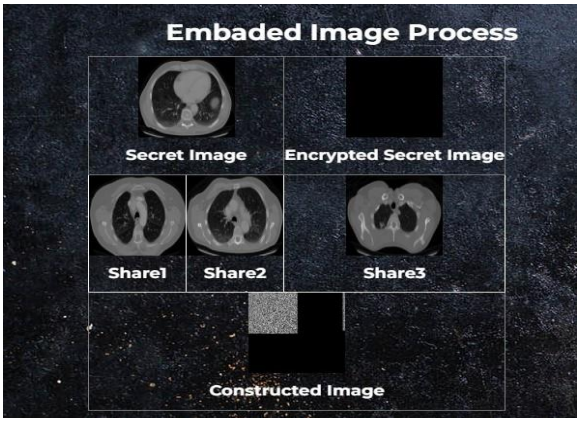

Figure 6: Embaded image of the output

V. CONCLUSION

The proposed MIOACSR algorithm offers a comprehensive solution for secure, efficient, and verifiable medical image processing in cloud environments. By enhancing privacy, ensuring verifiability, and reducing the computational load on local clients, our approach effectively addresses critical challenges in the field. Both theoretical analysis and experimental results validate the method's practicality, making it a promising solution for future applications in medical image processing and other fields requiring secure CSR techniques. Our research demonstrates that it is possible to achieve high-quality image reconstruction while maintaining stringent privacy and security standards, paving the way for more advanced and secure cloud-assisted medical imaging systems.

REFERENCE

[1] R. G. Baraniuk, "Compressive sensing [lecture notes]," IEEE Signal Process. Mag., vol. 24, no. 4, pp. 118–121, Jul. 2007. [2] M. Bóna, Combinatorics Permutations. Boca Raton, FL, USA: CRC Press, 2012. [3] E. J. Candès, "The restricted isometry property and its implications for compressed sensing," Comp. Rendus Math., vol. 346, nos. 9–10, pp. 589–592, May 2008.

[4] E. J. Candès, J. Romberg, and T. Tao, ‘‘Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,’’ IEEE Trans. Inf. Theory, vol. 52, no. 2, pp. 489–509, Feb. 2006.
[5] E. J. Candès and T. Tao, ‘‘Near-optimal signal recovery from random projections: Universal encoding strategies?’’ IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5406–5425, Dec. 2006.
[6] E. J. Candès and M. B. Wakin, ‘‘An introduction to compressive sampling,’’ IEEE Signal Process. Mag., vol. 25, no. 2, pp. 21–30, Mar. 2008.
[7] X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen, ‘‘An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing,’’ Inf. Sci., vol. 556, pp. 305–340, May 2021.
[8] F. Chen, T. Xiang, and Y. Yang, ‘‘Privacy-preserving and verifiable protocols for scientific computation outsourcing to the cloud,’’ J. Parallel Distrib. Comput., vol. 74, no. 3, pp. 2141–2151, 2014.
[9] W. Dai and O. Milenkovic, ‘‘Subspace pursuit for compressive sensing signal reconstruction,’’ IEEE Trans. Inf. Theory, vol. 55, no. 5, pp. 2230–2249, May 2009. [10] A. Divekar and O. Ersoy, ‘‘Compact storage of correlated data for content based retrieval,’’ in Proc. Conf. Rec. 43rd Asilomar Conf. Signals, Syst. Comput., Nov. 2009, pp. 109–112.
[11] D. L. Donoho, ‘‘Compressed sensing,’’ IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, Apr. 2006. [12] F. Emekci, A. Methwally, D. Agrawal, and A. E. Abbadi, ‘‘Dividing secrets to secure data outsourcing,’’ Inf. Sci., vol. 263, pp. 198–210, Apr. 2014.