**HYBRID IMAGE ENCRYPTION USING CHAOS MAPS AND DNA ENCODING**

Harshini J  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

Gerina Mary C  
line 2: *dept. name of organization*  
*(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCIDHarini V K  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

Renuka Devi S  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCIDNavnita  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

line 1: 6th Given Name Surname  
line 2: *dept. name of organization   
(of Affiliation)*  
line 3: *name of organization   
(of Affiliation)*line 4: City, Country  
line 5: email address or ORCID

*Abstract*— The exchange and capacity of large, digital images have gotten to be more troublesome due to the expanding sum of multimedia information on systems. This paper presents a novel approach for encrypting images by integrating chaos systems with DNA encoding techniques. Henon map and Lorenz system are used to generate random, chaos sequences for encrypting the pixel values in digital images. DNA encoding is used to convert the pixel values to complex DNA sequences to increase the security level and reduce the space required to store the image, differing from traditional cryptographic techniques like RSA and DES. This hybrid approach combines the power of chaos systems with the biological security paradigm provided by DNA encoding, resulting in a robust encoding scheme. The proposed method is very sensitive to the initial conditions and resistant to common encryption attacks, and the entropy and correlation are significantly better than the traditional encryption methods. This work provides an opportunity to develop relatively secure encryption methods suitable for applications that require data confidentiality and integrity.

Keywords—Image Encryption, Henon Map, Lorenz System, DNA Encoding

# Introduction

The project aims to develop a hybrid encryption technique that will provide a new paradigm of encryption. It tries to synergize two very different methodologies, chaotic maps and DNA encoding, in an attempt to come up with something that may go beyond the standard approaches to encryption to better assure data security against increasing cyber threats. Chaotic cryptology is based on mathematical chaos theory. By further exploiting the intrinsic unpredictability and complexity of chaotic maps, such as the very famous Lorenz system and the efficient Hénon map, we endow the process of encryption with unrivaled levels of randomness and obfuscation. In this mathematical basis, the resilience toward interception and decrypting attacks by adversaries is guaranteed for the protected data transmission and secured. Complementary to chaotic cryptography, DNA cryptography adds a completely new dimension to our hybrid encryption scheme. We conceal data using a DNA sequence's complex pattern and huge potential, emulating in some feel the conventional cryptographic algorithms like RSA and DES. Instead, this kind of biological encryption offers better security and variations in the face of encryption that make it extremely hard to decrypt the data without appropriate keys. Our hybrid encryption methodology seamlessly integrates chaotic maps and DNA encoding in this paper, hence changing the face of data security. It brings together the strength of chaotic systems and the biological complexity of DNA to give organizations and any individual a robust defence against cyber threats, so that, in this scarily connected world, they may be better protected against cyber threats.

# literature survey

The paper by Zhang, Liu, and Zou [1] presents a novel image encryption method that integrates the improved Lorenz chaotic system and Galois field operations. Within the broader context of image encryption techniques, this work builds upon the rich literature investigating the use of chaotic systems and mathematical operations for securing digital images. Chaotic systems, such as the Lorenz system, offer inherent properties of unpredictability and sensitivity to initial conditions, which have been extensively explored in encryption schemes to enhance security. Similarly, Galois field operations provide a mathematical framework for performing arithmetic operations on binary data, facilitating diffusion processes crucial for encryption. Recent advances in image encryption have emphasized the integration of multiple cryptographic primitives to achieve higher levels of security and efficiency, addressing challenges such as computational complexity and resistance to cryptanalysis. The proposed method contributes to this ongoing research by offering a hybrid approach that leverages the strengths of chaotic systems and Galois field operations, aiming to strike a balance between security, efficiency, and robustness. This work underscores the interdisciplinary nature of cryptographic research and the importance of innovative techniques in addressing the evolving threats to image security.The paper by Guodong Ye et al. [2] introduces a novel image encryption scheme that combines blind signature and an improved Lorenz system. This approach addresses the challenges associated with traditional encryption methods by leveraging chaotic systems and blind signature techniques. Through extensive experimentation and testing, the authors demonstrate the effectiveness of their scheme in resisting common attacks and ensuring robust security for image communication. The security analyses conducted encompass various aspects such as histogram analysis, correlation coefficients, information entropy, sensitivity analysis, differential attack analysis, robustness analysis, and normalized correlation analysis. These analyses collectively highlight the scheme's capability to provide secure encryption while maintaining the integrity and confidentiality of images. This innovative approach offers valuable insights for researchers and practitioners in the field of cybersecurity and image processing.The paper [3] proposes a Hybrid Adaptive Image Encryption (HAIE) scheme that uses statistical parameters like mean and variance to modify initial conditions and control parameters. This scheme generates pseudo-random sequences using two chaotic maps (logistic and tent), encodes them into DNA sequences, then applies the same algorithm to decode them. Against assaults, the algorithm is quite resilient. The suggested technique was also shown to be adaptive and resistant to known and deliberate plaintext assaults.The paper by C. Zou et al. [4] presents an image encryption method based on the Improved Lorenz System. The authors introduce the Lorenz system and its limitations in image encryption, motivating the need for improvements. They propose an enhanced version of the Lorenz system to address these limitations, leveraging its complex kinetic properties for more effective image encryption. The encryption algorithm involves diffusion, permutation, and confusion techniques to ensure robust security. The decryption procedure reverses the encryption process using formulas to remove diffusion effects, eliminate column and row confusion, and reconstruct the original image. The experimental results demonstrate the effectiveness of the proposed scheme in encrypting various types of images into random-like cipher-images, with high security levels validated through key sensitivity tests, statistical analyses, and resistance to attacks such as differential attacks and data loss. The paper contributes to the field of image encryption by providing a method that enhances security while maintaining efficiency, as evidenced by its performance in various experiments and analyses.The paper by Bhat Jasra and Ayaz Hassan Moon [5], presents a comprehensive investigation into color image encryption and authentication using dynamic DNA encoding and hyperchaotic systems. Drawing upon three distinct parts, the study delves into the integration of these advanced techniques to address the pressing challenges of data security and integrity in digital image processing. The authors explore the foundational principles of DNA computing and its potential applications in encryption, laying the groundwork for the subsequent sections. In, they delve into the intricacies of hyperchaotic systems, elucidating their chaotic dynamics and highlighting their suitability for cryptographic purposes. Finally, synthesizes these concepts, proposing a novel framework that synergistically combines dynamic DNA encoding with hyperchaotic systems to achieve robust image encryption and authentication. By leveraging the unique properties of DNA and hyperchaotic dynamics, the proposed approach offers enhanced security, resilience against attacks, and potential for real-world implementation in secure image communication systems. Through a meticulous synthesis of theoretical foundations and practical applications, the paper contributes significantly to the evolving landscape of image encryption and authentication methodologies.The two primary phases of the suggested scheme were DNA diffusion and chaotic key generation, as described in article [6]. First, the plain medical picture is subjected to the message digest algorithm 5 hash function. The hash value is then employed, together with the value of an input ASCII string, to establish initial conditions and control parameters for two chaotic systems (Bernoulli shift map and Zigzag map). Two distinct key matrices are then generated from these chaotic systems. Second, the encryption image is created via a row-by-row diffusion process employing the DNA XOR algebraic operation in an alternating pattern between the plain image matrix and the two chaotic key matrices. The rules for each row's DNA encoding and decoding are chosen using the logistic map.It was discovered that this suggested scheme was strong and impervious to several types of assaults.A picture encryption technique based on one-dimensional logistic maps, DNA encoding sequences, and multi-objective particle swarm optimization (MOPSO) is studied in paper [7]. The sub-key sequence chosen via particle swarm optimization (PSO), the plaintext image's hash value, and the shuffle mark bit made up the paper's key. Using a logistic map and DNA encoding, random DNA mask pictures were produced. then employed it in conjunction with the block-shuffled plaintext DNA encoding sequence to function as an encryption mechanism. Based on the information entropy and correlation coefficient, the iterative PSO method was assumed. In PSO, the location value of a particle indicates a position of the plaintext picture. The optimal ciphertext was eventually discovered, and it now yields the value of the best particle available. Excellent ciphertext entropy and correlation coefficient, as well as superior encryption effectiveness against a variety of common attacks, were demonstrated by simulation experiments and security analyses.The paper by B. Rahul, K. Kuppusamy, and A. Senthilrajan [8], presents a comprehensive image encryption scheme employing dynamic DNA cryptography, multiple chaotic maps, and the SHA-256 hash function. Beginning with an overview of existing encryption techniques, the paper delves into the theoretical foundations of chaotic maps and DNA encoding. It then details the proposed encryption algorithm, highlighting its use of chaotic sequences for pixel encoding and its dynamic key generation to thwart brute-force attacks. The study evaluates the scheme's security and efficiency through extensive testing, including sensitivity analyses to plaintext and keys, computational complexity assessments, and execution time analyses. Notably, the proposed scheme demonstrates improved performance metrics compared to existing algorithms, exhibiting faster execution speeds, lower computational complexities, and heightened sensitivity to both plaintext and keys. The paper concludes by outlining future research directions aimed at further streamlining key generation procedures to enhance encryption speed.In the paper[9], the Chen chaotic system is used to generate random sequences, which are then used to form arrays for key stream creation and picture permutation. Two distinct uses for these random sequences eliminate the need for separate computation times. Time complexity therefore diminishes. For the purpose of picture permutation, each color component of the plain image is transformed into a one-dimensional vector, and the permutation is carried out utilizing the chaotic arrays that are produced. A picture of chaos is created from the created key stream. Next, equal chunks of the chaotic picture and the permuted image are separated. DNA principles are used to encode the plain image blocks. With the use of a three-dimensional logistic map, the encoding rules are randomly selected.Ultimately, the encrypted picture is obtained by combining all of the encrypted blocks. The suggested strategy has a vast key space and is robust to various assaults, according to experimental data.A revised version of Rubik's Cube approach was developed by Abdullatif, A. A., F. A., & Naji, S. A. in their paper [10] for quickly creating uncertainty by scrambling the pixels in colored images. Using this method, the color channels are also jumbled in addition to the pixel positions. Following that, the values of the pixels are encrypted using the dynamic DNA encoding process. Together with a secret key, DNA encoding rules are employed. Our suggestion is to choose the DNA rules on-the-fly to improve security. This system's capability is evaluated using five fidelity measures. SSIM, NPCR, Entropy, CCA, and PSNR are these. The findings show that by improving the encryption image's confusion and dispersion qualities, the suggested solution strengthens the criteria for general security.Kumar, K., Roy, S., Rawat, U., & Malhotra, S., in their paper [11]. suggested an image cipher for color picture encryption that leverages Arnold's cat map and the logistic map. This study proposes an efficient image encryption method called IEHC that uses two chaotic maps. It also introduces a unique shuffling mechanism to scramble the pixels of an input color image. It effectively encrypts the plain photos while utilizing the features of Arnold's Cat map [6] and the Logistic Map [5]. Furthermore, a unique shuffling mechanism has also been presented to guarantee good confusion property throughout the encryption process. To safeguard digital medical pictures, Paper [12] discusses an encryption technique based on integer wavelet transform (IWT) combined with chaos and deoxyribonucleic acid (DNA). There are two stages to the suggested work: a diffusion phase and a two-stage shuffle phase. Block confusion is the first step of shuffling, while row and column shuffling of pixels is the second stage. At the initial step of diffusion, the shuffled image's pixels are bitwise rotated in a circle to strengthen the system's defense against differential attacks. DNA XOR and DNA coding operations provide the foundation of the second stage of diffusion operation.To assess the robustness of the method against statistical and differential assaults, experimental investigations were conducted using 100 DICOM test pictures with a 16-bit depth. As can be seen from the findings, our method outperforms several other cutting-edge methods, with an average maximum entropy of 15.79, an NPCR of 99.99, a UACI of 33.31, and a bigger keyspace of 10140.In article [13], a random number generator for cryptographic purposes is constructed by combining the extremely chaotic properties of hybrid chaos maps with neural networks. To make the generator more random, a custom neural network with a user-defined layer transfer function is constructed. To achieve high unpredictability, the control parameters and iteration value of the two-hybrid chaotic map are developed as a layer transfer function in this study. Using the recovered sequences and deoxyribonucleic acid encoding technology, color picture encryption is carried out. The generator is put through a number of tests, including the NIST, attractor test, and correlation, to see how random it is. The strength of the encryption method is demonstrated by simulation analyses such as keyspace, key sensitivity, statistical, differential analysis, and chosen-plaintext assault.A recently created evolutionary-based picture encryption technique is examined in the work [14]. A unique picture encryption technique is suggested, which is based on a hybrid model of genetic algorithm (GA), logistic map, and deoxyribonucleic acid (DNA) masking. In this work, the number of initial DNA masks is generated using logistic map functions and DNA, and the optimal mask for encryption is determined using a genetic algorithm. Enhancing the quality of DNA masks to find the best mask that works with simple photographs is this method's main benefit.It was noted that a logistic map and DNA sequence are used to create several DNA masks during the algorithm's initial phase. Subsequently, the GA determines the optimal DNA mask for encryption through an evolutionary process.The suggested scheme not only exhibits good encryption but also withstands a variety of common assaults, as confirmed by the experimental findings and computer simulations.Guesmi, R., & Farah, M. B. proposed a unique medical picture encryption method in the publication [15]. It is based on a new hybrid chaotic map, a secure hash technique called SHA-2, and a hybrid model of deoxyribonucleic acid (DNA) masking. Their research strengthened the cryptosystem by utilizing the chaotic hybrid map, DNA sequences, and operations. This approach's main benefits were achieving solid experimental findings, withstanding common assaults, and increasing information entropy—the most crucial aspect of randomness. The technique has a wide key space, a high key sensitivity, increases ciphertext security, improves encoding efficiency, and can withstand statistical and exhaustive assaults, according to theoretical analysis and experimental findings.

# Proposed WORK

The Lorenz system is used in this code for encryption and decryption of the images. This system, which is, in fact, indicated by three coupled nonlinear differential equations and erratic behavior, is useful and disadvantageous at the same time in cryptographic applications. One of them is the fact that it is inherently statistical, producing sequences that are difficult to predict and carrying seeming statistical randomness useful in the creation of codes. Also, Lorenz system is sensitive to the initial conditions, thus adding cryptographical appeal to the fact that even a small difference in input parameters will produce drastically different results. However, its sensitivity is also a problem, since even a slight change in the parameter of the system causes a decryption to fail or could result to a completely different decrypted image. Moreover, the solutions for the differential equations used in encryption and decryption functions may add more time for real time processing or may not be efficient in scalability if the resources are low. Nonetheless, the analysis has shown that due to its high sensitivity to initial conditions and effective encryption properties the Lorenz system can be effectively used in cryptographic tasks.  
The Henon map is similar to the Lorenz system, and for the same reason used for cryptographic applications because of chaotic nature and great sensitivity to initial conditions. This is an iterative two-dimensional equation which creates complex and rather chaotic sequences, which are highly appropriate for encryption. Its sensitivity implies that small changes in input parameters produce highly dissimilar outputs, thus adding on to the encryption’s resistance against predictive attacks. However, this sensitivity present some difficulties for it, because small changes in parameters of used systems can lead to inability to decrypt necessary information or, on the opposite, lead to radical changes in decrypted data. Further, the process of iterating the Henon map can take significantly longer especially if up real time, performing and computation resource limited environment. Nonetheless, because of the chaotic nature of the Henon map and its ability to generate robust encryption it can be used as a cryptographic tool although this will demand high computation and stability.

DNA encoding holds great opportunities for achieving image encryption and decryption in cryptography in terms of the capacity, complexity, and stability of DNA storage. Thus, on the one hand, DNA has the potential to store amounts of information in a very small space, which makes it possible to use it for the safe encryption of large image files. Furthermore, inherent randomness in cases of DNA sequences makes them extremely hard to hack and the redundancy in cases of replication processes help in natural error correction. Nevertheless, there is the problem of high costs and difficulty to synthesize DNA, relative to information encoding and decoding rates, and ethical issue to do with the privacy of genetic information. Nevertheless, DNA-based cryptography has a relative potential to improve the data security field in image encryption context.

A) Encryption with Hénon map and DNA encoding  
The Hénon map is a discrete, iterative transformation of the plane that has a complex behaviour and is frequently used for the generation of chaotic sequences. It is defined by the following equations:It is defined by the following equations:

*xn+1 = 1 – axn2 + yn*

*yn+1 = bxn*

where *xn* and *yn* are the current coordinates of the systems a and b are constant that define the behavior of the system.  
The Hénon map also encodes a DNA sequence if a chaotic sequence is generated with the help of it.

The chaotic sequence is in bits and there are two bits per symbol, and each of the symbols is one of the four nucleotides in DNA (A, T, C, G).

It also ensures encrypted data is in the form of ‘four letters’ of DNA and thus, cannot be decrypted in the ordinary course.  
An image taken and processed in grayscale is in the form of a two dimensional matrix.The Hénon mapping equations repeat to create a chaotic sequence. A chaotic sequence is transformed into a DNA sequence.

B) Encryption with the Lorenz system and DNA encoding

The Lorenz system is a set of three nonlinear differential equations that behave chaotically. It is defined as:

*x' = σ(y – x)*

*y’ = x(ρ – z) - y*

*z’ = xy - βz*

where *x*, *y*, and *z* are the state variables, and *σ*, *ρ*, and *β* are the system parameters.

Like in the case of the Hénon mapping method, the obtained chaotic sequence of the Lorenz system is converted into a DNA sequence.

A general grayscale image is converted to a 2D matrix or array. Chaotic sequence generation: One gets a sequence of numbers which is chaotic, where the Lorenz system equations are solved numerically. A rather random string is switched to the DNA chain.

C) Decryption

Decryption is the process of using the inverse of the encryption steps, or algorithm.

For this reason, the DNA sequence is decoded back into the chaotic sequence to present the original chaotic values.

Through the utilization of a chaotic sequence, as well as a related chaotic system (Hénon map or Lorenz system over a given time then encrypted picture is decrypted using the XOR technique with the result derived from the previous step.

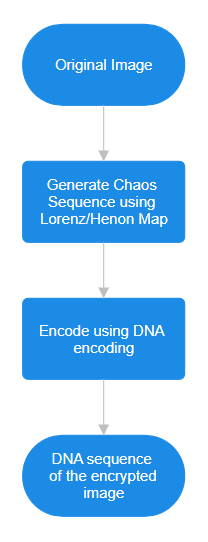


Fig 1. *encryption and encoding process*

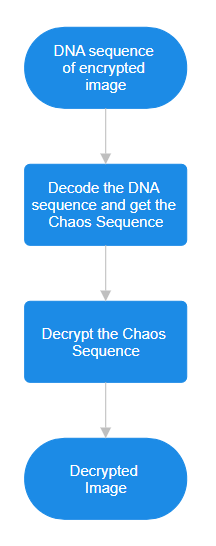


Fig 2. *Decryption and decoding process*

# RESULTS

The Hénon map successfully generated chaotic sequences, providing a high level of randomness for encryption as shown in Fig 4. DNA encoding effectively represented chaotic sequences, ensuring data was securely transformed into DNA sequences. Image encryption using the combination of Hénon map and DNA encoding resulted in robust protection against traditional decryption methods. Computational overhead for encryption was manageable, allowing for practical implementation.

The Lorenz system produced chaotic sequences with inherent unpredictability, enhancing encryption strength as shown in Fig 5. DNA encoding accurately represented chaotic sequences, ensuring secure transformation into DNA sequences. Image encryption using the Lorenz system and DNA encoding offered a formidable defense against decryption attempts. Computational resources required for encryption were within reasonable limits, enabling efficient implementation.

DNA decoding successfully restored chaotic sequences from DNA sequences, facilitating decryption. The XOR technique with chaotic sequences effectively decrypted images encrypted using both the Hénon map and the Lorenz system. Decryption processes were computationally feasible, allowing for the timely restoration of encrypted images.



Fig 3. Grayscale image before encryption

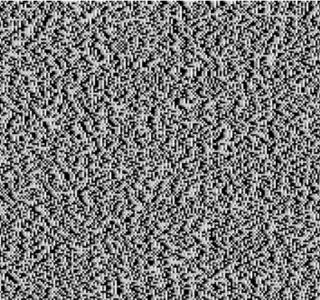


Fig 4. Image after encryption using henon map



Fig 5. Image after encryption using Lorenz map



Fig 6. Image after decryption

# CONCLUSION

The hybrid encryption methodology, combining chaotic maps (Hénon map and Lorenz system) with DNA encoding, demonstrated significant advancements in data security.By leveraging chaotic dynamics and DNA's inherent complexity, the proposed encryption framework offered robust protection against evolving cyber threats. The integration of chaotic systems and DNA encoding diversified the encryption landscape, presenting a formidable defense against traditional decryption methods. Practical implementation of the hybrid encryption technique is feasible, with manageable computational overhead and efficient decryption processes. Future research should focus on optimizing encryption and decryption algorithms, addressing scalability concerns, and exploring real-world applications of the proposed methodology to further enhance data security in diverse environments

# REFERENCES

[1] Xuncai Zhang, Guanhe Liu, Chengye Zou, An image encryption method based on improved Lorenz chaotic system and Galois field,Applied Mathematical Modelling,Volume 131,2024,Pages 535-558,ISSN 0307-904X , <https://doi.org/10.1016/j.apm.2024.04.023>. (<https://www.sciencedirect.com/science/article/pii/S0307904X24001720>)

[2] Guodong Ye, Huishan Wu, Min Liu, Yang Shi,Image encryption scheme based on blind signature and an improved Lorenz system,Expert Systems with Applications,Volume 205,2022,117709,ISSN 0957-4174 , <https://doi.org/10.1016/j.eswa.2022.117709>. (<https://www.sciencedirect.com/science/article/pii/S0957417422009964>)

[3] Mansoor, S., & Parah, S. A. (2023). HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing. *Multimedia Tools and Applications*, *82*(19), 28769-28796.

[4] C. Zou, Q. Zhang, X. Wei and C. Liu, "Image Encryption Based on Improved Lorenz System," in IEEE Access, vol. 8, pp. 75728-75740, 2020, doi: 10.1109/ACCESS.2020.2988880.

[5] Bhat Jasra, Ayaz Hassan Moon,Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system,Expert Systems with Applications,Volume 206,2022,117861, ISSN 0957-4174, <https://doi.org/10.1016/j.eswa.2022.117861>. (<https://www.sciencedirect.com/science/article/pii/S0957417422011162>)

[6] Dagadu, J. C., Li, J. P., & Aboagye, E. O. (2019). Medical image encryption based on hybrid chaotic DNA diffusion. *Wireless Personal Communications*, *108*, 591-612.

[7] Wang, X., & Li, Y. (2021). Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. *Optics and Lasers in Engineering*, *137*, 106393.

[8] B. Rahul, K. Kuppusamy, A. Senthilrajan,Dynamic DNA cryptography-based image encryption scheme using multiple chaotic maps and SHA-256 hash function,Optik,Volume 289,2023,171253, ISSN 0030-4026, <https://doi.org/10.1016/j.ijleo.2023.171253>.

[9] Yaghouti Niyat, A., & Moattar, M. H. (2020). Color image encryption based on hybrid chaotic system and DNA sequences. *Multimedia Tools and Applications*, *79*(1), 1497-1518.

[10] Abdullatif, A. A., Abdullatif, F. A., & Naji, S. A. (2019). An enhanced hybrid image encryption algorithm using Rubik’s cube and dynamic DNA encoding techniques. *Periodicals of Engineering and Natural Sciences*, *7*(4), 1607-1617.

[11] Kumar, K., Roy, S., Rawat, U., & Malhotra, S. (2022). IEHC: An efficient image encryption technique using hybrid chaotic map. *Chaos, Solitons & Fractals*, *158*, 111994.

[12] Ravichandran, D., Banu S, A., Murthy, B. K., Balasubramanian, V., Fathima, S., & Amirtharajan, R. (2021). An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. *Medical & biological engineering & computing*, *59*, 589-605.

[13] Patel, S., Thanikaiselvan, V., Pelusi, D., Nagaraj, B., Arunkumar, R., & Amirtharajan, R. (2021). Colour image encryption based on customized neural network and DNA encoding. Neural Computing and Applications, 33(21), 14533-14550.

[14] Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering*, *56*, 83-93.

[15] Guesmi, R., & Farah, M. B. (2021). A new efficient medical image cipher based on hybrid chaotic map and DNA code. Multimedia tools and applications, 80, 1925-1944.