Scientific Journal of Informatics
Vol. 11, No. 4, Nov 2024
p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji/index e-ISSN 2460-0040

Enhancing Medical Image Security Using Hyperchaotic Lorenz and Josephus Traversing Encryption

Eko Hari Rachmawanto[1*], Elkaf Rahmawan Pramudya[2], Zudha Pratama[3]
[1,2,3]Department of Informatics Engineering, Univeristas Dian Nuswantoro, Indonesia

Abstract.
Purpose: The present work focuses on developing a methodology to encrypt medical images using combined Hyperchaotic Lorenz systems with Josephus Traversing. This, therefore, forms the basis of the present paper to establish the efficacy of the proposed method against glioma, meningioma, and pituitary kinds of brain tumor images at 256 × 256 and 512 × 512 pixels image sizes.
Methods: In this regard, a state-of-the-art encryption technique based on the Hyperchaotic Lorenz systems for Josephus Traversing has been proposed against the medical images of glioma, meningioma, and pituitary tumor datasets obtained from the repository via medical imaging.
Result: The different distortion of test outcomes has the MSE value lying between 69.01 and 172.1, while fidelity preservation-PSNR lies between 12.971 and 18.321 dB for different tumor types and sizes of images. The UACI is between 3.625 and 11.34, while the NPCR is always greater than 99% to show very high tamper resistance. This approach is very new in integrating chaos and traversal algorithms for encrypting medical images. Hence, it has a great promising enhancement of security and protection of patient privacy.
Novelty: This research contributes a comprehensive investigation based on different metrics that allows exploring not only the efficiency but also strength against decryption techniques for a proposed encryption method. More investigations could be done for further research work in order to enhance the encryption speed, which would improve robustness against advanced decryption techniques in medical image security for digital health applications.

Keywords: Hyperchaotic lorenz system, Image encryption, Josephus traversing, Quality measurement
Received July 2024 / **Revised** October 2024 / **Accepted** February 2025

INTRODUCTION

Medical data security and privacy are at a premium in this digital era, since through the medical record one is able to refer to examinations and treatments, and it is an important document to the history of healthcare and the condition of patients' health [1] – [4]. Medical data encompass various types of images such as X-rays, Computer Tomography (CT), Magnetic Resonance Imaging (MRI), ultrasound, histology, and positron emission tomography (PET), each playing a specialized role in the medical field, all of which are highly sensitive and valuable information for both patients and healthcare providers. In light of sending the images over open networks such as the Internet, one would want the medical images strongly protected not to allow unauthorized access for manipulations, theft of valuable information, or leakage of sensitive data [5]. Finally, this shall be obtained by introducing unauthorized access into the medical images with strong security measures. The doctor or health care service provider has sought confidentiality of medical records under the applicable laws and regulations where security of patients' medical data is considered paramount in the care industry [6]. A solution that can be instituted for the improvement of the security features of medical record systems involves integrating encryption techniques [7], especially for the protection of very sensitive and also very valuable information in the medical images of patients and healthcare providers. All these schemes of image encryption are somewhat vulnerable in the presence of different types of attacks such as colour alteration, resizing, and other pre-processing-based image processing. Hence, strong encryption algorithms are in need [8].

Various researchers have done work in the enhancement of medical images for better security with good results. Hidayati et al. [9] presented the work by implementing AES and Camellia algorithms with their different modes of operations along with the quality check of encrypted images via NPCR and UACI tests.

*Corresponding author.
Email addresses: eko.hari@dsn.dinus.ac.id (Rachmawanto)
DOI: 10.15294/sji.v11i4.9815

It was observed that the NPCR values are 99.60% for AES CBC, 99.608% for AES CFB, 99.6093% for AES OFB, 99.6296% for Camellia ECB, 99.6072% for Camellia CBC, and 99.6124% for Camellia OFB. While in such modes of operations, the values of UACI were correspondingly 34.714%, 34.754%, 34.603%, 34.983%, 34.615%, and 34.707%. Wibowo et al. [10] proposed, for the securities of medical images in a web-based radiology system with its exposure to some passive attack modes such as ECB, CBC, CFB, and OFB, the Camellia algorithm. Performance analysis of the obtained results was carried out by a visual analysis of histogram, entropy, and PSNR to analyze the quality of the decrypted images. Results: ECB and OFB modes of operation had a good quality of images. In speed, ECB had higher speeds at encryption. For one to achieve the best security, one should not use the ECB mode of operation in encrypting.

In Wikarsa et al. [11] describes how blockchain technology secures an electronic medical record in private blockchains, using consensus of PoW with the SHA-256 cryptographic algorithm in developing encryption and decryption keys. Medical data stored on the blockchain were disseminated automatically in all health care services in the network, whereas physicians could view the clinical records via web-based systems using their tokens that were created when patients use the Android system. Yeni et al. [12] reviewed the application of LCG in block scrambling for image encryption using IDEA. The results demonstrated that, in consideration of a trade-off with image quality, it could potentially further reduce the correlation pattern of pixel blocks and increase the security of the generated images. The obtained results described that LCG was efficient for the improvement of the level of security of the encrypted image-meaning great contribution to security methods in digital image processing in the future. Indriyono et al. [13] combined ElGamal algorithm and Vigenere Cipher for enhancing the security of the text message. Results from these tests indicated that it made the entire access of the text message by unauthorized parties a little hard as characters had been shifted with more complicated keys being used.

A new strategy of providing higher security to medical images is proposed in this paper through an encryption scheme developed based on the combination of hyperchaotic Lorenz systems and Josephus traversal. Li et al. [14] proposed a holographic encryption algorithm in which hyperchaotic Lorenz systems are used for the confusion operation and bit-plane decomposition provides improved security to the plaintext images. It mainly consisted of the process of converting plain images into single-phase holograms, bit-plane decomposition, Arnold scrambling of sub-images, and XOR diffusion. It was observed that this encryption algorithm offered high-security performance and could resist any sort of attack very efficiently. Yang et al. [15] presented the encryption of medical images with Josephus traversal and a hyperchaotic Lorenz system to enhance security towards making the images more resistant to any type of attack. These experimental results verified that the proposed scheme of steganography could effectively mask medical image information and resolve the problems of damaged images in telemedicine. Meanwhile, Niu and Zhang [16] presented a digital image encryption method based on Josephus traversal variable and dynamic DNA coding to improve security during transmission and storage. Experimental results have verified that it could resist statistical attack and brute-force attack. The other involved SFC Y-index and Josephus variable-based image encryption schemes for improved security and effectiveness. This proposed algorithm achieves confusion-diffusion, where chaotic sequence maps are adopted for not only shuffling but also increasing the strength of confusion and diffusion characteristics, assisted by ciphertext feedback and chaotic sequence operation. The experimental results demonstrated good behavior and a higher security level than that of many other algorithms of image encryption [17]. It combines the hyperchaotic Lorenz systems to develop much stronger and more secure image encryption systems that can offer high security to medical images with more resistance against several kinds of attacks and image damages for telemedicine.

This paper develops a fresh medical image encryption method: combining the Hyperchaotic Lorenz system and Josephus traversal. Related research has identified a researcher who used an approach from one of the proposed methods. Previous related studies by Yang et al. [15] were based on the same method they successfully concealed medical image information and thus resolved the telemedicine problems caused by image corruption. However, this paper will consider some of them in the research developed by Yang et al. [15] starting from the optimization of the chaotic sequence processing algorithm, using a Cat mapping, and modification of the stage of pixel diffusion. In this way, with this approach, one expects to obtain better values of security, increasing resilience to various types of attack, with better protection for medical images in a telemedicine environment.

METHODS

The proposed approach has the objective of improving security for medical images with the use of a multilevel encryption technique. It first starts with a sample set of medical images and then generates an RNG key. It undergoes further processing with HLS to get a chaotic sequence out. In other words, the first level of encryption-the first cipher-is the randomization of the image with the Lorenz system. Noising the paint applied dispersed the values of the pixels, hence increasing the complexity for encoding. The Josephus path introduced one more layer of permutation by changing the positioning of the pixels with respect to the sequence of the Josephus problem. At last, a pixel is diffused, wherein it may help to create a small change in the image or key input that may create a huge difference in the final encrypted image, giving final encryption. The explanation of the flow done above can be viewed in Figure 1.

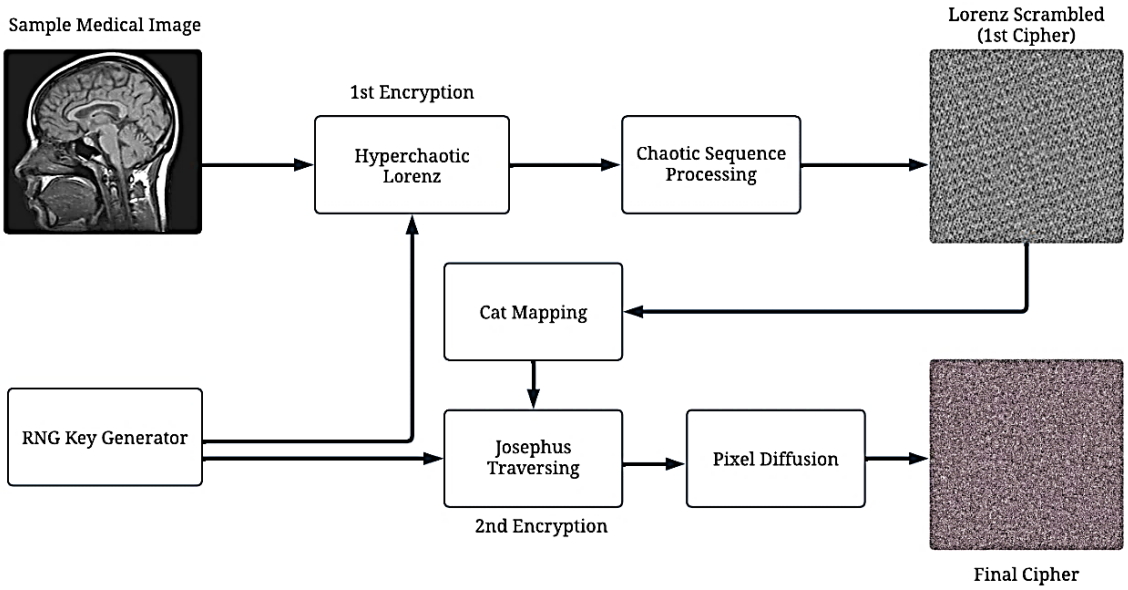


Figure 1. Proposed encryption

Random number generator (RNG) key generator

RNG [18] – [20] has a major role in the development of random keys for securing encryption. In a very important sense, it generates a set of random or pseudo-random values from given seeds or initial inputs to be used as keys to configure the encryption algorithm. In addition, cryptographic security is highly dependent upon the quality and strength of the key developed through the RNG key generator. It might also provide higher resistance against possible cryptanalysis attacks if strong, random keys were used. Hence, it enhances the security of sensitive medical information in, among others, telemedicine or electronic medical data storage. The general formula of the random number generator depends on the type of RNG to be used. However, this study will be using a Linear Congruence Generator that uses the equation presented in eq (1). Where X_n is the random value at iteration n, and a, c, m are predefined constant parametesr. These parameters influence the quality and distribution characteristics of the random numbers generated by the RNG.

$$X_{n+1} = (a \cdot X_n + C) \, mod \, m \tag{1}$$

Where X_n is the current value, and X_{n+1} represents the next value in the sequence. The constant a is the multiplier that scales the current value, while C is an increment that shifts the result. The modulus m ensures the output wraps around within the range 0 to $m - 1$, keeping the sequence within a fixed range.

Hyperchaotic lorenz system

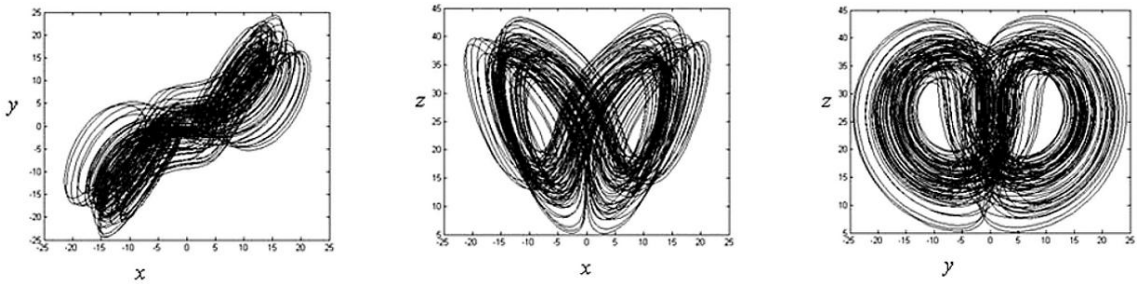
Hyperchaotic Lorenz Systems have also been used in medical image securities due to their enhancement in security because they exploit such complex dynamics and sensitivity of the initial conditions obtained from the system [21]. It is one modification of Lorenz's standard. This system contains coupled nonlinear differential equations; they show chaotic behavior [22]. Some of the equations of HLS are used in generating a chaotic value sequence in image encryption. This series is the key to scrambling the position

of pixels or its highly sensitive value change, even if the initial conditions of the system have changed a little. The equations governing a typical HLS can be seen in eq (2).

$$\begin{aligned} \frac{dx}{dt} &= a(y - x), \\ \frac{dy}{dt} &= x(b - z) - y, \\ \frac{dz}{dt} &= xy - cz. \end{aligned} \tag{2}$$

Here, x, y, and z are state variables, while a, b, and c are parameters; t is time. Such a set of equations provides the chaotic evolution of the state variables of the system-very important in generating unpredictable sequences that find use in the secure encryption of medical images.

Parameters in the above equations are: $a = 10, b = 28, c = \frac{8}{3}$, these give the standard projections of HLS, as can be seen in Figure 2 below. Due to the chaotic nature of this system, sensitivity to initial conditions creates these sorts of complex, never-repeating patterns. This is specified through equations developed here on how state variables x, y, and z will be changing with time, showing complex trajectories and playing an important role in generating unpredictable sequences.



(a) $x_n - y_n$ (b) $x_n - z_n$ (c) $y_n - z_n$

Figure 2. Projections of the hyperchaotic lorenz

Josephus traversing

Josephus Traversal is the rearrangement of pixel positions according to some eliminating sequence obtained from a Josephus problem [23], [24]. More permutation is introduced in the encryption procedure in order for the scheme to be complicated and stand against different kinds of cryptographic attacks. It defines how the pixels are going to shuffle through the sequence that is produced via Josephus Traversal; hence, it is very important to protect the original content in a medical image. Eq (3) shows that the formula for Josephus Traversing contains a recursive relationship.

$$(n, k) = (J(n - 1, k) + k) \; mod \; n \tag{3}$$

Where n represents the number of pixels or elements in the sequence, and k is the step size for elimination. In this, from the encryption process starting from the plain image to the encrypted image, a step-by-step procedure of randomization, naturalization, and permutation is to be performed based on the removal of Josephus. First of all, the plain image is allowed to be integrated with a random key provided from the RNG. From here, with the Josephus transfer parameter k, while considering the step of subtraction in a Josephus chain, along with the number of pixels or elements of the image n, we arrive at Eq (3) that computes any order of every pixel in an image for a rearrangement. After this rearrangement of the intensity values, the diffused pixel permutation of the encrypted image would ensure that even a minor disturbance in the raw image can lead to huge changes in the encrypted image.

RESULTS AND DISCUSSIONS

The following work is based on the Health Testing sample dataset taken from Kaggle, where different kinds of datasets regarding health are kept. All data processing and the implementation of the methodology were done in the MATLAB 2020a programming environment, which is very efficient for image processing and analysis. MATLAB 2020a offers some key advantages with respect to managing and analyzing complex data, such as medical images, by special features in view of visualization, signal processing, and numerical

modeling [25]. The encryption method is evaluated using image sizes of 256 x 256 and 512 x 512 pixels. The results of the proposed encryption method can be observed in Figure 3. This figure illustrates the encrypted image obtained through the application of the encryption algorithm, combining Hyperchaotic Lorenz systems and Josephus Traversing.

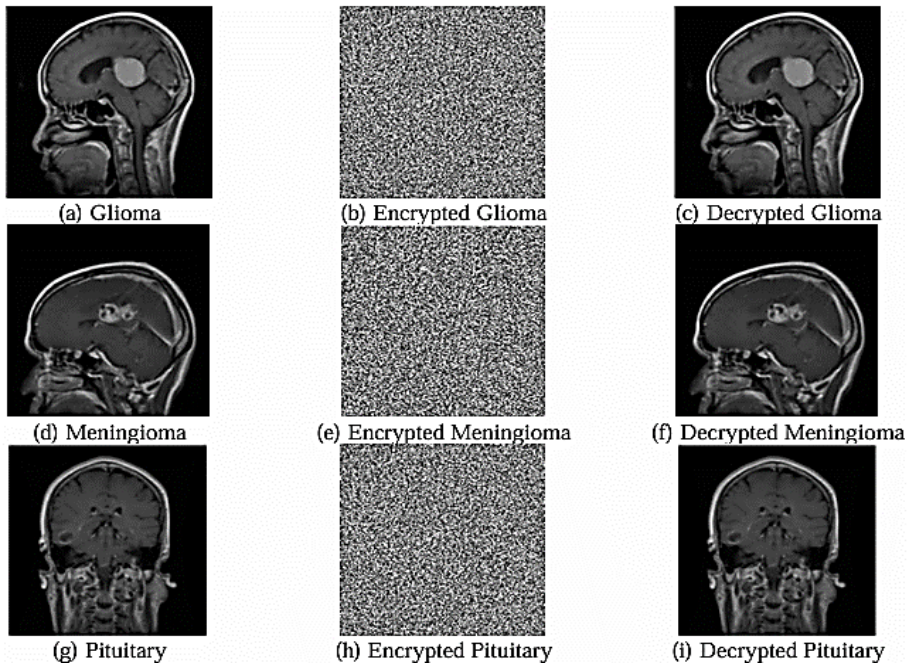


Figure 3. Results of proposed encryption (512 x 512)

In this study, the performance analysis of the proposed encription scheme based on various parameters: histogram analysis, MSE, PSNR, UACI, and NPCR. All these measurements are of essence in depicting various aspects of the quality and security of the encrypted medical images. Histogram analysis is really helpful in analyzing the distribution of pixel intensities in the encoded image. On the other hand, MSE quantifies the root mean square deviation between the source pixel and its encrypted. PSNR gives a logarithmic measure of the fidelity of the signal; hence, it underlines the quality of the image maintained with our approach. UACI and NPCR values will be great for assessing the alteration in pixels between the original image and the encrypted image to prove the resiliency of the method to tampering or attacks. The formula for each performance evaluation can be seen in eq (4) - (7).

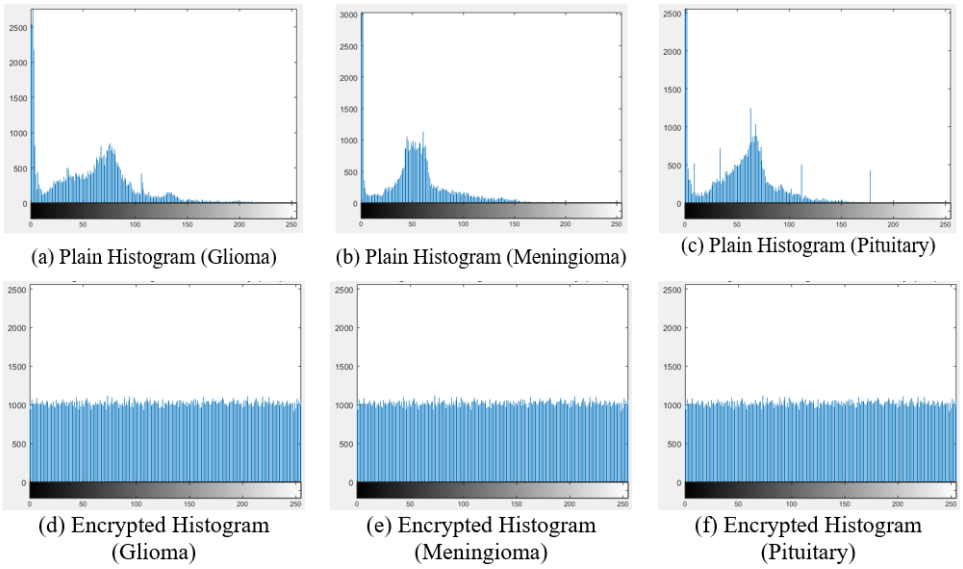


Figure 4. Results of histogram analysis (512 x 512)

Based on encrypted results of figure 3 (b), (e), and (h), The next evaluation is MSE and PSNR evaluation, as depicted in Table 1. Additionally, Table 2 will measure UACI and NPCR. These metrics are crucial for assessing the security and quality of the encrypted medical images.

Table 1. Results of MSE and PSNR

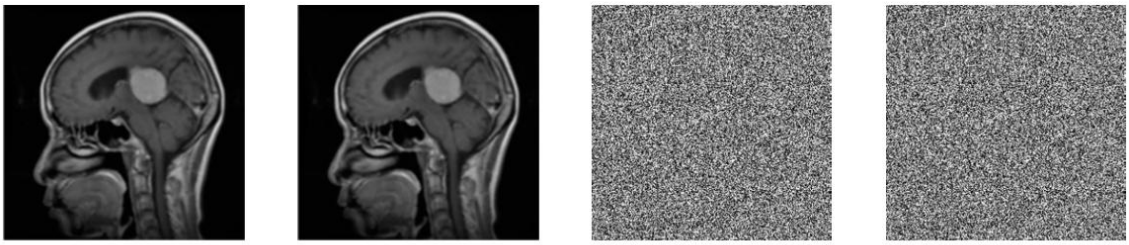
Encrypted Image	Sample Size	MSE	PSNR	Elapsed Time
Glioma	256 x 256	119.6	17.779 dB	6 Min 32 Sec
	512 x 512	172.1	13.746 dB	9 Min 17 Sec
Meningioma	256 x 256	108.8	18.321 dB	6 Min 16 Sec
	512 x 512	165.7	12.971 dB	10 Min 22 Sec
Pituitary	256 x 256	69.01	17.512 dB	6 Min 48 Sec
	512 x 512	113.2	13.945 dB	9 Min 42 Sec

Table 2. Results of UACI and NPCR

Encrypted Image	Sample Size	UACI	NPCR
Glioma	256 x 256	5.992	99.59
	512 x 512	3.625	99.44
Meningioma	256 x 256	7.072	99.31
	512 x 512	5.863	99.31
Pituitary	256 x 256	11.34	99.51
	512 x 512	9.676	99.54

The values of difference from Tables 1 and 2, with regard to MSE, PSNR, UACI, and NCPCR, prove that the encryption operation has greatly influenced the pattern of the pixels. This proves that there is significant variation in pixel values and their distribution between the original and encrypted images; it could therefore justify the potential capability of encryption methods in rendering sensitive information obscure to enhance information data security.

The decryption testing was done using the proper key, a slightly altered key, and a completely wrong key, respectively, which restored the images to their original form, as depicted in Figure 5. Figure 5 displays the comparison between the (a) plain image, (b) decrypted using the correct key, (c) decrypted using a slightly modified key, and (d) decrypted using a completely wrong key.



(a) Plain Image (b) Correct Key (c) Slightly Modified Key (d) Wrong Key

Figure 5. Decryption phase (512 x 512)

CONCLUSION

Some diversified but constant results of the proposed encryption scheme using Hyperchaotic Lorenz systems and Josephus Traversing applied on the glioma, meningioma, and pituitary brain tumor images for two different image sizes. Thus, MSE values fell between 69.01 and 172.1, hence showing distortion variation between original and encrypted images, and PSNR values ranged between 12.971 and 18.321 dB, which says that this method can preserve the image quality to different extents. Other quality measures, such as UACI and NPCR, fall within the range from 3.625 to 11.34, although most are very high; this is reflective of the very minimum rate of modification of pixels due to the high resistance against tampering. These obtained results confirm that the proposed methodology will be working well with medical images in the protection against unauthorized access and a possible data breach. For future research, exploring enhancements to further improve encryption speed and resilience against advanced decryption techniques could advance the field's capabilities in medical image security and privacy protection.

REFERENCES

[1] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, "High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD)," *Advance Sustainable Science, Engineering and Technology (ASSET)*, vol. 6, no. 1, 2024, doi: 10.26877/asset.v6i1.17186.

[2] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.

[3] W. Alexan, A. Hamza, and H. Medhat, "An AES Double–Layer Based Message Security Scheme," in *2019 International Conference on Innovative Trends in Computer Engineering (ITCE)*, IEEE, Feb. 2019, pp. 86–91. doi: 10.1109/ITCE.2019.8646461.

[4] I. P. Pujiono, E. H. Rachmawanto, and D. A. Nugroho, "The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images," *Journal of Applied Intelligent System*, vol. 8, no. 1, pp. 69–80, 2023.

[5] G. C. M. Purba, A. I. Hadiana, and I. Santikarama, "Pengamanan Citra Medis Berbasis Steganografi dan Kriptografi Dengan Menggunakan Metode End Of File Dan Advanced Encryption Standard," *Informatics And Digital Expert (INDEX)*, vol. 4, no. 1, pp. 1–9, 2022, [Online]. Available: https://e-journal.unper.ac.id/index.php/informatics

[6] R. Verma, A. Kumari, A. Anand, and V. S. S. Yadavalli, "Revisiting Shift Cipher Technique for Amplified Data Security," *Journal of Computational and Cognitive Engineering*, vol. 3, no. 1, pp. 8–14, Aug. 2022, doi: 10.47852/bonviewJCCE2202261.

[7] A. Nanda and T. Gelar, "ENKRIPSI SELEKTIF PADA CITRA MEDIS DENGAN MENGGUNAKAN LINEAR CONGRUENTIAL GENERATOR," *JIP (Jurnal Informatika Polinema)* , vol. 8, no. 2, pp. 1–8, 2022.

[8] R. Wijaya, "Enkripsi Nilai Piksel Pada Citra Digital Dengan Algoritma Piecewise Linear Chaotic Map," *Bulletin of Computer Science Research*, vol. 3, no. 1, pp. 161–169, Dec. 2022, doi: 10.47065/bulletincsr.v3i1.206.

[9] L. N. Hidayati, G. F. Fitriana, and I. F. Adam, "Perbandingan Keacakan Citra Enkripsi Algoritma AES dan Camelia Uji NPCR dan UACI," *JURIKOM (Jurnal Riset Komputer)*, vol. 8, no. 6, pp. 274–283, Dec. 2021, doi: 10.30865/jurikom.v8i6.3624.

[10] Z. Dhany Wibowo, I. Fuaddina Adam, and W. Andi Saputra, "IMPLEMENTASI ALGORITMA CAMELLIA UNTUK KEAMANAN CITRA MEDIS PADA SISTEM RADIOLOGI BERBASIS WEB," *JIP (Jurnal Informatika Polinema)* , vol. 6, no. 4, pp. 1–8, 2020.

[11] L. Wikarsa, T. Suwanto, and C. Lengkey, "Implementasi Algoritma Konsensus Proof-of-Work dalam Blockchain terhadap Rekam Medis Implementation of Proof-of-Work Consensus Algorithm in Blockchain for Medical Records," *Jurnal Pekommas*, vol. 7, no. 1, pp. 41–52, 2022, doi: 10.30818/jpkm.2022.2070105.

[12] M. Yeni, Tommy, and R. Siregar, "Enkripsi Citra Digital dengan IDEA Cipher: Pengacakan Blok Pseudorandom LCG dan Evaluasi Melalui Image Correlation Analysis," *SNASTIKOM*, pp. 142–149, 2023.

[13] B. V. Indriyono *et al.*, "Prosiding SEMNAS INOTEK (Seminar Nasional Inovasi Teknologi) 18," *INOTEK*, vol. 7, pp. 2549–7952, 2023.

[14] J. Li *et al.*, "Holographic encryption algorithm based on bit-plane decomposition and hyperchaotic Lorenz system," *Opt Laser Technol*, vol. 152, p. 108127, Aug. 2022, doi: 10.1016/J.OPTLASTEC.2022.108127.

[15] N. Yang, S. Zhang, M. Bai, and S. Li, "Medical Image Encryption Based on Josephus Traversing and Hyperchaotic Lorenz System," *J Shanghai Jiaotong Univ Sci*, vol. 29, no. 1, pp. 91–108, Feb. 2024, doi: 10.1007/s12204-022-2555-x.

[16] Y. NIU and X. Zhang, "Image Encryption Algorithm of Based on Variable Step Length Josephus Traversing and DNA Dynamic Coding," *Journal of Electronics & Information Technology*, vol. 42, no. 6, pp. 1383–1391, 2020.

[17] Y. Niu and X. Zhang, "An effective image encryption method based on space filling curve and plaintext-related josephus traversal," *IEEE Access*, vol. 8, pp. 196326–196340, 2020, doi: 10.1109/ACCESS.2020.3034666.

[18] H. Mahalingam *et al.*, "Neural Attractor-Based Adaptive Key Generator with DNA-Coded Security and Privacy Framework for Multimedia Data in Cloud Environments," *Mathematics*, vol. 11, no. 8, Apr. 2023, doi: 10.3390/math11081769.

[19] X. Chen *et al.*, "Pseudorandom Number Generator Based on Three Kinds of Four-Wing Memristive Hyperchaotic System and Its Application in Image Encryption," *Complexity*, vol. 2020, no. 1, p. 8274685, 2020.
[20] L.-H. Gong, H.-X. Luo, R.-Q. Wu, and N.-R. Zhou, "New 4D chaotic system with hidden attractors and self-excited attractors and its application in image encryption based on RNG," *Physica A: Statistical Mechanics and its Applications*, vol. 591, p. 126793, 2022.
[21] M. Gabr *et al.*, "Application of DNA Coding, the Lorenz Differential Equations and a Variation of the Logistic Map in a Multi-Stage Cryptosystem," *Symmetry (Basel)*, vol. 14, no. 12, Dec. 2022, doi: 10.3390/sym14122559.
[22] W. Alexan, N. Alexan, and M. Gabr, "Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs," *Fractal and Fractional*, vol. 7, no. 4, Apr. 2023, doi: 10.3390/fractalfract7040287.
[23] Y. Niu and X. Zhang, "A novel plaintext-related image encryption scheme based on chaotic system and pixel permutation," *IEEE Access*, vol. 8, pp. 22082–22093, 2020.
[24] R. Anandkumar and R. Kalpana, "A Fibonacci p-code traversing and unified chaotic map-based image encryption algorithm," *J Ambient Intell Humaniz Comput*, vol. 13, no. 8, pp. 3713–3727, 2022.
[25] W. Y. Yang *et al.*, *Applied numerical methods using MATLAB*. John Wiley & Sons, 2020.

.