A Review on Improved and Highly Secured Algorithms for Medical Image Encryption using MATLAB

Mohan Manju[1]*,Rajesh Kumar Pathak[2]

Research Scholar, Department of Computer Science, Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India[1]
Vice Chancellor, OPJS University, Churu, Rajasthan, India[2]

Abstract

With limited data transmission capacity, secure data transmission of images over internet communication channels includes compression and encryption methods. We propose an advanced-based hybrid image file compression and data encryption technique by combining a stacked autoencoder and logistic data map. The proposed stacked autoencoder structure has multiple layers, and the encryption algorithm is intended to extend the vector representation of information to a lower vector space. A randomly auto-generated key is used to set the initial conditions and control parameters of the logistic map. It then encrypts the compressed image by replacing and encoding the pixel sequence with the keystream sequence generated from the logistic map. The compression and encryption performance of the proposed algorithm is evaluated and analysed based on PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Squared Error), SSIM (Structural similarity Index Metric), statistics, differentiation, and entropy analysis. MATLAB results show that the proposed algorithm provides high-quality reconstructed images with good security level during transmission.

Keywords

Digital image encryptions, data hiding techniques, secure communication, medical encryption.

DOI: 10.48047/ecb/2022.11.10.37

1.Introduction

Many digital services require reliable security for the storage and transmission of digital images. Due to the rapid growth of the Internet in today's digital world, the security of digital images has become very important and has received a lot of attention. The prevalence of multimedia technologies in our society has encouraged digital images to play a more important role than traditional documents that require strict protection of user privacy in all applications. Encryption techniques and digital image steganography are very important and should be used to prevent adversary attacks on unauthorized access [1].

Digital images are exchanged over various networks. It is generally true that much of this information is private or confidential. Encryption is the preferred method for protecting transmitted data. Although there are various encryption methods for encrypting and decrypting image data, it can be argued that no single encryption algorithm is satisfactory for different types of images [2].

Although there are various encryption methods for encrypting and decrypting image data, it can be argued that no single encryption algorithm is satisfactory for different types of images.

We can encrypt the image manually using the plaintext algorithm, but this may not be a good idea for two reasons. First, the image size is usually larger than the text. Therefore, conventional encryption algorithms require a long time to directly encrypt image data. Second, the decrypted text must match the original text, but image data doesn't require this requirement [3].

Objective

In this paper, we survey many techniques for image encryption and develop an advanced encryption method for medical image encryption.

i. Design MATLAB based advanced grey medical image encryption over a firewall network.
ii. Real time Loop based secure wall encryption which helps to protect the image secure data.

*Author for correspondence

iii. Study and comparison different type of image encryption techniques.

2. Literature Review

Image encryption describes the process of converting an original image into a coded image. Protects images while transmitting over public networks. Information related to confidential image always needs to be protected to maintain its security and cannot be easily identified by anyone other than an authorized person. The encrypted image is then sent over an insecure channel to an authorized person. Decryption is a reversible encryption procedure that can convert an encrypted image back to its original format. In this process, an authorized person can only obtain the original image through the secret key and decryption algorithm. When the receiver receives the encrypted image, it decrypts it to get the original image. Because only the sender knows the key, decryption can only be done by someone with access to the secret key.

RSA (Rivest-Shamir-Adleman encryption)

The RSA algorithm is one of the most commonly used asymmetric algorithms that rely on public key cryptography. Typically, keys are used with private or public indices; the decryption process takes more time than encryption [1]. The first attempt to speed up the encryption process with the RSA algorithm was Fiat. Acceleration has been studied. For example, RSA algorithm. The first method is based on multi-prime technology. Reduced modules to speed up the decoding process. The second method is based on RSA-S1 [2]. Systems based on the selection of small numbers improve the decoding process. These procedures can use the RSA algorithm to speed up the encryption and decryption process. Decryption is much slower than the encryption process [3]. This is due to the complicated calculations in this process. However, since most of the decryption work is done through a regular computer with limited capabilities, even a small computer needs to speed up the process.

*DNA (Deoxyribonucleic Acid Encryption):*Another fast-emerging methodology in the coding domain is based on DNA sequences. DNA molecules with the ability to store, process and transmit information inspire the idea of DNA encoding. It works on the concept of DNA computing, which uses four bases: adenine (A), guanine (G), cytosine (C) and thymine (T) to perform a calculation. One of the advantages of DNA computation is the massively parallel processing of DNA molecules [4]. An in vitro assay can easily handle about 1018 processors working in parallel. Because of this massive parallelism, the trapdoor function, the basic secret of most existing cryptosystems, can be solved in polynomial time. So it's time to look for alternatives to traditional cryptosystems [5]. As the mathematical aspects of coding are replaced by DNA chemistry in the realm of DNA coding, this technology is virtually in hackable with conventional methods as well as quantum calculations.

Sequence Secure Force Algorithm

Secure Force algorithm based on Feistel architecture. Here, since the encryption and decryption processes are the same, the code size can be minimized to some extent. Low complexity architecture provided by SF algorithm for WSN implementation. The encryption process consists of only 5 encryption rounds [6]. This helps to improve energy efficiency. The smaller the number of encryption rounds, the more power consumption. Each encryption round involves 6 simple math operations that only operate on 4-bit data. This creates a decent amount of confusion and spread. Low Complexity Encryption Algorithms for Wireless Sensor Networks (WSNs) Overview: Because devices in Wireless Sensor Networks (WSNs) are typically small in size, resource constraints are one of the important issues to consider.

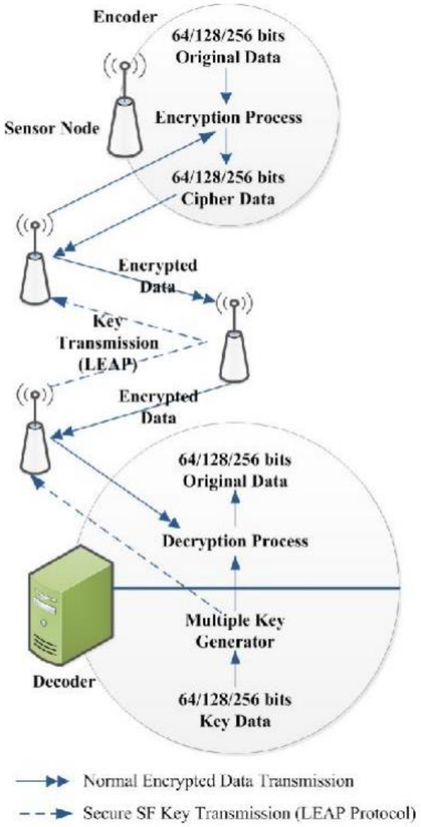


Figure 1 Sequence Secure Force Algorithm

Arnold Transform

In real-world applications, Arnold Transform encodes the number of iterations of a process, not only scrambles pixel positions, but also reduces key space for storage and transmission. There are several methods of scrambling, but only Arnold Transform [7], in which is an iterative process of shifting pixel positions, is described here. Suppose that the original image is ***NxN***a array and the coordinate of the pixel is ***F = {(x,y) | x,y =0,1,2,3,.....,N-1}***. The generalized two-dimension Arnold Transform is denoted by

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_{n-1} \\ y_{n-1} \end{bmatrix} modN \qquad \text{------eq. (1)}$$

where $\boldsymbol{x_n}$ and $\boldsymbol{y_n}$ are the transformed coordinates corresponding to and after iterations, respectively, and ***a*** are ***b*** positive integers, and ***N*** is the height or width of the square image processed.

Chaotic permutation

The encryption method has three blocks: a mixed process, a permutation process, and a diffusion process. The permutation and diffusion process are repeated for R (rounds) time to obtain highly correlated cryptographic images [5]. The blending process uses a logistic map. The blending process degrades the image quality before performing permutation and diffusion. The proposed encryption technique achieves the maximum-security level by first masking a normal image with a randomly generated mixed sequence, and then performing the required minimum number of rounds (Rounds=3) by repeating the permutation and diffusion process [4]. In the permutation process, the mixed image is converted to a binary sequence size of NxMx8. They are then fed into permutation and diffusion blocks. Figure 1 shows the proposed encryption scheme. In cryptographic algorithm K1, Kt is the secret key provided to the spread bit generator. A random index generator Kt is given to the tent map and repeated NxMx8 times.

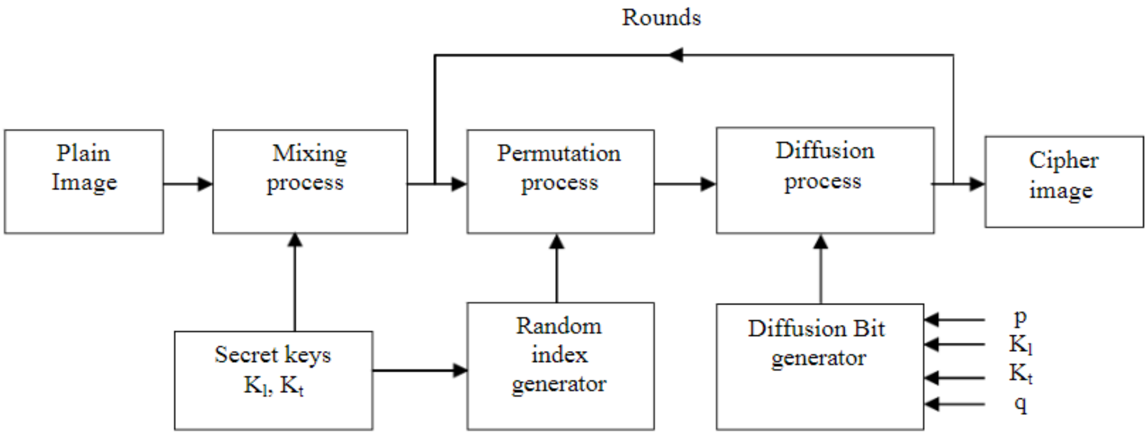


Figure 2 Chaotic Permutation Image encryption

Advanced Encryption Standard (AES)

In this method, multi-step bit permutation operations are performed with propagation rounds to achieve better encryption results. The main purpose of the method introduced in [8] is to design a dynamic S-box to achieve nonlinear properties and low autocorrelation. In image encryption by AES, which is a block encryption method, because the correlation between adjacent pixels is high, a shadow of the original image remains in the encrypted image after encryption. A key stream generator was introduced in [9] to overcome this problem. There are two types of stream generators including A5/1 and W7 key stream generators. This generator includes some register shifts and a set of functions and W7 shows better encryption performance than A5/1. The system first takes the original image as input. It then shifts the rows and columns of image pixels to the right by specific values to remove correlation between adjacent pixels. The next step is to create a key based on the position of the mouse on the screen [10]. By designating these keys as primary keys and using the key extension function, the 11 round keys of the AES algorithm are generated. This key is given sequentially to the AES algorithm to convert the original image into an encrypted image. This algorithm provides better encryption results when it comes to security against statistical attacks.

Blowfish

Blowfish is a symmetric block cipher, data encrypted in 8-byte blocks [8]. The Blowfish algorithm consists of two parts: data encryption and key expansion. Key extensions exchange variable-length keys of up to 64 bytes (512 bits) into an array of subkeys totalling 4168 bytes. The Blowfish algorithm, in which these keys are precomputed before data encryption or decryption, uses a large number of subkeys.

The P-array consists of 18, 32-bit subkeys:

P1, P2,… P18. There are also four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,.…, S1,255;

S2,0, S2,1,.…, S2,255;

S3,0, S3,1,.…, S3,255;

S4,0, S4,1,.…, S4,255;

The aspect behind Blowfish is the simplicity of the algorithms it is designed for and ease of implementation [11]. Using a streamlined Feistel network, a simple S-Box replacement, and a simple P-box replacement, while making and maintaining the body of Blowfish as simple as possible, the cryptographic properties of the desired structure.
The easiest way to format your manuscript is to simply download the template, and replace the content with your own material.This template provides authors with most of the formatting specifications needed for preparing electronic versions of their papers.

3. Methods

A major step for obtaining detailed medical images of our proposed algorithm. In the first step Plain images are encrypted and converted to unreadable images. Then apply decryption steps to recover normal image.

3.1 Encryption and Decryption of Image

The proposed method focuses on improving medical image security by integrating a brute force algorithm in chaotic systems. This integrated approach provides robust security for medical image data, addressing the challenges of protecting sensitive information during storage and transmission.

The main goal of the project is to develop an innovative firewall system that operates within an encryption ring. It uses advanced encryption algorithms such as loop Secure force algorithm and chaotic in an iterative manner, which ensures the complexity of the encryption process. Key management techniques are implemented to securely generate, store, and exchange encryption keys during the encryption cycle. The inclusion of steganography techniques provides additional security. It involves embedding encrypted data in cover media such as images or audio files to hide the true identity of the data. This method intelligently determines the optimal location for embedding while minimizing any variation in the appearance of the cover media. Secure mechanisms have been established to receive and decrypt data from steganographic carriers. The scheme addresses data fragmentation and fragmentation, splitting the original data into smaller pieces for efficient encryption and steganography. The process of reconstructing the original data involves decrypting and assembling the fragmented data in the correct order after extraction from the steganographic medium.

The proposed methodology emphasizes secure key management and exchange protocols, balancing security and performance considerations, integrating user authentication and authorization mechanisms, and implementing user-friendly interfaces for configuration, monitoring, and management. By adopting this approach, the project aims to achieve a comprehensive and advanced medical image security system that effectively protects critical medical image data while maintaining privacy and data confidentiality within digital networks.

Medical image encryption is considered one of the most dominant areas of encryption systems, which must be performed with algorithms that are time-consuming and inexpensive. In the process of encrypting an image, it is essential to apply a symmetric or asymmetric encryption algorithm to convert the input image to a cryptographic image using a symmetric or asymmetric key. Symmetric ciphers use one key for the encryption and decryption process, whereas asymmetric ciphers use different keys for encryption and decryption.

Medical image encryption can be performed using:

Different algorithms using different parameters Encryption of medical images can be done with fast scramble [14], bitwise XOR spread, chaos and edge maps, etc. The performance of algorithms used to encrypt medical images can be analysed using measures such as peak signal-to-noise ratio, bit error rate, fidelity, and mean squared error.

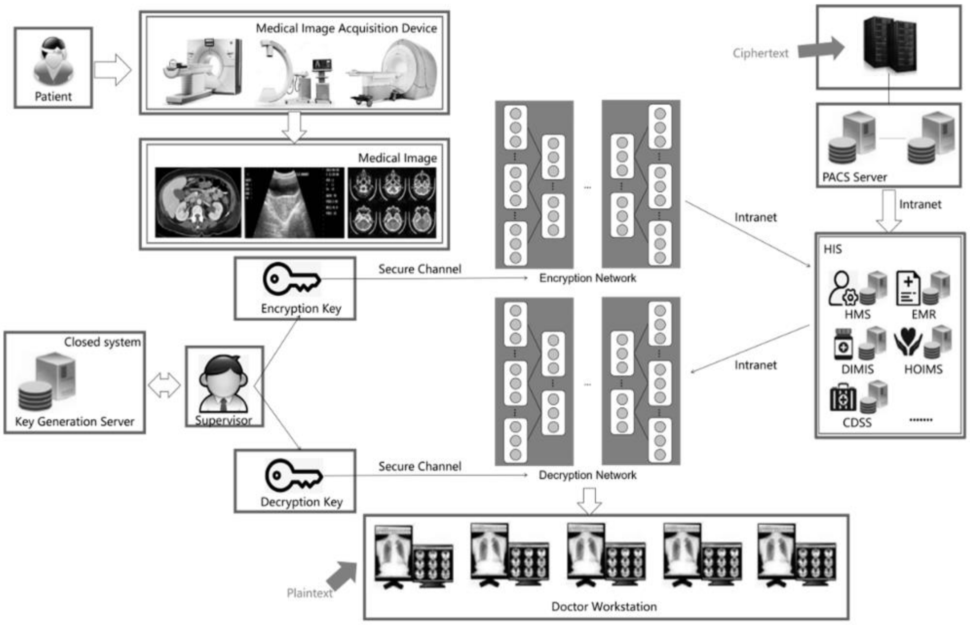


Figure 3 Medical Image Encryption systems over a cloud network

The main purpose of medical image encryption is to

• Safely transmit patient's medical records

• Ensuring confidentiality and integrity

• Avoid altering the medical image that could lead to an erroneous diagnosis

• Defend against cyber security attacks and threats.

4.Attacks in image encryption

Cyber criminals have the ability to launch active or passive attacks on encrypted data. As the terminology suggests, active attacks that have the ability to modify or replace system files present a more significant threat than passive attacks that simply inspect or intercept data. This emphasizes the need for programmers to have a broad understanding of various cryptographic attack techniques in order to effectively mitigate the associated risks. This essential knowledge empowers programmers to implement proper security and protection protocols. This is an important step in combating potential breaches, unauthorized data management and restricted access:

A. Brute force Attacks

Brute force is a simple and straightforward encryption attack that tries every possible password or key to access a file containing information. Cyber criminals conduct these attacks by using their vast processing power to systematically guess the passwords that protect cryptographic information. Based on this, the time taken to find the password in these attacks depends on the length of the key.

Therefore, a brute force attack can only succeed if sufficient time is allowed. As the length of the key is added, the number of potential combinations doubles [15], doubling the time required to successfully launch a brute force attack.

B. Replay Cryptography Attack

Replay attacks are used in cryptographic algorithms without temporal protection. In this situation, cybercriminals intercept encrypted messages between two individuals, request authentication, and replay the captured messages to start a new session [16]. A replay attack is best performed by using timestamps in communications and setting a timeout period for each message.

C. Man in the Middle Attack

As the name suggests, a man-in-the-middle attack occurs when cybercriminals sit between communicating parties and intercept all communications, including how to establish an encrypted session. In response to the initiation request, the hacker penetrates the session and establishes a secure session with the sender of the communication [15]. The malicious party then starts a second secure session with the original recipient using another key impersonating the sender. The individual then sits in between communications and reads any traffic or information that the sender delivers to the intended recipient.

D. Implementation Attack

Implementation attacks exploit weaknesses or vulnerabilities while implementing cryptographic systems. These attacks only focus on software code, errors, and other flaws within the logical implementation of a cryptographic system.

E. Statistical Attack

These decrypt attacks exploit statistical weaknesses in cryptographic systems such as the inability to generate random numbers and floating-point errors. Statistical attacks target vulnerabilities in the operating system or hardware hosting functional cryptographic tools.

F. Frequency Analysis and Cipher text-Only Attacks

Cipher text only attacks allow cybercriminals to know the cipher text used for various communications encrypted using similar encryption algorithms. However, the attacker's task is to figure out the key used to decrypt the message. So, to decipher the information, they use frequency analysis, a simple technique that counts the number of times every character appears in a cipher text [15]. Cybercriminals use several variants and techniques to perform frequency analysis. For example, knowing that the letters T, O, N, E, and A are common in English words, you can test some hypotheses. Compared to other cryptographic attacks, cipher text-only attacks are the easiest to commit, especially if the cipher text is captured by a malicious person. However, implementing it on data using advanced encryption is quite difficult.

G. Selected Cipher text Attack

In this attack, the hacker identifies some or part of the decrypted cipher text and compares it to the plaintext to determine the encryption key. Obviously, this is quite difficult.

H. Known Plain Text

Unlike cipher text-only attacks, cybercriminals who launch known plaintext attacks already have a copy of the encrypted message and the plaintext data used to generate the cipher text. With this knowledge, attackers can break weak cryptographic code and launch new attacks [9].

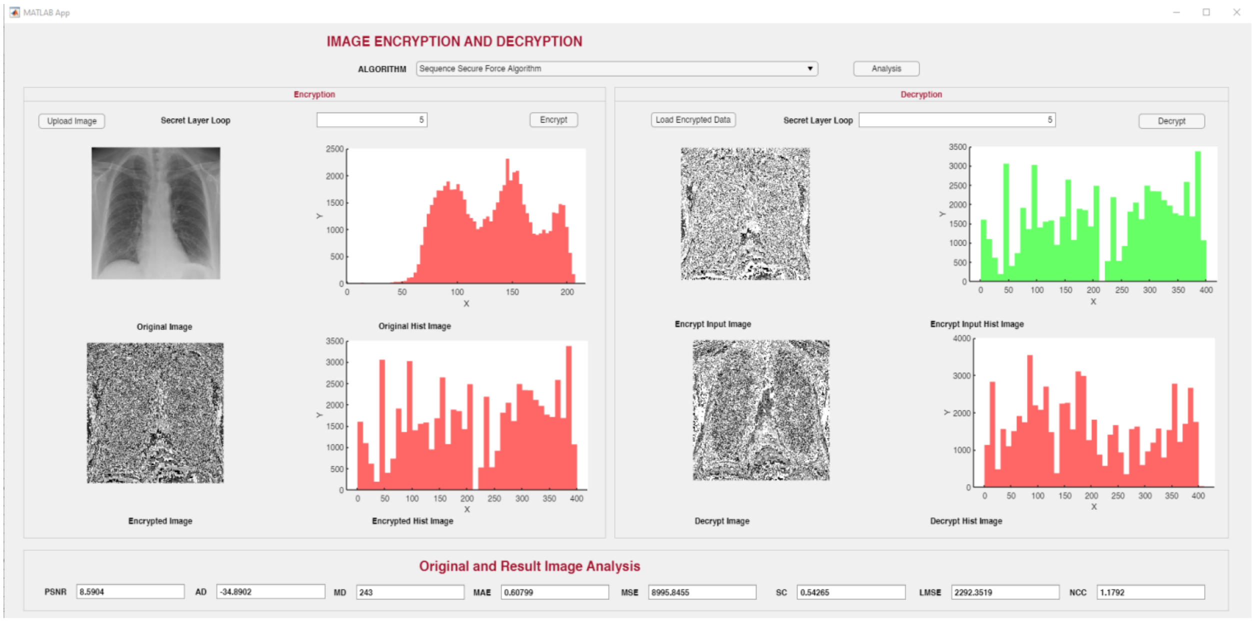
I. Selected Plaintext Attack

Selected plaintext attacks are very similar to known plaintext attacks. However, in this attack, the cybercriminal gambles by choosing the plaintext that matches the generated cipher text. You can then analyse both words to determine the key and learn more about the entire encryption process, so you can decrypt the other message.

5. Discussion and Outcomes

We survey many techniques in this paper, we expected that we design a GUI based MATLAB model where we can encrypt image using AES and Arnold transform for medical image processing. We also expected this system valuable for colour and grey both images. Image processing is a mechanism that converts an original image into a digital image, converts it to a digital format, and processes it to obtain useful information. A type of signal processing where the input is an image and the output can be an image or a characteristic/feature associated with that image.

In recent years, advances in communication technology have increased interest in digital image transmission. However, the growth of computer processors in possession of power and storage has made illegal access easier. Encryption involves applying special mathematical algorithms and keys to convert digital data into a cipher code before transmission, while decryption involves applying mathematical algorithms and keys to recover the original data from the cipher code. The scientific community has shown great interest in image transmission. Information privacy is a challenge.



ALGORITHM: Sequence Secure Force Algorithm

Secret Layer Loop: 5

Secret Layer Loop: 5

PSNR 8.5904 AD -34.8902 MD 243 MAE 0.60799 MSE 8995.8455 SC 0.54265 LMSE 2292.3519 NCC 1.1792

Figure 4 Comparison of different methods in MATLAB GUI application

Also, encryption/decryption of data or images is essential to protect valuable data or images from unwanted readers. As such, in this paper, an encryption-based technique is proposed for secure image transmission through a channel.

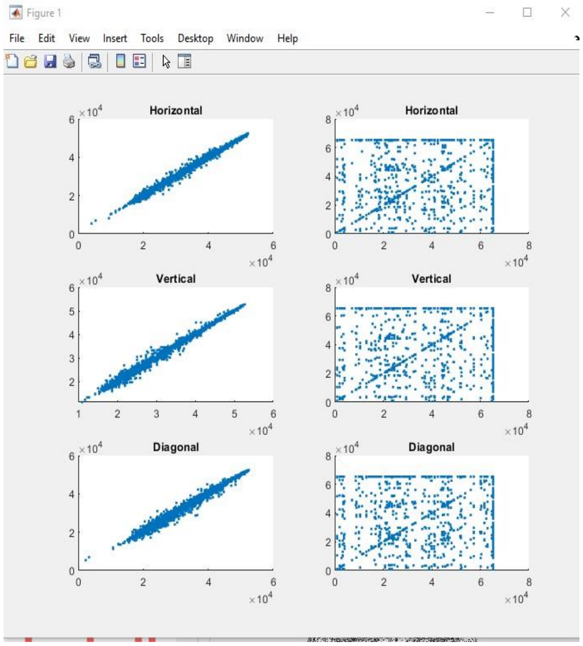


Figure 5 Secure image and decrypted image pixel information

6. Conclusion

In this research paper, the main focus is on addressing the critical security concerns when sending sensitive medical images over networked computers. Traditional encryption methods often fail to ensure the confidentiality and integrity of these images, especially in the context of emerging telemedicine practices. To overcome these challenges, the study presents a pioneering approach by incorporating image encoding techniques into the encoding process. By combining established methods, the researchers aim to develop a robust medical image encryption and decryption system that effectively protects against unauthorized access and data loss. The investigation also evaluates the performance of the proposed security method through in-depth testing and comparative analysis with existing encryption techniques. In summary, this research contributes to the field of information security by introducing a new method to improve the security of medical image data during network transmission. By blending the concepts of encryption and image processing, the proposed method provides a promising solution to the unique security challenges posed by medical imaging. This work not only demonstrates a technological breakthrough, but also highlights the growing need for security measures designed around the ever-evolving landscape of medical data exchange.

Acknowledgment

Expression of giving thanks is just a part of those feelings which are too large for words but shall remain as memories of beautiful people with whom I have got the pleasure of working during the completion of this work. I am grateful to Shri Rawatpura Sarkar University, Raipur, (C.G.), which helped me to complete my work by giving an encouraging environment. I want to express my truthful gratitude to HOD Department of Computer Science, Kranti Kumar Dewangan. His comprehensive knowledge and his logical way of thinking have been of great value to me. His understanding, encouragement, and personal guidance have provided a sound basis for the present work.

Conflicts of interest

The authors have no conflicts of interest to declare.

Author's contribution statement

For this research work all authors' have equally contributed in Conceptualization, methodology, validation, resources, writing—original draft preparation, writing—review and editing.

References

[1] S. Chepuri, "An RGB Image Encryption using RSA Algorithm," *International Journal of Current Trends in Engineering & Research (IJCTER),* vol. 3, no. 3, 2017.

[2] K. Zhu, Z. Lin and Y. Ding, "A New RSA Image Encryption Algorithm Based on Singular Value Decomposition," *International Journal of Pattern Recognition and Artificial Intelligence,* vol. 33, no. 1, 2019.

[3] L. Zhou, Y. Xiao and W. Chen, "Machine-learning attacks on interference-based optical encryption: experimental demonstration," *Optics Express,* vol. 27, no. 18, 2019.

[4] X. Chai, X. Fu, Z. Gan, Y. Lu and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing,* vol. 155, 2019.

[5] Q. Zhang, L. Guo and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling,* vol. 52, no. 11-12, 2010.

[6] Y. Q. Zhang, J. L. Hao and X. Y. Wang, "An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map," *IEEE Access,* vol. 8, 2020.

[7] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Optics and Lasers in Engineering,* vol. 110, 2018.

[8] A. Devi, A. Sharma and A. Rangra, A Review on DES, AES and Blowfish for Image Encryption & Decryption, vol. 4, 2015.

[9] Y. Zhang, Test and Verification of AES Used for Image Encryption, vol. 9, 2018.

[10] P. Gaur, "AES Image Encryption (Advanced Encryption Standard)," *International Journal for Research in Applied Science and Engineering Technology,* vol. 9, no. 12, 2021.

[11] P. Parida, C. Pradhan, X. Z. Gao, D. S. Roy and R. K. Barik, "Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps," *IEEE Access,* vol. 9, 2021.

[12] S. Priya and B. Santhi, "A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images," *Mobile Networks and Applications,* vol. 26, no. 6, 2021.

[13] J. Ning, J. Xu, K. Liang, F. Zhang and E. C. Chang, "Passive attacks against searchable encryption," *IEEE Transactions on Information Forensics and Security,* vol. 14, no. 3, 2019.

[14] P. B. Narasingapuram and M. Ponnavaikko, "A novel attack detection and encryption framework for distributed cloud computing," *Indian Journal of Computer Science and Engineering,* vol. 12, no. 1, 2021.

[15] N. Nandy, D. Banerjee and C. Pradhan, "Color image encryption using DNA based cryptography," *International Journal of Information Technology (Singapore),* vol. 13, no. 2, 2021.

[16] U. H. Mir, D. Singh and P. N. Lone, "Color image encryption using RSA cryptosystem with a chaotic map in Hartley domain," *Information Security Journal,* vol. 31, no. 1, 2022.

[17] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin and S. Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications,* vol. 284, no. 1, 2011.

[18] M. Liu and G. Ye, "A new DNA coding and hyperchaotic system based asymmetric image encryption algorithm," *Mathematical Biosciences and Engineering,* vol. 18, no. 4, 2021.

[19] R. Lin and S. Li, "An Image Encryption Scheme Based on Lorenz Hyperchaotic System and RSA Algorithm," *Security and Communication Networks,* vol. 2021, 2021.

[20] H. Li, L. Deng and Z. Gu, "A Robust Image Encryption Algorithm Based on a 32-bit Chaotic System," *IEEE Access,* vol. 8, 2020.

[21] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Archives of Computational Methods in Engineering,* vol. 27, no. 1, 2020.

[22] L. Jingfeng, S. Yi and L. Chen, "An image encryption algorithm for preventing known plaintext attacks," *IPPTA: Quarterly Journal of Indian Pulp and Paper Technical Association,* vol. 30, no. 7, 2018.

[23] X. Jin, S. Yin, N. Liu, X. Li, G. Zhao and S. Ge, "Color image encryption in non-RGB color spaces," *Multimedia Tools and Applications,* vol. 77, no. 12, 2018.

[24] Y. Hui, H. Liu and P. Fang, “A DNA image encryption based on a new hyperchaotic system,” *Multimedia Tools and Applications,* 2021.

[25] J. Hao, H. Li, H. Yan and J. Mou, “A New Fractional Chaotic System and Its Application in Image Encryption with DNA Mutation,” *IEEE Access,* vol. 9, 2021.

[26] H. V. Gamido, A. M. Sison and R. P. Medina, “Modified AES for text and image encryption,” *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 11, no. 3, 2018.

[27] X. Q. Fu, B. C. Liu, Y. Y. Xie, W. Li and Y. Liu, “Image encryption-then-transmission using DNA encryption algorithm and the double chaos,” *IEEE Photonics Journal,* vol. 10, no. 3, 2018.

[28] C. Cao, K. Sun and W. Liu, “A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map,” *Signal Processing,* vol. 143, 2018.

[29] D. M. Alsaffar, A. S. Almutiri, B. Alqahtani, R. M. Alamri, H. F. Alqahtani, N. N. Alqahtani, G. M. Alshammari and A. A. Ali, “Image Encryption Based on AES and RSA Algorithms,” 2020.

[30] P. T. Akkasaligar and S. Biradar, Selective medical image encryption using DNA cryptography, vol. 29, 2020.

[31] M. Manju and R. K. Pathak, “A Survey of Image Encryption Algorithms for Biomedical Images,” *I-Manager’s Journal on Pattern Recognition,*vol. 9, no. 2, 2022.

ABOUTTHEAUTHORS

Mrs. Mohan Manju is a Ph.D. Research Scholar (CS), Department of Computer Science from Shri Rawatpura Sarkar University, Raipur, Chhattisgarh, India. She is working as an Assistant Professor, Department of Computer Science & IT, Kamla Nehru Mahavidyalaya, Korba, Chhattisgarh, India accredited by NAAC and affiliated to Atal Bihari Vajpayee Vishwavidyalaya, Bilaspur, Chhattisgarh, India. She has 12yrs of Teaching Experience and managing projects in academic level and giving sessions on different subjects like Computer Architecture, Operating System, Software Engineering, Oracle, Visual Basic, etc. and handling Projects. She holds Masters in Computer Application.
Email: manjupillai111@gmail.com

Dr. Rajesh Kumar Pathak is currently working as a Vice Chancellor in OPJS University, Rajasthan, India. He worked as the Director in Greater Noida, Institute of Technology (GNIOT)and his key role was of administrator, researcher, academician and motivator and been worked as a Vice Chancellor at Shri Rawatpura Sarkar University, Raipur Chhattisgarh, India. He holds Doctorate in Computer Science with 20 years of experience in academic and administrative. Prior to this, gained experience as Pro Vice Chancellor and campus Director in Shri Venkateshwara University, Meerut campus and as an Advisor in Vishveshwarya Group of Institution.
He had been worked as Group Director (Vishveshwarya Group of Institution) and as a Professor and Head of Department of CSE, coordinator of M. Tech (CSE) and CEOSCA (center of excellence for open source computing and application at Greater Noida Institute of Technology, Gr.Noida. Also worked as a Dean and HOD (CSE) at SIET Pilkhwa Ghaziabad and A.P. in Department of CSE at ABES Engineering College Ghaziabad taught different subjects such as Operating System, data mining, etc. and other role to get involved to motivate students for their future career guidance.
Email: drrkpathak20@gmail.com

Appendix I

S.no.	Abbreviation	Description
1.	DNA	Deoxyribonucleic Acid Encryption
2.	MSE	Mean Squared Error
3.	PSNR	Peak Signal-to-Noise Ratio
4.	RSA	Rivest-Shamir-Adleman encryption
5.	SSIM	Structural similarity Index Metric
6.	WSNs	Wireless Sensor Networks