A Novel Medical Image Encryption Scheme Based On AI Feature Encoding And Decoding

Mr. K. Anil Kumar[1], Bijjala Shiva Shankar[2], Challa Vinuthna[3], Kolluri Deekshitha[4]

[1]Assistant Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus

[2,3,4]B.Tech Students, Department of Information Technology, Guru Nanak Institutions Technical Campus

ABSTRACT

Medical image encryption is critical to safeguarding patient privacy and maintaining the confidentiality of sensitive medical records. Leveraging advancements in artificial intelligence, we propose an innovative medical image encryption and decryption system that integrates deep learning-based encryption with QR code technology. This system enables users to upload a medical image, which is encrypted into a QR code format and paired with a uniquely generated key. Both the QR code and key are securely stored for subsequent retrieval decryption, users can upload the QR code and the corresponding key to reconstruct the original image with high fidelity. The encryption process employs advanced neural network-based feature encoding, ensuring robustness against attacks such as noise, cropping, and brute force. Additionally, the system incorporates a reversible neural network to optimize decryption accuracy and reconstruction quality. Experimental results highlight the system's efficiency in preserving image integrity, resisting various attacks, and maintaining end-to-end security in medical image encryption. This approach not only strengthens the privacy and security of medical data but also provides a user-friendly framework for securely transmitting and storing sensitive medical images.

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.

2-LITERATURE SURVEY

A Medical Image Encryption Technique Using XOR with Josephus Traversing and Cat, **Yang et al, 2023,** This paper focuses on improving medical image encryption using chaotic systems, specifically the Lorenz system. It integrates XOR operations with Josephus traversal and Cat mapping to enhance security. The combination of SHA-512 hashing strengthens the cryptographic process, making the system resilient to potential attacks. The Lorenz chaotic system's unpredictable behavior is leveraged to increase the complexity of encryption, ensuring that unauthorized access is difficult. This paper proposes a medical image encryption technique using XOR operations combined with chaotic systems (Lorenz system) and SHA-512 hashing. It improves security by introducing Josephus traversal and Cat mapping, making the encryption more complex and resistant to attacks.

A New 6-D Hyperchaotic System with Bit-Level Permutation and DNA Encoding for Medical Image Encryption., **Wang and Wang., 2022,** This study introduces a 6-dimensional hyperchaotic system, offering enhanced security for medical image encryption. It uses bit-level permutation and DNA encoding to transform the image into a highly secure format. By applying these techniques, the method increases the unpredictability of the encryption, thus preventing potential attacks like brute force. This approach aims to balance security with computational efficiency. The authors introduce a 6-dimensional hyperchaotic system for medical image encryption. They apply bit-level permutation and DNA encoding to enhance the security of the encryption process. This approach aims to balance computational efficiency with high-level security.

Key Generation Network Using GAN for Medical Image Encryption**, Ding et al, 2022,** explores the use of Generative Adversarial Networks (GANs) for key generation in medical image encryption. The GAN model generates a private key, which is then used in conjunction with XOR operations to encrypt the medical images. The model utilizes the adversarial nature of GANs to produce highly unpredictable keys, which add an additional layer of security to the image encryption process. This method aims to enhance encryption by generating dynamic, difficult-to-guess keys. This study explores the use of GANs for key generation in image encryption. The GAN model generates unpredictable keys that are combined with XOR operations to encrypt medical images, enhancing security and making decryption more difficult for unauthorized users.

Random Sequence Generation Using Stack Autoencoder for Image Encryption, Maniyath and Thanikaiselvan, **2021**

the authors use stack autoencoders to generate random sequences that improve the mixing process of image encryption. By leveraging the autoencoder's ability to learn complex patterns, the method generates more secure random sequences for image encryption. This approach helps enhance the diffusion process in the encryption algorithm, making it more resistant to cryptographic attacks. The random sequences ensure that even minor changes in the image or key result in significantly different encrypted outputs. This paper uses stack autoencoders to generate random sequences for encrypting images. The random sequences improve the mixing and diffusion processes, making the encryption more secure and resistant to cryptographic attacks.

Color Image Encryption System Using LSTM for Training Chaotic Signals, **Zhou et al, 2022,** Zhou et al. propose using Long Short-Term Memory (LSTM) networks to train chaotic signals for medical image encryption. LSTM networks, a type of recurrent neural network, are used to predict and generate chaotic sequences that drive the encryption process. This method enhances the security of the encryption by leveraging the complex temporal dependencies within the LSTM model, allowing it to create dynamic encryption keys that are difficult to reverse-engineer. The method aims to improve the overall performance of medical image encryption systems, particularly for color images The authors use LSTM networks to generate chaotic signals for encrypting color images. LSTM networks enhance the encryption process by creating dynamic, unpredictable keys, thus improving the security of medical image encryption systems.

3-REQUIREMENTS ENGINEERING

We can see from the results that on each database, the error rates are very low due to the discriminatory power of features and the regression capabilities of classifiers. Comparing the highest accuracies (corresponding to the lowest error rates) to those of previous works, our results are very competitive.

HARDWARE REQUIREMENTS

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. They are used by software engineers as the starting point for the system design. It should what the system do and not how it should be implemented.

- PROCESSOR : DUAL CORE 2 DUOS.
- RAM :4GB DD RAM
- HARD DISK :250 GB

SOFTWARE REQUIREMENTS

The software requirements document is the specification of the system. It should include both a definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team's progress throughout the development activity.

- Operating System: Windows 7/8/10
- Platform : Spyder3
- Programming Language : Python
- Front End : Spyder3

FUNCTIONAL REQUIREMENTS

A functional requirement defines a function of a software-system or its component. A function is described as a set of inputs, the behavior, Firstly, the system is the first that achieves the standard notion of semantic security for data confidentiality in attribute-based deduplication systems by resorting to the hybrid cloud architecture.

NON-FUNCTIONAL REQUIREMENTS

The major non-functional Requirements of the system are as follows

Usability

The system is designed with completely automated process hence there is no or less user intervention.

Reliability

The system is more reliable because of the qualities that are inherited from the chosen platform python. The code built by using python is more reliable.

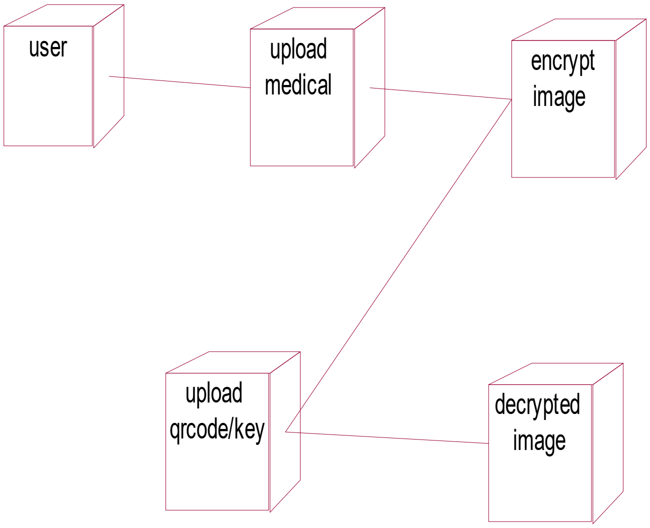
Performance

This system is developing in the high level languages and using the advanced back-end technologies it will give response to the end user on client system with in very less time.

4-DESIGN ENGINEERING

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering.

DEPLOYMENT DIAGRAM



Deployment Diagram is a type of diagram that specifies the physical hardware on which the software system will execute. It also determines how the software is deployed on the underlying hardware. It maps software pieces of a system to the device that are going to execute it.

SYSTEM ARCHITECTURE

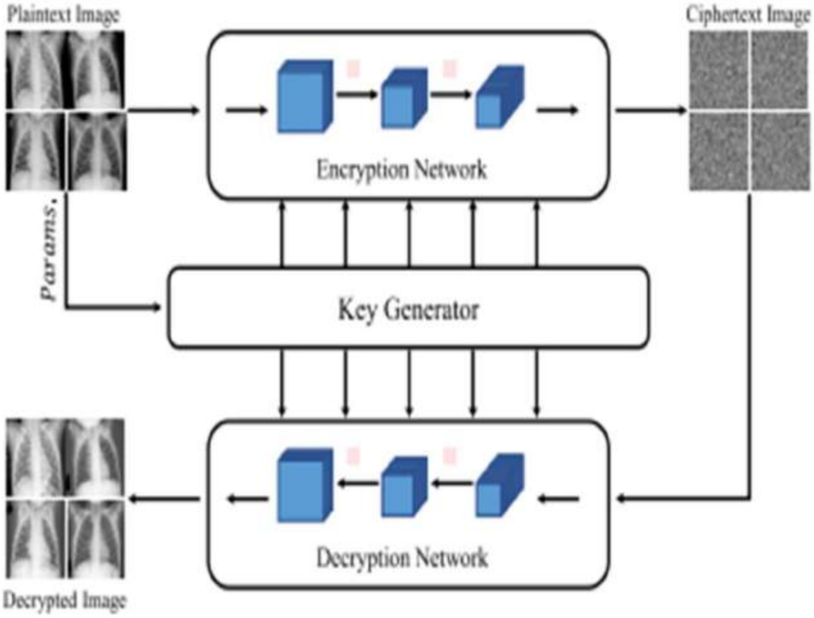
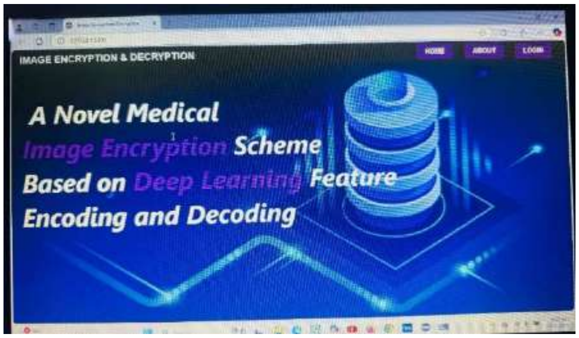
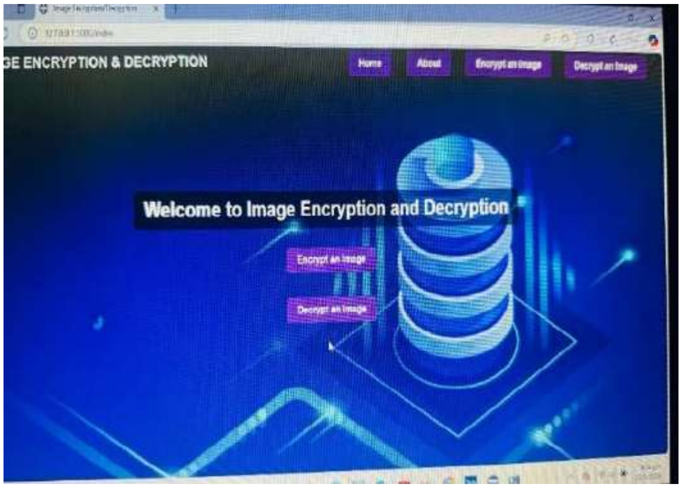


Fig 4.11: System Architecture

5-SNAPSHOTS

This project is implements like application using python and the Server process is maintained using the SOCKET & SERVERSOCKET and the Design part is played by Cascading Style Sheet.




GE ENCRYPTION & DECRYPTION
Home
About
Encrypt an image
Decrypt an Image
Welcome to Image Encryption and Decryption
Encrypt an Image
Decrypt an Image

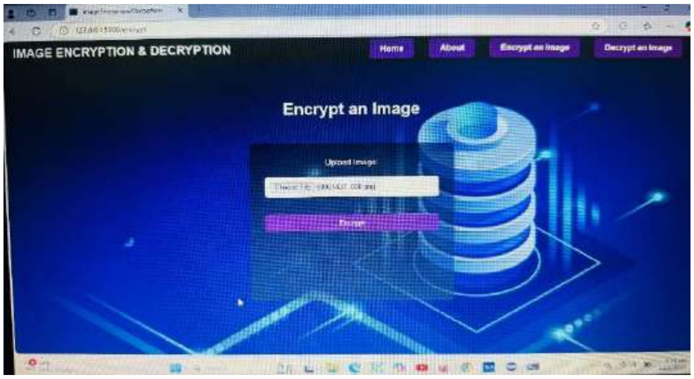


IMAGE ENCRYPTION & DECRYPTION
Home
About
Encrypt an Image
Decrypt an Image
Encrypt an Image
Upload Image
Choose File
Encrypt

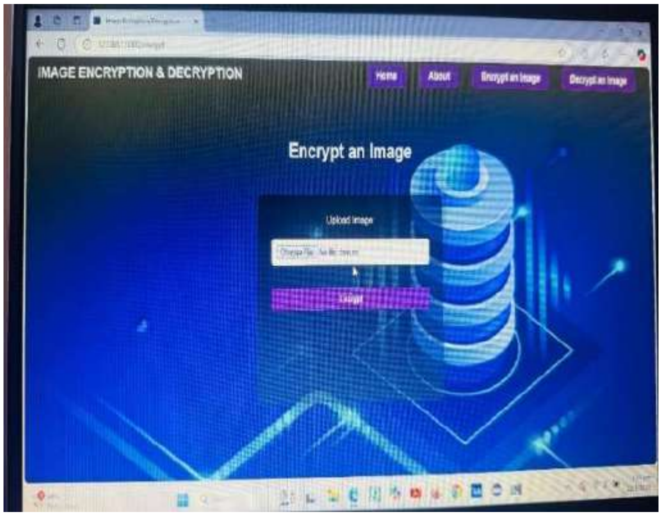


IMAGE ENCRYPTION & DECRYPTION
Home
About
Encrypt an Image
Decrypt an Image
Encrypt an Image
Upload Image
Choose File No file chosen
Encrypt

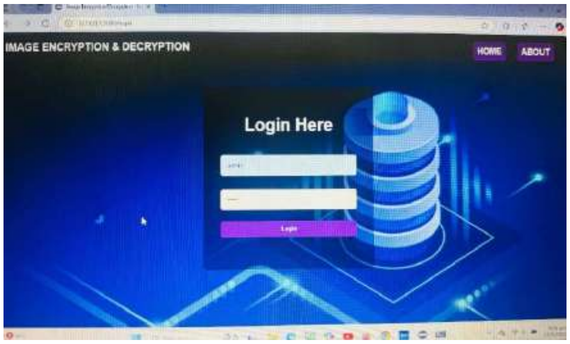
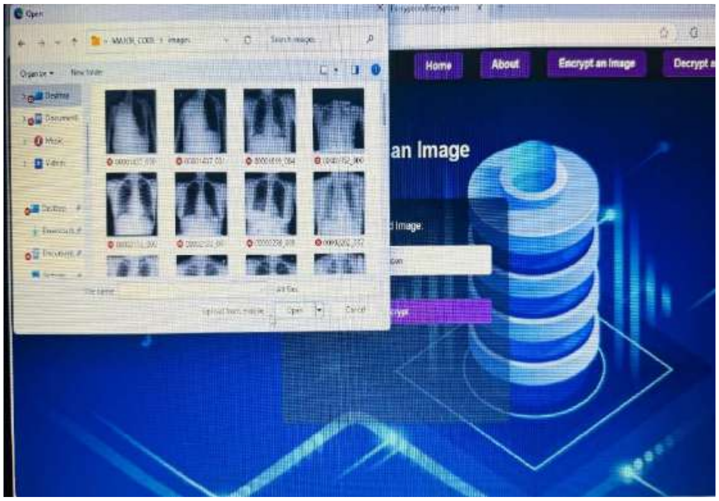
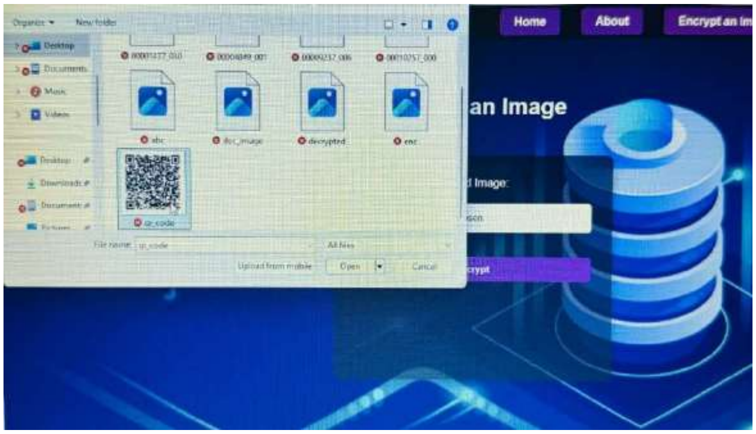
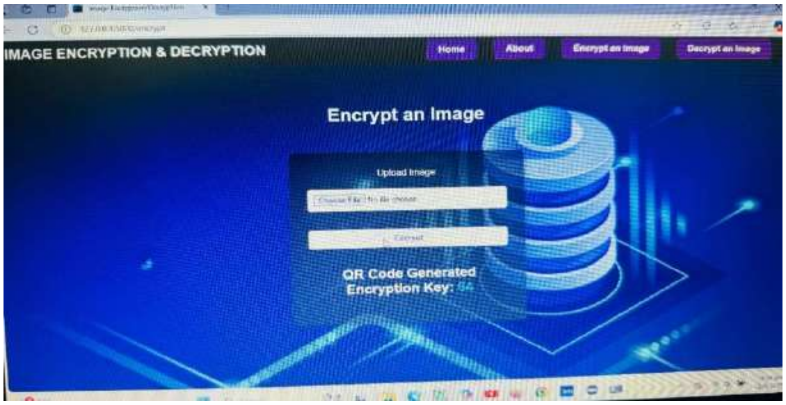


IMAGE ENCRYPTION & DECRYPTION
HOME
ABOUT
Login Here
Login


Open
MAJOR_CODE > images
Search images
Organize
New folder
Desktop
Documents
Music
Videos
Downloads
Home
About
Encrypt an Image
Decrypt a
an Image
Image:
File name:
All files
Upload from mobile
Open
Cancel


Organize
New folder
Desktop
Documents
Music
Videos
Downloads
Pictures
abc
dec_image
decrypted
enc
qr_code
File name: qr_code
All files
Upload from mobile
Open
Cancel
Home
About
Encrypt an Im
an Image
Image:



QR Code Generated
Encryption Key: 64

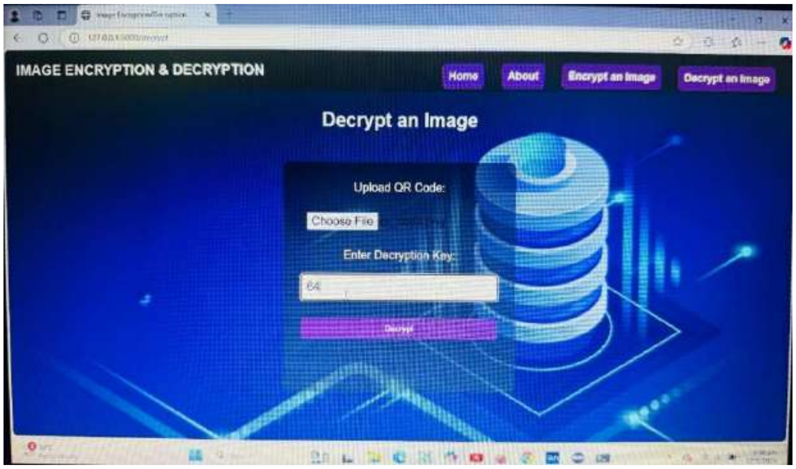
6- TESTING

Software Testing

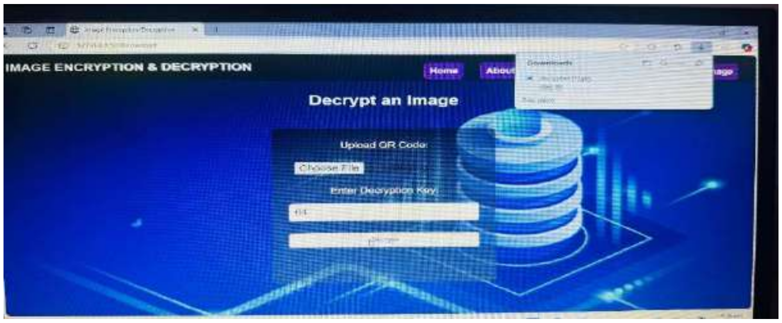
The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Unit testing

Unit testing involves the design of test cases that validate that the internal program logic is



Enter Decryption Key: 64



Enter Decryption Key: 64

functioning properly, and that program input produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Functional test

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration-oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

7-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.

8-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.