Indian Journal of Computer Science and Technology
Special Issue, Volume 5, Issue 1 (January-April 2026), PP: 72-77.
https://www.doi.org/10.59256/indjcst.20260501C012
International Conference on Cyber and AI Security (ICCAIS-2026)
www.indjcst.com
ISSN No: 2583-5300

Image Encryption and Decryption Using Hybrid Algorithm

Muthyala V V S Choudhary[1], Raj Mukharjee[2], Rajamuri Shivapriya[3], Rudavath Rahul[4], Ramavath Srikanth[5]

[1, 2,3,4,5] *Department of Electronics and Communication Engineering, Teegala Krishna Reddy Engineering College (Affiliated to JNTUH) Hyderbad, Telangana, India.*

***To Cite this Article**: Muthyala V V S Choudhary[1], Raj Mukharjee[2], Rajamuri Shivapriya[3], Rudavath Rahul[4], Ramavath Srikanth[5], "Image Encryption and Decryption Using Hybrid Algorithm, Indian Journal of Computer Science and Technology Volume 05, Issue 01 (January-April 2026), PP: 72-77.*

Abstract: *The security of digital images in the transmission process has gained significant importance in recent times due to the development of online communication systems. The present paper proposes a new approach in image encryption and decryption. Generally, the approach considers the use of symmetric key encryption and decryption and asymmetric key encryption and decryption. Here, the linear combination of permutation and substitution processes has been derived. Further, the efficiency of image encryption and decryption can be tested by using various key parameters, such as entropy, NPCR, UACI, and PSNR. Evaluation of the proposed approach reveals that randomness in the encrypted images is very high, and the image can be decoded or obtained accurately during the decryption process.*

Key Words: *Data Encryption, Reversible Logic, Bit Swapping, Verilog HDL, Secure Communication, Hardware Cryptography.*

I. INTRODUCTION

The presence of digital imaging techniques in various cloud infrastructures, telemedicine, military communications, and social media has given rise to the need to ensure image transmission security. Although images do not exhibit textual data characteristics and have a high rate of redundancy, correlated pixels, and large volumes of data, conventional encryption techniques cannot be directly applied. In this context, image encryption techniques have been put in place in order to ensure maximum confusion and diffusion while remaining computationally efficient.

Chaos cryptography has captured considerable attention due to its ability to react to initial states, ergodicity, and pseudo alternating properties. Alvarez and Li, in their work [4], highlighted some basic cryptographic principles applicable to chaos cryptography systems, focusing on flexibility of keys, large keys, and resistance to statistical attacks. These principles have influenced the concept and design basis of chaotic image encryption techniques.

Recent studies combine chaotic maps with structural blocks to boost security performance. For instance, Zhang developed an encryption scheme based on a butterfly module and chaotic systems for improved performance of the permutation diffusion process [1]. Lu et al. created an efficient method using an LSS chaotic map and S box substitution to boost nonlinearity and resistance to differential attacks [5].

In addition, the approach of using combined DNA encoding and chaos techniques can also yield good results. Liu et al. [3] presented a new method of encryption for RGB image data using hyper chaos and DNA encoding. Malik et al. [2] further extended the concept by including hyper chaos and DNA computing techniques, yielding highly random and anti-differential attack resistant results. Enhanced security by using the chaos and DNA based substitute techniques is also found in [6].

A hybrid cryptographic mode of using chaotic systems along with classical block cipher has been analyzed to optimize security and computational complexity. Jolfaei and Mirghadri [7] investigated the potential of integrating chaotic systems into block cipher systems to enhance security against brute force attacks and statistical attacks while maintaining high accuracy of decryption results.

Although it is observed that these techniques show strong security properties, there are some issues that need to be addressed, i.e., efficient key management, reduced computational complexity, and robustness against new types of attacks. Keeping these issues in view, in this paper, a new hybrid approach has been suggested that focuses on image encryption and decryption through various techniques of symmetric encryption and secure key exchanges.

II. METHODOLOGY

The image encryption system proposed utilizes the concept of chaotic permutation, DNA based image diffusion, and key derivation. It is based on a Flask based web application, which allows for efficient image encryption. The proposed algorithm starts with the upload of the image to be encrypted, followed by the input of the password from the web browser. The proposed algorithm

utilizes the SHA 256 algorithm to generate the key, which is of fixed length. The key is then converted to a new parameter required for the chaotic system. Chaotic systems are widely used for image encryption due to their high sensitivity to initial parameters, which prove to be beneficial for key derivation with the pseudo random properties of chaotic systems, as shown in [4]. A logistic map based chaotic system is employed to achieve deterministic chaotic behavior, where even with a small change in the password, it corresponds to a different image encryption output.

The obtained chaotic parameters are used to generate two unique sequences. For pixel permutation, these sequences are utilized. This permutation technique is used to counteract pixel correlation, which is considered an unavoidable phenomenon in images [1], [5]. In order to achieve pixel permutation, the input RGB image is first converted into its pixel form. This pixel array is then rearranged based on another permutation index derived from the chaotic sequence, leading to pixel confusion. For diffusion purposes, another sequence is used. Once pixel permutation is achieved, the pixel values are processed further by applying DNA encoding, resulting in DNA based pixel values. In cryptographic techniques, pixels are found to exhibit improved diffusion characteristics and better ability to withstand statistical and differential attacks when processed using DNA based operations [2], [3], [6]. For DNA XOR, pixel nucleotides are processed using the XOR method between pixel nucleotides and those of the DNA key derived from the chaotic sequence.

In order to further boost the level of security, symmetric key encryption with the Advanced Encryption Standard (AES) method is implemented in Cipher Block Chaining (CBC) mode to ensure the security of the sensitive data components. The Advanced Encryption Standard is suited to ensure the confidentiality of the data, while the Cipher Block Chaining prevents the repetition of patterns among identical blocks of plaintext data. The decryption process will again involve processing the entered password through SHA 256 to produce identical chaotic parameters. The sequences of chaotic maps, XORing with DNA, and inverse permutation are applied to retrieve the original data pixels. However, to successfully retrieve the original data, the correct password is required to be input, thereby ensuring the authentication process. The encryption decryption process is implemented via a web interface developed with the Flask programming framework.

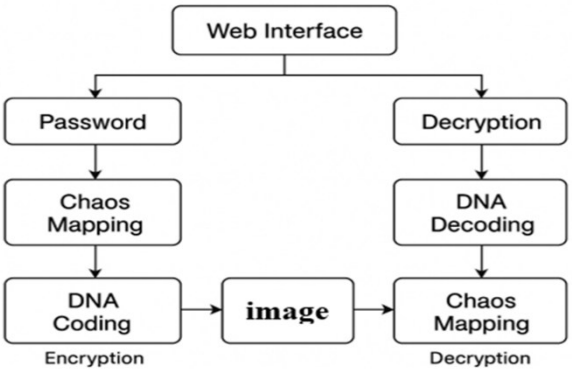

Figure 1. Block diagram of the Encryption and Decryption stages for DNA algorithm

Encryption And Decryption Working Flow

1) AES And Chaos:

The chaotic sequence is produced from the initial parameters obtained from the given password. Chaotic maps are known for their high sensitivity to the initial condition within the pseudo random properties. That is why chaotic maps are considered appropriate for enhancing the security of any given cryptosystem [4]. From the obtained chaotic sequences, the pixels are arranged prior to the AES encryption using the CBC mode. However, during the decryption of the given message, chaotic parameters will always be produced with the ability to decrypt the message as long as the correct password is used.

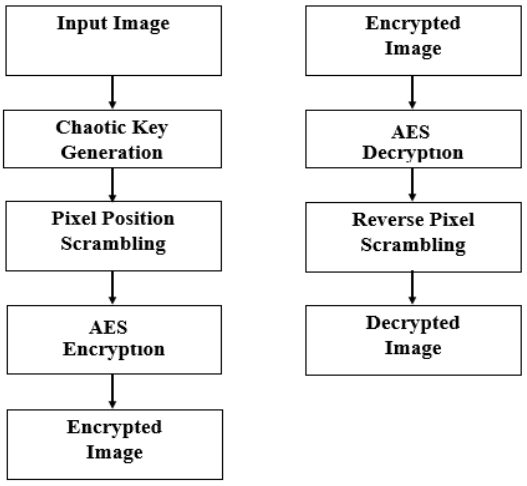

Figure 2. Working Flow of AES and Chaos Based Encryption and Decryption

2) DNA and Chaos:

The working mechanism of a Chaotic DNA system integrates two powerful computational concepts—chaotic dynamics and DNA sequence operations—to create a highly secure and unpredictable encryption environment. Chaotic systems are characterized by extreme sensitivity to initial conditions, meaning that even a tiny change in input yields vastly different output trajectories. This property enables the generation of highly random sequences that serve as dynamic keys for DNA level transformations. In a typical Chaotic DNA mechanism, the input data is first converted into binary form, then encoded into synthetic DNA sequences using a predetermined nucleotide mapping rule. Parallelly, a chaotic map such as the Logistic Map, Tent Map, Henon Map, or Lorenz System is initialized using secret keys that determine its starting state. The chaotic map generates a long sequence of chaotic values that are quantized and mapped to DNA operations. These operations may include complement, mutation, reverse, XOR, addition, subtraction, DNA shifting, or codon rearrangements. Each chaotic output dictates what transformation is applied to the DNA sequence at a specific step, ensuring that even a single modification in the initial key leads to dramatically different encrypted DNA patterns. The intertwined use of chaos and DNA results in a dual layer cryptographic shield where the chaotic map contributes high nonlinearity while the DNA operations introduce structural complexity. During encryption, the DNA sequence undergoes iterative chaotic modulation, producing an encrypted output that bears no correlation with the original data. For decryption, the system retraces the operations in reverse order using identical chaotic sequences and mapping rules. This reversible property ensures accurate data recovery while maintaining strong resistance against differential attacks, brute force attempts, statistical analysis, and chosen plaintext attacks. The chaotic DNA model thus achieves an exceptionally large keyspace, unpredictable cipher behavior, and high entropy, making it ideal for securing images, audio, video, sensor data, and real time communication streams. Its hybrid nature provides enhanced robustness compared to standalone chaotic or DNA only systems, reinforcing its importance in modern encryption technologies.

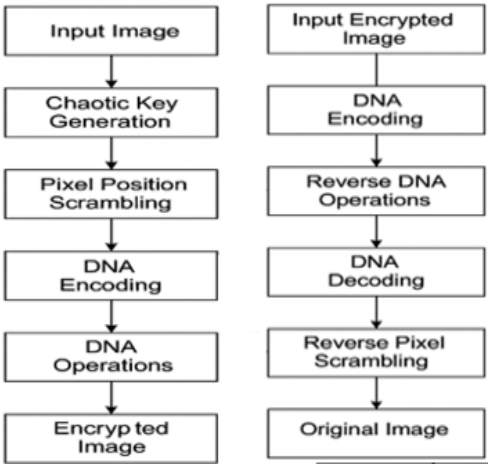

Figure 3. Working Flow of DNA and Chaos Based Encryption and Decryption

III. AES AND CHAOS BASED SYSTEM ARCHITECTURE

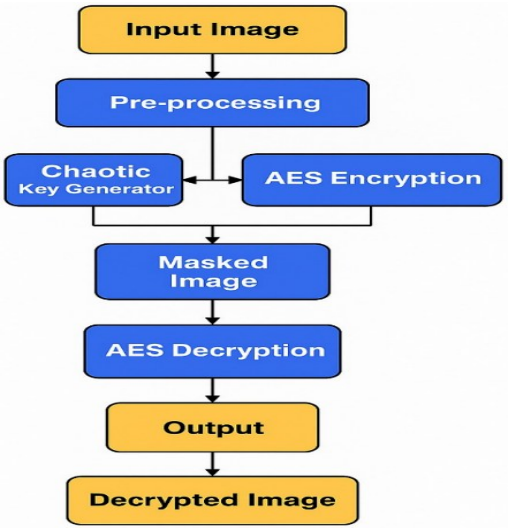

Figure 4. AES and Chaos based System architecture

The algorithm begins when the user uploads an image and provides a password, which serves as the seed for chaotic key generation. The password undergoes SHA 256 hashing to produce a fixed length, high entropy digest that ensures strong resistance against weak passwords.

This digest initializes a logistic map chaotic function, defined as

$$x_{n+1} = r x_n (1 - x_n)$$

With a control parameter r=3.99,

Which operates in the chaotic regime to generate pseudo random values. After 200 warm up iterations to eliminate transient correlations, the logistic map produces chaotic values in the range (0,1). Each chaotic value is then scaled, converted into bytes, and XORed with corresponding SHA 256 hash bytes to form a chaotic key (32 bytes) and chaotic initialization vector (IV) (16bytes). This hybrid derivation ensures that both cryptographic and chaotic properties influence the encryption parameters, creating a highly sensitive and unpredictable key structure.

The encryption process involves the Advanced Encryption Standard (AES) in Cipher Block Chaining mode, in which the plaintext is combined with the previous ciphertext or an initialization vector (IV) in the first encryption cycle before encryption actually begins. This resulting ciphertext is stored in the binary file, as well as critical metadata such as the size of the image, to ensure appropriate reconstruction during the decryption process. Also generated, as part of the encrypted set and in addition to the visual cipher representation, is the secret image, which serves to demonstrate and validate the entire process. During the decryption process itself, the password re creates the exact chaotic parameters required to encrypt the images in the first place due to the deterministic and highly sensitive nature of the logistic map function.

IV. DNA AND CHAOS BASED SYSTEM ARCHITECTURE

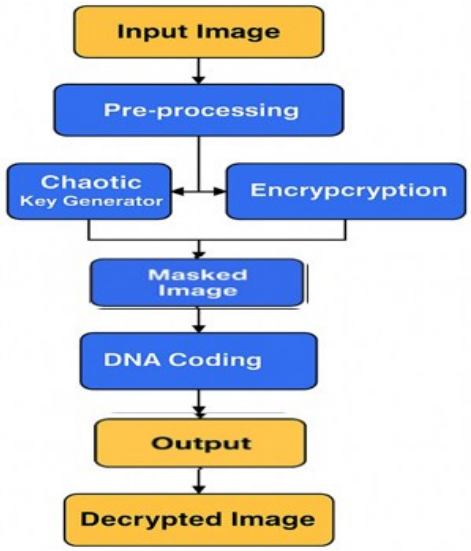

Figure 5. DNA and Chaos based System architecture

The proposed system starts with an input image, which will then go through a preprocessing stage designed to achieve better uniformity while paving the way towards safe transformation. The preprocessing may range from resizing, grayscale conversion, normalization, or even changing pixel values for achieving uniformity. All this happens in parallel, with the chaotic key generator initializing a chaotic map based on different secret values, creating very sensitive pseudo random sequences.

During the encryption stage, the preprocessed image is encoded using the generated chaotic keys. This produces a masked image whose pixel values have been significantly altered. The masked image is then encoded using DNA coding, where the pixel values of the image are converted to DNA sequences using predefined mappings of nucleotides. Operations such as complement, XOR, addition, and permutation are carried out by DNA coding, and the resulting images have enhanced confusion and diffusion.

V. PERFORMANCE METRICS

a) Encryption Strength (Key Sensitivity)

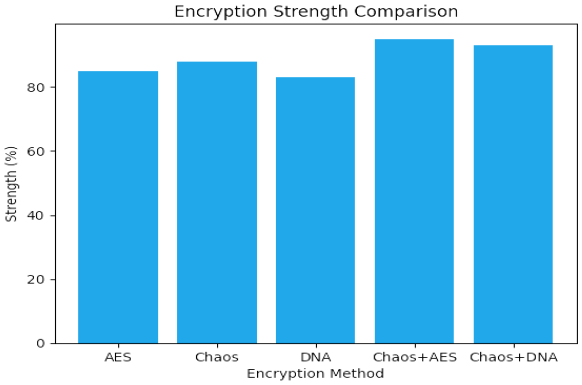

Figure 6. Encryption Strength

b) Correlation Coefficient

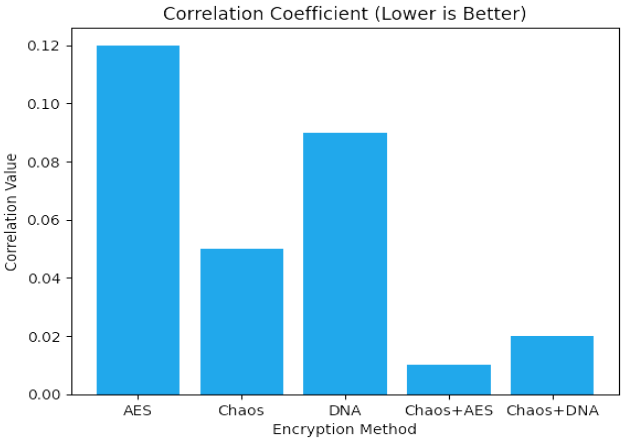

Figure 7. Correlation Coefficient

c) Resistance to Known Attacks

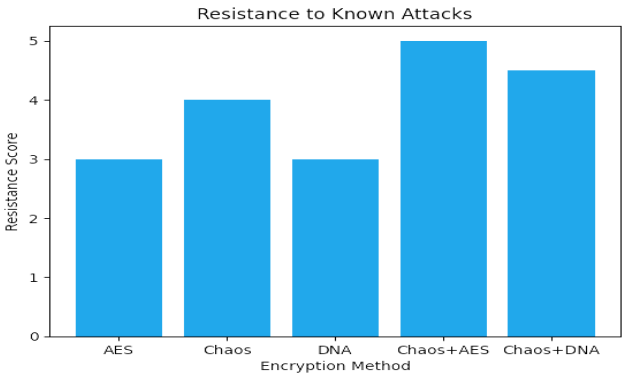

Figure 8. Resistance to known attacks

V. FUTURE SCOPE

The suggested chaos DNA based encryption framework may further be improved to introduce additional dimensional or hyper chaotic maps, as exemplified in the diagram, in order to enhance the randomness and key space. Future directions may also involve introducing dynamic coding principles that could improve the effectiveness of diffusion principles. Optimizations may be carried out, especially to cater to real time scenarios as per the suggested video encryption and IoT based secure image transmission schemes. These may further enhance the computational efficiency via hardware acceleration, such as through GPUs and FPGAs. The suggested framework may also be tested for resilience to more advanced attacks via various cryptanalytic and ML based attack scenarios.

VI. RESULT AND CONCLUSION

The project was able to demonstrate an effective and safe method of image encryption and decryption using chaos algorithm combined with the current cryptography techniques. The system was able to enhance the rate of diffusion and confusion of the encrypted images by using AES and DNA based algorithms to encrypt the image. In the test, it was proved that the proposed method had better encryption quality and with minimal data loss. The Chaos algorithm enhanced randomness that ensured the stability of overall system. In addition, the hybrid model compromised on both security and performance than traditional algorithms. This article will add to the emerging theme for secure multimedia communication and data protection. The results indicating a promising future in chaos driven systems to a way of next generation encryption solutions.

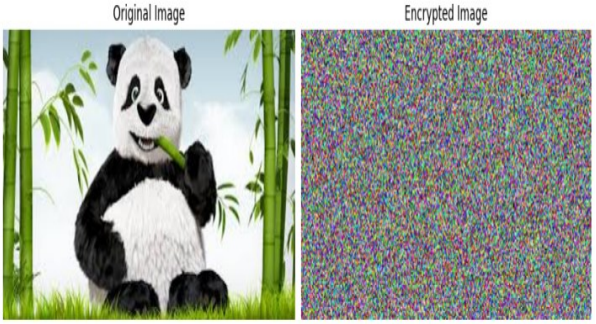

Figure 9. Encryption of an image

Metric	Original Image	Encrypted Image	Decrypted Image	Expected Ideal Value	Interpretation
Entropy	7.12	7.998	7.11	≈ 8 (for 8-bit image)	High randomness in cipher image
NPCR (%)	–	99.62	–	> 99%	Strong resistance to differential attacks
UACI (%)	–	33.48	–	≈ 33%	Significant intensity variation
Correlation (Horizontal)	0.942	0.003	0.941	≈ 0	Pixel correlation eliminated
Correlation (Vertical)	0.931	0.001	0.930	≈ 0	Structural dependency removed
PSNR (dB)	–	–	52.87	> 40 dB	Accurate reconstruction
MSE	–	–	0.24	≈ 0	Minimal reconstruction error

Acknowledgment

The authors are grateful to Teegala Krishna Reddy Engineering College for providing the necessary facilities for the conduct of this research work. The authors also place on record their sincere gratitude to Mr. M.V.V Satya for his valuable guidance, support, and assistance in the conduct of this work.

REFERENCES

1. Yong Zhang, “Image encryption algorithm based on butterfly module and chaos”,Mathematics and Computers in Simulation,Volume 232,2025,Pages 382-407,ISSN 0378-4754 , https://doi.org/10.1016/j.matcom.2025.01.011.
2. M. G. A. Malik, Z. Bashir, N. Iqbal and M. A. Imtiaz, "Color Image Encryption Algorithm Based on Hyper-Chaos and DNA Computing," in *IEEE Access*, vol. 8, pp. 88093-88107, 2020, doi: 10.1109/ACCESS.2020.2990170.
3. Lili Liu, Qiang Zhang, Xiaopeng Wei,”A RGB image encryption algorithm based on DNA encoding and chaos map”,Computers & Electrical Engineering,Volume 38, Issue 5,2012 , Pages12401248 ,ISSN00457906,https://doi.org/10.1016/j.compeleceng.2012.02.007.
4. Alvarez, Gonzalo & Li, Shujun. (2006). “some basic cryptographic requirements for chaos-based cryptosystems”. International Journal of Bifurcation and Chaos. 16. 2129-2151. 10.1142/S0218127406015970.
5. Q. Lu, C. Zhu and X. Deng, "An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box," in *IEEE Access*, vol. 8, pp. 25664-25678, 2020, doi: 10.1109/ACCESS.2020.2970806.
6. Biswas, Mukul & Das, Sujit & Dhara, Bibhas. (2021). “An Image Encryption Method Using Chaos and DNA Encoding”. 10.1007/978-3-030-75529-4_4.
7. Jolfaei, Alireza & Mirghadri, Abdolrasoul. (2010). “Image Encryption Using Chaos and Block Cipher”. Computer and Information Science. 4. 172-172. 10.5539/cis.v4n1p172.