Advancing Image Security through Deep Learning and Cryptography in Healthcare and Industry

Prajwal Kumar
Maharshi Dayanand University
Computer Science Engineering
Haryana, India
prajwalkumar111299@gmail.com

Ankur Laroia
University of Texas at Dallas
Ms in Business Analytics
Texas, United States
ankurlaroia1@gmail.com

Mehul Kumar
Amity University
Computer Science Engineering
Uttar Pradesh, India
kumarmehul1784@gmail.com

Avi Laroia
Birla Institute of Technology
Civil Engineering
Pilani, India
avilaroia1@gmail.com

Kamal Upreti
Christ University
Dept. of Computer Science
Delhi NCR Campus, India
kamalupreti1989@gmail.com

Jyoti Parashar
ADGIPS
Dept. of Computer Science and Engineering
Delhi, India
jyoti.parashar123@gmail.com

2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) | 979-8-3503-5326-6/24/$31.00 ©2024 IEEE | DOI: 10.1109/ETNCC63262.2024.10767450

***Abstract*—Securing electronic health records (EHRs) in the Internet of Medical Things (IoMT) ecosystem is a key concern in healthcare due to the sector's differed environment. As the evolution of technology continues, ensuring the confidentiality, integrity, and accessibility of EHRs becomes more and more challenging. To enhance the confidentiality of healthcare picture data, this study explores the combined use of deep learning and cryptography methods. Through the utilization of weight analysis for improving encryption strength and the combination of chaotic systems to generate undetectable encryption patterns, it explores how deep neural networks can be modified for use in encryption. It also provides a survey of the present scenario of deep learning-based image detection of anomalies methods in working environments, such as network typologies, supervision levels, and assessment norms. Techniques in cryptography provide an effective means to protect confidential medical picture data while it's being transmitted and stored. Deep learning, on the other hand, has the ability to entirely change cryptography by providing robust encryption, resolution augmentation, and detection capabilities for medical image security. The paper outlines future research approaches to overcome these problems and tackles the opportunities and obstacles in medical image cryptography and industrial picture anomaly detection. Through this work, picture privacy in the healthcare and industrial sectors is advanced, opening the door to enhanced privacy, integrity, and availability of vital image data by overcoming the gap between deep learning and cryptography.**

Keywords—Deep Learning, Cryptography, Medical Image Security, Image Encryption

I. INTRODUCTION

The healthcare sector has consistently embraced advances in technology in order to enhance overall healthcare delivery, expedite procedures, and improve patient care. A significant factor contributing to this change has been information technology (IT), which has transformed healthcare processes by encouraging improved efficiency, collaboration, and interaction [1-4]. Ensuring the safety and security of healthcare pictures transmitted via the Internet is an essential challenge for healthcare institutions and technology providers in the mostly IT-driven environment of today [5-8]. Three practical approaches have been developed for addressing these security problems: image authentication, image steganography, and image encryption [8–10]. These approaches attempt to balance the crucial need for security with the fundamental characteristics of medical images. Medical pictures are vulnerable to unauthorized use because they are not just processed, transferred, and stored online [11]. This approach provides an effective defence against unwanted breaches and ensures that confidential medical data remains protected for the duration of its existence.

Medical images differ from characteristic images in terms of reliability, high pixel correlation, and large data size. Encrypting medical pictures has distinct obstacles, especially in terms of data extraction speed and accuracy. Traditional techniques for encryption might not always be effective in protecting huge medical photos. As a result, it is essential to protect the algorithms used in the processing of medical images against possible risks [12]. Chaos systems are commonly employed for producing pseudo-random numbers, for enhancing the efficiency of encryption. These systems have the ability of producing very random sequences, allowing for the development of strong encryption keys [13]. Using chaotic systems for producing encryption keys can help healthcare providers. Deep learning advancements provide possibilities to enhance the confidentiality of patients, safeguard against fraudulent activity, and ensure the accuracy and legitimacy of the analysis of healthcare images [14-17]. Researchers are constantly investigating new methods to improve amongst protecting personal data and using it for fundamental therapeutic and research purposes. Conducting in-depth review of existing papers is essential for obtaining an unambiguous understanding of the advancements in this rapidly changing field. In this study, we provide a comprehensive examination on how cryptography approaches have been incorporated into deep learning-based medical image processing.

This paper aims to serve as a road-map for future investigations in this field, as well as providing several crucial contributions:

1. An outline of recent & incipient secrecy conservancy is presented, via special emphasis on how they can be applied in ‘deep learning-based’ therapeutic picture examination. Given the field's complexity, that involves patients, hospitals, research centers, and corporate people involved, there is an urgent need to tackle issues about data transparency, patterns of use, and individual privacy.
2. Using a methodical categorization of these papers based on the use of cryptoanalysis in ‘deep learning-driven’ medicinal image examination, this review

979-8-3503-5326-6/24/$31.00 ©2024 IEEE

provides insights into task-specific problems and provide solutions based on current literature.

II. RELATED WORK

Numerous previous study efforts have focused on picture security in a variety of contexts [18], with an emphasis on medical imagery [19]. The effectiveness of the proposed algorithms in securing data and images depends on the level of security of the encryption technology used. A number of methods have been published in the literature, having a focus on generating secure and unpredictable keys [20]. For example, a particular method suggested an approach for obtaining a secure key with minimal latency by using cardiogram data for encryption purposes [21].

Another study provided a better approach for effectively concealing and scattering healthcare imaging information using Fibonacci sequences [22–23]. Furthermore, in order to generate random numbers, the AES method was used to enhance the safekeeping of the depictions that were generated [24]. In addition, an adaptive cypher system based on state estimation principles was implemented for key development [25]. Efforts were also made to increase the challenges associated with generating extremely random keys that develop with time and operation [26], so greatly enhancing the security of medical images transferred between both parties.

Despite substantial advances in the procedure of deep learning for analysis of medical descriptions in the medical field, it is still exposed to a wide range of security threats, such as model inversion attacks [27], poison attacks [28], and many other security weaknesses [29–31]. Among these threats, adversarial attacks on medical imaging have garnered significant attention within the deep learning community, given their potential to pose significant safety and security risks.

Advancements in computer science, computer analysis, and image processing have revolutionized disease analysis and treatment, particularly through the utilization of deep learning techniques. These techniques, that utilize X-rays or magnetic resonance imaging (MRI), have greatly improved doctors' ability for providing precise and rapid treatment. For example, the DCNN (Deep Convolutional Neural Network) technique has been used to detect hemorrhages in images from endoscopy of the capsule [37].

Similar investigations have utilized completely supported as well as fully stacked FCN (Fully Convolutional Network) networks combined with the LSTM (Long Short-Term Memory) to examine large data sets by dividing them into smaller segments for the extraction of features [38]. Another approach involved employing a hybrid method to extract features and classify them using CNNs (Convolutional Neural Networks) to identify digestive diseases in MRI images [39].

Furthermore, an efficient feature extraction method based on CNN approaches was developed for identifying inflammatory gastrointestinal disorders in WCE (Wireless Capsule Endoscopy) videos, and the recovered features were subsequently categorized using SVM (Support Vector Machine) [40]. These new applications demonstrate the significance of deep learning in medical analysis of pictures and recognizing diseases.

A tumor can be described as abnormal proliferation of cells in a particular part of the body. Tumors can be divided into two types: tumours that are benign (non-cancerous) and tumors that are malignant (cancerous). In an investigation conducted by [41], an approach was applied to diagnose tumors from mammograms in a database which includes 482 pictures. Before analysis, ambiguity in the photos was removed with a median filter. These characteristics were used in the categorization approach to figure out the existence of disease [42]. These methods emphasise the different approaches used in medical imaging analysis that help in tumour identification and classification.

TABLE I. Comparison of existing encryption algorithms.

Study	Organ	Modality	Function	Metrics	Encryption Algorithm
[35] 2023	Eye	MRI, CT	Classification, Segmentation	Dice similarity coefficient, Hausdorff distance, MSE, Accuracy	U Net, ResUNet
[33] 2023	Chest, Cervix, Eye	X-ray, Fundoscopy, CT scan	Classification, Detection	Speed and Accuracy	Explainable machine learning
[32] 2023	Skin	Dermoscopy	Classification	PSNR, SSIM, Correlation Coefficient, Entropy	Cycle-GAN network
[34] 2022	Chest	X-ray	Classification	Accuracy	Image diffusion with dilated ResNet
[36] 2021	Brain	MRI	Segmentation	Dice, Positive predictive value (PPV), and Sensitivity	Two-stage generative adversarial neural network (ToStaGAN)

In dermatology, imaging and colouring techniques are essential for providing an in-depth comprehension of various skin disorders. For better examination accuracy, methods such as DNN (Deep Neural Networks) are being utilised[50]. Recent research in this area has been centred on employing DNN applications to identify cancer cells in the colon [43, 44]. Thoracic lymph nodes and interstitial lung disease were additionally investigated with the CNN (Convolutional Neural Network) algorithm. These studies used standardised datasets to train the RNN (Recurrent Neural Network) algorithm, which produced positive outcomes in early illness identification and advancement management. These developments in AI-based imaging analysis hold the potential to significantly enhance diagnostic capabilities in dermatology and other medical areas[48,49].

III. RESEARCH METHODOLOGY

A. Procedure

The increasing popularity of medical imaging techniques has altered diagnostic and treatment methods in healthcare. Chest CT scans and brain MRIs, for example, can provide essential information into diseases such as lung disease and brain tumors, allowing for more precise identification. However, the delicate condition of these medical photographs raises privacy concerns, as unauthorized access may violate the confidentiality of patients and result in legal implications for organizations providing healthcare. As a result, efforts have been made to develop security mechanisms, such as cryptographic approaches, that safeguard these photos while safeguarding patient privacy. The encrypted results or predictions are then sent back to healthcare facilities. It's important to note that while the results are depicted as encrypted in the image, this may not always be the case. Authorized healthcare professionals decrypt these results for further analysis and decision-making purposes.

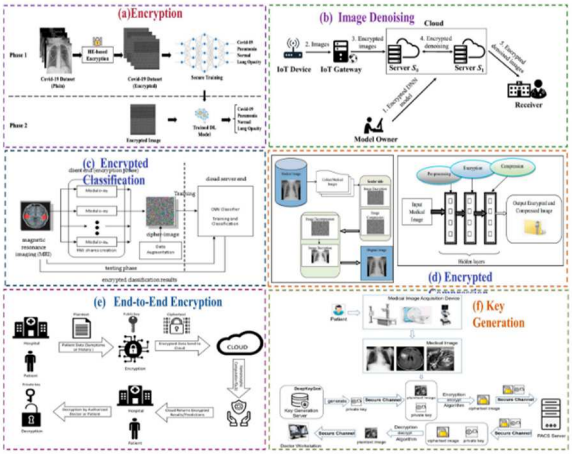

Fig. 1. Cryptography procedures for medical image processing

Cryptographic methods find extensive application in various facets of deep learning-driven medical image processing, as evidenced in existing literature. The subsequent sections delineate relevant studies concerning distinct cryptographic approaches. Figure 1 elucidates the manifold utilization of cryptographic techniques in securely managing medical images via deep learning. The illustration demonstrates an encryption strategy employed in medical image processing, alongside encrypted denoising techniques within IoT-centric healthcare frameworks. Furthermore, it showcases tumor classification predicated on encrypted MRI images through deep learning-infused medical image analysis. Additionally, the figure portrays the encryption of Chest X-ray images before compression, subsequent processing through deep learning algorithms, and eventual decompression and decryption by authorized medical practitioners. This underscores an end-to-end encryption protocol within cloud-based services, leveraging homomorphic encryption to bolster security during deep learning-powered medical image analysis. Lastly, it introduces a deep learning-driven key generation method for encrypting medical images during diverse analytical tasks in deep learning-based medical image analysis.

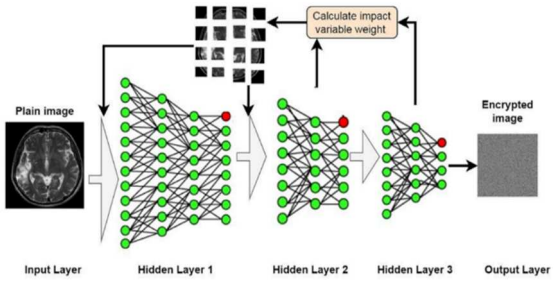

Fig. 2. Behaviour of proposed image encryption within deep learning algorithm

The overall methodology of the study comprises two primary components. Firstly, it focuses on enhancing the encryption method to ensure the security of medical image data. Secondly, it involves the classification of features extracted from the image using deep learning and DNN algorithms. In encryption, the process consists of two stages: confusion and diffusion. The proposed method contributes to both aspects of the work. In the confusion stage, pixel positions and sub-blocks are randomly selected with the assistance of the DNN algorithm. Additionally, the pixel values are altered under the control of the same algorithm.

ALGORITHM 1 Inclusive projected phase for image encryption using DNN.

1- **Read** images from the dataset
2- **For** all images do
   2.1 Preprocessing given image
   2.2 Extract features from the image
   2.3 Create Neural Network
   2.4 Determine effective parameters in the network

3- **Update** hidden layers and nodes according to certain parameters

4- Confusion process

4.1 **Use** DNN to select the partition of an image4.2 For each partition, use DNN to scramble

4.3 **Update** cipher key

5- **Diffusion** process

5.1 **While** not EOI Do 5.1 Move pixels into vector

5.2 **Use** DNN to change pixel value (vertically and horizontally)

5.3 **Update** cipher key

6- **Save** the encrypted image to a file or transmit it through a secure channel for storage or further processing

7- **Return** to step 2

The algorithm outlined in Algorithm 1 presents a generalized approach for image encryption utilizing a DNN (Deep Neural Network). Initially, the images are read from the dataset, and for each image, a series of preprocessing steps are carried out. These include steps such as noise reduction and normalization to enhance the quality of the image data. Subsequently, features are extracted from the pre-processed image, which involves identifying key patterns or characteristics within the image that are relevant for encryption. A neural network is then created, and its parameters are determined based on the specific requirements of the encryption process. In the subsequent stage, the algorithm begins the confusion process, which involves dividing the image using the DNN to identify particular areas for encryption. Within every single partition, the DNN is used again to jumble the pixel values, adding unpredictability and complexity to the encryption procedure. To ensure security, the cypher key is regularly updated.

After the confusion procedure. the algorithm moves on to the diffusion stage. The pixels are shifted into a vector, and the DNN is used to modify the pixel values vertically and horizontally. This diffusion stage assists in disseminating the encrypted information throughout the image, thereby improving security. Again, the cypher key has been altered to reflect the modifications. Once the encryption procedure is finished, the encrypted image is saved to a file or sent via an encrypted connection for storing or further processing. The algorithm then returns to the initial step to process the next image in the dataset, iterating through the entire process until all images have been encrypted. Overall, this algorithm demonstrates a systematic approach to image encryption using DNN, combining both confusion and diffusion techniques to ensure robust security measures.

IV. RESULTS & DISCUSSION

A. Experimental Setup

In addition, deep learning techniques are exposed to adversarial attacks, which endanger the security and reliability of encrypted healthcare information. To improve robustness to such attacks, future research should focus on creating robust methods for training and incorporating protective mechanisms into deep learning models. These models often demand expensive hardware and long training times, which makes them unfeasible in real-time or resource-constrained applications. To tackle this issue, future studies should concentrate on the creation of hardware accelerators, optimise techniques, and more efficient algorithms for accelerating cryptographic operations and reducing computing cost. By tackling these challenges and exploring new ways, researchers might pave the way to subsequent medical image cryptography systems that are more robust and efficient.

B. Benchmarking

Comparing the histograms of the encrypted image and its pain-image, you can see how encryption affects image data. Essentially, what we desire in such cases is for the two images to have similarities in their histogram shapes and forms. This would be an indication that the encryption process upholds at least some of the underlying patterns as well as key characteristics of the source image without compromising safety. Any inconsistencies or changes in this histogram imply possible problems, including information loss or distortion during encryption activities. Examining the histograms of both images is essential to assessing the effectiveness of the encryption method for safeguarding the confidentiality and safety of medical image data. It enables researchers and professionals to evaluate the impact of encryption on image quality and identify potential weaknesses that must be addressed in order to guarantee accurate and safe transmission of medical images.

TABLE II: Comparing of correlation coefficient results with known approaches.

Methods	Horizontal	Vertical	Diagonal
[47]	0.094	0.005	0.006
[46]	0.002	0.001	0.001
[45]	−0.001	0.009	0.003
Proposed	−0.007	0.005	−0.041

Table 2 presents a benchmark comparison of correlation coefficient values obtained using different methods for various directions, namely horizontal, vertical, and diagonal. Among the existing methods evaluated, a method [49] yields correlation coefficients of 0.094 for horizontal, 0.005 for vertical and 0.006 for diagonal directions. Method [47] shows notably lower correlation coefficients of 0.002 for horizontal, 0.001 for vertical and 0.001 for diagonal directions. Conversely, method [46] demonstrates mixed results, with a correlation coefficient of -0.001 for horizontal, 0.009 for vertical, and -0.003 for diagonal directions.

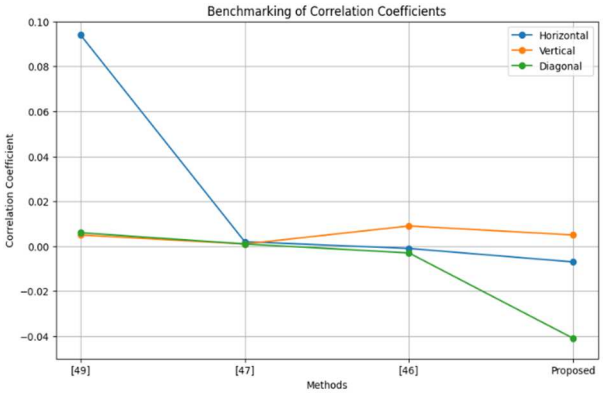

Fig. 3. Benchmarking of Correlation Coefficients

C. Discussion

In comparison, the proposed method yields correlation coefficients of -0.007 for horizontal, 0.005 for vertical and -0.041 for diagonal directions. These values suggest a weaker correlation compared to some existing methods, particularly in the horizontal and diagonal directions. However, it is important to note that correlation coefficient values closer to zero indicate weaker linear relationships, which may not necessarily imply inferior performance. Instead, they may reflect different characteristics of the data or methodological differences. Overall, the benchmarking analysis provides insights into the performance of the proposed method relative to existing approaches in terms of correlation coefficients for different directional components. In addition, analysis and confirmation of these results would be required for fully evaluating the efficiency and practicality of every approach in particular circumstances or applications.

V. CONCLUSION

The in-depth assessment carried out in this paper provides light on the widespread adoption of DL-based algorithms for analysis of medicinal imageries, emphasizing significance of security issues. Modern neural network-based deep learning algorithms have shown efficacy in a wide range of healthcare image processing tasks, including categorization, detection, and segmentation across various subfields. However, with increasing reliance on technologies for deep learning, there is an urgent need to address weaknesses in security. This investigation investigated into six different aspects of cryptography, with a particular focus on enhancing security, safeguarding privacy, investigating different encryption methods, developing complete encryption, and integrating safety measures using deep learning algorithms. The

investigation highlights the significance of exploring distinctive security techniques customized to a lot presenting formats of medical pictures, as well as the implementation of deep learning algorithms. The proposed method in this paper uses deep neural networks to improve the security of medical images through techniques consisting of segmentation, random distribution of image components, and pixel randomization. The deep neural network approach enables secure encryption by enhancing the randomness that comes from confusion and diffusion processes. Particularly, the algorithm encourages the distribution and division of image blocks depending on characteristics that have the biggest impact on the deep neural network's outputs. Furthermore, the technique suggested uses pixel bit scrambling to alter pixel values, which enhances image security. The proposed algorithm's effectiveness has been confirmed by evaluating it against multiple parameters and measuring it against previous investigations. The results indicate that merging advanced safety precautions with deep learning algorithms has tremendous potential to enhance medical picture analysis in smart healthcare applications.

REFERENCES

[1] Lee, D.; Yoon, S.N. Utilization of Artificial Intelligence-Based Technologies in the Healthcare Sector: Prospects and Challenges. Int. J. Environ. Res. Public Health 2021, 18, 271.

[2] Tortorella, G.L.; Saurin, T.A.; Fogliatto, F.S.; Rosa, V.M.; Tonetto, L.M.; Magrabi, F. Influence of Healthcare 4.0 Digital Technologies on Hospital Resilience. Technol. Forecast. Soc. Change 2021, 166, 120666.

[3] Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and Health: Integration of Internet of Things, Big Data, and Cloud Computing for Healthcare Advancement. J. Ind. Inf. Integr. 2020, 18, 100129.

[4] Dhanvijay, M.M.; Patil, S.C. Internet of Things: An Examination of Enabling Technologies in Healthcare and Its Practical Applications. Comput. Netw. 2019, 153, 113–131.

[5] Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Framework for Ensuring Security in the Internet of Medical Things. Internet Things 2019, 8, 100123.

[6] Somasundaram, R.; Thirugnanam, M. Analysis of Security Challenges in Healthcare Internet of Things. Wirel. Netw. 2021, 27, 5503–5509.

[7] Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security Considerations in IoMT Communications: A Comprehensive Review. Sensors 2020, 20, 4828.

[8] Priyadharshini, A.; Umamaheswari, R.; Jayapandian, N.; Priyananci, S. Enhancement of Medical Image Security Through Encryption and LSB Steganography. In Proceedings of the 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 19–20 February 2021; pp. 1–5.

[9] Magdy, M.; Hosny, K.M.; Ghali, N.I.; Ghoniemy, S. Ensuring Security of Medical Images for Telemedicine: A Methodical Review. Multimed Tools Appl. 2022, 81, 25101–25145.

[10] Hasan, M.K., Islam, S., Sulaiman, R., et al.: Enhancing Medical Image Security for Internet of Medical Things Applications Using Lightweight Encryption Techniques. IEEE Access 9(6), 47731–47742 (2021).

[11] El-Shafai, W., Khallaf, F., El-Rabaie, E.S.M., El-Samie, F.E.A.: DNA-Chaos Cryptosystem-Based Robust Encryption for Secure Telemedicine and Healthcare Applications. J. Ambient Intell. Hum. Comput. 12(10), 9007–9035 (2021).

[12] Avudaiappan, T., Balasubramanian, R., Pandiyan, S.S., Saravanan, M., Lakshmanaprabu, S.K., Shankar, K.: Dual Encryption with Oppositional-Based Optimization Algorithm for Medical Image Security. J. Med. Syst. 42(11), 1–11 (2018).

[13] Khalid, N.; Qayyum, A.; Bilal, M.; Al-Fuqaha, A.; Qadir, J. Techniques and Applications of Privacy-Preserving Artificial Intelligence in Healthcare. Comput. Biol. Med. 2023, 158, 106848.

[14] Ding, Y.; Tan, F.; Qin, Z.; Cao, M.; Choo, K.-K.R.; Qin, Z. DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption. IEEE Trans. Neural Netw. Learn. Syst. 2022, 33, 4915–4929.

[15] Kaissis, G.A.; Makowski, M.R.; Rückert, D.; Braren, R.F. Secure, Privacy-Preserving, and Federated Machine Learning in Medical Imaging. Nat. Mach. Intell. 2020, 2, 305–311.

[16] Gayathri, S.; Gowri, S. Deep Learning Network-Based Medical Image Privacy Preservation in Cloud Environments. J. Cloud Comput. 2023, 12, 40.

[17] Li, C., Zhang, Y., Xie, E.Y.: A Comprehensive Review of Attacker-Cipher Interaction in 2018. J. Inf. Secur. Appl. 48(3), 102361 (2019).

[18] Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A., Arunkumar, N.: Hybrid Optimization with Cryptography Encryption for Enhanced Medical Image Security in Internet of Things. Neural Comput. Appl. 32(15), 10979–10993 (2020).

[19] Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A.K., Yang, P., Huang, H., Hou, G.: A Secure and Robust Fragile Watermarking Scheme for Medical Images. IEEE Access 6(8), 10269–10278 (2018).

[20] Ghafoor, R., Saleem, D., Jamal, S.S., Ishtiaq, M., Ejaz, S., Jamal Malik, A., Khan, M.F.: Survey on Reversible Watermarking Techniques for Echocardiography. Secur. Commun. Network 2021, 8820082 (2021)

[21] Salem, N., Elnaggar, F.: RIFD Fibonacci-Zeckendorf Hybrid Encoding and Decoding Algorithm for Medical Image Compression and Reconstruction. In: Proceedings of the 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA), Valencia, Spain, pp. 66–73 (2020)

[22] Guo, C., Liu, J., Li, W., et al.: Imaging Through Scattering Layers Exceeding Memory Effect Range by Leveraging Prior Information. Opt. Commun. 434, 203–208 (2019)

[23] Hua, Z., Yi, S., Zhou, Y.: Medical Image Encryption Using High-Speed Scrambling and Pixel Adaptive Diffusion. Signal Process. 144, 134–144 (2018)

[24] Biswas, M., Kuppili, V., Saba, L., et al.: State-of-the-Art Review on Deep Learning in Medical Imaging. Front. Biosci. 24(3), 380–406 (2019)

[25] Abd-El-Atty, B., Iliyasu, A.M., Alaskar, H., Abd El-Latif, A.A.: A Robust Quasi-Quantum Walks-Based Steganography Protocol for Secure Transmission of Images on Cloud-Based E-Healthcare Platforms. Sensors 20(11), 3108 (2020)

[26] Fredrikson, M.; Jha, S.; Ristenpart, T. Model Inversion Attacks Exploiting Confidence Information and Basic Countermeasures. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery. New York, NY, USA, 12 October 2015; pp. 1322–1333.

[27] Tayyab, M.; Marjani, M.; Jhanjhi, N.Z.; Hashem, I.A.T.; Usmani, R.S.A.; Qamar, F. A Comprehensive Review on Deep Learning Algorithms: Security and Privacy Issues. Comput. Secure. 2023, 131, 103297.

[28] Razzak, M.I.; Naz, S.; Zaib, A. Deep Learning for Medical Image Processing: Overview, Challenges, and the Future. In Classification in BioApps: Automation of Decision Making; Dey, N., Ashour, A.S., Borra, S., Eds.; Lecture Notes in Computational Vision and Biomechanics; Springer International Publishing: Cham, Switzerland, 2018; pp. 323–350. ISBN 978-3-319-65981-7.

[29] Finlayson, S.G.; Bowers, J.D.; Ito, J.; Zittrain, J.L.; Beam, A.L.; Kohane, I.S. Adversarial Attacks on Medical Machine Learning. Science 2019, 363, 1287–1289.

[30] Panwar, K.; Singh, A.; Kukreja, S.; Singh, K.K.; Shakhovska, N.; Boichuk, A. Encipher GAN: Color Image Encryption System Using a Deep Generative Model. Systems 2023, 11, 36.

[31] Gaudio, A.; Smailagic, A.; Faloutsos, C.; Mohan, S.; Johnson, E.; Liu, Y.; Costa, P.; Campilho, A. DeepFixCX: Privacy-Preserving Image Compression for Explainable Medical Image Analysis. WIREs Data Min. Knowl. Discov. 2023, 13, e1495.

[32] Zhu, L.; Qu, W.; Wen, X.; Zhu, C. FEDResNet: Flexible Image Encryption and Decryption Based on End-to-End Image Diffusion with Dilated ResNet. Appl. Opt. 2022, 61, 9124–9134.

[33] Pati, S.; Thakur, S.P.; Hamamcı, ˙I.E.; Baid, U.; Baheti, B.; Bhalerao, M.; Güley, O.; Mouchtaris, S.; Lang, D.; Thermos, S.; et al. GaNDLF: Nuanced Deep Learning Framework for Scalable End-to-End Clinical Workflows in Medical Imaging. Commun. Eng. 2023, 2, 23.

[34] Ding, Y.; Zhang, C.; Cao, M.; Wang, Y.; Chen, D.; Zhang, N.; Qin, Z. ToStaGAN: Two-Stage Generative Adversarial Network for Brain Tumor Segmentation. Neurocomputing 2021, 462, 141–153.

[35] Öztürk, ¸S., Özkaya, U.: Gastrointestinal Tract Classification Using Improved LSTM-Based CNN. Multimedia. Tools Appl. 79(39), 28825–28840 (2020)

[36] Min, J.K., Kwak, M.S., Cha, J.M.: Deep Learning in Gastrointestinal Endoscopy: An Overview. Gut Liver 13(4), 388 (2019)

[37] Charfi, S., El Ansari, M., Ellahyani, A., El Jaafari, I.: Ulcer and Red Lesion Detection in Wireless Capsule Endoscopy Images Using CNN. In: Convolutional Neural Networks for Medical Image Processing Applications, pp. 91–108. CRC Press, Boca Raton, FL (2022)

[38] Naz, J., Sharif, M., Yasmin, M., Raza, M., Khan, M.A.: Machine Learning-Based Detection and Classification of Gastrointestinal Diseases. Curr. Med. Imaging 17(4), 479–490 (2021)

[39] Özyurt, F., Sert, E., Avci, E., Dogantekin, E.: Brain Tumor Detection Based on Convolutional Neural Network with Neutrosophic Expert Maximum Fuzzy Sure Entropy. Measurement 147, 106830 (2019)

[40] Tiwari, P., Pant, B., Elarabawy, M.M., Abd-Elnaby, M., Mohd, N., Dhiman, G., Sharma, S.: CNN-Based Multiclass Brain Tumor Detection Using Medical Imaging. Comput. Intell. Neurosci. 2022, 1830010 (2022)

[41] Shadab, S.A., Ansari, M.A., Singh, N., Verma, A., Tripathi, P., Mehrotra, R.: Cancer Detection from Histopathology Medical Image Data Using Machine Learning with CNN ResNet-50 Architecture. In: Computational Intelligence in Healthcare Applications, pp. 237–254. Academic Press, Cambridge, MA (2022)

[42] Razzak, M.I., Naz, S., Zaib, A.: Deep Learning for Medical Image Processing: Overview, Challenges and the Future. In: Classification in BioApps: Automation of Decision Making, pp. 323–350. Springer, Berlin (2018)

[43] Soffer, S., Morgenthau, A.S., Shimon, O., Barash, Y., Konen, E., Glicksberg, B.S., Klang, E.: Artificial Intelligence for Interstitial Lung Disease Analysis on Chest Computed Tomography: A Systematic Review. Acad. Radiol. 29(1), S226–S235 (2022)

[44] Chai, X., Gan, Z., Yuan, K., Chen, Y., Liu, X.: A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput. Appl. 31(5), 219–237 (2019)

[45] Chandrasekaran, J., Thiruvengadam, S.J.: A hybrid chaotic and number theoretic approach for securing DICOM images. Secure. Commun. Network 2017, 6729896 (2017)

[46] Kumar, S., Panna, B., Jha, R.K.: Medical image encryption using fractional discrete cosine transform with chaotic function. Med. Biol. Eng. Comput. 57, 2517–2533 (2019).

[47] M. S. Nasir, M. S. Alam, F. I. Shahi, M. S. Kamal, K. Upreti and P. Vats, "Transformative Insights: Unveiling the Potential of Artificial Intelligence in the Treatment of Sleep Disorders - A Comprehensive Review," 2023 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 2023, pp. 1-6, doi: 10.1109/ETNCC59188.2023.10284945.

[48] Upreti, K., Mittal, S., Vats, P., Haque, M., Pawar, V., Haque, M. (2023). Development and Evaluation of an Artificial Intelligence-Based System for Pancreatic Cancer Detection and Diagnosis. In: Shaw, R.N., Paprzycki, M., Ghosh, A. (eds) Advanced Communication and Intelligent Systems. ICACIS 2023. Communications in Computer and Information Science, vol 1920. Springer, Cham. https://doi.org/10.1007/978-3-031-45121-8_3.

[49] K. Upreti, S. Arora, A. K. Sharma, A. K. Pandey, K. K. Sharma and M. Dayal, "Wave Height Forecasting Over Ocean of Things Based on Machine Learning Techniques: An Application for Ocean Renewable Energy Generation," in IEEE Journal of Oceanic Engineering, doi: 10.1109/JOE.2023.3314090.

[50] Upreti Kamal, Peng Sheng-Lung, Kshirsagar Pravin Ramdas, Chakrabarti Prasun, Al-Alshaikh Halah A., Sharma, A. K., Poonia Ramesh Chandra, (2023) A multi-model unified disease diagnosis framework for cyber healthcare using IoMT- cloud computing networks, Journal of Discrete Mathematical Sciences and Cryptography, 26:6, 1819–1834, DOI: 10.47974/JDMSC-1831.