JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IMAGE ENCRYPTION AND DECRYPTION USING CHAOTIC AND DNA ALGORITHMS

[1]G.Bhargavi, [2]G.Jahnavi Lakshmi, [3]G.Yamini, [4]B.Prasanna Lakshmi,[5]A.Siva Sai kumar

[1]UG Scholar, [2]UG Scholar, [3]UGScholar, [4]UGScholar,,[5]Assistant Professor
Department of Electronics and Communication Engineering,
Narayana Engineering College, Nellore, India.

***Abstract*:** In recent years, the demand for secure image communication over public networks has increased significantly. To address this demand, this project presents a novel approach to image encryption and decryption using chaotic and DNA algorithms. The proposed method leverages the chaotic properties of chaotic maps to generate pseudo-random sequences for encryption, while DNA encoding techniques are employed to enhance the security and robustness of the encryption process. In the encryption phase, the original image is transformed into a chaotic domain using a chaotic map, and then further encrypted using DNA-based techniques. The decryption process involves the reverse transformation, where the encrypted image is decoded using the same DNA encoding scheme and chaotic map to retrieve the original image. Experimental results demonstrate the effectiveness and security of the proposed method against various cryptographic attacks, including statistical analysis and brute-force attacks. Furthermore, the method exhibits high computational efficiency, making it suitable for real-time image encryption applications. Overall, the proposed approach offers a promising solution for secure image communication in applications requiring high levels of confidentiality and integrity. Future research directions may include exploring optimization techniques to further enhance the performance and scalability of the proposed method. This abstract provides a brief overview of the model's objectives, methodology, results, and potential implications, serving as a concise summary for readers.

Index Terms— Encryption, Decryption, Cryptography, Chaotic, DNA encoding.

I. INTRODUCTION

Cryptography is the science of information security which has become a very critical aspect of modern computing systems towards secured data transmission and storage. The exchange of digital data in cryptography results in different algorithms that can be classified into two cryptographic mechanisms: symmetric key in which same key is used for encryption and decryption and asymmetric key in which different keys are used for encryption and decryption. Asymmetric key algorithms are more secured when compared with symmetric key algorithms. Nowadays, information security is primarily based on data storage and transmission. Images are broadly used in numerous processes. As a result, the safety of image data from unauthorized access is crucial at the hands of user. Image encryption plays a significant role in the field of information hiding. Image hiding or encryption methods and algorithms ranges from simple spatial domain methods to more complicated and reliable frequency domain.

As the information is shared over a single band of frequency which can be questioning the security of personal information from the end user side. Therefore the techniques used in order to secure the information plays an important role in maintaining integrity, privacy and authentication of the data which is shared from unauthorized users. In this present era of technology and digitization, security plays an important role, so encryption is one of the ways to secure our data from hacking. In this project we will be discussing algorithms to encrypt images efficiently using different techniques. Many encryption techniques have been proposed, each of them have their own advantages and disadvantages. Among these there is one algorithm known as chaos based cryptographic algorithm. This algorithm is suggested to be efficient in encrypting images. Chaos algorithm for encryption is considered good, as it provides high speed, reasonable computation, and good security. This system contains some noisy behavior but it is exactly deterministic. If initial value and its parameters are given then we can generate a confusion matrix. This map is extremely sensitive to initial conditions. Here in this model we have also used DNA encoding technique that helps to make the encryption far more confusing and random. DNA encoding is a technique to encode the pixel values into a DNA sequence of nucleic acid bases A, T, G, C. The proposed method is a new approach to encrypt images using chaotic logistic mapping and DNA encoding in order to get secure encrypted image. Many techniques are presently there for encryption and decryption of multimedia data of 1D, 2D and 3D level. Image encryption techniques are studied frequently in order to meet the demand for real-time information security when data is being transferred over internet. Traditional algorithm i.e., Advanced Encryption Standard (AES) has many disadvantages like low-level efficiency with large multimedia, used basically for data encryption not for multimedia. The chaotic and DNA encryption has being suggested to be fast and highly secured technique for encryption.

II. RELATED WORK

A Color image encryption scheme based on chaos and Customized Globally Coupled Map Lattices is presented in [1]. The proposed scheme comprises four phases. Firstly, the color decomposition method is used to decompose the RGB image into its three components and a key image equal to the size of original image is generated with the help of CML-based logistic map. Secondly, the image is divided and shuffled into four images, i.e., red image, green image, blue image and RGB image, each of which is the same size. Finally,

the confusion operations will be performed in order to choose the key image out of the four images. Later, the remaining three images are combined to obtain the cipher image. Experimental analysis and simulations show that the presented image encryption algorithm is highly resistant against certain security risks and attacks.

Another color image encryption technique based on the combination of spatiotemporal chaotic system and DNA sequences is presented in [2]. In order to achieve more random sequences, the Logistic-Sine system (LSS) is employed in the CML and a new spatiotemporal chaotic system is constructed. Initially, the key image is generated from the original image and secret keys provided in the spatiotemporal sequences. The pixel values are interrupted by applying exclusive-OR operations. In addition, DNA deletion and DNA insertion pseudo-operations are performed to confuse the DNA encoded diffused image under the supervision of key streams. Lastly, the DNA encoded mage is decoded to acquire the encrypted image. Experimental results and theoretical analysis exhibit that the presented image cryptosystem achieves high accuracy in performance and is robust against various attacks including differential and statistical attacks.

In [3] the authors have highlighted the problem of key diffusion in chaotic image encryption algorithms and therefore presented a solution in this regard. The proposed algorithm replaces half of the iterations with iterations of a CML during the transient period. Various aspects of the designated scheme such as sensitivity on keys or resistance against differential attacks are presented. Moreover, a detailed analysis of recent techniques is discussed and compared with the proposed algorithm on the basis of widely used performance metrics. The results conclude that the proposed scheme outperforms other approaches by achieving high values of Unified Average Changing Intensity (UACI) and entropy.

III. METHODOLOGY

In this proposed method, chaotic and DNA algorithms are used to encrypt and decrypt the data in an image that aims at improving the information security. DNA is considered a hi-gh speed cryptography technique, which is suitable to encrypt large volume of data and chaotic algorithms utilize chaos theory to generate random keys for encryption. In chaotic algorithms, the initial conditions and parameters are used to create a chaotic system for generating encryption keys. DNA algorithms involve encoding image data into DNA sequences and performing operations inspired by genetics for encryption.

Chaotic algorithms scramble the pixel values of an image based on the chaotic system created by the key. DNA algorithms encode the image pixels into DNA sequences, apply genetic operations, and then decode back to image format. The encryption process ensures that the original image data is protected from unauthorized access.

The combination of chaotic and DNA algorithms provides a dual-layered security approach for image encryption.These methodologies offer high resistance to attacks such as brute force and statistical analysis due to their complex nature.

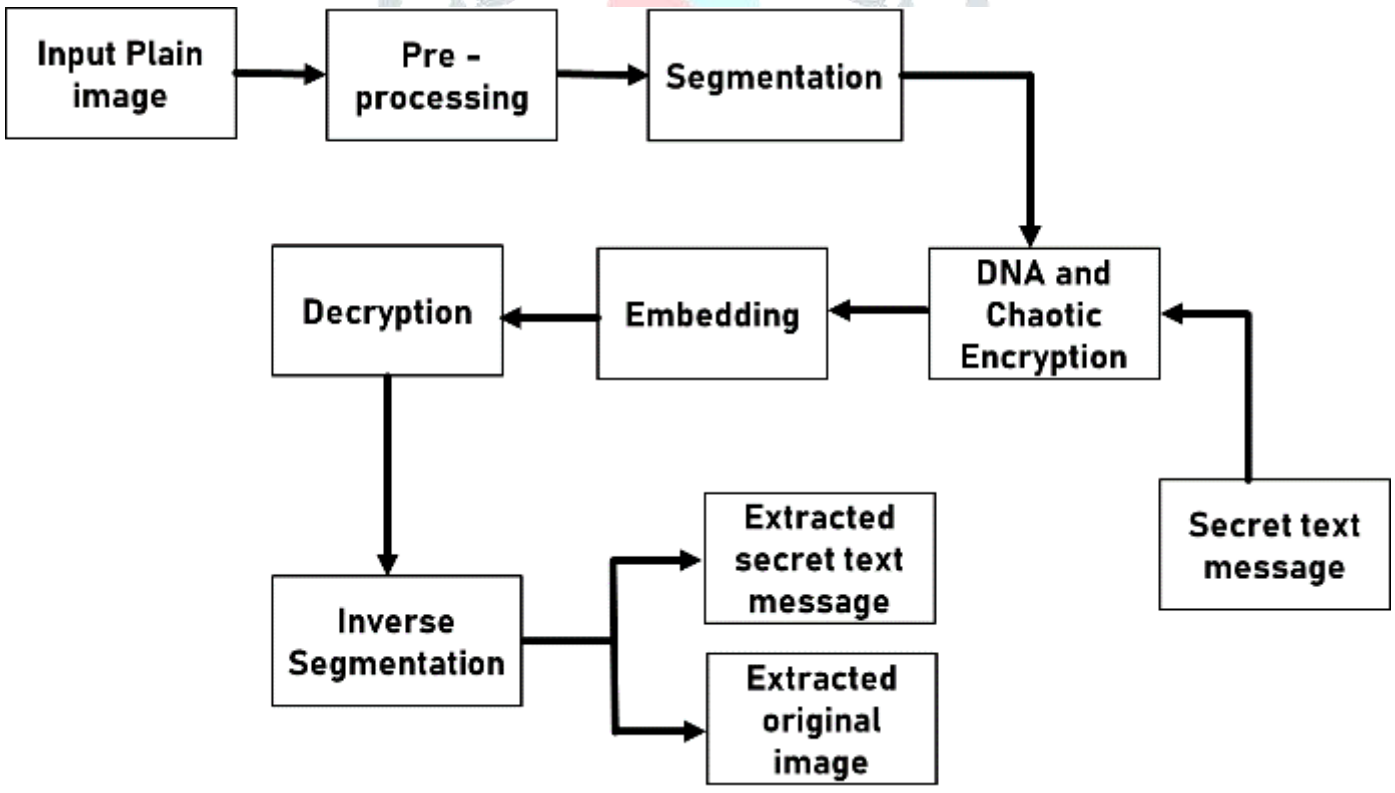

Figure 1 block diagram for encryption and decryption

3.1 Chaotic Logistic Map

The chaotic theory is the mathematics considering dynamic behavior of the natural and artificial systems which are sensitive to the initial conditions like weather, climate and traffic on road. It can be analyzed using chaotic mathematical model or can also be done using recurrence plots and Poincare maps. Chaos theory is used for emerging technologies such as neurology, cardiology, control and circuit theory, weather prediction, etc. Chaos -"when the present determine the future but the approximate present cannot approximately determine the future". In chaos even small change in initial conditions can lead to totally uncorrelated sequence. It is been said and proved that chaos function can be used for encryption giving good results. Logistic function is one of the chaos functions varying with initial conditions with high sensitivity and generated non periodic pseudo random sequence and it will be entirely unpredictable if proper choice of bifurcation

parameter „r" has been taken in to consideration. Implementing image encryption by using chaotic theory is simple, computationally faster and impregnable.

"Chaotic" typically refers to systems that exhibit complex, unpredictable behavior even though they are governed by deterministic rules. Chaos theory deals with such systems, which often show sensitivity to initial conditions, non-linear dynamics, and a high degree of complexity.

So, a "CHAOTIC algorithm" could refer to an algorithm inspired by or utilizing principles from chaos theory. This could mean algorithms designed to exploit chaotic behavior for specific purposes, such as randomness generation, optimization, or simulation of complex systems. Without further context or a specific definition, it's challe-nging to provide a precise interpretation of what a "CHAOTIC algorithm" entails. If this term is used within a specific context or domain, such as a particular research field or industry, its meaning might be more specific and well-defined within that context.

3.2 DNA Encoding

DNA encoding in image encryption, it involves using the genetic code of DNA sequences to encrypt images. The basic idea is to convert the pixel values of an image into DNA sequences and then decode them back to retrieve the original image. To do this, each pixel value of the image is converted into a corresponding DNA base pair sequence. For example, you could map different pixel values to specific combinations of nucleotides (A, T, C, G). This mapping creates a DNA sequence representing the image. During decryption, the DNA sequence is converted back into pixel values, reconstructing the original image. This method can be used for secure image encryption as DNA sequences are complex and can provide a high level of encryption.

Table 1 dna rules

1	2	3	4	5	6	7	8
00-A	00-A	00-C	00-C	00-G	00-G	00-T	00-T
01-C	01-G	01-A	01-T	01-A	01-T	01-C	01-G
10-G	10-C	10-T	10-A	10-T	10-A	10-G	10-C
11-T	11-T	11-G	11-G	11-C	11-C	11-A	11-A

3.3 Pre Processing

3.3.1 Resize

Image interpolation occurs when you resize or distort your image from one pixel grid to another. image resizing is necessary when you need to increase or decrease the total number of pixels, whereas remapping can occur when you are correcting for lens distortion or rotating an image. zooming refers to increase the quantity of pixels, so that when you zoom an image.

3.3.2 Conversion

RGB to Gray

For this process we are converting color image to gray scale image by the calculation of average value. that means 3 channels can be converted into single channel.

3.3.3 Median filtering

Median filtering is a common nonlinear method noise suppression that has unique characteristics. it does not use convolution to process the image with a kernel of coefficients. rather, in each position of the kernel frame, a pixel of the input image contained in the frame is selected to become the output pixel located at the coordinates of the kernel center.

3.4 Segmentation

Image Segmentation is the process by which a digital image is partitioned into various subgroups (of pixels) called Image Objects, which can reduce the complexity of the image, and thus analyzing the image becomes simpler.

Wavelet transformation

Wavelet transformation is a mathematical tool that can help analyze images at different scales. It's often used in image processing to detect edges and boundaries in images. By applying wavelet transformation, you can break down an image into different frequency components, which can then be used for segmentation. It's a powerful technique that can help extract meaningful information from images. The formula for wavelet transformation can be expressed as follows:

$$W(a, b) = \int f(t)\psi((t-b)/a)\, dt$$

In this formula,

W(a, b) represents the wavelet coefficient at scale a and position b.

f(t) is the input image.

ψ is the wavelet function

a and b control the scale and position of the wavelet transformation.

To perform image segmentation using wavelet transformation, you can apply the wavelet transformation to the image and then analyse the resulting wavelet coefficients. By thresholding or analysing the coefficients, you can identify edges and boundaries in the image, which can be used for segmentation.

3.5 Chaotic encryption

Chaotic systems are highly sensitive to initial conditions, making them suitable for encryption purposes. Common chaotic algorithms include the logistic map, the Henon map, and the Lorenz system. The chaotic map generates a stream of pseudo-random numbers which are used to scramble the image data.

3.6 DNA encryption

DNA-based algorithms use the principles of DNA sequences for encryption. These algorithms typically involve encoding the image data into DNA sequences and manipulating them using DNA operations such as crossover, mutation, and selection.

3.7 Embedding

In image processing, embedding refers to the process of hiding or inserting additional information within an image. This can be done by modifying the image's data to include extra data or functionality while maintaining the image's visual appearance. The purpose of embedding is often to add extra features or enhance the image in some way.

It's important to note that image embedding can have both legitimate and potentially malicious appli-cations. It can be used for watermarking, copyright prote-ction, or data hiding.

3.8 Decryption

Decryption is the process of converting encrypted data back into its original, readable form. It's like unlocking a secret message. When data is encrypted, it is scrambled using a specific algorithm and a key. To decrypt it, you need the corresponding key to reverse the encryption process and make the data readable again. It's an essential part of ensuring secure communication and protecting sensitive information.

3.9 Inverse segmentation

Inverse segmentation in image processing typically refers to a technique that aims to separate the foreground objects from the background in an image. It is the opposite of traditional segmentation, where the goal is to identify and extract the objects of interest. In inverse segmentation, the algorithm or method focuses on isolating the background or unwanted regions of the image. This can be useful in various applications, such as image editing, object removal, or background replacement. By applying inverse segmentation techniques, it becomes possible to manipulate or replace the background while preserving the foreground objects. This can be particularly handy in scenarios like video conferencing, virtual reality, or creating composite images.

The algorithm for image encryption is

Step 1: Resize the input image and convert it into gray scale.
Step 2: Take the pixel value and convert the pixel value into binary.
Step 3: Apply any one of eight rules of the DNA encoding to convert the input image into DNA encoded image.
Step 4: Take the secret text and convert it into cipher text using cipher techniques mentioned before.
Step 5: Convert cipher text into binary and then apply same DNA rule which applied earlier for image encoding.
Step 6: Now as the cipher text and the encoded input image are DNA encoded, by applying “xor” for both the encoded input image and the cipher text using DNA rules to get an encrypted DNA encoded image.
Step 7: Now as the output image from step 6 is DNA encoded, will be converting each pixel to decimal value using rules to get the final encrypted image.

The algorithm for image decryption is

Step 1: Take the encrypted image and the cipher text.
Step 2: Obtaining the decomposition image by applying the transformation technique.
Step 3: Reconstruction of original image by decryption.
Step 4: Extracting the secret data.

IV. Results & Discussion

The process of image encryption and decryption also hiding and extracting the secret data are shown in following figures from Fig1 to Fig13 and finally performance analysis of parameters are shown in Fig14 which will be displayed by clicking the validate.

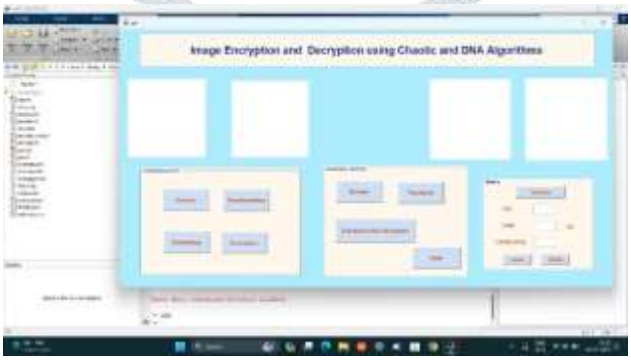

Fig 1. Browse the input test image

Fig 2. Selecting the input test image

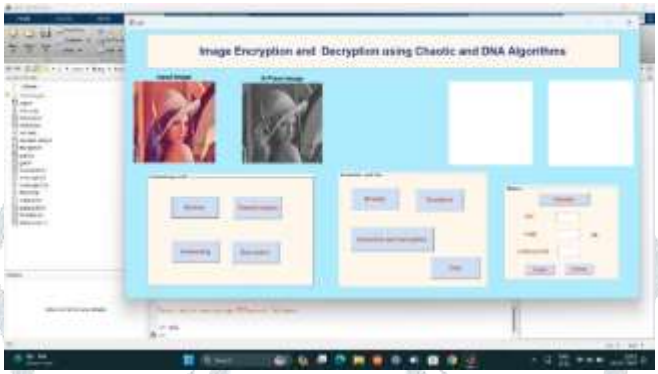

Fig 3. Converting the input image into B plane image

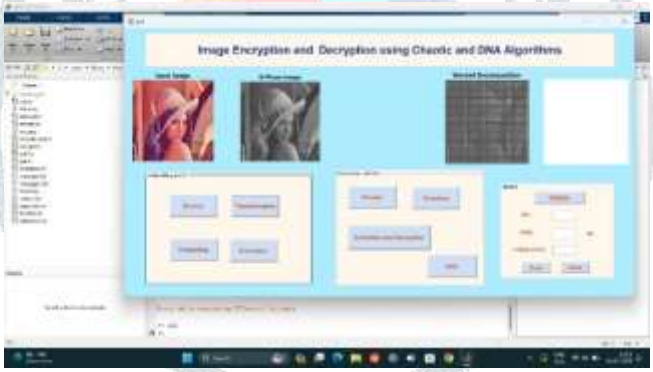

Fig 4. Wavelet Decomposition image

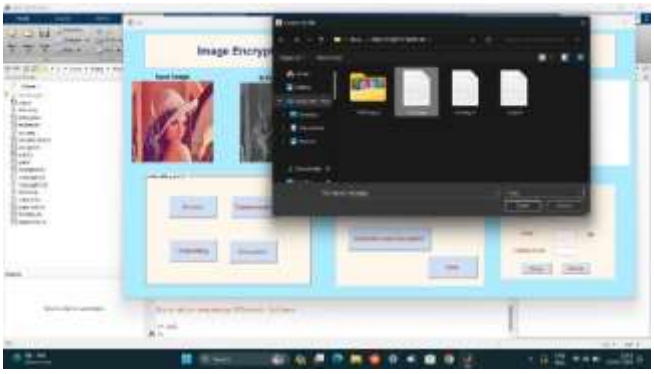

Fig 5. Selecting the secret text message

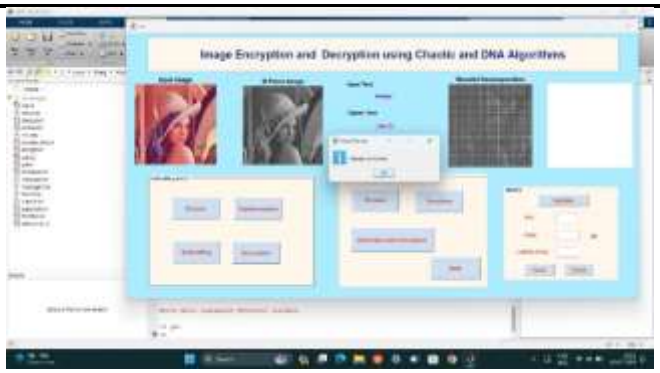

Fig 6. Converting the secret text message into cipher text

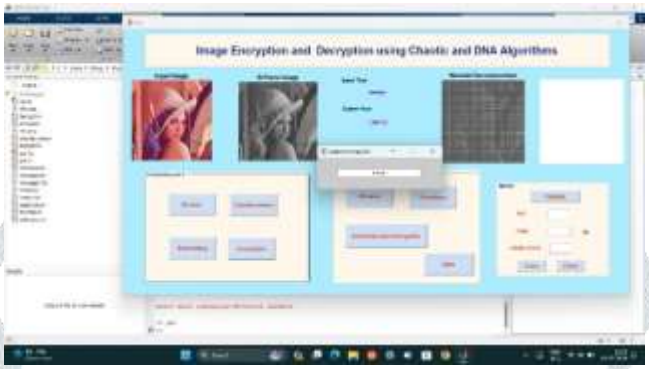

Fig 7. Entering the password for more security

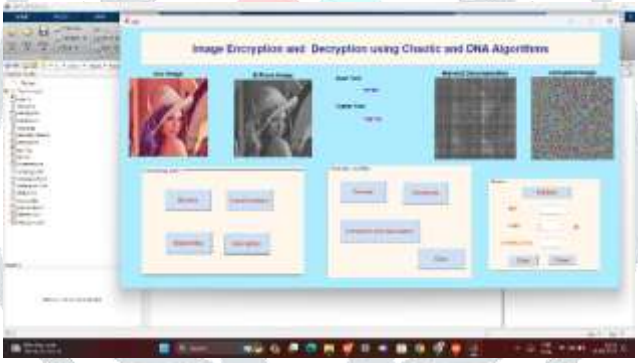

Fig 8. Getting the Encrypted image

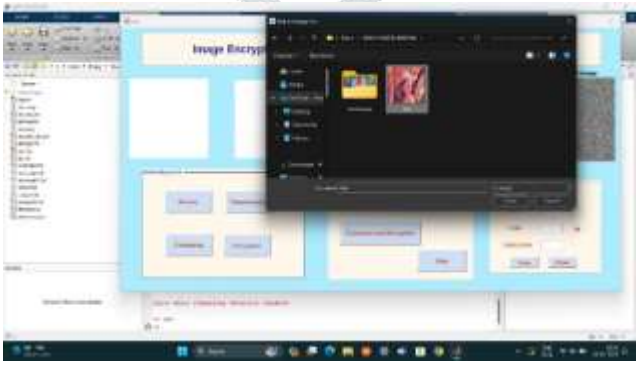

Fig 9. Browse the Encrypted image

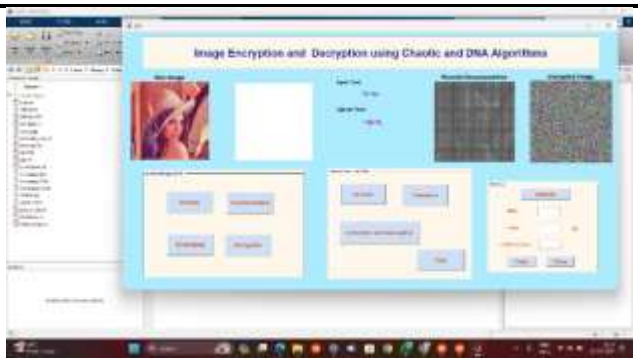

Fig 10. Encrypted output image

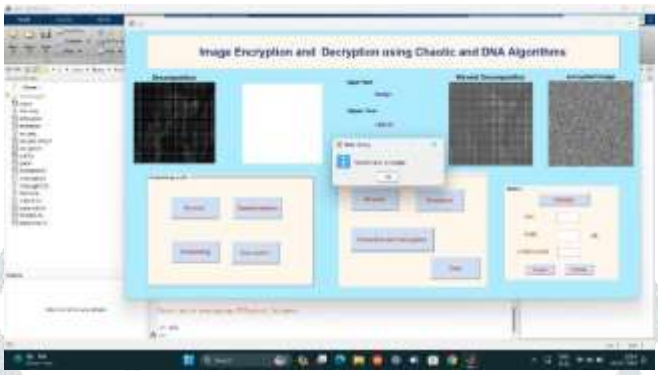

Fig 11. Decomposition of Encrypted image

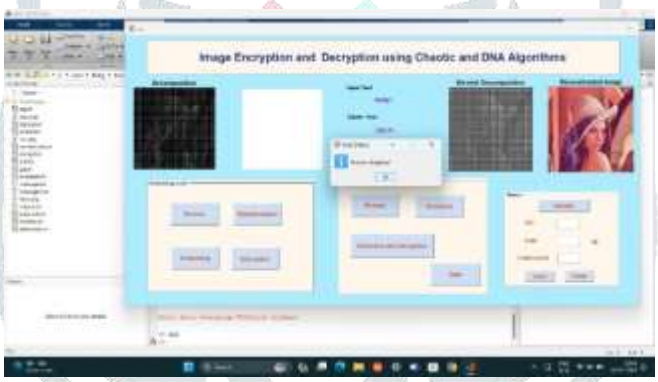

Fig 12. Reconstruction of original image

Fig 13. Extracting the secret data

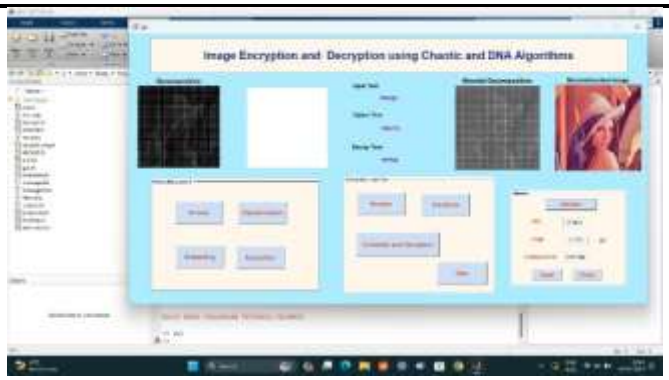

Fig 14. Performance Analysis Parameters

V. Conclusion & Future scope

The findings of this study underscore the potential of chaotic and DNA algorithms in advancing the state-of-the-art in image encryption and decryption. By leveraging the inherent properties of chaotic systems and the information-coding capabilities of DNA sequences, we have laid the groundwork for developing more secure and reliable encryption methods for protecting sensitive image data in various applications.

The future scope of image encryption and decryption is characterized by continuous innovation. These algorithms offer high security and efficiency for safeguarding images. They can be used in healthcare, military, and other sectors for secure data handling. Ongoing research to enhance these algorithms and explore new techniques will further improve their effectiveness.

VI. Acknowledgement

Our sincere thanks to Dr. P. Narayana, Ph.D., Founder; Dr. Dattatreya sharma, Ph.D., Director; Dr. G. Srinivasulu Reddy, M.Tech., Ph.D., Principal; Dr. K. Murali, M.Tech, Ph.D , Professor & HOD.

References

1. Wang, X., Qin, X., Liu, C.: Color image encryption algorithm based on customized globally coupled map lattices. Multimedia Tools Appl. 78(5), 6191–6209 (2019)
2. Hu, T., Liu, Y., Gong, L.H., Guo, S.F., Yuan, H.M.: Chaotic image cryptosystem using dna deletion and dna insertion. Signal Process. 134, 234–243 (2017)
3. Oravec, J., Turan, J., Ovsenik, L.: Image encryption technique with key diffused by coupled map lattice. In: 2018 28th International Conference Radioelektronika (RADIOELEKTRONIKA), IEEE, pp. 1–6 (2018)
4. Wang, X., Zhao, H., Wang, M.: A new image encryption algorithm with nonlinear-diffusion based on multiple coupled map lattices. Opt. Laser Technol. 115, 42–57 (2019)
5. Nematzadeh, H., Enayatifar, R., Motameni, H., Guimarães, F.G., Coelho, V.N.: Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt. Lasers Eng. 110, 24–32 (2018)
6. Xingyuan, W., Le, F., Shibing, W., Zhang, C., Yingqian, Z.: Spatiotemporal chaos in coupled logistic map lattice with dynamic coupling coefficient and its application in image encryption. IEEE Access 6, 39,705–39,724 (2018)
7. Yu W, Liu Y, Gong L, Tian M, Tu L (2019) Double-image encryption based on spatiotemporal chaos and dna operations. Multimedia Tools Appl. 78(14), 20,037–20,064
8. Zhang, Y.Q., He, Y., Wang, X.Y.: Spatiotemporal chaos in mixed linear-nonlinear two-dimensional coupled logistic map lattice. Phys. A Stat. Mech. Appl. 490, 148–160 (2018)
9. 9Yj, Sun, Zhang, H., Xy, Wang, Xq, Wang, Pf, Yan: 2d non-adjacent coupled map lattice with q and its applications in image encryption. Appl. Math. Comput. 373(125), 039 (2020)
10. Zhang, H., Wang, X., Xie, H., Wang, C., Wang, X.: An efficient and secure image encryption algorithm based on non-adjacent coupled maps. IEEE Access 8, 122,104–122,120 (2020)