IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

Privacy Enhanced and Verifiable for Medical Image Processing on the Cloud

[1]Bandari Ravi, [2]Tirumanyam Guru Akash, [3]Pasupula Sai Kiran, [4]Rudavath Premchand
Assistant Professor, Guru Nanak Institute of Technology, CSE Department, Hyderabad[1]
Student, Guru Nanak Institute of Technology, CSE Department, Hyderabad[2,3,4]

Abstract: *The well-known compressed sensing reconstruction (CSR) uses the sparse characteristics of the signal to obtain discrete samples with the compression (i.e. measurement) algorithm, and then perfectly reconstructs the signal through the reconstruction algorithm. Benefiting from the storage savings, the CSR has been widely used in the field of large-scale image processing. However, the reconstruction process is computationally overloaded for resource-constrained clients. Therefore, designing a cloud-aided CSR algorithm becomes a hot topic. In this paper, we investigate the existing secure CSR algorithms within a cloud environment and propose a new privacy-enhanced and verifiable CSR outsourcing algorithm for online medical image processing services. Compared with previous work, our new design can efficiently achieve more extensive security. Precisely, (1) our algorithm realizes the privacy preservation of the original image, as well as the input/output information of the reconstruction process under the chosen-plaintext attack, (2) our design is based on a malicious cloud server model and can verify the correctness of the cloud returned result with a probability of approximating 1, and (3) our algorithm is highly efficient and can make the local client achieve decent computational savings. The main technique of our design is a combination of linear transformation, permutation and restricted random padding which is concise and high efficiency. We analyze the above claims with rigorous theoretical arguments and comprehensive experimental analysis.*

Keywords: compressed sensing reconstruction

I. INTRODUCTION

In recent years, the COVID-19 pandemic has greatly boosted the development of online diagnosis and treatment, in which paradigm, potential patients with the new coronary disease can first take CT images of their lungs with the medical data acquisition device, and then send the images to the doctor. After that, the doctor can judge the disease and present the corresponding treatment planning based on the received images. In this case, the resolution of the image will greatly affect the doctor's judgment. Low-resolution images could make the doctor present wrong judgments, while high-resolution images will make the doctor's judgment more accurate. However, images with high qualities are usually too large to store. Generally, we can employ the compressed sensing reconstruction (CSR) algorithm to solve this problem. The CSR is an efficient signal sampling technique proposed by Donoho et al. For any compressible image, it can accurately reconstruct the original image from a set of far fewer samples than those required by the Shannon–Nyquist sampling theorem. Therefore, the acquisition device can sample the medical image with CSR algorithm and send the compressed image (i.e. sample) to the doctor. Since the size of a sample is always smaller than that of the original image, this method can evidently reduce the storage overhead. Yet there still exist many practical concerns for CSR -based image processing. On one hand, in the current big data era, the scale of the tackled medical images is usually very large, the storage savings with CSR may not be enough for local resource-constrained medical institutes. On the other hand, the reconstruction processing of CSR is time-consuming, it may be overloaded for most data acquisition devices. Fortunately, the promising cloud computing paradigm exactly solve these two problems. That is, the resource-constrained data acquisition device can upload the compressed images to a resource-abundant cloud server and, meanwhile, the cloud server can assist the doctor in realizing the images reconstruction.

DOI: 10.48175/IJARSCT-22634

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

II. LITERATURE SURVEY

X. Chai, H. Wu, Z. Gan, D. Han, Y. Zhang, and Y. Chen has designed an efficient visually meaningful double color image encryption algorithm is proposed by combining 2D compressive sensing (CS) with an embedding technique. First, two color images are measured by measurement matrices in two directions to achieve simultaneous compression and encryption, in which low-dimensional matrices generated from Logistic-Sine system (LSS) are extended with Kronecker product (KP), and the resulting high-dimensional matrices optimized by singular value decomposition (SVD) are employed as measurement matrices. Second, the compressed cipher images are confused by index sequences produced by a 6D hyperchaotic system. Finally, a visually meaningful cipher image is obtained by embedding permutated cipher images into a color carrier image. The final cipher image and plain image are of the same size, which greatly reduces the storage space and transmission bandwidth. To enhance the relationship of our algorithm with plain images and prevent vulnerability to known-plaintext and chosen-plaintext attacks, SHA 256 hash values and feature parameters of plain images are combined to generate the initial values of the LSS and 6D hyperchaotic system, and these parameters are both embedded into the carrier image to avoid additional transmission and storage. Simulation results and performance analyses demonstrate the effectiveness and security of the proposed image encryption scheme.

G. Kuldeep and Q. Zhang has designed the multi-class privacy-preserving cloud computing scheme (MPCC) leveraging compressive sensing for compact sensor data representation and secrecy for data encryption. The proposed scheme achieves two-class secrecy, one for superuser who can retrieve the exact sensor data, and the other for semi-authorized user who is only able to obtain the statistical data such as mean, variance, etc. MPCC scheme allows computationally expensive sparse signal recovery to be performed at cloud without compromising the confidentiality of data to the cloud service providers. In this way, it mitigates the issues in data transmission, energy and storage caused by massive IoT sensor data as well as the increasing concerns about IoT data privacy in cloud computing. Compared with the state-of-the-art schemes, we show that MPCC scheme not only has lower computational complexity at the IoT sensor device and data consumer, but also is proved to be secure against ciphertext-only attack.

Z. Wang, Z. S. Hussein, and X. Wang, has designed secure compressive sensing based on a combination of the chaotic discrete wavelet transform (DWT) basis and chaotic discrete cosine transform (DCT) measurement matrix is proposed. In the proposed scheme, a logistic map is employed to generate two chaotic sequences that are used to scramble the rows of the conventional DCT and original DWT matrix to form a chaotic measurement matrix and sparse basis matrix, respectively. The original image is first transformed into a sparse domain signal by the obtained chaotic DWT matrix. Thereafter, the resulting signal is compressively sampled by the obtained chaotic DCT measurement matrix. Numerical experiments show that the proposed scheme not only achieves image encryption and compression simultaneously but also enlarges the key space and improves the quality of the reconstructed image compared to that of the conventional chaotic measurement matrix method.

III. METHODOLOGY

The methodology for privacy-enhanced and verifiable medical image processing on the cloud using Java technology involves encrypting medical images both at rest and in transit using strong encryption algorithms, ensuring secure access through role-based access control and multi-factor authentication, and anonymizing sensitive data. It incorporates data integrity and verifiability by using hashing and digital signatures for image verification, along with immutable audit logs and blockchain for tracking image processing events. The medical image processing pipeline utilizes Java-based image processing libraries and cloud-based distributed computing tools for scalability

DISADVANTAGES OF EXISTING SYSTEM:

- Verifiability method is low efficiency.
- Many security and efficiency issues.
- The quality of the reconstructed image with a sample as small as possible.

PROPOSED SYSTEM

The suggested system presents an environment that the medical institute aims to rent a resource powerful cloud server to securely store and reconstruct the large-scale medical images with CSR technique, and design a new efficient and

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

secure cloud-aided diagnosis algorithm. Our design is privacy-enhanced and Our algorithm is designed under a malicious cloud server. Our privacy preservation approach is on basis of linear transformation, permutation and restricted random padding techniques, which can be efficiently implemented.

ADVANTAGES OF PROPOSED SYSTEM:

- Our goal is to design a correct, high-efficiency.
- Secure medical image compression and reconstruction outsourcing model.
- Our design is a combination of linear transformation, permutation and restricted random padding which is concise.

IV. SYSTEM ARCHITECTURE

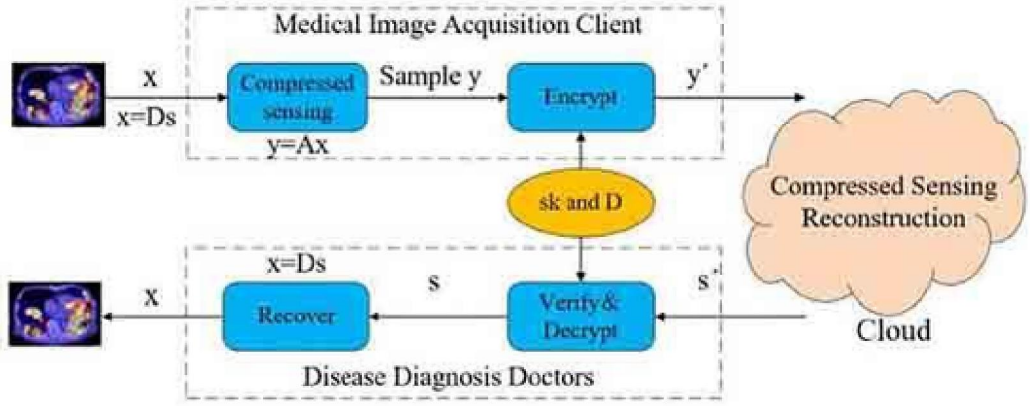


Figure: System Architecture

MODULES:

User Interface Design: To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.

Cloud Server: Cloud Server can accept new client request and View Accepted clients. Cloud Server can accept client messages with Owners and receiver images data. It accept multiple doctor details. View Accepted Messages from who can send the message and who can receive the message.

Client: The client utilizes an encryption key to encrypt the original image by an encryption algorithm (e.g., stream cipher or homomorphic encryption), and distributes the encrypted image to a doctor for data hiding multiple clients. In the proposed model, the original image is converted into multiple encrypted images of the same size as the original image, and the encrypted images are distributed to multiple different client for data. First, the medical image acquisition client adopts compressed sensing technology to obtain the patient's image sample data.

Doctor: In the doctor phase, with a doctor key kh, embeds data into an encrypted image to generate a marked encrypted image. Then the generated encrypted images are distributed to a doctor for clients. In this model, the doctor has a control center and multiple storage and processing centers. The control center performs the distribution and collection of encrypted images, while the storage and processing centers perform clients. Limited by the storage and computing capabilities, The medical image acquisition device and disease diagnosis doctor use compressed sensing technology to reduce storage, and at the same time leverage resource-rich cloud servers to achieve reconstruction tasks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

V. IMPLEMENTATION

Compressed Sensing Reconstruction (CSR):

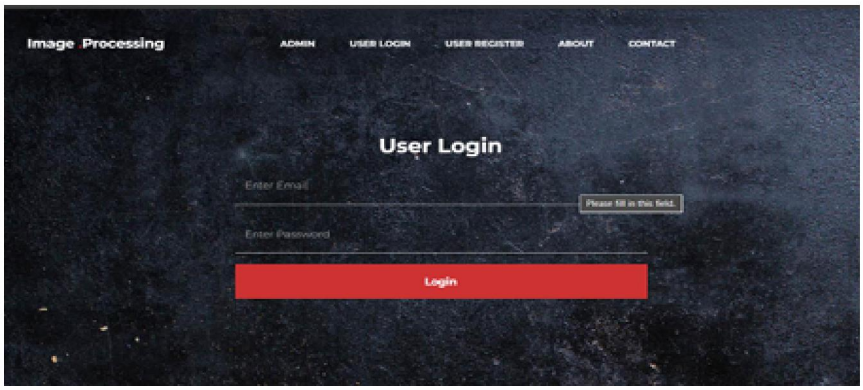
To achieve privacy-enhanced and verifiable medical image processing on the cloud using Compressed Sensing Reconstruction (CSR) and Convolutional Neural Networks (CNNs) in Java, the methodology involves encrypting medical images both during transmission and storage using advanced cryptographic techniques such as homomorphic encryption. CSR is applied to reduce the number of samples required for image reconstruction, thus ensuring efficient use of storage and computational resources on the cloud while maintaining privacy. The encrypted compressed image data is sent to the cloud, where a CNN-based model is used to process the image. The model is trained locally to ensure that sensitive data remains encrypted throughout the processing stage. During this process, the cloud server performs the necessary computations without ever seeing the raw data, ensuring that patient privacy is preserved.

Convolutional Neural Networks (CNNs):

To enhance verifiability, the system integrates cryptographic verification techniques like zero-knowledge proofs or verifiable computation protocols, which ensure that the cloud server computes the image processing tasks correctly without revealing sensitive medical data. The use of blockchain or immutable audit logs is also implemented to track all operations performed on the data, providing a transparent, tamper-proof record. This approach ensures that the results of the image processing, such as the reconstructed medical images or diagnosis outcomes, are accurate and verifiable. Java frameworks like Spring Security and custom encryption libraries are employed for secure data handling, while libraries such as Deeplearning4j are used to implement the CNN models. This solution guarantees privacy, security, and verifiability, making it suitable for medical image processing applications on the cloud.

VI. EXPERIMENTAL RESULTS

USER LOGIN PAGE



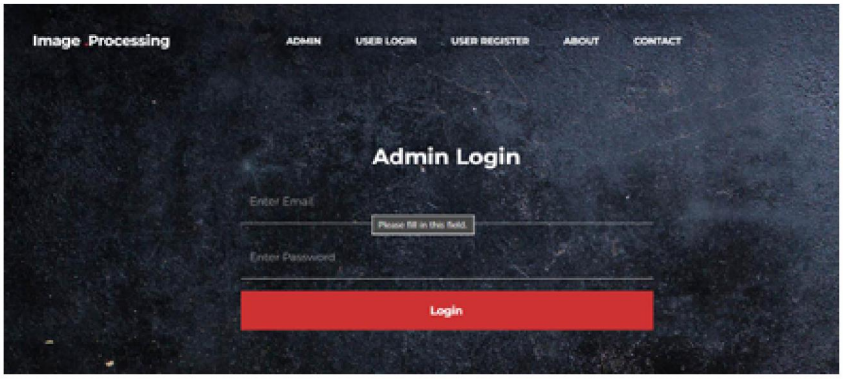
EXPLAINATION:

A login page for employees typically allows authorized personnel to access company resources or systems, usually requiring a username and password. It's a way to ensure security and control access to sensitive information or tools within an organization

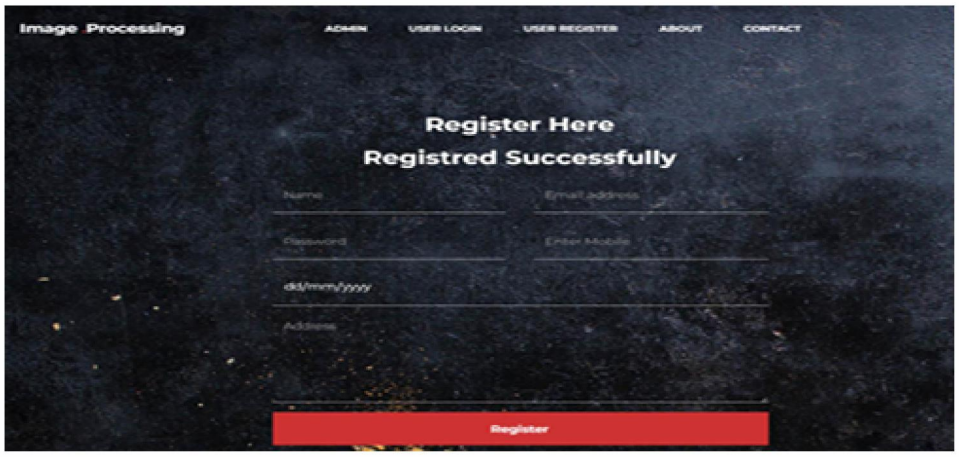
ADMIN PAGE :

An administrator login page serves as a gateway for individuals with administrative privileges to access and manage various aspects of a system or platform. It often requires higher-level credentials and grants access to settings, user management, and other administrative functions critical for maintaining and overseeing the system

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024



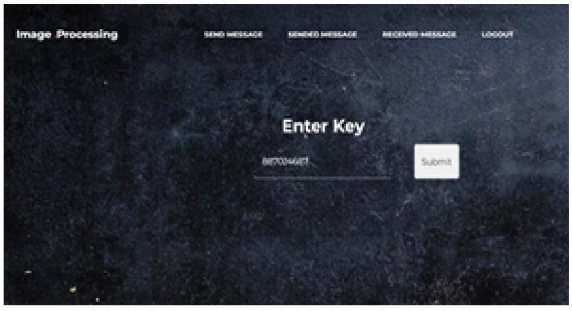
REGISTER PAGE



EXPLAINATION

A registration form is used to collect information from users who are signing up for a service, website, or event. It typically includes fields such as name, email address, username, password, and sometimes additional information depending on the specific requirements

FINAL RESULT DETECTION PAGE



EXPLAINATION:A key is generated on the receiver's side, which is visible only to the authorized recipient. The user must enter this key to decrypt the encrypted images. Once the correct key is entered, the user gains access to the actual medical image, ensuring that only the intended recipient can view the sensitive data, while preventing unauthorized

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, December 2024

access. This mechanism adds an extra layer of security by ensuring that the image remains confidential and accessible only to those with the proper authorization.

VII. CONCLUSION

We designed a secure outsourcing algorithm for CSR of medical images. This algorithm enables the medical institute and the doctor to securely store and reconstruct the medical images with the help of a cloud server. In addition to keeping the privacy of the original image and the input/output information of the reconstruction process, our design also can enable the doctor to detect the correctness of the result sent from the cloud with a probability of approximating 1. Finally, we theoretically and experimentally analyze the efficiency of the proposed outsourcing algorithm. The results generated represent a good and efficient performance.

VIII. FUTURE ENHANCEMENT

Fortunately, the promising cloud computing paradigm provides an effective solution to these two key challenges. First, in medical image processing, data acquisition devices like medical imaging devices (e.g., MRI machines or X-ray systems) often face resource constraints, such as limited computational power and storage capacity. These devices may struggle to handle the large-scale image data generated during imaging procedures.

REFERENCES

[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. .