IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 6, November-December 2024

Impact Factor: 7.394

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 6, November-December 2024 ||

DOI:10.15680/IJARETY.2024.1106032

Privacy Enhanced and Verifiable for Medical Image Processing on the Cloud

Mr.K. Vigneshwar[1], Ms.M.Vaishali Gopal[2], Ms. J. Devarani[3], Ms. M. Akshaya[4]

Assistant Professor, Department of Computer Science & Engineering, Guru Nanak Institute of Technology, India[1]

Student, Department of Computer Science & Engineering, Guru Nanak Institute of Technology, India[2]

Student, Department of Computer Science & Engineering, Guru Nanak Institute of Technology, India[3]

Student, Department of Computer Science & Engineering, Guru Nanak Institute of Technology, India[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, our algorithm realizes the privacy preservation of the original image, as well as the input/output information of the reconstruction process under the chosen-plain text attack, 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 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.

I. INTRODUCTION

In recent years, the COVID-19p and emichas 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. The size of a sample is always smaller than that of the original image, this method can evidently reduce the storage overhead. Yet therestill 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. Although cloud computing can provide a flexible storage and processing infrastructure, many security issuesarise. First, the image data is usually private, the leakage of these data may cause significant property losses to the outsourcer (e.g. individuals or enterprises). Second, the cloud server is remote and thus out of control. It may grab valuable information from the received information and the intermediate calculated result, or even deliberately send a forged result to fool the outsourcer. Finally, due to some unforeseeable reasons, hardware damage or software errors may encounterwhencomputingortransmittingthedata.Therefore,itisofgreat significancetodesign a secure cloud-assisted CSR algorithm, which, besides achieving considerable computational savings on the local side, should assure the privacy of the outsourcer's sensitive information and the verifiability of the server returned result. Along this direction, many different methods have been developed to securely out source the CSR task to a remote cloud server. However, there still exist many security and efficiency issues, which will be discussed in the following separate subsection, needing to be further investigate.

II. LITERATURE SURVEY

X. Chai (2021)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 a6D hyperchaotic system. Finally, a visually meaningful cipher image is obtainedby 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.

J.Liu et. al(2020) Recognition and classification tasks in images or videos are ubiquitous, but they can lead to privacy issues. People increasingly hope that camera systems can record and recognize important events and objects, such as real-time recording of traffic conditions and accident scenes, elderly fall detection, and in-home monitoring. However, people also want to ensure these activities donot violate the privacy of users or others. The sparse representation classification recognition algorithms based on compressed sensing (CS) are robust at recognizing human faces from frontal views with varying expressions and illuminations, as well as occlusions and disguises. This is a potential way to perform recognition tasks while preserving visual privacy. In this paper, an improved Gaussian random measurement matrix is adopted in the proposed multilayer CS (MCS) model to realize multiple image CS and achieve a balance between visual privacy-preservingandrecognitiontasks.Thevisualprivacy-preservinglevel evaluationforMCS images has important guiding significance for image processing and recognition. Therefore, we propose an image visual privacy-preserving level evaluation method for the MCS model (MCS- VPLE) based on contrast and salient structural features. The basic concept is to use the contrast measurement model based on the statistical mean of the asymmetric alpha-trimmed filter and the salient generalized center-symmetric local binary pattern operator to extract contrast and salient structural features, respectively. Thefeatures are fed into a support vector regression to obtain the image quality score, and the fuzzy c-means algorithm is used for clustering to obtain the final evaluated image visual privacy-preserving score. Experiments on three constructed databases show that the proposed method has better prediction effectiveness and performance than conventional methods.

III. METHODOLOGIES

Modules Name

- User Interface Design
- Cloud Server (CS)
- Client
- Doctor
- Distribution and Collection
- Receiver

Modules Explanation:

1. User Interface Design: Users can log in with credentials or register their details if new. The system manages user accounts for accessing queries and maintaining upload activities.

2. Cloud Server: The cloud server accepts client requests, manages user data, and facilitates secure communication between clients and doctors for medical image sharing and analysis.

3. Client: Clients encrypt medical images using secure algorithms, distribute encrypted data for analysis, and store it safely in the database.

4. Doctor: Doctors embed data into encrypted images, manage their distribution and processing, and use cloud resources for efficient storage and analysis.

5. Distribution and Collection: Encrypted images are distributed to doctors for analysis and collected back securely, with no data expansion or loss of privacy.
6. Receiver(Data extraction and Image recovery): The receiver reconstructs the original image and extracts embedded data using encrypted images while ensuring security against tampering or malicious actions.

Existing System Disadvantages:

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

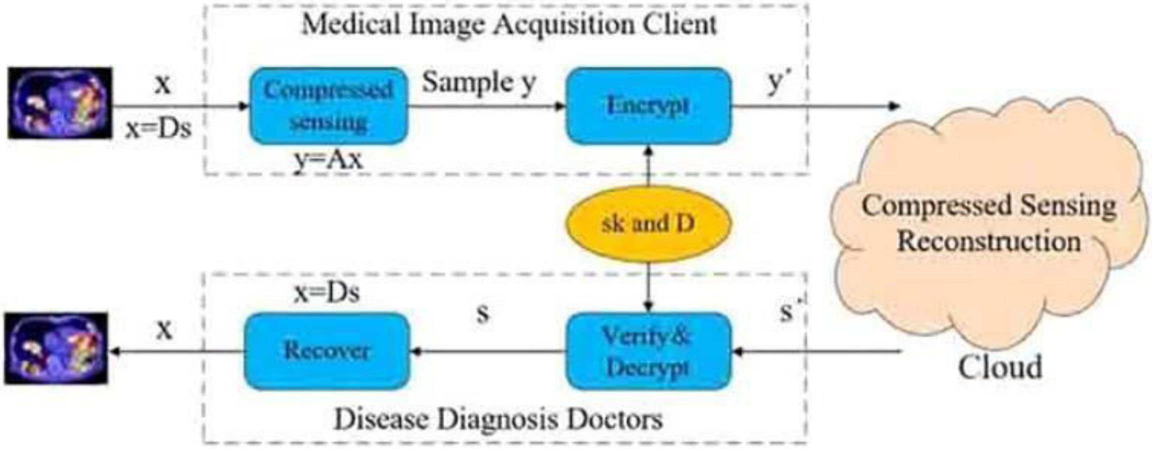
Proposed System

- In this paper, we focus on the setting that the medical institute aims to rent are source- powerful cloud server to securely store and reconstruct the large-scale medical images with CSR technique, and design a new efficient and 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.

Proposed System Advantages:

- In this paper, we focus on the setting 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 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.

System Architecture

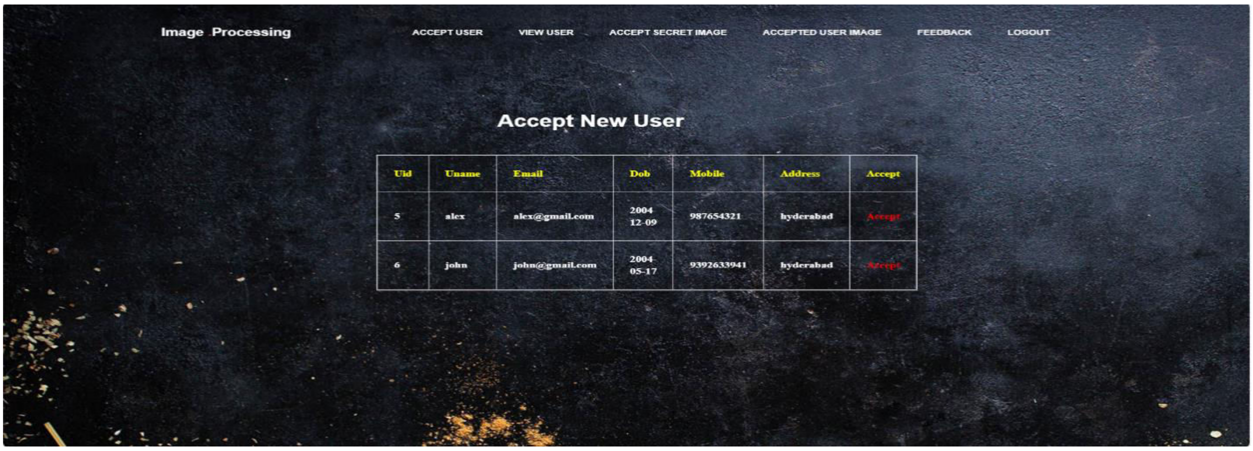

Medical Image Acquisition Client
x
x=Ds
Compressed sensing
y=Ax
Sample y
Encrypt
y'
sk and D
Compressed Sensing Reconstruction
Cloud
x=Ds
x
Recover
s
Verify& Decrypt
s'
Disease Diagnosis Doctors

The system architecture ensures secure and efficient medical image processing using the cloud. First, medical images are compressed to reduce size and encrypted to protect privacy before being sent to the cloud. The cloud handles reconstruction while keeping the data secure. When doctors access the data, they decrypt and verify it to ensure authenticity, then recover the original image for diagnosis. This process ensures privacy, reduces storage and transmission costs, and maintains the integrity of medical images.

Implementation
User Interface Design
Input: Enter Login name and Password
Output: If valid user name and password then directly open the home page otherwise show error message and redirect to the registration page.

Cloud Server
Input : Enter all details Login then verify client data and send to CS
Output : CS verify all client requests and accept client data then data send to client.
Client
Input : Enter the name and password and send data to receiver client.
Output : If valid client name and password then directly open the client home page.All the resources added by client options. Distributes the encrypted image the doctor for data hiding.
Doctor
Input : Doctor Hider Login name and Password
Output : The encrypted image to obtain the corresponding marked encrypted image.
Distribution and Collection
Input : Distribute the encrypted images to multiple different clients for data hiding.
Output : Although the model generates multiple encrypted images.
Receiver (Data extraction and Image recovery)
Input : Receiver side verify images.
Output : Data extraction is separated from the image restoration, that is, the embedded data is extracted in the encrypted domain.

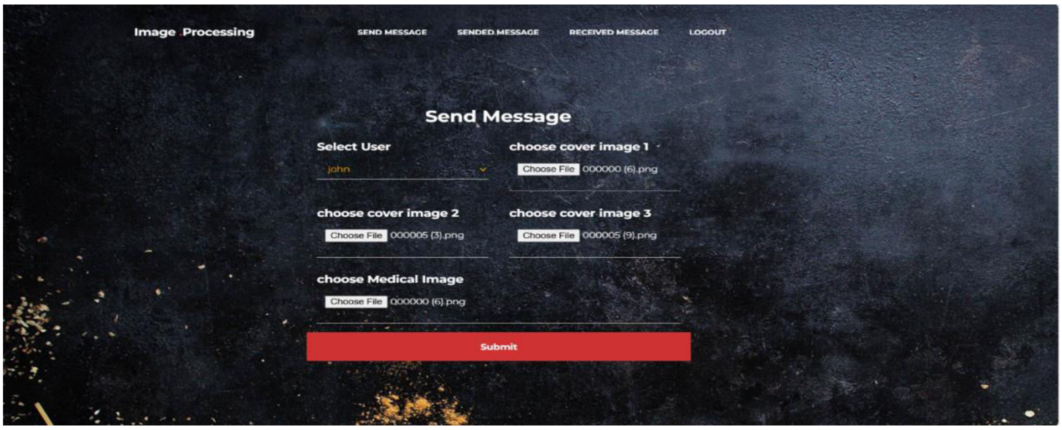
Experimental Results



Accept New User

Uid	Uname	Email	Dob	Mobile	Address	Accept
5	alex	alex@gmail.com	2004 12-09	987654321	hyderabad	Accept
6	john	john@gmail.com	2004 05-17	9392633941	hyderabad	Accept

Admin Accepting New Registrations



Send Message

Select User: john

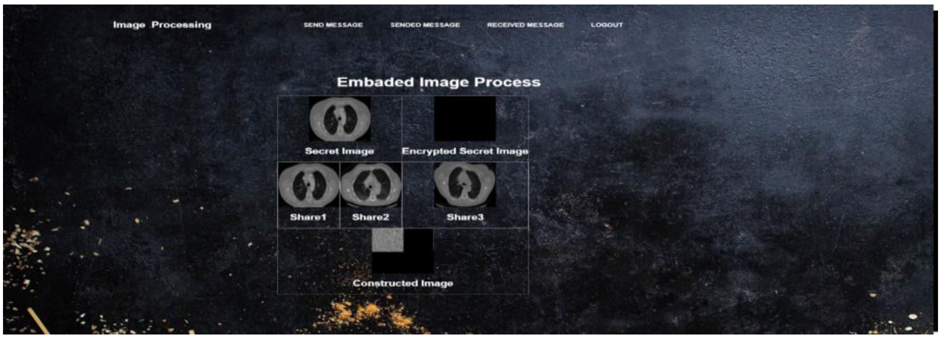
choose cover image 1: Choose File 000000 (6).png

choose cover image 2: Choose File 000005 (3).png

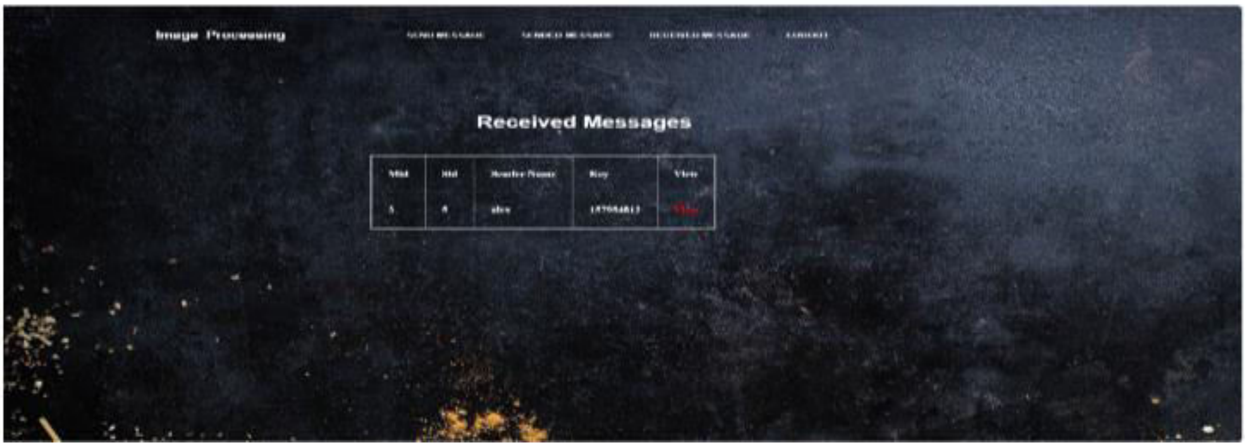
choose cover image 3: Choose File 000005 (9).png

choose Medical Image: Choose File 000000 (6).png

Encrypted Image



Generated Secret Image



Received Messages

Mid	Hid	Sender Name	Key	View
5	8	alex	[illegible]	[illegible]

IV. CONCLUSION

In this paper, we design 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

V. FUTURE ENHANCEMENT

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.

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.

[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.

[13] G. Hu, D. Xiao, T. Xiang, S. Bai, and Y. Zhang, ``A compressive sensing based privacy preserving outsourcing of image storage and identity authentication service in cloud," Inf. Sci., vol. 387, pp. 132-145, May 2017.

[14] A. J. Jerri, ``The Shannon sampling theorem-Its various extensions and applications: A tutorial review," Proc. IEEE, vol. 65, no. 11, pp. 1565-1596, Nov. 1977.

[15] G. Kuldeep and Q. Zhang, ``Compressive sensing based multi-class privacy-preserving cloud computing," in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2020, pp. 1-6.

[16] X. Lei, X. Liao, T. Huang, and F. Heriniaina, ``Achieving security, robust cheating resistance, and high-efficiency for outsourcing large matrix multiplication computation to a malicious cloud," Inf. Sci., vol. 280, pp. 205-217, Oct. 2014.

[17] H. Liu, H. Zhang, L. Guo, J. Yu, and J. Lin, ``Privacy-preserving cloud aided broad learning system," Comput. Secur., vol. 112, Jan. 2022, Art. no. 102503.

[18] J. Liu, Z. Tang, N. Sun, G. Han, and S. Kwong, ``Visual privacy-preserving level evaluation for multilayer compressed sensing model using contrast and salient structural features," Signal Process., Image Commun., vol. 89, Nov. 2020, Art. no. 115996.

[19] A. Orsdemir, H. O. Altun, G. Sharma, and M. F. Bocko, ``On the security and robustness of encryption via compressed sensing," in Proc. IEEE Mil. Commun. Conf. (MILCOM), Nov. 2008, pp. 1-7.

[20] Y. Rachlin and D. Baron, ``The secrecy of compressed sensing measurements," in Proc. 46th Annu. Allerton Conf. Commun., Control, Comput., Sep. 2008, pp. 813-817.

[21] K. Ren, C. Wang, and Q. Wang, ``Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69-73, Jan./Feb. 2012.

[22] C. Tian, J. Yu, H. Zhang, H. Xue, C. Wang, and K. Ren, ``Novel secure outsourcing of modular inversion for arbitrary and variable modulus," IEEE Trans. Services Comput., vol. 15, no. 1, pp. 241-253, Jan. 2022.

[23] C. Wang, B. Zhang, K. Ren, and J. M. Roveda, ``Privacy-assured outsourcing of image reconstruction service in cloud," IEEE Trans. Emerg. Topics Comput., vol. 1, no. 1, pp. 166-177, Jun. 2013.

[24] C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu, ``A privacy-aware cloud-assisted healthcare monitoring system via compressive sensing," in Proc. IEEE Conf. Comput. Commun. (INFOCOM), Apr. 2014, pp. 2130-2138.

[25] M. Wang, D. Xiao, and J. Liang, ``Low complexity secure P-tensor product compressed sensing reconstruction outsourcing and identity authentication in cloud," in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Jun. 2021, pp. 2630-2634.

[26] Z. Wang, Z. S. Hussein, and X. Wang, ``Secure compressive sensing of images based on combined chaotic DWT sparse basis and chaotic DCT measurement matrix," Opt. Lasers Eng., vol. 134, Nov. 2020, Art. no. 106246.

[27] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, ``Edge computing security: State of the art and challenges," Proc. IEEE, vol. 107, no. 8, pp. 1608-1631, Aug. 2019.

[28] W. Xue, C. Luo, Y. Shen, R. Rana, G. Lan, S. Jha, A. Seneviratne, and W. Hu, ``Towards a compressive-sensing-based lightweight encryption scheme for the Internet of Things," IEEE Trans. Mobile Comput., vol. 20, no. 10, pp. 3049-3065, Oct. 2021.

[29] X. Yuan, X. Wang, C. Wang, J. Weng, and K. Ren, ``Enabling secure and fast indexing for privacy-assured healthcare monitoring via compressive sensing," IEEE Trans. Multimedia, vol. 18, no. 10, pp. 2002-2014, Oct. 2016.

[30] F. Zhang, X. Ma, and S. Liu, ``Efficient computation outsourcing for inverting a class of homomorphic functions," Inf. Sci., vol. 286, pp. 19-28, Dec. 2014.

[31] H. Zhang, P. Gao, J. Yu, J. Lin, and N. Xiong, ``Machine learning on cloud with blockchain: A secure, verifiable and fair approach to outsource the linear regression for data analysis," IEEE Trans. Netw. Sci. Eng., early access, Sep. 3, 2021, doi: 10.1109/TNSE.2021.3110101.

[32] Y. Zhang, Y. Xiang, L. Y. Zhang, L.-X. Yang, and J. Zhou, ``Efficiently and securely outsourcing compressed sensing reconstruction to a cloud," Inf. Sci., vol. 496, pp. 150-160, Sep. 2019.

[33] Y. Zhang, L. Y. Zhang, J. Zhou, L. Liu, F. Chen, and X. He, ``A review of compressive sensing in information security field," IEEE Access, vol. 4, pp. 2507-2519, 2016.

[34] Y. Zhang, J. Zhou, L. Y. Zhang, F. Chen, and X. Lei, ``Support-set-assured parallel outsourcing of sparse reconstruction service for compressive sensing in multi-clouds," in Proc. Int. Symp. Secur. Privacy Social Netw. Big Data (SocialSec), Nov. 2015, pp. 1-6.

IJARETY

INNO SPACE
SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर
NISCAIR

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975

Impact Factor: 7.394

www.ijarety.in

editor.ijarety@gmail.com