Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 03 Issue: 12 | Dec-2025
ISSN (O) 3107-6696

Secure Image Management in Healthcare and Industry through Deep Learning and Cryptographic Approaches

Babagana Ali Dapshima[1], Samaila Kasimu Ahmad[2], Hauwa Hamman[3], Nuba Osinda[4], Mohammed H. Wali[5]

[1,2,3,4,5] *Federal University of Agriculture and Entreprenership Bama, Borno State, Nigeria*
[1] *babaganadapshima@gmail.com*, [2] *samailakasimu@gmail.com*

---***---

Abstract - Securing electronic health records (EHRs) within the Internet of Medical Things (IoMT) ecosystem remains a major challenge due to the complex and evolving nature of healthcare environments. As digital systems expand, maintaining the confidentiality, integrity, and accessibility of medical image data becomes increasingly difficult. Cryptographic techniques offer a foundational approach for protecting sensitive medical images during transmission and storage, while deep learning provides new opportunities to transform traditional encryption processes. This study investigates the integration of deep learning and cryptography to strengthen medical image security. It examines methods such as weight analysis to enhance encryption robustness and the use of chaotic systems to generate highly secure, undetectable encryption patterns. The study also reviews current deep learning–based anomaly detection approaches used in operational settings, focusing on network architectures, supervision models, and evaluation standards. Findings indicate that combining deep learning with cryptographic methods provides strong protection, improved resolution, and enhanced detection capabilities for medical image security. The paper further identifies challenges and opportunities in healthcare and industrial image protection, highlighting the need for continued research to address emerging threats and optimize system performance. By bridging the gap between deep learning and cryptography, this work contributes to improved privacy, integrity, and availability of critical image data across healthcare and industrial sectors.

Keywords: Deep Learning, Cryptography, Medical Image Security, Image Encryption.

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. Thus, it becomes imperative to protect patient privacy, as their medical records are often highly sensitive and confidential. Image encryption, which involves protecting the data in a way that makes it available to only authorized workforce members, is one of the most effective methods to protect the confidentiality of patients [11]. Healthcare institutions can reduce the risk of unauthorised access and protect the confidentiality of patients by encrypting medical images during the time they are being recorded and sent. 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]. Encryption depends mainly on random number generation, which serves as a basis for establishing keys for encryption. The unpredictability of the generated numbers has an important effect on the effectiveness of encryption. 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 improve the privacy of healthcare picture data and reduce the possibility of unauthorized use or breaches. 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 the privacy of healthcare picture data utilizing deep learning capabilities. The topic of secure and confidentiality-preserving deep learning methods includes strategies for bridging the gap between securing confidential information and utilizing it for basic therapeutic and research applications. 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 overview of recent and improving privacy preservation techniques is presented, with a special emphasis on how they can be applied in deep learning-based medical picture analysis. Given the field's complexity, that involves patients, hospitals, research centres, and corporate people involved, there is an urgent need to tackle issues about data transparency, patterns of use, and individual privacy.

2. Employing a methodical classification of these studies based on the implementation of cryptography in deep learning-driven analysis of healthcare pictures medic analysis, researchers provide insights into task-specific difficulties as well as solutions based on the latest literature.

3. We additionally carry out an in-depth examination of the current status of the discipline, noting significant issues, unresolved challenges, and potential fields for future research. This critical assessment aims to inform researchers and practitioners about existing gaps and help them in develop new approaches that effectively tackle these challenges.

LITERATURE REVIEW

Numerous study efforts have focused on picture security in a variety of contexts previously [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, the Advanced Encryption Standard (AES) technique was used to generate random numbers with electricity-driven impulse generators, improving the privacy of the pictures produced [24]. In addition, an adaptive cipher 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 utilization of deep learning for analysis of medical picture 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 [29–30]. 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. Adversarial attacks not only disrupt the inference process of deep learning algorithms but also have the capability to circumvent manual scrutiny by experts due to their observed similarity to clean images. Attackers can manipulate medical images in subtle ways to mislead deep learning models. These alterations may cause simulations to give erroneous or misleading outcomes, which could result in misdiagnosis or compromising treatment of patients [31].

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 utilise X-rays or MRI, have greatly developed doctors' ability for providing precise and rapid treatment. For example, the DCNN technique has been deployed to detect haemorrhages 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 categorised using SVM (Support Vector Machine) [40]. These new applications demonstrate the significance of deep learning in healthcare pictures analysis and recognizing diseases.

A tumour can be described as abnormal proliferation of cells in a particular part of the body. Tumours can be divided into two types: tumours that are benign (non-cancerous) and tumours that are malignant (cancerous). In an investigation conducted by [41], an approach was applied to diagnose tumours from mammograms in a database which includes 482 pictures. Before analysis, ambiguity in the photos was removed with a median filter. Many investigations make use of the SVM classifier for the classification of features collected from mammograms in order to determine type of tumours. In addition, in another investigation, the CNN approach was utilized to analyse radiographic pictures, extracting features such as the degree of clustering identified throughout different regions. 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.

In dermatology, imaging and colouring techniques are essential for providing an in-depth comprehension of various skin disorders. For better examination accuracy, approaches on AI (artificial intelligence) such as DNN (Deep Neural Networks) are being utilised. 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.

METHODOLOGY

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 tumours, 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. Therefore, efforts have been undertaken to build security measures, like cryptographic approaches, that safeguard these photos while safeguarding patient privacy. Figure 5 illustrates a typical secured cloud-based IoMT system deployed in a diversified health care environment. In such systems, medical pictures are encrypted before being sent to the cloud, where central computational systems equipped with deep learning methods execute numerous picture processing. 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.

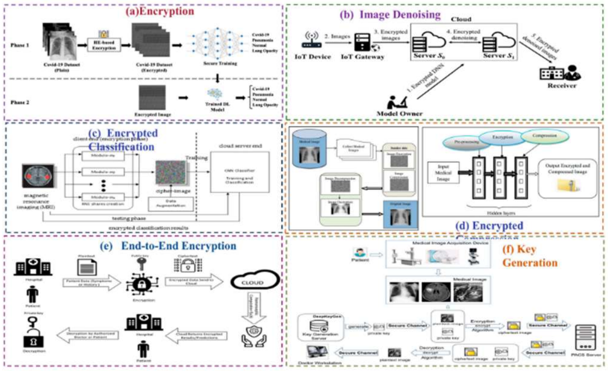


Fig. 1. Cryptography techniques used in medical image processing

Cryptographic techniques are widely used in numerous aspects of deep learning-based processing of medical pictures, as documented in a literature review. Subsequent sections detail the publications that are relevant to each classified cryptographic technique. Figure 6 illustrates the many advantages of cryptographic methods in securely analysing healthcare picture with deep learning. Figure 6a displays an encryption method used in medical image processing, while Figure 6b depicts encrypted noise reduction techniques in IoT-based medical systems.Figure 6c shows cancer categorization using encrypted MRI images and analysis based on deep learning of healthcare images. Additionally, figure 6d illustrates the encryption of Chest X-ray images prior to compressionand then processed using deep learning methods. Subsequently, these pictures are then decrypted and decompressed by certified medical professionals.. Figure 6e demonstrates a scheme in cloud-based services that uses end-to-end encryption, employing homomorphic encryption for enhanced security during deep learning-based healthcare picture analysis. Lastly, Figure 6f depicts a generation of key method for encrypting health care pictures that also relies on deep learning during various analytical tasksin medical image analysis.

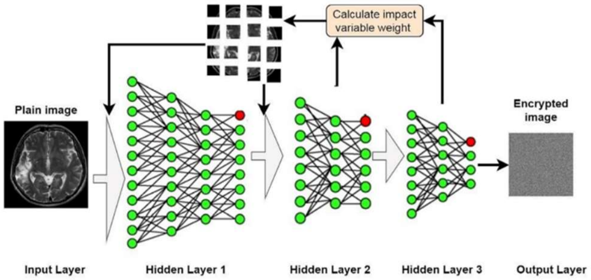
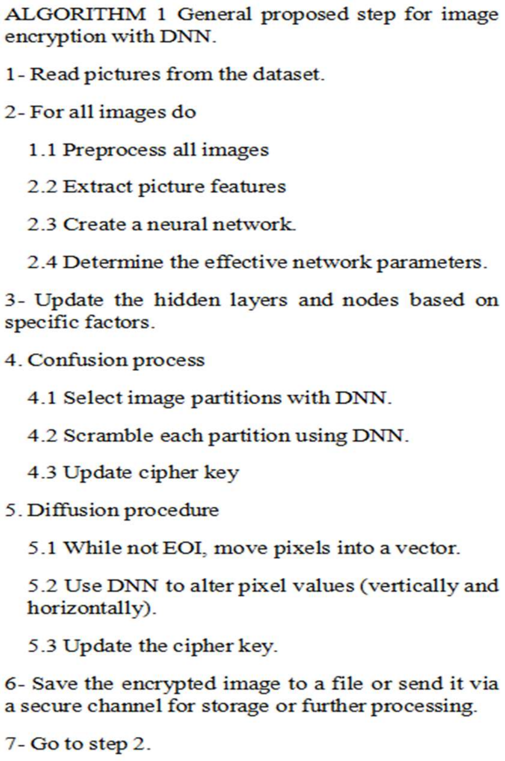


Fig. 2. The performance of proposed image encryption within a deep learning method

The overall methodology of the study comprises two primary components. Firstly, it focuses on enhancing the encryption method to ensure the safety of medical image data. Secondly, it involves the classification of features derived from the picture using deep learning 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. Encryption involves concealing image information to ensure security, making it inaccessible without the unique encryption key. It relies on the non-uniform scattering of data, which cannot be reorganized in the absence of encryption algorithm.



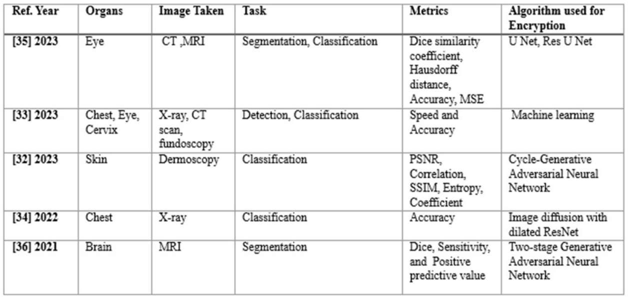
```
ALGORITHM 1 General proposed step for image
encryption with DNN.
1- Read pictures from the dataset.
2- For all images do
    1.1 Preprocess all images
    2.2 Extract picture features
    2.3 Create a neural network.
    2.4 Determine the effective network parameters.
3- Update the hidden layers and nodes based on
specific factors.
4. Confusion process
    4.1 Select image partitions with DNN.
    4.2 Scramble each partition using DNN.
    4.3 Update cipher key
5. Diffusion procedure
    5.1 While not EOI, move pixels into a vector.
    5.2 Use DNN to alter pixel values (vertically and
    horizontally).
    5.3 Update the cipher key.
6- Save the encrypted image to a file or send it via
a secure channel for storage or further processing.
7- Go 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 derived 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 cipher 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 cipher 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.

RESULTS & DISCUSSION

Medical imaging data is highly sensitive and holds significant importance within information systems. Ensuring the secure transmission of medical images over networks requires a robust encryption scheme capable of withstanding various adversarial or cryptographic attacks. Confidentiality, along with integrity and availability, is one of the most important security objectives for protecting information systems. Specifically concerning the encryption of medical images during processing by deep learning algorithms, two main techniques are commonly discussed in the literature: cryptography and homomorphic encryption. These methods play an important role in preserving the confidentiality of medical imaging data, thereby enhancing overall security measures in healthcare information systems.

Table 1. Collection of complete encrypted or security techniques which employ a deep learning techniques



Ref. Year	Organs	Image Taken	Task	Metrics	Algorithm used for Encryption
[35] 2023	Eye	CT ,MRI	Segmentation, Classification	Dice similarity coefficient, Hausdorff distance, Accuracy, MSE	U Net, Res U Net
[33] 2023	Chest, Eye, Cervix	X-ray, CT scan, fundoscopy	Detection, Classification	Speed and Accuracy	Machine learning
[32] 2023	Skin	Dermoscopy	Classification	PSNR, Correlation, SSIM, Entropy, Coefficient	Cycle-Generative Adversarial Neural Network
[34] 2022	Chest	X-ray	Classification	Accuracy	Image diffusion with dilated ResNet
[36] 2021	Brain	MRI	Segmentation	Dice, Sensitivity, and Positive predictive value	Two-stage Generative Adversarial Neural Network

Researchers as well as professionals in the field of healthcare image cryptography must recognize the limitations of deep learning and consider possible future advancements. Understanding these limitations is critical for conquering challenges and identifying areas for progress. Deep learning in healthcare picture cryptography has some major drawbacks, including limited generalization capabilities and vulnerability to malicious attacks. Some of the deep learning techniques that have been skilled on a specific type of dataset may fail to adapt to new or diverse medical picture data, risking performance and security. To address this issue, models must be developed that can more effectively expand across different imaging modalities, diseases, and characteristics of patients.

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. Additionally, the computational complexity of the deep learning models used in healthcare picture cryptography contributes to the challenge. 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.

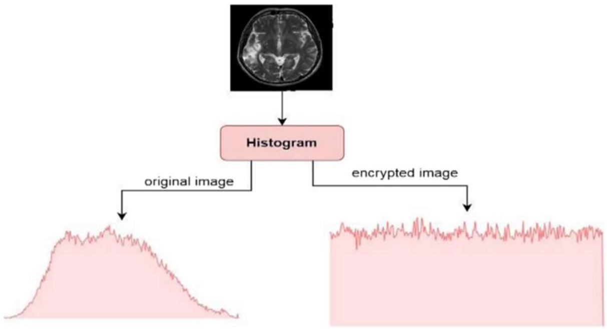


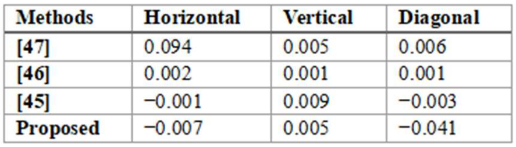
Fig. 3 Plain image & encrypted image histograms.

Figure 3 illustrates histograms comparing a pain image to the equivalent encrypted image. Histograms are visual representations of the distribution of the intensity of pixels within a picture.

In this instance, the pain image is the original medical picture that represents a specific disease or condition, whereas the encrypted image is the final outcome of employing the methods of cryptography to secure the original picture. The histogram of the pain picture represents the number of times of occurrence of different pixel intensities, which usually range from 0 (black) to 255 (white). Peaks in the histogram show areas of high pixel magnitude, whereas troughs represent areas of low magnitude. In comparison, the histogram of the encoded picture emphasizes the pattern of distribution of pixel intensity following encryption.

Comparing the histogram of the encoded picture and its pain-picture, 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 measure 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 2: 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. The correlation coefficient is an n-point estimate of the magnitude as well as the direction of a linear connection between the two variables, with values varying from -1 to 1, where 1 represents a positive correlation, -1 a negative correlation, and 0 no connection. 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.

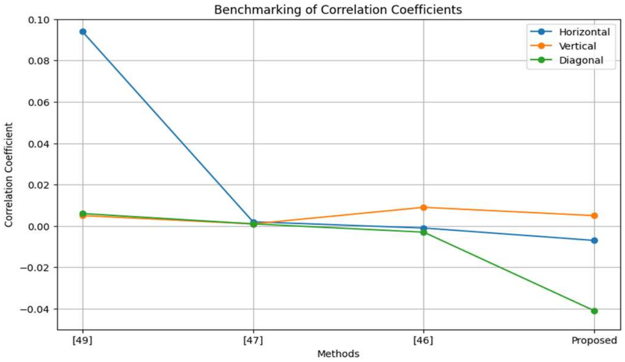


Fig. 4. Benchmarking of Correlation Coefficients

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. However, it is crucial 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 bench-marking analysis provides insights into the results of the suggested approach relative to present 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.

CONCLUSION

The in-depth assessment carried out in this paper provides light on the widespread adoption of deep learning-based techniques for analysis of healthcare picture, emphasising the 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 customised to the a lot presenting formats of medical pictures, also the execution of deep learning algorithms. The suggested method in this survey uses DNN 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. However, further research is required to safeguard the safety and privacy of healthcare picture data, particularly in the deployment of deep learning-based systems, and also to adapt these methods to imaging modalities where they are not yet widespread.

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).