

Deep Learning Algorithms for Medical Image Encryption to Ensure Secure Data Transfer

Siju John^{1,2}, S.N. Kumar^{2,*}

Abstract

Deep learning has significantly impacted various fields, including medical imaging, by offering new ways to encrypt medical images for secure data transfer. This research work examines how deep learning algorithms are used to enhance medical image security during transmission. Given the high sensitivity and privacy requirements of medical data, it's crucial to maintain its confidentiality. Traditional encryption techniques, while reliable, often struggle with issues like scalability, computational efficiency, and the ability to handle the specific features of medical images. This review focuses on recent developments in deep learning, such as convolutional neural networks (CNNs), Autoencoders, and generative adversarial networks (GANs), and their potential to create strong encryption methods. It compares these advanced algorithms with standard encryption methods to highlight the advantages of deep learning in security, efficiency, and flexibility. Additionally, the paper looks at the prospects and challenges in this developing area, seeking to foster new advancements for the secure transmission of medical data in today's digital world.

Keywords: Encryption, medical imaging, deep learning, Generative Adversarial Networks (GANs), secure transmission, Convolutional Neural Networks (CNNs), artificial intelligence (AI)

INTRODUCTION

The rise of digital technologies in the healthcare sector has fundamentally transformed how medical data are stored, accessed, and transmitted. In this digital era, medical imagery, such as X-rays, MRI, and CT scans, has become pivotal in the diagnosis, treatment planning, and continuous care of patients. These images, which are generated by various diagnostic modalities, are rich in sensitive patient information, necessitating stringent security measures for their storage and transmission [1, 2]. Consequently, integrating digital imaging technologies into healthcare infrastructure has highlighted the critical need for effective encryption strategies to safeguard against unauthorized access and confidentiality breaches. Historical encryption techniques, primarily based on cryptographic algorithms, have been somewhat effective in securing transit data.

*Author for Correspondence

S.N. Kumar
E-mail: snkumar@amaljyothi.ac.in

¹Assistant Professor, Department of Computer Science and Engineering, Amal Jyothi College of Engineering, Kanjirappally, Kerala, India

¹Research Scholar, Lincoln University College, Jalan Lembah Sireh, 15050 Kota Bharu, Kelantan, Malaysia

²Associate Professor, Department of Electrical and Electronics Engineering, Amal Jyothi College of Engineering, Kanjirappally, Kerala, India

Received Date: August 31, 2024

Accepted Date: September 23, 2024

Published Date: October 11, 2024

Citation: Siju John, S.N. Kumar. Deep Learning Algorithms for Medical Image Encryption to Ensure Secure Data Transfer. Journal of Image Processing & Pattern Recognition Progress. 2024; 11(3): 28–36p.

However, these conventional methods often struggle to meet the specific demands posed by medical imagery, such as high resolution, substantial file sizes, and the need for instantaneous encryption and decryption to support urgent clinical decisions [3, 4]. Moreover, there is a pressing need to preserve the integrity and confidentiality of patient data against the backdrop of the ever-evolving landscape of cybersecurity threats. Classical encryption involves conventional cryptographic techniques for data security, utilizing symmetric key algorithms such as Advanced

Encryption Standard (AES) and Data Encryption Standard (DES), where the same key encrypts and decrypts data, alongside asymmetric key algorithms such as Rivest–Shamir–Adleman (RSA), which employ distinct keys for encryption and decryption processes. These core methods safeguard privacy, integrity, and verification of information in electronic communications [, 6].

In response to these challenges, deep learning, a branch of machine learning characterized by its use of neural network architecture mirroring the brain’s functionality, has emerged as a significant force. Deep learning has already demonstrated advantages across a range of domains, including image recognition and natural language processing, and is now making strides in the domain of data encryption and decryption [, 8]. In the context of medical image encryption, deep learning presents an innovative frontier to bolster healthcare data security [9, 10].

This study delves into how deep learning algorithms, particularly convolutional neural networks (CNNs), autoencoders [11, 12], and generative adversarial networks (GANs) [13] can redefine the landscape of medical image encryption. These technologies offer versatile, efficient, and powerful solutions for encrypting medical images, adept at managing the complexities and voluminous nature of such data while ensuring that they remain accessible solely to authorized entities [14, 15].

The subsequent sections of this paper cover the foundational principles of deep learning technology, its utility in medical imaging, the inherent challenges in encrypting medical image data, and an in-depth examination of specific deep learning algorithms for encryption purposes [16, 17]. Through a thorough comparative analysis, this study seeks to underscore the superiority of deep learning techniques over traditional encryption methodologies and discuss prospective avenues for the secure transmission of healthcare data in the future.

DEEP LEARNING ALGORITHMS AND THEIR APPLICATIONS

Deep learning, a forefront branch of artificial intelligence (AI), has revolutionized the domain of medical imaging, introducing significant improvements in the analysis, interpretation, and utilization of medical images. Central to deep learning is the use of layered neural networks, which allow the modeling of intricate data patterns. This section delves into the essential concepts underpinning deep learning technologies and their deployment within the sphere of medical imaging. Deep learning frameworks, particularly CNNs, are engineered to autonomously and flexibly identify patterns and features within extensive datasets. These structures emulate the approach of the human brain to processing visual inputs, rendering them highly effective for tasks such as image identification. Through a layered network structure, deep learning algorithms process data and successively learn to identify features with escalating complexity. This layered learning approach equips deep learning systems with the precision required for complex tasks, including image categorization, segmentation, and identification of irregularities [18–20].

Deep learning technologies have significantly improved the analysis of medical imagery by offering advanced capabilities in several key areas.

- *Classification:* Deep learning systems are adept at categorizing medical images with high precision and are capable of distinguishing between different tumor types or identifying lesions as benign or malignant.
- *Segmentation:* These systems are particularly effective in dividing images into specific regions of interest, facilitating the detailed measurement and evaluation of anatomical features and irregularities.
- *Anomaly detection:* With deep learning, it is possible to identify unusual patterns, such as fractures, in X-ray images or signs of disease on MRI scans, often achieving greater accuracy than experienced medical professionals.
- *Image enhancement:* Techniques powered by AI are employed to enhance the quality of images, minimize noise, and boost resolution, contributing to more accurate diagnoses and visual assessments.

The influence of deep learning transcends mere analysis, transforming the methods used to encrypt and decrypt medical images for secure communication. Through the recognition of intricate patterns and representations of data, deep learning algorithms present a refined strategy for safeguarding the confidentiality and integrity of healthcare information.

The integration of deep learning in the encryption of medical images highlights its adaptability and strength. By mastering data representations, deep learning models are adept at crafting encryption algorithms that are both highly secure and efficient. This capability not only safeguards sensitive patient data but also guarantees that such data remains promptly accessible to authorized individuals, thereby supporting the prompt making of critical healthcare decisions.

CONVOLUTIONAL NEURAL NETWORKS

Convolutional neural networks are a class of deep neural networks that are highly effective for analyzing visual imagery. They are particularly well suited for image recognition and classification tasks because of their architecture, which is inspired by the organization of the animal visual cortex, as shown in Figure 1 [21].

The typical structure of a CNN can be divided into two parts: feature extraction and classification.

1. *Input*: This is the initial image fed into the network, which will undergo various transformations.
2. *Convolution*: In the first step of feature extraction, convolutional layers apply a set of filters to the input to create the feature maps. These filters detect spatial hierarchies of features, such as edges, textures, and more complex patterns.
3. *Pooling*: Following convolution, pooling (often max pooling) layers reduce the spatial size of the feature maps, decreasing the number of parameters and computations in the network, which helps control overfitting.
4. *Fully connected*: After several convolutional and pooling layers, high-level reasoning in the neural network occurs. The feature maps were flattened into a vector and fed through fully connected layers for the final classification.
5. *Output*: The last fully connected layer outputs the network predictions. In classification tasks, this typically involves a SoftMax function that converts the outputs into probability scores corresponding to each class.

The image shows how an input image is transformed through a series of convolutional and pooling layers, which extract and condense features before being classified into fully connected layers, resulting in a predicted output.

AUTOENCODERS

Autoencoders are neural networks designed for the unsupervised learning of compressed data encodings. They work by narrowing the input data to a smaller encoded representation and then expanding it back to its original form. The network has two main components.

1. *Encoder*: This segment of the network condenses the input into lower-dimensional code, effectively summarizing the essential features of the data within a more compact representation.
2. *Bottleneck*: This is the layer containing the encoded representation of the input data. It serves as the compressed knowledge center of the network.
3. *Decoder*: Acting as the inverse of the encoder, the decoder reconstructs the input data from the encoded representation to match the original input as closely as possible.

The training objective of an autoencoder is to reduce the difference between the original input and its reconstruction, thereby forcing the network to prioritize the most salient features in the encoding process. Autoencoders are used in tasks that require dimensionality reduction, noise reduction, feature extraction, etc., serving as foundational blocks in more complex neural network architectures.

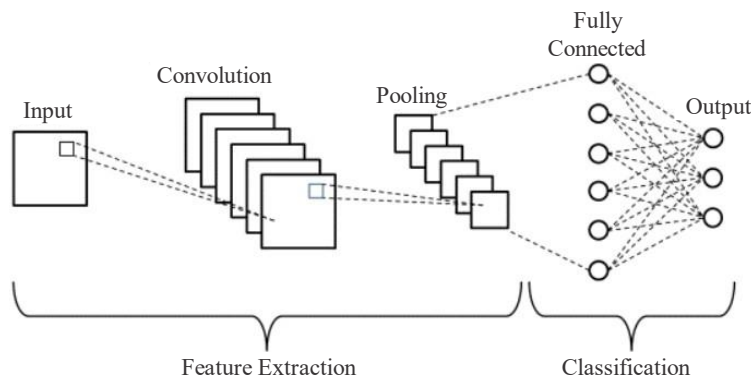


Figure 1. Architecture of convolutional neural networks.

Autoencoders are specialized neural networks utilized for unsupervised learning, aiming to encode data efficiently and often to reduce dimensions or feature extraction. The fundamental characteristics are as follows.

1. *Data-dependent:* Autoencoders are tailored to the specific nature of the data they process, learning representations that are particularly useful for the dataset at hand.
2. *Imperfect reconstruction:* Typically, autoencoders create an output that is an approximation of the input, deliberately focusing on the most relevant aspects of the data while potentially losing some nuances.
3. *Self-supervised:* Operating without the need for labeled data, autoencoders use the input data to supervise themselves and learn to predict their inputs.
4. *Bottleneck feature:* The bottleneck, a key feature of the autoencoder, is a compressed representation that encapsulates the essence of the input data and serves as the code from which the reconstruction begins.
5. *Compression for simplification:* Autoencoders compress data, similar to Principal Component Analysis (PCA), but with the added capability of capturing non-linear relationships.
6. *Learning representations:* Through the encoding layers, autoencoders learn salient features from data that can be leveraged for classification or detecting outliers.
7. *Minimizing reconstruction error:* The goal of an autoencoder is often to minimize the error between the input and its reconstruction, using metrics such as mean squared error or cross-entropy.
8. *Diverse variants:* Autoencoders come in various forms, including denoising autoencoders that clean the input data, variational autoencoders that understand data distributions, and sparse autoencoders that impose constraints on the sparsity in the code.
9. *Generation capabilities:* Variational autoencoders, a generative variant, can produce new data samples akin to the training data.

The versatility of autoencoders allows them to be used for noise reduction, reducing dimensionality for visualization, as generative tools, and for pretraining networks to identify useful data features [21].

The image illustrates as shown in Figure 2 the structure of an autoencoder, a neural network model designed for learning efficient data encodings in an unsupervised manner. A detailed explanation of its functionality is provided below:

1. *Encoder:* This stage processes the input image and methodically reduces its dimensionality while retaining significant features. The transformation of the encoder compresses the data into a lower-dimensional space.
2. *Bottleneck:* At the heart of the model, the bottleneck captures the essence of the input data, which is now represented in a compressed format known as the latent space representation. This condensed representation contains the key characteristics necessary to rebuild the input.

3. *Decoder*: The decoder component reconstructs the original data from a compressed representation of the bottleneck. It gradually upscales the information, effectively reversing the encoder process until it achieves an output that closely resembles the original input.
4. *Reconstructed image*: The end product of the autoencoder, that is, the reconstructed image, should ideally be a close approximation of the input image. The difference between the two, or the reconstruction loss, is used to fine-tune the network during the learning phase.

Throughout the training, the autoencoder refines its weights and biases to minimize the reconstruction loss, leading to a more accurate representation of the input within the latent space. The ability of the autoencoder to distill the input into a more manageable form without supervision makes it valuable for denoising, dimensionality reduction, and feature extraction in further machine learning tasks. The model's performance is contingent upon how well the reconstructed outputs match the original inputs, with better accuracy indicating a more nuanced understanding of the data structure.

GENERATIVE ADVERSARIAL NETWORKS

Generative adversarial networks, developed by Ian Goodfellow et al. in 2014, [12] are an innovative class of AI frameworks comprising two dueling neural networks: a generator and a discriminator. These networks underwent simultaneous training through a competitive process, as shown in Figure 3.

1. *Generator*: Operates by taking random noise and output data, aiming to replicate the distribution of real-world input data; in this context, images.
2. *Discriminator*: Evaluates both genuine real-world images and synthetic images from the generator, tasked with discerning their authenticity.
3. *Adversarial Dynamics*: In training, the generator's goal is to create data indistinguishable from reality, whereas the discriminator becomes more adept at telling real from fake, akin to a strategic game between the two.
4. *Training feedback (loss)*: The loss metric reflects the discriminator's performance in classifying data, which also guides the generator in refining its output. As the training progresses, the generator outputs increasingly resemble authentic data distribution.
5. *Authentic data source*: Real-world images provide the standard against which the discriminator hones its classification skills.
6. *Source of variability (latent random variable)*: This is a random input that seeds the generator's creative process, typically drawn from a predefined probability distribution.

The ultimate aim is to refine the generator to such an extent that the discriminator can no longer reliably distinguish between the actual and generated images, indicating a well-trained GAN. GANs have broad applications including synthesizing images, enhancing image resolution, and transferring styles, among other creative and analytical tasks.

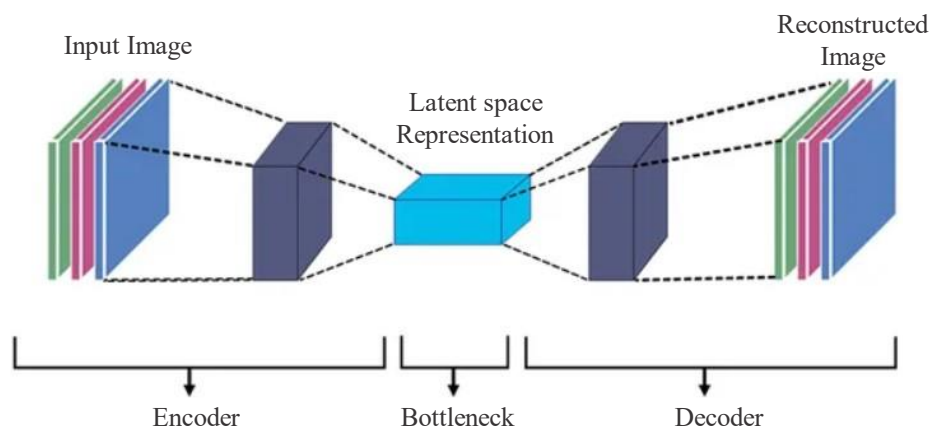


Figure 2. Autoencoder architecture.

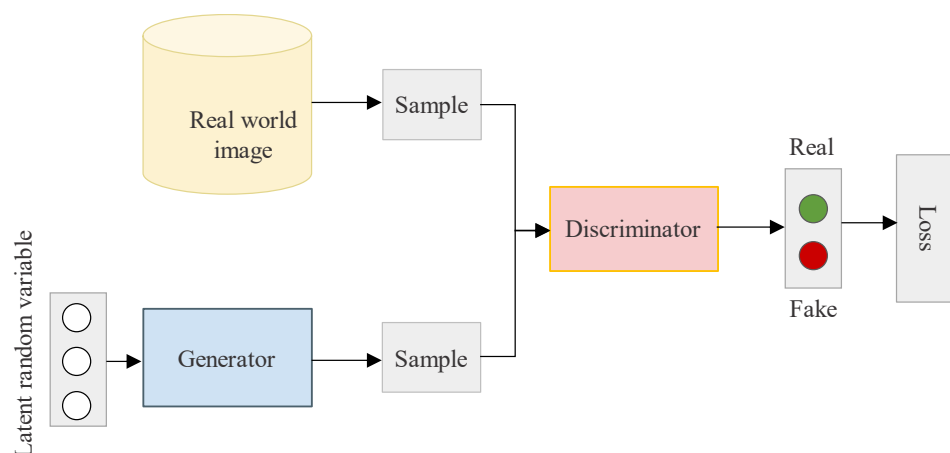


Figure 3. The fundamental architecture of a GAN.

CHALLENGES ASSOCIATED WITH MEDICAL IMAGE ENCRYPTION AND THE IMPLICATION OF DEEP LEARNING MODELS

The forthcoming sections explore the unique challenges associated with encrypting medical images and how deep learning algorithms propose cutting-edge solutions. This represents a pivotal transition away from conventional encryption techniques towards more flexible, scalable, and robust encryption technologies, specifically designed for the modern digital healthcare environment.

Encrypting medical imagery involves navigating a complex array of challenges related to the inherent characteristics of the images, specific requirements of the healthcare sector, and the comprehensive necessity for adhering to security and privacy standards. Understanding these obstacles is essential for developing efficient encryption methods powered by deep learning technology.

COMPLEXITY AND SIZE OF MEDICAL DATA

Medical imaging, including MRI and CT, features high-resolution images filled with intricate details, leading to substantial file sizes. The complexity and sheer volume of these data demand encryption algorithms that balance security with efficiency, ensuring that the process of encrypting and decrypting images does not degrade their quality or require prohibitive computational resources.

NEED FOR IMMEDIATE ENCRYPTION AND DECRYPTION

In the context of healthcare, the swift availability of medical images is often vital for patient care. Therefore, encryption techniques must be capable of real-time operations to prevent delays in diagnosis or treatment. Balancing rapid processing with stringent security measures is a considerable challenge.

MAINTAINING DATA INTEGRITY AND PRIVACY

Encryption strategies must ensure that medical data remains unaltered during transmission, as any unauthorized changes could have serious implications for diagnosis and treatment. Furthermore, these strategies must protect the privacy of patient information, complying with legal and ethical guidelines such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. Deep learning technologies have introduced groundbreaking approaches to overcome the obstacles of encrypting medical imagery. This section covers a range of pivotal algorithms and their roles in facilitating the secure and efficient exchange of medical data.

LEVERAGING CONVOLUTIONAL NEURAL NETWORKS FOR SELECTIVE FEATURE ENCRYPTION

CNNs are adept at pinpointing and encrypting distinct features in medical imagery, enabling the encryption of vital data while retaining crucial information. This method of selective encryption significantly boosts efficiency without sacrificing the level of security provided.

UTILIZING AUTOENCODERS FOR EFFICIENT IMAGE COMPRESSION AND ENCRYPTION

Autoencoders, specialized neural networks crafted for data compression, play a dual role in image encryption. They initially compressed the image to a more manageable size, effectively addressing the issue of large data volumes. The process then encrypts the compressed data, ensuring a layer of security that is both strong and streamlined.

EMPLOYING GENERATIVE ADVERSARIAL NETWORKS FOR ENCRYPTION AND SYNTHETIC IMAGE GENERATION

GANs have the unique ability to create synthetic medical images that aid in training, thereby bolstering the resilience of the encryption algorithm. These networks can also encrypt actual images in a manner that renders the encrypted content seemingly random noise, thereby enhancing the overall security measures.

COMPARATIVE INSIGHTS INTO DEEP LEARNING ALGORITHMS

An analytical comparison of these deep learning techniques sheds light on their advantages and drawbacks. CNNs have been noted for their efficiency and suitability for the encryption of specific features. Autoencoders are recognized for their dual capability of compression and encryption, offering flexibility across a range of uses. GANs are particularly valued for their data obfuscation abilities and for delivering superior security at the expense of greater computational demands.

ANTICIPATED DEVELOPMENTS AND PERSISTING OBSTACLES IN MEDICAL IMAGE ENCRYPTION

Advancements in medical image encryption are expected to continue incorporating deep learning innovations to boost both security and operational efficiency. Future research directions might explore the creation of hybrid models that merge the benefits of various algorithms, delve into the potential of quantum computing in encryption, and investigate the application of blockchain for secure data management. However, challenges such as establishing universal benchmarks for assessing encryption techniques, achieving a balance between computational efficiency and security, and keeping pace with changing legal and ethical norms remain critical hurdles.

Table 1 presents a structured framework for evaluating the deep learning algorithms utilized in the encryption of medical images. This comparative outline considered several critical aspects.

- *Efficiency*: This measures the effectiveness of the algorithm in processing extensive datasets and intricate images without degrading performance.
- *Speed of encryption/decryption*: The rate at which an algorithm can encrypt, and decrypt images is a crucial factor for applications demanding immediate data access.
- *Security level*: Assesses the robustness of encryption to safeguard data from unauthorized access and security breaches.
- *Complexity of implementation*: Evaluate the level of effort and expertise necessary to deploy and manage the encryption framework.
- *Handling of data volume*: Examine the algorithm's capacity to manage and process large quantities and sizes of medical images efficiently.
- *Capability for real-time processing*: The algorithm's proficiency in executing encryption and decryption processes instantly is essential in various medical scenarios.
- *Robustness*: The resilience of the algorithm in sustaining consistent performance under different scenarios and against cyber threats.
- *Adaptability*: The flexibility of the algorithm to accommodate new medical imaging types or adapt to changes in the encryption protocols.
- *Resource demands*: The computational and memory resources the algorithm requires.

Table 1. Comparison table outline for deep learning algorithms in medical image encryption.

Feature	CNNs	Autoencoders	GANs	Traditional encryption methods
Efficiency	High	Moderate to high	Moderate	Low to moderate
Encryption speed	Fast	Moderate	Slow	Varies
Decryption speed	Fast	Moderate	Slow	Varies
Security level	High	High	Very high	High
Complexity (implementation)	Moderate	High	Very high	Low to high
Data volume handling	Large volumes well	Very efficient	Less efficient	Less efficient
Real-time processing	Suitable	Suitable	Less suitable	Varies
Robustness	High	High	Very high	Moderate to high
Adaptability	High	High	High	Low
Resource consumption	Moderate	High	Very high	Low to moderate

This outline was designed to facilitate a detailed comparison of the advantages and limitations associated with each deep learning approach. By filling this table with data derived from your investigations and citing relevant studies or experiments, you can offer readers a comprehensive view of the current state and potential of deep learning to enhance the security and efficiency of medical image encryption. This comparative analysis aimed to elucidate the dynamic field of medical image encryption technology and underscore the significant contributions of deep learning algorithms to the secure transmission of healthcare data.

CONCLUSION

The utilization of deep learning techniques for the encryption of medical imagery has marked a significant advancement toward achieving secure data exchange within the healthcare sector. Deep learning addresses the specific complexities involved in encrypting medical images and presents novel approaches that surpass the capabilities of conventional encryption strategies. As ongoing research progresses, the role of deep learning in this area is expected to substantially influence the security, effectiveness, and dependability of transferring medical information, thereby contributing to improved patient care and privacy protection.

Declaration of Interest

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Acknowledgment

The authors would like to acknowledge support from the Schmitt Center of Biomedical Instrumentation, Amal Jyothi College of Engineering, Kerala, India.

REFERENCES

1. Alom MZ, Taha TM, Yakopcic C, Westberg S, Sidike P, Nasrin MS, et al. The history began from AlexNet: A comprehensive survey on deep learning approaches. [Preprint] arXiv:1803.01164. 2018.
2. Esteva A, Kuprel B, Novoa RA, Ko J, Swetter SM, Blau HM, Thrun S. Dermatologist-level classification of skin cancer with deep neural networks. *Nature*. 2017;542(7639):115–8. DOI: 10.1038/nature21056.
3. Gulshan V, Peng L, Coram M, Stumpe MC, Wu D, Narayanaswamy A, et al. Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs. *JAMA*. 2016;316(22):2402–10. DOI: 10.1001/jama.2016.17216.
4. Abadi M, Barham P, Chen J, Chen Z, Davis A, Dean J, et al. TensorFlow: A system for large-scale machine learning. 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16); Nov 2-4, 2016; Savannah, GA, USA. p. 265–83.

5. Tschandl P, Rosendahl C, Kittler H. The HAM10000 dataset, a large collection of multi-source dermatoscopic images of common pigmented skin lesions. *Sci Data*. 2018;5:180161. DOI: 10.1038/sdata.2018.161.
6. Minaee S, Boykov Y, Porikli F, Plaza A, Kehtarnavaz N, Terzopoulos D. Image segmentation using deep learning: A survey. *IEEE Trans Pattern Anal Mach Intell*. 2022;44(7):3523–42. DOI: 10.1109/TPAMI.2021.3059968.
7. LeCun Y, Bengio Y, Hinton G. Deep learning. *Nature*. 2015;521(7553):436–44. DOI: 10.1038/nature14539.
8. Litjens G, Kooi T, Bejnordi BE, Setio AAA, Ciompi F, Ghafoorian M, et al. A survey on deep learning in medical image analysis. *Med Image Anal*. 2017;42:60–88. DOI: 10.1016/j.media.2017.07.005.
9. Ding Y, Wu G, Chen D, Zhang N, Gong L, Cao M, Qin Z. DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things. *IEEE Internet Things J*. 2020;8(2):1504–18. DOI: 10.1109/JIOT.2020.3012452.
10. Panwar K, Singh A, Kukreja S, Singh KK, Shakhovska N, Boichuk A. Encipher GAN: An end-to-end color image encryption system using a deep generative model. *Systems*. 2023;11(1):36. DOI: 10.3390/systems11010036.
11. Kingma DP. Auto-encoding variational Bayes. [Preprint] arXiv:1312.6114. 2013.
12. Goodfellow I, Pouget-Abadie J, Mirza M, Xu B, Warde-Farley D, Ozair S, et al. Generative adversarial nets. *Adv Neural Inf Process Syst*. 2014;27:2672–80.
13. Ronneberger O, Fischer P, Brox T. U-Net: Convolutional networks for biomedical image segmentation. In: Navab N, Hornegger J, Wells W, Frangi A, editors. *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015*. MICCAI 2015. Lecture Notes in Computer Science, vol. 9351. Springer, Cham; 2015. p. 234–41. DOI: 10.1007/978-3-319-24574-4_28.
14. Chai X, Zhang J, Gan Z, Zhang Y. Medical image encryption algorithm based on Latin square and memristive chaotic system. *Multimed Tools Appl*. 2019;78(24):35419–53. DOI: 10.1007/s11042-019-08168-x.
15. Pan C, Schoppe O, Parra-Damas A, Cai R, Todorov MI, Gondi G, et al. Deep learning reveals cancer metastasis and therapeutic antibody targeting in the entire body. *Cell*. 2019;179(7):1661–76.e19. DOI: 10.1016/j.cell.2019.11.013.
16. Vu L, Thuy HV, Nguyen QU, Ngoc TN, Nguyen DN, Hoang DT, Dutkiewicz E. Time series analysis for encrypted traffic classification: A deep learning approach. 18th International Symposium on Communications and Information Technologies (ISCIT); 2018 Sep 19-21; Hanoi, Vietnam. *IEEE*; 2018. p. 121–6. DOI: 10.1109/ISCIT.2018.8587975.
17. Xu M, Papageorgiou DP, Abidi SZ, Dao M, Zhao H, Karniadakis GE. A deep convolutional neural network for classification of red blood cells in sickle cell anemia. *PLoS Comput Biol*. 2017;13(9):e1005746. DOI: 10.1371/journal.pcbi.1005746.
18. Ciompi F, Chung K, Van Riel SJ, Setio AAA, Gerke PK, Jacobs C, et al. Towards automatic pulmonary nodule management in lung cancer screening with deep learning. *Sci Rep*. 2017;7:46479. DOI: 10.1038/srep46479.
19. Zhang Y, Xiang Y, Zhang LY, Rong Y, Guo S. Secure wireless communications based on compressive sensing: A survey. *IEEE Commun Surv Tutor*. 2018;21(2):1093–111. DOI: 10.1109/COMST.2018.2878943.
20. Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N. Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE Trans Netw Sci Eng*. 2019;8(3):1242–55. DOI: 10.1109/TNSE.2019.2961932.
21. Hinton GE, Salakhutdinov RR. Reducing the dimensionality of data with neural networks. *Science*. 2006;313(5786):504–7. DOI: 10.1126/science.1127647.