A NOVEL MEDICAL IMAGE ENCRYPTION SCHEME BASED ON DEEP LEARNING FEATURE ENCODING AND DECODING

Ruma Hameed[1], Dr. C. Berin Jones[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad,
rumahameed83@gmail.com
[2]Professor, Department of CSE, Shadan Women's College of Engineering and Technology
jonesberin@gmail.com

ABSTRACT

In this study, high school students at Little Scholars Matriculation Hr. Sec. School in Thanjavur, Tamil Nadu, India, are asked about the prevalence and effects of social anxiety. The 17-item Social Phobia Inventory (SPIN) questionnaire, which asks about social interactions, fear of being judged, and discomfort in different social settings, was used to collect data from students. The study analyses student replies and determines the degree of social anxiety using this dataset and a Random Forest machine learning technique. Through the identification of important characteristics that lead to higher degrees of discomfort, the model seeks to predict social anxiety levels. By use of feature selection and correlation analysis, the research reveals intricate connections among many facets of social interactions that impact anxiety. Accuracy and predictive power are used to assess the Random Forest model's performance, showing that it can accurately predict high school students' social anxiety. In order to improve mental health support systems for high school kids, the study suggests more research to improve predictive models and emphasises the potential of Random Forest for precisely pinpointing important elements linked to social anxiety.

1. INTRODUCTION

The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling the efficient distribution of medical images among patients and doctors. However, this increased accessibility also raises significant concerns regarding the confidentiality and integrity of sensitive medical data during storage and transmission. To address these challenges, we propose an innovative medical image encryption system that combines the advantages of deep learning with modern encryption techniques for enhanced security and usability. This system allows users to upload medical images, which are encrypted into a QR code format along with a unique key number. The generated QR code and key are securely stored in a designated folder for future use. During decryption, users can upload the stored QR code and key, enabling the system to reconstruct the original image with high accuracy. Our encryption process leverages the power of deep learning-based neural networks, which are inherently non-linear and well-suited for handling image encryption tasks. A feature encoding mechanism ensures robustness against attacks such as cropping, noise, and brute force. Furthermore, we utilize QR codes for compact and secure transmission, adding an additional layer of encryption and simplifying the sharing of encrypted images. Unlike traditional cryptosystems, which struggle with the unique characteristics of image data (e.g., redundancy and spatial correlation), our system employs a deep neural network-based end-to-end encryption approach. The network directly learns the encryption process, enhancing security and eliminating the need for manual algorithm design. Advanced cryptographic features, such as chaotic mapping and loss functions optimized for encryption tasks, ensure resilience against known plaintext attacks, statistical attacks, and other security threats. This approach not only ensures the protection of sensitive medical data but also provides a user-friendly mechanism for secure image storage and retrieval, leveraging the advantages of IoMT while addressing its privacy concerns effectively. combination of speed, complexity, high security, reasonable computational overhead, and computational power consumption. Many chaotic systems, including high and one-dimensional systems, have been proposed for image encryption. High-dimensional chaotic systems, such as the Rössler system and the Lorenz chaotic system, are commonly employed in image encryption. Yang et al. [5] proposed a medical image encryption technique using exclusive OR (XOR) with Josephus traversing and cat mapping on the basis of the Lorenz chaotic system and SHA-512. Additionally, some researchers have also proposed new high-dimensional chaotic systems to enhance cryptographic security. Wang and Wang [6] proposed a new 6-D hyperchaotic system and employed bit-level permutation and DNA encoding to strengthen the security of the cryptosystem. However, although high-dimensional chaotic systems may offer increased security, their complexity can pose challenges for circuit implementation or encryption efficiency. On the other hand, one-dimensional chaotic systems are vulnerable to attack based on phase space reconstruction [7]. To address these limitations, some researchers have proposed enhancing one-dimensional chaotic maps by incorporating additional methods. Sun and Chen [8] proposed a method for enhancing the security of image encryption by employing a one-dimension chaotic system (logistic map) and an improved Arnold algorithm for image permutation and diffusion. However, the outputs of these chaotic systems are non-uniform To improve safety, they proposed an improved method that concatenated the plaintext image with random images as inputs into the encryption network, performed further diffusion and outputted the result as a ciphertext image to improve the avalanche effect. Subsequently, some improvements have been proposed in [32] and [33]. In addition to GAN-based methods, sang et al. [7] proposed a novel image encryption method based on logistic chaotic systems and deep autoencoder, which scrambled the plaintext image using a logistic chaotic system and then encoded the scrambled image with a deep autoencoder to generated the ciphertext image. Zhu et al. [34] proposed an end-to-image image diffusion model, Erdenet, and a novel loss function based on pixel entropy to enhance the security of ciphertext images. To strengthen the security of the encrypted network, Li and Peng [35] introduced an attention mechanism to enhance the model's response to the region of interest within the medical image. However, these algorithms do not exhibit stronger enough resistance against cropping and noise attacks for transmitting in complex networks.

OBJECTIVE

This project is to develop a secure, efficient, and user-friendly medical image encryption and decryption system to protect sensitive patient data. The system aims to utilize deep learning techniques for robust encryption, converting medical images into QR codes along with unique keys for secure storage and transmission. Additionally, the system focuses on enabling accurate image decryption by reconstructing the original image using the QR code and key, ensuring confidentiality and integrity of medical data against various security threats. This project seeks to address privacy concerns in facilitating secure and seamless sharing of medical images among authorized personnel.

2.1 PROBLEM STATEMENT

The increasing digitization of healthcare has made the secure transmission and storage of medical images such as X-rays, MRIs, and CT scans a critical concern. Traditional encryption methods often struggle to provide the necessary robustness against sophisticated cyber threats while maintaining the quality and integrity of the original image. Additionally, many existing solutions lack user-friendly mechanisms for secure sharing and reliable decryption, which limits their practical applicability in clinical environments. To address these challenges, this project proposes the development of an advanced medical image encryption and decryption system that leverages deep learning and QR code technology. The system allows users to upload a medical image, which is then encrypted using a neural network-based feature encoding technique and transformed into a QR code format. A unique encryption key is generated and stored securely alongside the QR code. For decryption, users can upload both the QR code and the corresponding key to accurately reconstruct the original image using a reversible neural network. This approach ensures high resistance to attacks such as noise, cropping, and brute-force methods, while also preserving the image's fidelity. By combining AI-driven security with the convenience of QR codes, this system offers a robust, secure, and user-friendly solution for protecting sensitive medical data.

2.2 Existing System

GAN-based models offer advanced encryption capabilities, they face several challenges and limitations. One significant drawback is the complexity of training GANs, as the generator and discriminator must reach a delicate balance; otherwise, issues like mode collapse may occur, resulting in poor encryption quality. Additionally, GANs often require extensive computational resources and high-quality hardware, making them unsuitable for resource-constrained environments or real-time applications. Another limitation is the potential lack of reliability in generating consistent and robust encrypted outputs, as GANs can sometimes produce outputs that deviate from expected patterns. Furthermore, GAN-based encryption methods may introduce overhead in both encryption and decryption processes, which can increase latency and reduce system efficiency. Lastly, the reliance on adversarial training can lead to challenges in maintaining model stability, making GANs less predictable and harder to fine-tune for specific use cases. These limitations highlight the need for more efficient and practical alternatives for medical image encryption.

Disadvantage of Existing System

- GAN training is complex and prone to instability, leading to issues like mode collapse.
- Increased overhead in encryption and decryption processes can lead to higher latency.
- May produce inconsistent encrypted outputs, reducing reliability.

2.3 Proposed System

The proposed system aims to enhance the security of medical image storage and transmission by incorporating AI-based encryption and decryption, alongside the use of the pyqrcode library for QR code generation and secure key management. The system allows users to upload a medical image, which is then encrypted using a secure cryptographic key generated from the image features.

This key is encoded into a QR code using the pyqrcode library, providing a portable and secure means of transferring the key. The encrypted image, along with the QR code, is stored in a secure location. To decrypt the image, users scan the QR code to extract the encrypted key, which is validated before being used to reverse the encryption process. This ensures that only authorized users with the correct key can access the original image, preserving confidentiality and integrity. The use of AI-based encryption models, secure key generation, and QR code scanning ensures that the system is both secure and user-friendly, providing protection against unauthorized access and various attacks. This approach simplifies the process of sharing medical images securely while maintaining high levels of encryption effectiveness.

Advantages of Proposed System

- ➢ Improved security with AI-based encryption.
- ➢ Easy key management via QR codes.
- ➢ User-friendly process for encryption and decryption.
- ➢ Ensures confidentiality and integrity of medical images.
- ➢ Efficient image storage and transfer with QR codes.

2. RELATED WORKS

In recent years, numerous studies have explored the application of encryption techniques and artificial intelligence in securing medical data, particularly medical images. Traditional image encryption methods, such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard), have been widely used for protecting digital images. However, these methods often struggle with maintaining a balance between security, computational efficiency, and resistance to image processing attacks. To overcome these limitations, researchers have begun integrating deep learning approaches into the field of image encryption.

One significant advancement involves the use of convolutional neural networks (CNNs) and autoencoders to encode image features in a non-human-interpretable format, making them highly secure against unauthorized access. Some studies have proposed hybrid encryption methods that combine deep learning with classical cryptographic techniques to enhance security and reduce redundancy. Additionally, reversible data hiding techniques and generative adversarial networks (GANs) have been used to embed encrypted information into cover images or noise patterns to further obfuscate sensitive data.

Another notable trend is the incorporation of QR code technology in secure data transmission. Researchers have developed systems that convert encrypted medical data into QR codes to facilitate easy storage and sharing while preserving data confidentiality. These QR-based systems are particularly useful in telemedicine and remote diagnosis, where quick and secure access to medical images is essential.

Overall, while existing works have laid a strong foundation for secure medical image handling, they often face challenges in usability, robustness against image manipulation, and scalability. The proposed project builds upon these existing approaches by introducing a deep learning-based encryption mechanism combined with QR code technology and a reversible neural network to provide a more secure, efficient, and user-friendly solution for medical image encryption and decryption.

3. METHODOLOGY OF PROJECT

The methodology of the proposed project involves a systematic integration of deep learning and QR code technology to ensure secure encryption and decryption of medical images. The process begins with the acquisition and preprocessing of medical images, where uploaded images are resized, normalized, and prepared for encryption. The core of the system lies in a deep learning-based encryption model, typically a convolutional neural network or autoencoder, which encodes the critical features of the image into a compressed and secure format. Alongside this, a unique encryption key is generated for each image, essential for its subsequent decryption. The encrypted data is then converted into a QR code, which serves as a compact and easily shareable medium for storing and transmitting the encrypted image. Both the QR code and the encryption key are stored securely or shared with authorized users. For decryption, the user uploads the QR code and provides the corresponding key, which allows the system to decode the encrypted data and reconstruct the original image using a reversible neural network. This model ensures high fidelity in image reconstruction and is robust against various attacks such as noise, cropping, and brute-force attempts. The entire methodology ensures an end-to-end secure, reliable, and user-friendly framework for handling sensitive medical images.

MODULE DESCRIPTION:

User:

The process begins with the user, who wants to secure a medical image. This could be a doctor, healthcare provider, or authorized personnel responsible for handling medical data.

Upload Medical Image:

The user uploads the medical image to the system. This image could be anything from X-rays, MRIs, or CT scans that need protection for privacy and confidentiality.

Encrypt Image:

The uploaded image is then encrypted using an AI-based encryption model. This step ensures that the image is transformed into a secure format that is unreadable without the appropriate decryption key, protecting the image's sensitive information.

Generate QR Code and Key:

After the image is encrypted, a secure key is generated. This key, which is used to decrypt the image later, is then encoded into a QR code. The QR code acts as a secure means of transferring and storing the key, ensuring only authorized individuals can access the key.

Upload Generated QR Code and Key:

The generated QR code and encryption key are uploaded, either for storage or transmission. These QR codes and keys are stored securely, and only authorized users can retrieve them to decrypt the image.

Decrypt Image:

When the authorized user needs to access the original medical image, they upload the QR code and key. The system uses the key from the QR code to decrypt the image, restoring it to its original form for viewing and analysis.

4. ALGORITHM USED IN PROJECT

The proposed system begins with the user uploading a medical image that needs to be protected. Once the image is uploaded, it is encrypted using a deep learning-based encryption algorithm, which ensures that the contents are scrambled and unreadable without the appropriate decryption key. A secure key is then generated using the secure_key library, which is essential for decrypting the image later. The generated key is encoded into a QR code using the pyqrcode library, providing a compact and secure way to store and transfer the key. This QR code is saved or shared with authorized users who need access to the encrypted image. When decryption is required, the authorized user uploads the QR code containing the key. The system then uses the secure key to decrypt the image, reversing the encryption process to restore the original medical image. Finally, the decrypted image is displayed, allowing authorized users to access it for diagnosis or treatment. This workflow ensures that the medical image remains secure throughout storage and transmission, with only authorized users able to decrypt and view the image.

5. SYSTEM ARCHITECTURE

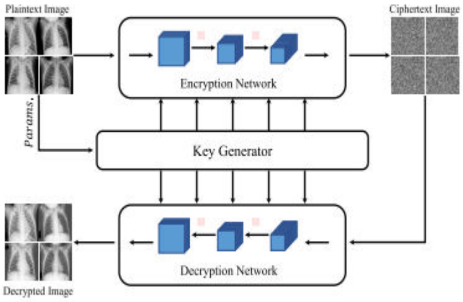

Fig: 7 System Architecture Of Project

6. DATA FLOW DIAGRAM

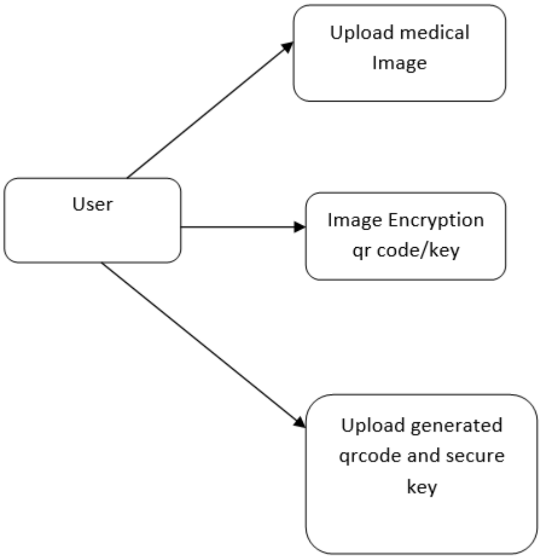
Upload medical Image
User
Image Encryption qr code/key
Upload generated qrcode and secure key

Fig: 6 Flow Diagram

7. RESULTS

For better diagnosis implementing a more sophisticated key management system with multifactor authentication would increase security image compression techniques can be used to reduce file sizes without compromising security allowing faster transmission.

Real-time encryption and decryption can also be introduced to support live medical image processing incorporating blockchain for data integrity would ensure that the medical images remain tamper-proof.

To improve accessibility the system can be made compatible with multiple platforms like mobile and web.

8. FUTURE ENHANCEMENT

In the future, several enhancements can be made to improve the medical image encryption system. First, integrating advanced encryption algorithms, such as homomorphic encryption, can further secure the data against emerging threats. The system can be expanded to handle color medical images, such as MRI or CT scans, by implementing adaptive encryption techniques. Additionally, cloud storage integration would allow encrypted images to be securely stored and shared remotely, enhancing flexibility for telemedicine. AI-driven image enhancement can be introduced to improve decrypted image quality for better diagnosis. Implementing a more sophisticated key management system with multi-factor authentication would increase security. Image compression techniques can be used to reduce file sizes without compromising security, allowing faster transmission. Real-time encryption and decryption can also be introduced to support live medical image processing. Incorporating blockchain for data integrity would ensure that the medical images remain tamper-proof. To improve accessibility, the system can be made compatible with multiple platforms like mobile and web.

9. CONCLUSION

In conclusion, the proposed system leveraging deep learning-based encryption, utilizing the pyqrcode and secure_key libraries, presents a secure and efficient solution for medical image protection. By combining feature encoding and decoding with encryption and decryption techniques, this system ensures that sensitive medical data is securely encrypted and can only be decrypted by authorized individuals. The integration of chaotic system-generated keys further enhances security, while the use of QR codes for key storage simplifies the process of key management. This approach demonstrates resilience against various security threats, including unauthorized access and data tampering, ensuring privacy and integrity of medical images during storage and transmission. The user-friendly workflow of image upload, encryption, QR code generation, and decryption makes it a practical solution for healthcare professionals. Overall, the system offers a promising framework for safeguarding medical images, paving the way for more secure healthcare data handling in the future.

REFERENCES:

[1] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, ‘‘Recent advances in the Internet-of-Medical-Things (IoMT) systems security,’’ IEEE Internet Things J., vol. 8, no. 11, pp. 8707–8718, Jun. 2021.

[2] T. N. Lakshmi, S. Jyothi, and M. R. Kumar, Image Encryption Algorithms Using Machine Learning and Deep Learning Techniques—A Survey. Cham, Switzerland: Springer, 2021, pp. 507–515.

[3] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, ‘‘An overview of encryption algorithms in color images,’’ Signal Process., vol. 164, pp. 163–185, Nov. 2019.

[4] M. Kaur and V. Kumar, ‘‘A comprehensive review on image encryption techniques,’’ Arch. Comput. Methods Eng., vol. 27, no. 1, pp. 15–43, Jan. 2020.

[5] N. Yang, S. Zhang, M. Bai, and S. Li, ‘‘Medical image encryption based on Josephus traversing and hyperchaotic Lorenz system,’’ J. Shanghai Jiaotong Univ., vol. 29, no. 1, pp. 91–108, Dec. 2022.

[6] T. Wang and M.-H. Wang, ‘‘Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding,’’ Opt. Laser Technol., vol. 132, Dec. 2020, Art. no. 106355.

[7] Y. Sang, J. Sang, and M. S. Alam, ‘‘Image encryption based on logistic chaotic systems and deep autoencoder,’’ Pattern Recognit. Lett., vol. 153, pp. 59–66, Jan. 2022.

[8] X. Sun and Z. Chen, ‘‘A new image encryption strategy based on Arnold transformation and logistic map,’’ in Proc. 11th Int. Conf. Comput. Eng. Netw. Singapore: Springer, 2022, pp. 712–720.

[9] C. Pak and L. Huang, ‘‘A new color image encryption using combination of the 1D chaotic map,’’ Signal Process., vol. 138, pp. 129–137, Sep. 2017.

[10] J. Tang, F. Zhang, and H. Ni, ‘‘A novel fast image encryption scheme based on a new one-dimensional compound sine chaotic system,’’ Vis. Comput., vol. 39, no. 10, pp. 4955–4983, Oct. 2023.

[11] Z. Hua, Y. Zhou, and H. Huang, ‘‘Cosine-transform-based chaotic system for image encryption,’’ Inf. Sci., vol. 480, pp. 403–419, Apr. 2019.

[12] S. Zhu, X. Deng, W. Zhang, and C. Zhu, ‘‘Secure image encryption scheme based on a new robust chaotic map and strong S-box,’’ Math. Comput. Simul., vol. 207, pp. 322–346, May 2023. [13] F. Wang, J. Sang, C. Huang, B. Cai, H. Xiang, and N. Sang, ‘‘Applying deep learning to known-plaintext attack on chaotic image encryption schemes,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), May 2022, pp. 3029–3033.

[14] K. Panwar, S. Kukreja, A. Singh, and K. K. Singh, ‘‘Towards deep learning for efficient image encryption,’’ Proc. Comput. Sci., vol. 218, pp. 644–650, Jan. 2023.

[15] C. Wang and Y. Zhang, ‘‘A novel image encryption algorithm with deep neural network,’’ Signal Process., vol. 196, Jul. 2022, Art. no. 108536.

[16] Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, ‘‘Double image encryption algorithm based on neural network and chaos,’’ Chaos, Solitons Fractals, vol. 152, Nov. 2021, Art. no. 111318.

[17] S. R. Maniyath and V. Thanikaiselvan, ‘‘An efficient image encryption using deep neural network and chaotic map,’’ Microprocessors Microsyst., vol. 77, Sep. 2020, Art. no. 103134. [18] S. Patel, V. Thanikaiselvan, D. Pelusi, B. Nagaraj, R. Arunkumar, and R. Amirtharajan, ‘‘Colour image encryption based on customized neural network and DNA encoding,’’ Neural Comput. Appl., vol. 33, no. 21, pp. 14533–14550, Nov. 2021.

[19] Y. Ding, F. Tan, Z. Qin, M. Cao, K. R. Choo, and Z. Qin, ‘‘DeepKeyGen: A deep learning-based stream cipher generator for medical image encryption and decryption,’’ IEEE Trans. Neural Netw. Learn. Syst., vol. 33, no. 9, pp. 4915–4929, Sep. 2022.

[20] O. D. Singh, S. Dhall, A. Malik, and S. Gupta, ‘‘A robust and secure immensely random GAN based image encryption mechanism,’’ Multimedia Tools Appl., vol. 82, no. 13, pp. 19693–19743, May 2023.

[21] S. Zhou, Z. Zhao, and X. Wang, ‘‘Novel chaotic colour image cryptosystem with deep learning,’’ Chaos, Solitons Fractals, vol. 161, Aug. 2022, Art. no. 112380.

[22] E. Abdellatef, E. A. Naeem, and F. E. A. El-Samie, ‘‘DeepEnc: Deep learning-based CT image encryption approach,’’ Multimedia Tools Appl., vol. 83, no. 4, pp. 11147–11167, Jan. 2024.

[23] Y. He, Y.-Q. Zhang, X. He, and X.-Y. Wang, ‘‘A new image encryption algorithm based on the OF-LSTMS and chaotic sequences,’’ Sci. Rep., vol. 11, no. 1, p. 6398, Mar. 2021. [24] Y. Liu, G. Cen, B. Xu, and X. Wang, ‘‘Color image encryption based on deep learning and block embedding,’’ Secur. Commun. Netw., vol. 2022, pp. 1–14, Oct. 2022.

[25] J. Liang, Z. Song, Z. Sun, M. Lv, and H. Ma, ‘‘Coupling quantum random walks with long- and short-term memory for high pixel image encryption schemes,’’ Entropy, vol. 25, no. 2, p. 353, Feb. 2023.

[26] A. Elsonbaty, A. A. Elsadany, and W. Adel, ‘‘On reservoir computing approach for digital image encryption and forecasting of hyperchaotic finance model,’’ Fractal Fractional, vol. 7, no. 4, p. 282, Mar. 2023.

[27] H. Lin, C. Wang, L. Cui, Y. Sun, C. Xu, and F. Yu, ‘‘Brain-like initialboosted hyperchaos and application in biomedical image encryption,’’ IEEE Trans. Ind. Informat., vol. 18, no. 12, pp. 8839–8850, Dec. 2022.

[28] X. Chai, Y. Tian, Z. Gan, Y. Lu, X.-J. Wu, and G. Long, ‘‘A robust compressed sensing image encryption algorithm based on GAN and CNN,’’ J. Modern Opt., vol. 69, no. 2, pp. 103–120, Jan. 2022.

[29] J. Chen, X.-W. Li, and Q.-H. Wang, ‘‘Deep learning for improving the robustness of image encryption,’’ IEEE Access, vol. 7, pp. 181083–181091, 2019.

[30] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, ‘‘DeepEDN: A deep-learning-based image encryption and decryption network for Internet of Medical Things,’’ IEEE Internet Things J., vol. 8, no. 3, pp. 1504–1518, Feb. 2021.

[31] Z. Bao and R. Xue, ‘‘Research on the avalanche effect of image encryption based on the cycle-GAN,’’ Appl. Opt., vol. 60, no. 18, pp. 5320–5334, 2021.

[32] K. Panwar, A. Singh, S. Kukreja, K. K. Singh, N. Shakhovska, and A. Boichuk, ‘‘Encipher GAN: An end-to-end color image encryption system using a deep generative model,’’ Systems, vol. 11, no. 1, p. 36, Jan. 2023.

[33] J. Wu, W. Xia, G. Zhu, H. Liu, L. Ma, and J. Xiong, ‘‘Image encryption based on adversarial neural cryptography and SHA controlled chaos,’’ J. Modern Opt., vol. 68, no. 8, pp. 409–418, May 2021.

[34] L. Zhu, W. Qu, X. Wen, and C. Zhu, ‘‘FEDResNet: A flexible image encryption and decryption scheme based on end-to-end image diffusion with dilated ResNet,’’ Appl. Opt., vol. 61, no. 31, pp. 9124–9134, 2022.

[35] X. Li and H. Peng, ‘‘Chaotic medical image encryption method using attention mechanism fusion ResNet model,’’ Frontiers Neurosci., vol. 17, 2023, Art. no. 1226154.

[36] T. Karras, S. Laine, M. Aittala, J. Hellsten, J. Lehtinen, and T. Aila, ‘‘Analyzing and improving the image quality of StyleGAN,’’ in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Jun. 2020, pp. 8110–8119.

[37] A. N. Gomez, M. Ren, R. Urtasun, and R. B. Grosse, ‘‘The reversible residual network: Backpropagation without storing activations,’’ in Proc. Adv. Neural Inf. Process. Syst., vol. 30, 2017, pp. 2214–2224.

[38] E. Ustinova and V. Lempitsky, ‘‘Learning deep embeddings with histogram loss,’’ in Proc. Adv. Neural Inf. Process. Syst., vol. 29, 2016, pp. 4170–4178.

[39] Y. Wu, J. P. Noonan, and S. Agaian, ‘‘NPCR and UACI randomness tests for image encryption,’’ Cyber J. Multidiscip. J. Sci. Technol. J. Sel. Areas Telecommun., vol. 1, no. 2, pp. 31–38, 2011.

[40] C. Ledig, L. Theis, F. Huszár, J. Caballero, A. Cunningham, A. Acosta, A. Aitken, A. Tejani, J. Totz, Z. Wang, and W. Shi, ‘‘Photo-realistic single image super-resolution using a generative adversarial network,’’ in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Jul. 2017, pp. 4681–4690.

[41] S. Jaeger, S. Candemir, S. Antani, Y. X. Wang, P. X. Lu, and G. Thoma, ‘‘Two public chest X-ray datasets for computer-aided screening of pulmonary diseases,’’ Quant. Imag. Med. Surg., vol. 4, no. 6, p. 475, Dec. 2014.

[42] D. S. Kermany et al., ‘‘Identifying medical diagnoses and treatable diseases by image-based deep learning,’’ Cell, vol. 172, no. 5, pp. 1122–1131, Feb. 2018.