ASJET

Al-Salam Journal for Engineering and Technology
Journal Homepage:
http://journal.alsalam.edu.iq/index.php/ajest
e-ISSN: 2790-4822 p-ISSN: 2958-0862

Henon Chaotic Map and RC6 Block Algorithm Cascaded Design-Based Medical Image Encryption

Mustafa Q. Ali[1]*

[1]College of Islamic Sciences, University of Baghdad, Baghdad, Iraq.

*Corresponding Author: Mustafa Q. Ali

DOI: https://doi.org/10.55145/ajest.2026.05.01.019
Received May 2025; Accepted June 2025; Available online Febuary 2026

ABSTRACT: Protecting sensitive medical images is essential in modern healthcare systems, where security and robustness are critical. This study presents a hybrid image encryption scheme combining the chaotic Henon map with the RC6 algorithm to ensure secure and efficient image transmission. The method leverages the high sensitivity and unpredictability of the Henon map alongside RC6's strong diffusion and noise resistance. Experimental results demonstrate strong robustness, evidenced by uniform pixel distributions, high entropy (7.999), and resistance to statistical attacks. Compared with AES, the proposed approach more effectively reduces pixel correlation, exhibits high key sensitivity, and provides strong protection against brute-force attacks due to its large key space.

Keywords: RC6 block cipher, cryptographic algorithms, Henon chaotic map, hybrid encryption, security analysis

1. INTRODUCTION

Telemedicine technologies are reshaping healthcare delivery by enabling rapid diagnosis and enhancing emergency response through advanced digital tools. A key component of these systems is the transmission of digital data, particularly medical images that contain highly sensitive and private information [1].

Conventional encryption algorithms such as DES and AES are widely employed to protect digital data. Nevertheless, when applied to image data, these techniques often exhibit limitations due to the intrinsic properties of images, including large data volumes, high redundancy, and strong spatial correlations among adjacent pixels. These characteristics reduce the effectiveness of traditional encryption schemes in safeguarding image data against unauthorized access or analytical attacks [2].

To fulfill this requirement, recent research has focused on chaos-based encryption techniques derived from chaos theory. Chaotic systems are particularly well-suited for secure image encryption owing to their inherent features, such as extreme sensitivity to initial conditions, unpredictability, and pseudo-random behavior. Among the various chaotic models, the Henon chaotic map has attracted considerable interest for its ability to generate secure key sequences and enable nonlinear pixel transformations [3,4]. This study proposes a novel hybrid encryption scheme that integrates the RC6 block cipher with a chaotic Henon map.

2. Related Work

Medical image encryption has shifted from costly traditional ciphers (e.g., AES, DES, RC4) to chaos-based methods. Early studies used quadratic maps, followed by Henon-based schemes with enhanced security, including multi-block substitution and bidirectional diffusion, proposed between 2020 and 2022. Additionally, Guesmi and Farah [5] (2021) combined hybrid chaotic maps with DNA-based encoding to further strengthen medical image encryption security.

*Corresponding author: author@organization.edu.co

3. Research Gap

In 2021, Ibrahim Yasser et al. [6] introduced a chaotic-map encryption scheme that improves perturbation algorithms to overcome weaknesses in conventional chaos-based confusion and diffusion, achieving high speed and strong robustness against medical image cyber-attacks. In 2022, Belazi et al. [7] proposed a sine–tangent chaotic-map-based encryption method aimed at enhancing sensitivity and resistance to cryptanalytic attacks. The scheme maintained a high level of entropy and defended well against various forms of statistical and differential attacks, protecting medical images as expected.

Al-Khuzaay and Al-Jawher (2022) [8], put forward two further models of Mixed Transforms, which are the new hybrid of linear and nonlinear Transformation techniques. The first mixed transform is formulated in three steps: compute 2D discrete cosine transform (DCT) of the image, apply Arnold Transform (AT) to the DCT coefficients, and apply discrete Wavelet Transform (DWT) to the result "CAW". The second blended consisted of first computing the discrete Fourier transform (DFT), net applying AT, and finally computing the discrete Wavelet Transform (DWT), which was abbreviated as (FAW). The results obtained showed that CAW and FAW transforms yielded a classification rate higher than that achieved with the conventional transforms DCT, DFT, and DWT. Besides, it contributes to the development of a family of directional and multi-transformation bases for image processing.

Hussain and Khodher (2023) [9] Implemented three types of chaotic maps for constructing a strategy of digital image encryption based on a chaotic system. These chaotic maps include: the logistic map, Arnold Cat's map, and Baker's map. Furthermore, the triple data encryption standard (3DES) encryption scheme is utilized in conjunction with the aforementioned chaotic maps. Experimental results showed that the intended image encryption method is efficient and secure, which is useful in uncontrolled networks. For the dual-directional data communication between the server and client over the network, the Transmission Control Protocol (TCP)/Internet Protocol (IP) suite was employed.

Prakash et al. (2024) [10], introduced a selective encryption technique that targets encrypting only the medically relevant parts of multidimensional medical images. The method was focus on the crucial areas of image by using masks on segmentation and Henon chaotic map for a specific purpose image encryption. The system under consideration showed 47% faster on retrieval time for brain CT images compared with full-image encryption techniques, which shows improvement in the efficiency, but still preserving a composed level of the security.

4. Proposed Methodology

To increase the security of the medical image encryptions, the RC6 block cipher and the Henon chaotic map have been integrated in this method. The security keys and the pixel positions to be changed are generated using the Henon map to ensure high levels of confusion and diffusion [11]. The RC6 block cipher has strong cryptographic capabilities that allow for quick and low-resource encryption and decryption. This method guarantees a high entropy and a low correlation to make the combination of these methods extremely resistant to statistical analysis and differential attacks. The method is precisely considered to achieve a secure transmission and a secure storage of the medical images while ensuring optimal efficiency. A full overview of the proposed method is shown in Fig. 1.

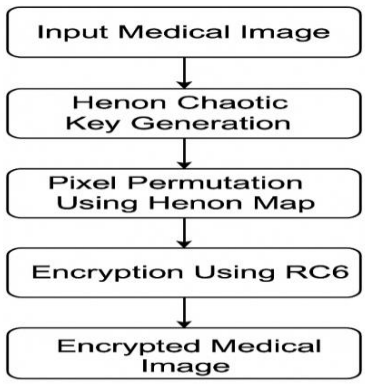

FIGURE 1 Structure of the proposed RC6–Henon chaos-based encryption framework

4.1 RC6 Block Cipher

The RC6 is a symmetric-key block cipher that enhances the RC5 structure by joining the data-dependent rotations, the XOR operations, and the modular addition. RC6 operates on 128-bit blocks with variable key lengths (128, 192, and 256 bits) and using four working registers to improving security and efficiency. Fig. 2 shows the function of the RC6 cipher algorithm [12].

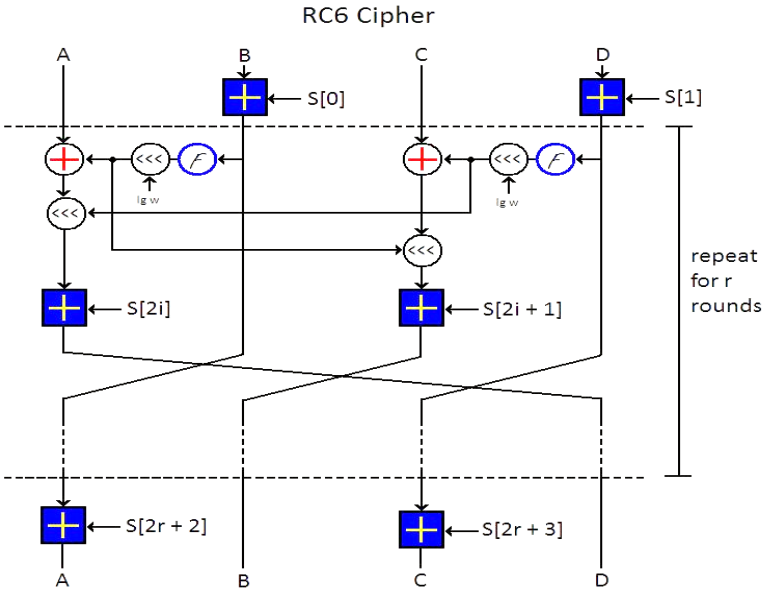

FIGURE 2 RC6 cipher algorithm

4.2 Henon Chaotic Map

The Henon chaotic map was two dimensional with discrete time dynamic system that shows chaotic behavior. It is mathematically defined as [13]:

$$x_{n+1} = 1 - ax_n^2 + y_n \quad (1)$$

$$y_{n+1} = bx_n \quad (2)$$

where: ($x_n y_n$) are state variables, and (a), (b) are control limitations typically set as a=1.4 and b=0.3 to guarantee the chaotic behavior. The Henon map generates random pseudocode sequences that are sensitive to initial conditions, making it useful for encryption applications. Fig.3 expresses the Henon chaotic map attractor with an unpredictable and complex structure that's ideal for encryption applications [14].

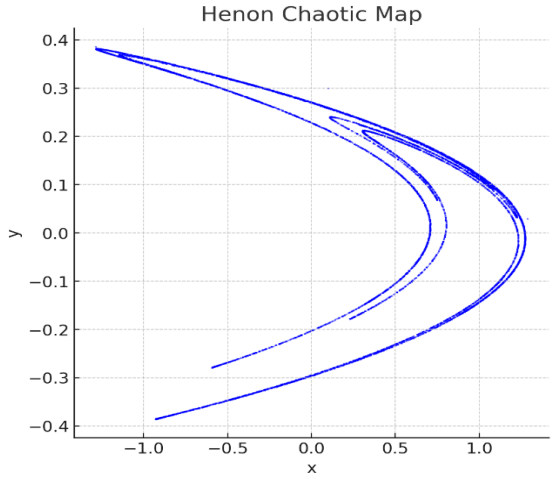

FIGURE 3 The Henon chaotic map

4.3 Encryption Process

The encryption process is started with key generation, and the Henon chaotic map is used to produce control parameters with highly unpredictable initial conditions. The RC6 encryption algorithm was served by these values as the basis for key expansion, which ensures a dynamic and secure cryptographic key set. When the keys are generated, the pixel variation and substitution stage is performed. The input of the medical image undergoes a scrambling operation based on the Henon chaotic sequence, effectively dispersing pixel positions in a nonlinear manner. This step

significantly enhances confusion to make the process difficult to recognize any patterns in the encrypted image. Following the permutation. The RC6 cipher is then applied, either under Electronic Codebook mode or Cipher Block Chaining mode, to encrypt each segment individually, after the segments have been decrypted into the predefined order .The encryption takes place with strong diffusion by including bitwise rotations, modular computations, and XORs to make the output of the encryption extremely resistant to cryptographic attacks. At last, the cipher image is achieved, which is the medical image after encryption in its complete form. This encryption renders the image safe for the transferring process, protecting the sensitive information against unauthorized access while ensuring the integrity of the data, which requires no loss of sensitive data confidentiality.

5. Experimental Results and Analysis

To test the effectiveness of the encryption scheme, standard medical images like MRIs, CT scans, and X-ray images were selected. The performance evaluation was carried out using different security measures, which included the analysis of histograms, the calculation of entropy, correlation coefficient measurements, and the evaluation of key sensitivity.

5.1 Histogram Analysis

Histogram analysis evaluated pixel uniformity, as shown in Fig. 4, [15] (a) original image; (b,d,f) histograms of original, encrypted, and decrypted images; and (c,e) RC6-encrypted and decrypted images.

The encrypted histograms are nearly uniform, revealing no image features, which confirms strong resistance to statistical attacks.

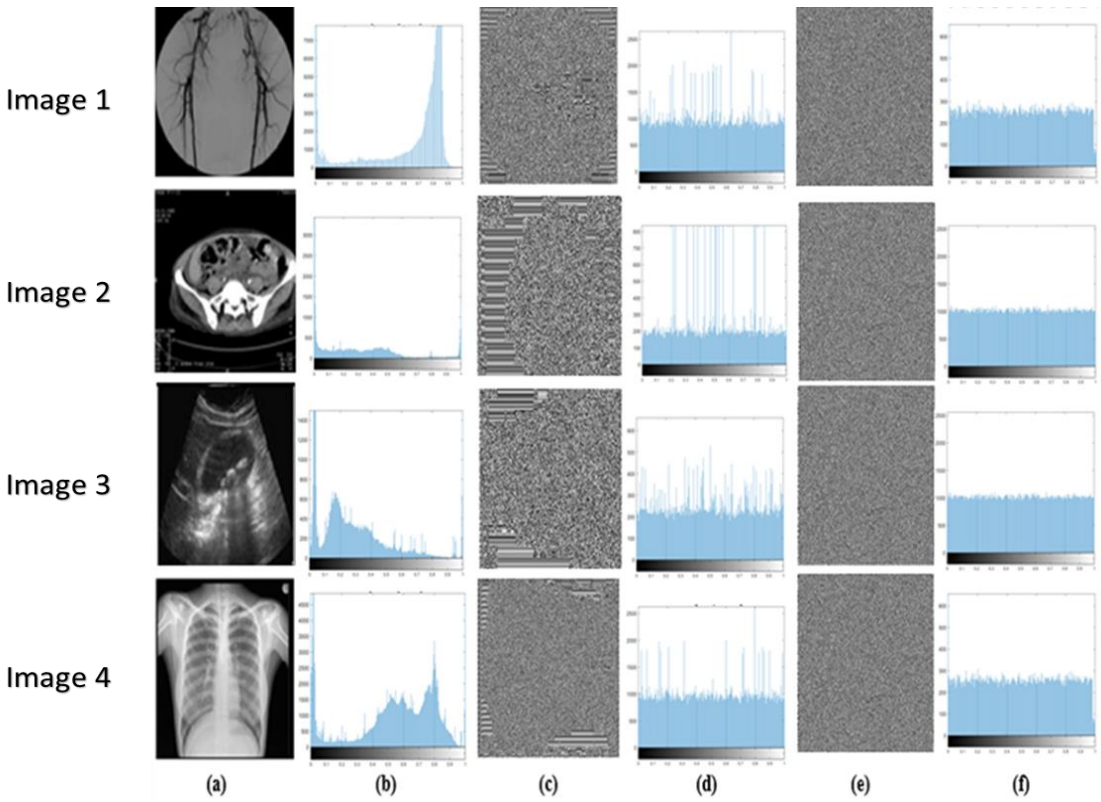

FIGURE 4 Encryption and Decryption images

5.2 Entropy Calculation

The primary goal of image encryption is to provide strong security against cryptanalysis. Shannon's entropy is a widely used metric for assessing encryption strength, as it measures the randomness and uncertainty of pixel intensity distributions.

$$H = -\sum_{K=0}^{g-1} P(k)\ log_2\left(P(k)\right) \qquad (3)$$

Here, P(k) represents the probability of a pixel with intensity level kkk, GGG denotes the grayscale range (0–255), and HHH is the entropy measure. Table 1 compares the entropy of original and encrypted images using AES and the proposed RC6–Henon scheme. The results show that the proposed method achieves higher entropy than AES, indicating stronger randomness. Additionally, dividing the image into multiple sub-blocks before scrambling further improves encryption performance and security.

In Table 2, we analyze the entropy values alongside multiple modern algorithms and the proposed method. The finding supports the idea that the RC6 + Henon Chaotic Map Method has the highest value of entropy, thus increasing its resistance to statistical attacks. As can be noted in Tables I and II, the suggested method continues improving upon other methods in high entropy and enhanced security attributes.

Table 1 Comparison between images with AES and proposed algorithms

Image	Plain Image	Cipher Image (AES)	Cipher Image (Proposed: RC6 + Henon)
1.	4.1205	6.0129	7.9835
2.	5.8710	6.7214	7.9945
3.	2.3445	6.8682	7.9967
4.	5.8712	6.5910	7.9835

Table 2 Entropy comparison with different algorithms

Reference	Entropy Value
[24]	7.997
[25]	7.991
[26]	7.998
[27]	7.990
Proposed (RC6 + Henon)	7.999

The proposed encryption scheme achieved entropy values close to this ideal, confirming high security.

5.3 Correlation Coefficients

Correlation analysis helps examine the independence level of a given condition with predetermined factors [28], in the images and their corresponding encryptions. An image should yield a low correlation on the amount of adjacent pixels in the encrypted image, so that the structure of the initial picture is unrecognizable [16]. This relationship is measured with the cross-correlation coefficient, and mathematically it can be expressed as [17]:

$$C = \frac{n\sum_i x_i y_i - \sum_i x_i \sum_i y_i}{\sqrt{(\sum_i x_i^2) - (\sum_i y_i^2)}} \qquad (4)$$

C represents the correlation coefficient, n is the total number of pixels in the image, xi is the intensity pixel in the original image, and yi is the intensity pixel of the corresponding encrypted image.

The values of correlation coefficients between the original images and their AES-encrypted versions, as well as those encrypted using the proposed RC6 + Henon chaotic map, are illustrated in Table 3. The results determine that the proposed technique performs much lower, suggesting that the encrypted images exhibit a more random and unpredictable structure compared to encrypted images with the AES algorithm in terms of correlation values.

Table 3 Correlation coefficients

Im.	Original Image (H)	Original Image (V)	Original Image (D)	AES Encrypted (H)	AES Encrypted (V)	AES Encrypted (D)	Proposed Encrypted (H)	Proposed Encrypted (V)	Proposed Encrypted (D)
1	0.8575	0.7647	0.7328	0.0417	0.0263	0.0056	0.0017	-0.0071	-0.0084
2	0.9823	0.9793	0.9605	0.0135	0.0052	0.0157	0.0014	0.0023	-0.0056
3	0.9140	0.8956	0.8616	0.0108	0.0097	0.0152	-0.0214	-0.0093	0.0063
4	0.9815	0.9871	0.9678	0.0017	0.0051	0.0034	0.0015	0.0025	–0.0055

The low correlation coefficients that obtained from the proposed method determine that the pixel intensities in the ciphered images are very uncorrelated, confirming that the RC6 and the Henon chaotic map approach provide a stronger security comparing with AES aproch. This randomness is definitive in avoiding statistical attacks and to ensure the confidentiality of the medical images. Table 4 presents the correlation coefficients between various widely

used encryption methods with the proposed approach. As realized, the proposed approach achieves good results and validates its effectiveness in decorating image pixels and preventing statistical patterns.

Table 4 Correlation coefficients of the encrypted images by using different algorithms

References	H	V	D
[31]	0.0092	0.0203	-0.0073
[32]	0.0086	-0.0027	-0.0013
[33]	-0.0021	0.0027	-0.00032
Proposed (RC6 + Henon)	-0.0142	0.0018	-0.0015

The medical images naturally hold a strong correlation between the adjacent pixels. The proposed approach reduces that between neighboring pixels, as shown in Fig. 5, to ensure better security against variance attacks.

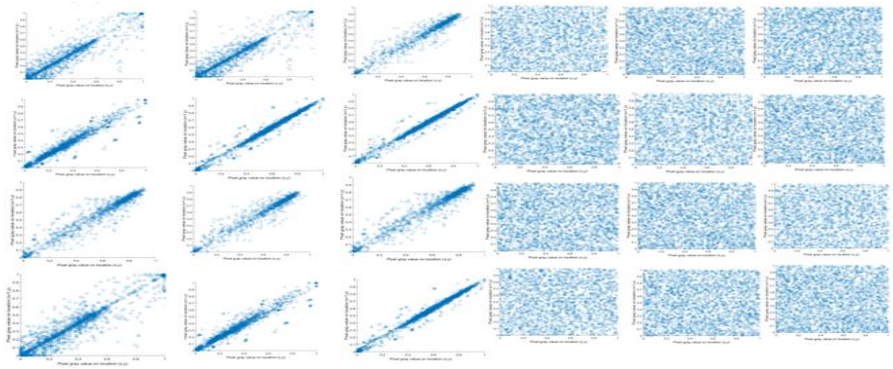

FIGURE 5 Comparison of adjacent pixel correlation distributions for the original image and its encrypted versions using AES and the proposed method

5.4 Key Sensitivity Analysis

The critical characteristic of any encryption scheme is the robustness and unpredictability of its secret keys [34]. The encryption algorithm must exhibit an appropriately large key space to resist brute-force attacks [35]. The proposed encryption scheme integrates the Henon chaotic map and the RC6 block cipher to contribute to the vastness and complexity of the key space. The Henon map introduces two control parameters, x0 and a, that represent the double precision floating point numbers, and resilient approximately 1014 possible values for each parameter. Therefore, the chaotic key space alone approximates to (1014)2 = 1028 ≈ 293.

Compared to AES (2^{128}), RC6 uses a 512-bit user-defined key, expanding the key space to about 2^{221} and significantly enhancing resistance to brute-force attacks. Key sensitivity is confirmed, as slight changes (10^{-10}) in Henon parameters cause decryption failure and severe distortion, demonstrating high sensitivity to initial conditions and strong security [18].

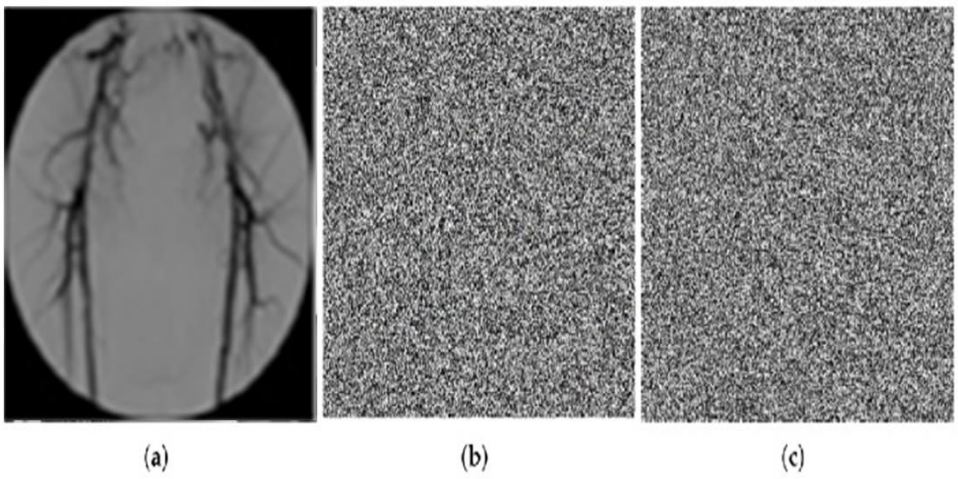

FIGURE 6 Key sensitivity analysis of the proposed algorithm. (a) Decrypted image using the correct key. (b) Decrypted image with x0+10−10. (c) Decrypted image with a+10−10

6. Conclusions

This study introduces a hybrid image encryption scheme that combines the RC6 block cipher with the Henon chaotic map to achieve high security and efficiency. RC6 improves confusion and diffusion, while the Henon map enhances key nonlinearity and unpredictability. Experimental results show superior histogram uniformity, reduced pixel correlation, high entropy (≈7.999), and strong key sensitivity compared with AES-based methods. The large key space ($\sim 2^{221}$) provides strong resistance to brute-force attacks, and even slight key variations cause decryption failure. Overall, the proposed approach offers an effective solution for the secure transmission and storage of medical images in modern healthcare systems.

FUNDING

None

ACKNOWLEDGEMENT

The authors would like to thank the anonymous reviewers for their efforts.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

[1] S. Jiang and E. Kumar, "Investigation of Biomedical Cell Image Cryptography Based on RC4 Technique," bioRxiv, pp. 2012–2023, 2023. https://doi.org/10.1101/2023.12.29.573618

[2] N. H. Hussein, "Digital Image Authentication Algorithm Based on Fragile Invisible Watermark and MD-5 Function in the DWT Domain," Journal of Engineering, vol. 21, no. 04, pp. 21–41, 2015. https://doi.org/10.31026/j.eng.2015.04.02

[3] N. M. Ghadi and N. H. Salman, "Deep learning-based segmentation and classification techniques for brain tumor MRI: A review," Journal of Engineering, vol. 28, no. 12, pp. 93–112, 2022. https://doi.org/10.31026/j.eng.2022.12.07

[4] S. P. Raja, "Secured medical image compression using DES encryption technique in Bandelet multiscale transform," Int J Wavelets Multiresolut Inf Process, vol. 16, no. 04, p. 1850028, 2018. https://doi.org/10.1142/s0219691318500285

[5] R. Guesmi and M. A. Ben Farah, "A new efficient medical image cipher based on hybrid chaotic map and DNA code," Multimed Tools Appl, vol. 80, pp. 1925–1944, 2021.

[6] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A robust chaos-based technique for medical image encryption," IEEE Access, vol. 10, pp. 244–257, 2021. https://doi.org/10.1109/access.2021.3138718

[7] A. Belazi et al., "Improved Sine-Tangent chaotic map with application in medical images encryption," Journal of Information Security and Applications, vol. 66, p. 103131, 2022. https://doi.org/10.1016/j.jisa.2022.103131

[8] M. I. M. Al-Khuzaay and W. A. M. Al-Jawher, "New Proposed Mixed Transforms: CAW and FAW and Their Application in Medical Image Classification," International Journal of Innovative Computing, vol. 13, no. 1–2, pp. 15–21, 2022. https://doi.org/10.11113/ijic.v13n1-2.414

[9] A. Z. Hussain and M. A. A. Khodher, "Medical image encryption using multi chaotic maps," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 21, no. 3, pp. 556–565, 2023.

[10] S. A. Prakash, A. G. Kumar, L. Anandavel, and A. L. Narayanan, "Selective Encryption using Segmentation Mask with Chaotic Henon Map for Multidimensional Medical Images," arXiv preprint arXiv:2403.04781, 2024.

[11] R. Donev, A. Alsadoon, P. W. C. Prasad, A. Dawoud, S. Haddad, and A. Alrubaie, "A novel secure solution of using mixed reality in data transmission for bowel and jaw surgical telepresence: enhanced rivest cipher RC6 block cipher," Multimed Tools Appl, vol. 80, pp. 5021–5046, 2021. https://doi.org/10.1007/s11042-020-09934-y

[12] V. T. Hoang and P. Rogaway, "On generalized Feistel networks," in Annual Cryptology Conference, Springer, 2010, pp. 613–630.

[13] C. S. Hsu, Cell-to-cell mapping: a method of global analysis for nonlinear systems, vol. 64. Springer Science & Business Media, 2013.

[14] V. Rathore and A. K. Pal, "An image encryption scheme in bit plane content using Henon map based generated edge map," Multimed Tools Appl, vol. 80, no. 14, pp. 22275–22300, 2021.

[15] S. Roy, K. Bhalla, and R. Patel, "Mathematical analysis of histogram equalization techniques for medical image enhancement: a tutorial from the perspective of data loss," Multimed Tools Appl, vol. 83, no. 5, pp. 14363–14392, 2024.

[16] X. Tong et al., "Image registration with Fourier-based image correlation: A comprehensive review of developments and applications," IEEE J Sel Top Appl Earth Obs Remote Sens, vol. 12, no. 10, pp. 4062–4081, 2019.

[17] N. Moriya, "Noise-related multivariate optimal joint-analysis in longitudinal stochastic processes," Progress in applied mathematical modeling, pp. 223–260, 2008.

[18] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," Signal Process Image Commun, vol. 80, p. 115670, 2020. https://doi.org/10.1016/j.image.2019.115670