CRYPT-IMAGE

Submitted in partial fulfilment of the requirements of the degree of

BACHELOR OF COMPUTER ENGINEERING

by

Ashutosh Rawat (20102066)

Gaurang Sant (20102116)

Kunal Saini (20102154)

Raj Rehpade (20102053)

Guide:

Under the guidance of Prof. Archana Kotangale

Department of Computer Engineering

A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

(2023-2024)

A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

CERTIFICATE

This is to certify that the project entitled "CRYPT-IMAGE" is a bonafide work of **"Ashutosh Rawat" (20102066), "Kunal Saini" (20102154) "Gaurang Sant" (20102116), "Raj Rehpade" (20102053)** submitted to the University of Mumbai in partialfulfilment of the requirement for the award of the degree of **Bachelor of Engineering** in **Computer Engineering.**

Prof. Archana Kotangale	**Prof. Rushikesh Nikam**	**Prof. Sachin Malave**	**Prof. Uttam Kolekar**
Guide	**Project Coordinator**	**Head of Department**	**Principal**

A. P. SHAH INSTITUTE OF TECHNOLOGY, THANE

Project Report Approval for B.E.

This project report entitled CRYPT- IMAGE by **"Ashutosh Rawat" (20102066), "Kunal Saini" (20102154), "Gaurang Sant (20102116), "Raj Rehpade" (20102053)** is approved for the degreeof ***Bachelor of Engineering*** in ***Computer Engineering***, ***2023-24***.

Examiner Name	Signature
1._____	_____
2._____	_____

Date:

Place:

Declaration

We declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Ashutosh Rawat (20102066)

Gaurang Sant (20102116)

Kunal Saini(20102154)

Raj Rehpade (21202018)

Date:

Abstract

As the need for secure data transmission and storage increases in the digital age, image encryption techniques have become crucial for protecting sensitive visual information. An innovative approach to image encryption combining DNA coding and chaotic mapping, which aims to improve the security and reliability of the encryption process. The proposed method exploits the complexity and randomness of DNA sequences and chaotic systems to achieve high cryptographic strength. First, the image is converted into a digital representation and then encoded into a DNA sequence. This DNA sequence is further processed using a chaos map, which adds a layer of dynamic and unpredictable behavior to the encryption process. Chaotic mapping parameters such as initial conditions and control parameters are dynamically generated based on the secure key, making it resistant to brute force and cryptanalysis attacks. The resulting encrypted image is very random and complex, making it very difficult for unauthorized persons to decipher it. Experimental results and comparative analysis demonstrate the effectiveness and robustness of the proposed encryption scheme against various attacks, including statistical, differential, and brute force attacks. Additionally, the encryption process has a negligible effect on image quality, ensuring that encrypted images remain visually intact and suitable for practical applications. In conclusion, the combination of DNA coding and chaotic mapping offers a promising approach to image encryption that offers high levels of security, adaptability, and resistance to attacks. This research contributes to ongoing efforts to strengthen data security in the digital age and finds applications in areas such as secure image transmission, medical imaging, and confidential document storage.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVATION

DNA	Deoxyribonucleic Acid
DICOM	Digital Imaging and Communications in Medicine
RGB	Red, Green, Blue

CHAPTER 1

Introduction

In the era of digital information and image-based communication, the need for efficient and secure image analysis methods has become extremely important. Traditional image analysis techniques are often based on mathematical algorithms and data processing, but recent advances have introduced innovative approaches inspired by nature and chaos theory. One such pioneering approach combines the principles of DNA coding and chaotic mapping to revolutionize image analysis. DNA, the fundamental molecule of life, is known for its extraordinary information storage properties. Based on the new chaos medical image encryption system. It is based on a combination of scene chaos and DNA counting two rounds of encryption preceded by a key generation layer and follows a permutation-substitution-diffusion structure. The SHA-256 function with the original secret keys is used to generate secret keys for chaotic systems. Age the cycle of the proposed algorithm includes six steps, i.e., block-wise permutation, pixel-wise substitution, DNA encoding, bit-level substitution (i.e., DNA completion), DNA decoding, and bit level propagation. Time pixel-wise substitution and bit-level substitution are used sequentially to encode the image. The bit-level replacement keys are based on the logistics. Super encrypted images are obtained by repeating the previous steps once new secret keys. And information security analyzes and computer simulations to confirm that the proposed system is robust enough against all various attacks. Its low complexity shows its great potential for real-time and secure image processing applications[1] Improve various security features and encryption and decryption rates of dynamic DNA coding in image encryption, selective image a new encryption method based on chaotic map and dynamic DNA coding is proposed. In this paper, we first constructed the one-dimensional chaos map above Lyapunov exponent and better dynamic behavior and then the local graph was improved texture algorithm for better image region selection and use the constructed chaos map generates pseudo-random sequences that are encoded dynamically and manipulate the selected DNA region and finally create a complete encoded picture Experimental results show that compared to existing methods, the proposed algorithm has a large enough key space, better statistics and differential properties and can resist common attacks such as selected plaintext attacks, noise attacks and breakout attacks.[2]

CHAPTER 2

Literature Survey

With the rapid development of network and information technology, people pay more attention to information security, especially the protection of digital images. Because of its sensitivity to discontinuity and initial value, the chaos map appears to be a tool that can be used to encrypt images. Recent work has shown that quantum chaotic 7 the map is very sensitive to a slight change in initial conditions. sensitivity A quantum chaos map can greatly increase the complexity of cryptographic algorithms. There is currently a wide variety of DNA-based image encryption algorithms coding is proposed where the pixel values of the image are coded with four bases DNA pairs to achieve image pixel dispersion, but most methods are optional. The rules of DNA coding are set. A new image encryption algorithm with quantum chaos map, Lorenz chaos map and DNA coding, which uses four DNA base pairs, dynamically selects eight types of coding DNA rules and eight types of DNA addition and XOR rules. This strategy led to a significant improvement in reliability and safety. Through simulation experiments Histogram results, correlations, and pixel numbers change (NPCR) analyzes show that the proposed algorithm is of advanced level security and can successfully resist various attacks such as brute force attacks and statistical attacks[3]We investigate the use of two chaotic systems (Bernoulli shift map and Zigzag map). With coding deoxyribonucleic acid in a medical image coding system paper. The system consists of two main steps: chaotic key generation and DNA propagation. First, the hash function of Message Digest Algorithm 5 is performed on a standard medical image, and the hash value is used with the input ASCII string value create initial conditions and control parameters for two chaotic systems (Bernoulli exchange card and zigzag card). These chaotic systems are later used to produce two separate key matrices. Second, the line-by-line spread function between the normal image matrix and two chaotic key matrices, the DNA XOR algebraic operation is performed alternately to obtain the ciphertext. A logistic map is used select the DNA encoding and decoding rules for each line. Experimental results of statistical, differential and centrality analyze show that the proposed system is robust and resists various attacks.[4]

In today's technological age, the growing desire for e-health care has increased the focus on cyber security. attacks When transmitting digital medical images over a public network, an appropriate level of security is required to protect One of the most important technologies is encryption, which protects medical images. This document recommends using DICOM image encryption based on chaotic attractors in the frequency domain using integer wavelet transform (IWT) and combined. a deoxyribonucleic acid (DNA) sequence with a space domain. The proposed algorithm uses a chaotic 3D Lorenz tractor and logistic map to generate pseudo-random keys for encryption. The algorithm includes the following steps, viz. permutation, substitution, encoding, augmentation and decoding. Various analyzes are performed to confirm the robustness of the proposed algorithm. were studied for 256 × 256 DICOM images, achieving an average entropy of 7.99, a larger key space of 10,238, and a non-zero correlation. The overall results confirm that the proposed algorithm is robust against brute force attacks.[5] An image encryption technique that uses DNA (deoxyribonucleic acid) operations. and chaos maps are proposed in this paper. First, the input image is DNA encoded and the mask is created using a 1D chaos map. This mask is added with DNA encoded image using a DNA insert. The intermediate is completed with DNA by the complement matrix produced by two 1D chaotic maps. The finally obtained matrix is permuted using a 2D chaotic map followed by DNA decoding to produce a ciphertext. The proposed technique is fully translatable and immune to known statistical plaintext attacks and breakout attacks.[5] RGB image encoding algorithm based on DNA coding combined. A chaos map is provided to target RGB image functions. The algorithm first runs the DNA encoding the R,G,B components of the RGB image; then understand the addition of R,G,B with DNA addition and performs the complementation operation using the DNA sequence Matrix, managed by Logistic; after decoding, three gray images are obtained; eventually will mixed RGB images by reconstructing the R, G, B components using image pixels perturbed by a logistic chaos sequence.. At the same time, it can resist exhaustive attack, statistical attack, so it is suitable for RGB image encryption.[6] A new technique to mask images before encryption, which is a keyless process but helps increase the originality picture chance. The mask image is then scrambled and hashed, resulting in an encrypted image with no observational or statistical data. A generalized Arnold catnap to generate confusion.

In addition, a new diffusion process has been introduced that works on both pixel and DNA levels. It contains all possible DNA encoding, decoding, and XOR rules chosen pseudo randomly from a chaotic 2D logistic sine. Aggregation of map values. So, it strengthens the ciphertext against brute force and statistical attacks and almost an intruder cannot obtain the original image without knowing the correct key. But the original image can be decrypted with a valid key without data loss, which is very important for medical images. One round masking, obfuscation and spreading are sufficient to obtain a cipher. Testing many medical and nature images, as well as homogeneous and textured patterns. The resulting encrypted images have a low interpixel correlation coefficient of approximately 0 and a high entropy of nearly 8 bits per symbol. In addition, the proposed analysis method for other parameters such as key difference, key sensitivity, encryption statistics and differential, occlusion and noise attacks also give satisfactory results needed for a secure image encryption system[7] Cryptography is a method of secure communication that hides information with secret keys so that only authorized users can read and process it. Powerful random sequence generators provide robust cryptographic design for cryptographic applications. Moreover, these sequences are used to encrypt data. This article discusses the ultra-chaotic nature of hybrid chaos maps, and a neural network is combined to create a random number generator for cryptographic applications. Custom Neural Network a user-defined layer transfer function is created to increase the randomness of the generator. In this work, the two-hybrid the control parameters and iteration value of the chaos map are designed as the transfer function of the layer to achieve high randomness. Color image coding is performed using extracted sequences and deoxyribonucleate coding technology. Various tests such as NIST, attractor test and correlation are applied to the generator to show the degree of randomness. Simulation analysis such as key spacing, key sensitivity, statistical, differential analysis and selected plaintext attack shows
the strength of the encryption algorithm[8]

1.1 Literature Survey Table:

Year	Author	Methodology	Infrastructure	Conclusion
2019	Akram Belazi, Muhammad Talha, Sofiane Kharbech, Wei Xiang	DNA encoding, bit-level substitution and sine-Chebyshev map	Biomedical imaging	The paper's chaos-based encryption scheme for medical images meets essential encryption criteria, including a large key space and resistance to various attacks. It also exhibits efficient computational performance compared to recent image encryption algorithms, affirming its effectiveness and security for medical image encryption.
2021	Qiqi Cun, Xiaojun Tong, Zhu Wang, and Miao Zhang	DNA encoding, 1D chaotic mapping, Lyapunov exponent	cryptosystems	The paper concludes that the selective image encryption method based on the new one-dimensional chaotic map and dynamic DNA coding offers improved encryption and decryption speed while maintaining security. The algorithm demonstrates better statistical and differential

				characteristics and can resist common choice plaintext attack and noise attack.
2018	Jian Zhang	DNA encoding and quantum logistic chaotic mapping	Cryptosystems	The paper introduces a novel image encryption algorithm merging the three-dimensional quantum logistic map and dynamic DNA encoding to bolster security by generating more random sequences and resisting statistical attacks. Analyses confirm the encrypted images exhibit strong security, diffusion, and confusion characteristics, with a balanced grayscale distribution and high information entropy. Overall, the algorithm presents promising results for image encryption.

2019	JoshuaC.Dagadu, Jian-PingLi, EmeliaO. Aboagye	Hybrid chaotic DNA diffusion Bernoulli shift and zigzag maps	Wireless personal communications	The proposed medical image encryption scheme combines multiple chaotic systems, MD5 hash function, and DNA XOR algebraic operation, achieving robust encryption that resists various attacks and maintains image quality. The scheme proves effective in resisting statistical attacks, information leakage, and partial key guessing, making it a secure and efficient method for medical image encryption.
2015	Anchal Jain and Navin Rajpal	DNA encoding, chaotic mapping and DNA sequencing	cryptosystems	This paper introduces a modified image encryption scheme using DNA operations and chaotic maps, enhancing a previous technique. It involves creating a mask matrix using a 1D chaotic map combined with DNA encoding of the input

				image. The intermediate result is complemented using a complement matrix generated by two 1D chaotic maps, followed by permutation with a 2D chaotic map. This method is both reversible and resistant to known plaintext, statistical, and differential attacks.
2012	L. Liu et al.	DNA encoding, logistic mapping, and Chebyshev's Map	High power computing and DNA computing	The paper's RGB image encryption algorithm, employing DNA encoding and chaos maps, effectively eliminates pixel correlation in RGB images' spatial domain. It combines chaotic systems and DNA operations for heightened security and boasts dual security measures. Simulations confirm its efficacy, simplicity, and extensive secret key space, making it suitable for RGB image encryption, with potential applications in encrypting diverse multimedia data.

2022	Sakshi Patel, V. Thanikaiselvan	Genetic algorithms, neural networks and latin square	Cryptosystems	This paper introduces an image encryption algorithm utilizing a custom neural network-based pseudorandom number generator (PRNG) and Latin square operations. The PRNG generates chaotic sequences for diverse applications. The algorithm's effectiveness is demonstrated through simulations, showing resistance to various attacks and highlighting the robustness of the proposed PRNG.

CHAPTER 3

Limitation of Existing system

Complexity of DNA encoding: DNA encoding is a highly specialized field, and converting image data into DNA sequences can be complex and error prone. Ensuring accurate and efficient coding remains a challenge**.**

Scalability: DNA-based storage and processing has scalability limits, especially for large or high-resolution images. Controlling and manipulating DNA molecules on this scale can be technically challenging and expensive.

Error rates: DNA-based systems are susceptible to errors during the coding, decoding, and reproduction processes. These errors can lead to data corruption, so it is necessary to develop robust error correction mechanisms.

Speed: DNA-based operations are slow compared to traditional digital computing. Analyzing images in real time or at low latency can be difficult with DNA encoding, especially in applications that require rapid decision making.

Biological limitations: Biological factors such as DNA degradation over time and environmental sensitivity can affect the stability and longevity of DNA-encoded information. These limitations may limit the practicality of using DNA for long-term image storage.

Complexity of Chaotic Mapping: Chaotic mapping techniques increase the complexity of the image analysis process. Chaotic algorithms can be difficult to design and implement, and their effectiveness depends on careful parameter tuning.

Security Issues: While chaos mapping can improve security, it can also create vulnerabilities if not properly designed and secured.

Interdisciplinary Challenges: Connecting DNA biology to chaotic systems requires expertise in both biology and chaos theory, making it difficult to find experts who can effectively connect these fields. Resource intensity: DNA synthesis and analysis require expensive laboratory equipment and reagents, which can be expensive in many research and application scenarios.

Regulatory and Ethical Considerations: The use of DNA-based techniques in image analysis can raise regulatory and ethical issues, particularly in relation to data protection and handling of biological materials.

CHAPTER 4

Problem Statement, Objectives and Scope

4.1 Problem Statement

The project aims to create an image encryption system using DNA encoding techniques to provide a secure and robust method for protecting sensitive medical images during transmission and storage. The system should leverage DNA encoding principles to ensure confidentiality, and it should be resistant to common cryptographic attacks while offering efficient encryption and decryption processes.

4.2 Objectives

Secure Image Encryption:

Develop a robust image encryption method based on DNA encoding and chaotic maps for secure data transmission.

Efficient Image Compression:

Create an efficient image compression technique using DNA encoding and chaotic mapping to reduce storage and transmission overhead.

Robust Image Watermarking:

Embed imperceptible watermarks into images using DNA encoding and chaotic mapping for copyright protection.

Image Authentication:

Implement an image authentication system that verifies the integrity of images through DNA-encoded signatures and chaotic mapping.

Pattern Recognition:

Develop a DNA-based pattern recognition system with chaotic mapping for accurate object detection and classification in images.

Medical Image Analysis:

Apply DNA encoding and chaotic mapping to enhance the analysis and diagnosis of medical images for improved healthcare outcomes.

Image Restoration:

Restore degraded or damaged images by leveraging DNA encoding and chaotic mapping to recover missing or corrupted information.

CHAPTER 5

Proposed System

5.1 Architecture Diagram: -

We have an sender and receiver ends which tranfer images for encryption and decryption process where in algorithms are used and for securiity purpose we use a key for authentication of image transferred .This encryption and decryption has the encryption key as most valuable component of this image transfer.

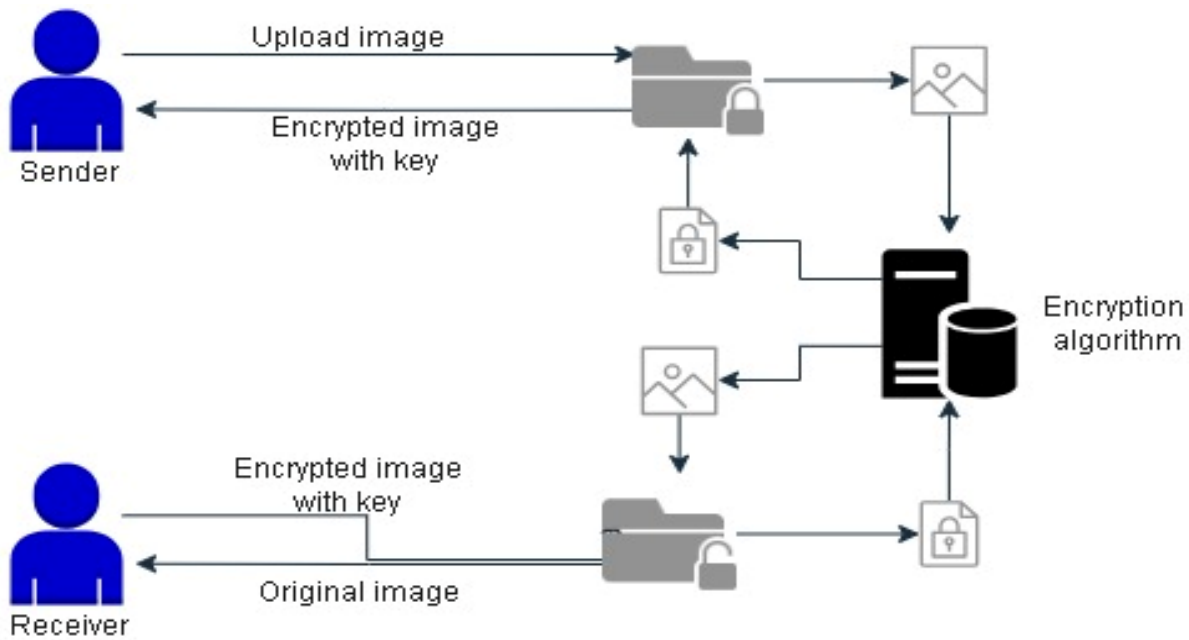


Fig 5.1 Architecture Diagram

5.2 Flowchart: -

User will upload an image to get encrypted and then getting a key we use it for decryption process also. The decrypted image can only be available after adding correct encryption key.

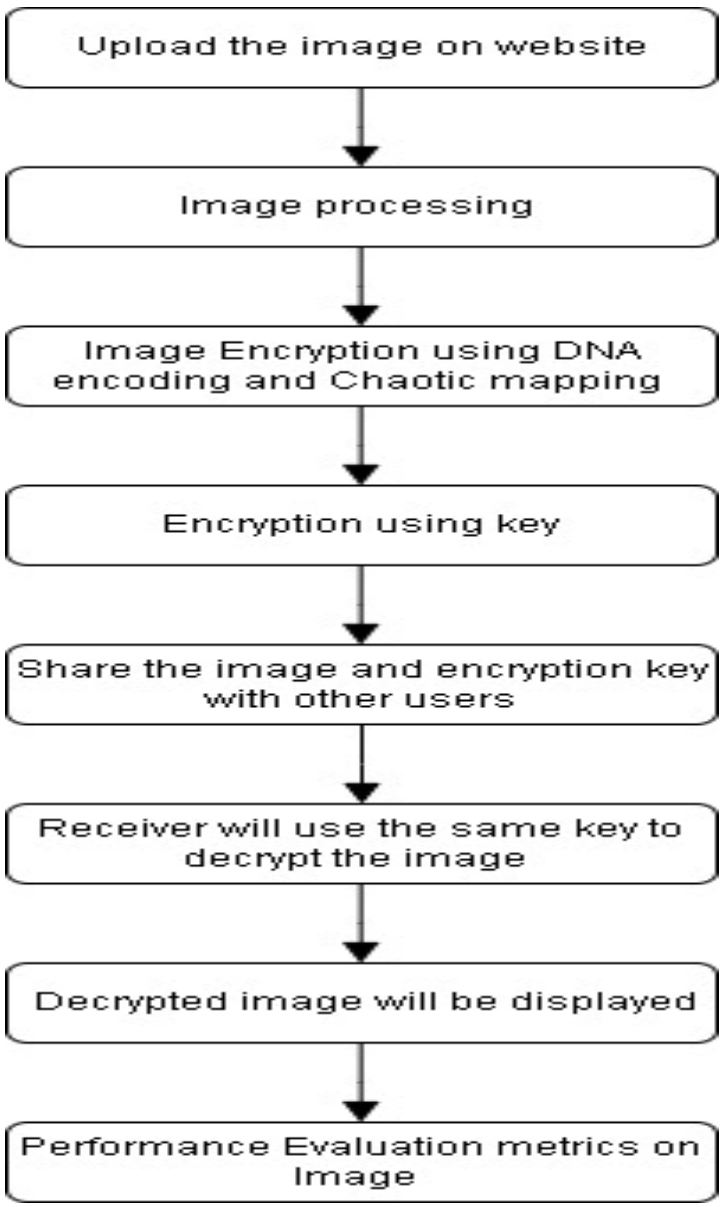


Fig 5.2 Flowchart

5.3 Use-Case : -

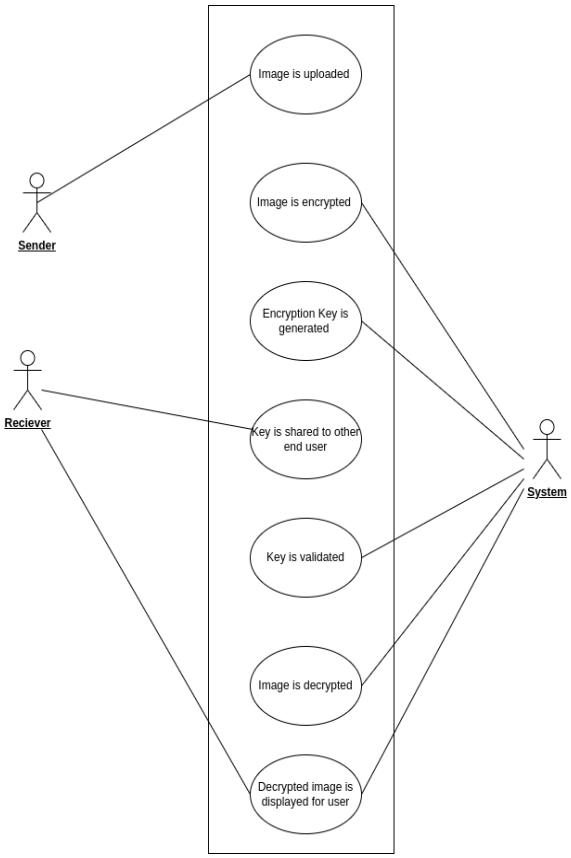


Fig 5.3 Use Case Diagram

5.4 DFD Level 0: -

User uploads an Image; the Encryption algorithm gives the Encrypted Image with Decryption key. When Encrypted Image with key is uploaded Encryption algorithms gives Original Image.

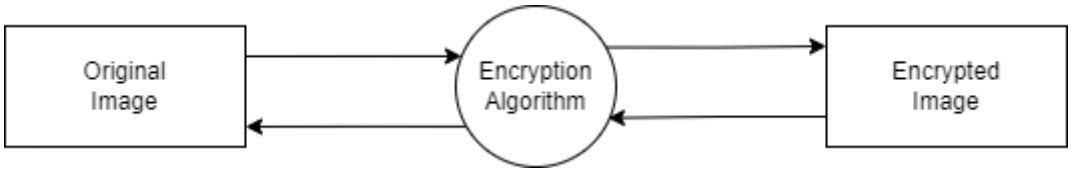


Fig 5.4 DFD Level 0

5.5 DFD Level 1: -

User uploads an Image; the Encryption algorithm gives the Encrypted Image with a Decryption key. Users can share the Encrypted Image and Decryption key to another User who can upload the Encrypted Image and Decrypted Key to get the Original Image. When Encrypted Image with key is uploaded Encryption algorithms gives Original Image.

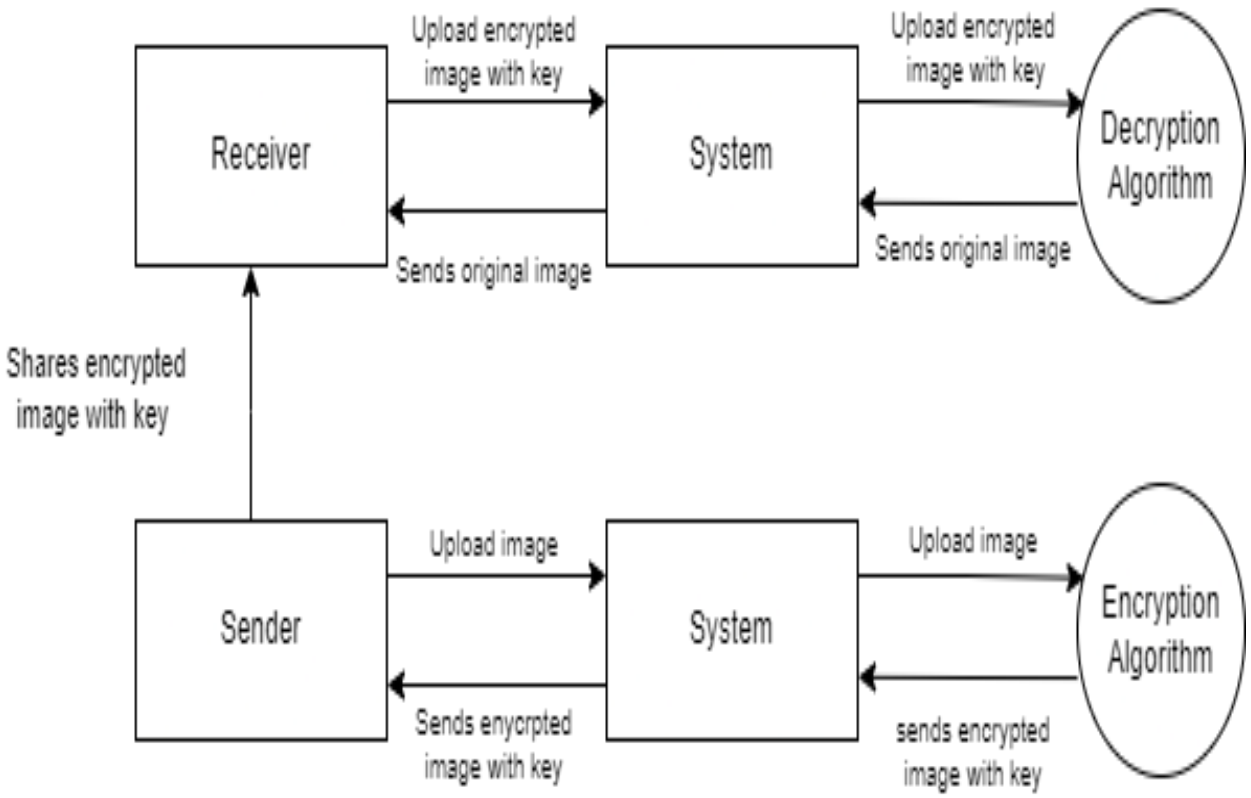


Fig 5.5 DFD Level 1

5.6 Activity Diagram: -

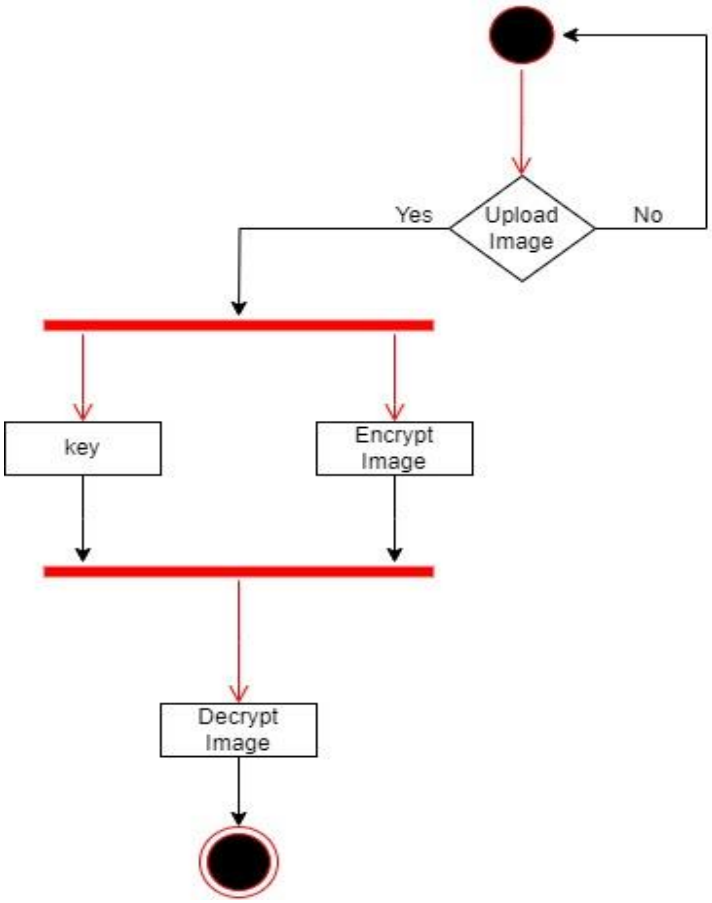


Fig 5.6 Activity Diagram

\

5.7 Sequence Diagram: -

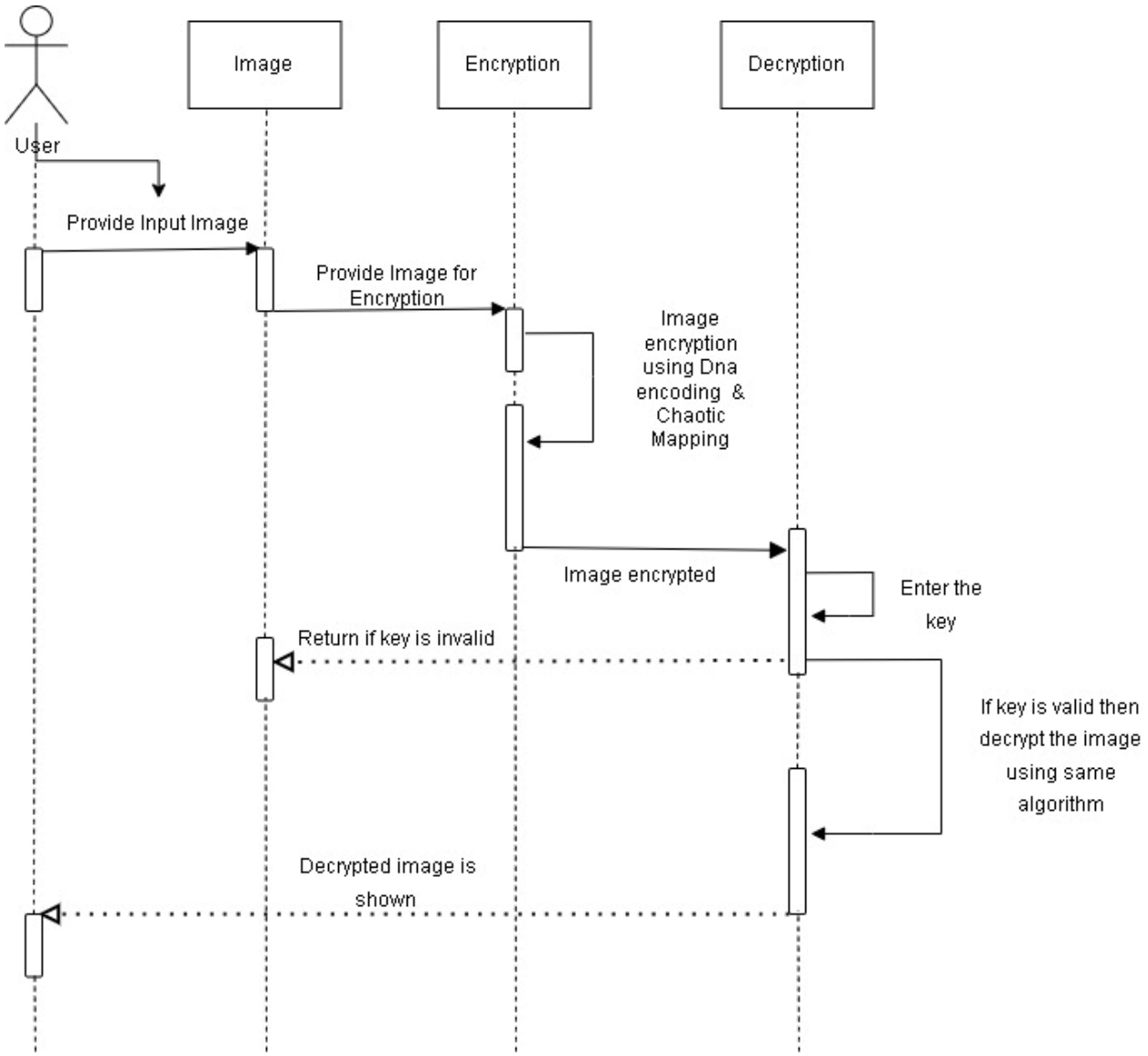


Fig 5.7 Sequence Diagram

Methodology: -

1. Project Initiation:

Define the objectives, scope, and constraints of the project. Determine the intended use and application of the image encryption system.

2. Research and Analysis:

Conduct a thorough literature review to understand existing encryption methods, DNA encoding techniques, and chaotic mapping algorithms. Identify potential gaps in the existing solutions that your project can address.

3. Requirement Specification:

Clearly document the functional and non-functional requirements for the image encryption system. Define the data types and formats that the system will support.

4. Data Preparation:

Prepare the image data by resizing, normalizing, and converting it into a suitable format for encryption, such as grayscale or binary data.

5. Key Generation:

Develop a secure key generation method that can generate encryption keys, including DNA sequences or other cryptographic keys. Ensure key uniqueness and randomness.

6. DNA Encoding:

Design an encoding scheme to convert the image data into DNA sequences. Define encoding rules, such as mapping pixel values to DNA sequences.

7. Chaotic Mapping:

Select an appropriate chaotic mapping algorithm (e.g., Logistic Map, Henon Map, or any other suitable chaotic system). Implement the chaotic mapping algorithm and ensure it exhibits desired chaotic behavior.

8. Encryption Process:

Define the encryption process, which typically involves combining the DNA encoding and chaotic mapping. Develop a reversible encryption algorithm that ensures data integrity and confidentiality.

9. Decryption Process:

Implement the decryption algorithm, which reverses the encryption process using the same keys and methods. Ensure the algorithm's accuracy and efficiency.

CHAPTER 6

Experimental Setup

6.1 Software Requirements: -

Operating System Compatibility:

- Windows 10 or later
- macOS 10.14 or later
- Linux (Ubuntu 16.04 or higher)
- Game Development Engine:

Engine used:

- Unity

Scripting Language:

- C#

Authentication:

- Authentication handled using Firebase.

Networking:

- Photon.

Testing:

- Parallel Sync

6.2 Hardware Requirements: -

CPU (Central Processing Unit):

- A multi-core processor with at least a dual-core CPU for a smooth experience is required.

RAM (Random Access Memory):

- A minimum of 8GB of RAM is recommended for optimal performance.

Graphics Card:

- An integrated graphics card is the minimum requirement to handle low-poly assets and low-resolution textures. However, for an enhanced experience, a dedicated GPU with DirectX 11 support is preferred.

Internet Connection:

- A stable and fast internet connection is crucial for the proper functioning of the application. A broadband connection with reliable speeds is recommended.

Input Devices:

Standard input devices, such as a keyboard and mouse, are sufficient for running the application

6.3 Performance Evaluation Parameters.

Evaluating the performance of an image encryption project that uses DNA encoding and chaotic mapping is essential to ensure the security and effectiveness of the encryption scheme. Below are some key parameters and metrics you can use for performance evaluation:

Security Analysis:

Avalanche Effect: Measure how changes in the input image (even small changes) affect the encrypted image. A good encryption scheme should exhibit a strong avalanche effect, where a small change in the input results in a significantly different output.

Key Sensitivity Analysis:

Assess the sensitivity of the encryption algorithm to changes in the encryption keys. Ensure that a small change in the key results in a drastically different encrypted image.

Statistical Analysis:

Histogram Analysis: Evaluate the histogram of the encrypted image to ensure it is uniformly distributed, which is a sign of strong encryption.

Correlation Analysis:

Measure the correlation between adjacent pixels in the encrypted image. A lower correlation indicates better security.

Entropy Measurement:

Calculate the entropy of the encrypted image. Higher entropy suggests stronger encryption.

Error Analysis:

Mean Square Error (MSE): Compare the original and decrypted images using the MSE metric to quantify the quality of reconstruction.

Peak Signal-to-Noise Ratio (PSNR):

Measure the quality of the decrypted image in comparison to the original image using PSNR. Higher PSNR values are desirable.

Key Space Analysis:

Determine the size of the key space. A larger key space makes it more difficult for attackers to perform a brute-force attack.

Speed and Efficiency:

Encryption/Decryption Speed: Measure the time it takes to encrypt and decrypt an image. A practical encryption scheme should be efficient in terms of computational time.

Robustness Analysis:

Resistance to Attacks: Evaluate the encryption scheme's resistance to common attacks such as chosen-plaintext attacks, known-plaintext attacks, and differential attacks.

Randomness and Chaotic Behavior:

Lyapunov Exponent: Analyze the Lyapunov exponent of the chaotic map to assess the quality of chaos and randomness generated for encryption.

Pseudo-Random Number Generator (PRNG) Analysis:

Assess the statistical properties of the PRNG used in the encryption process.

Key Management:

Key Distribution and Management: Evaluate the security of the key distribution and management mechanisms. Ensure that keys are generated, distributed, and stored securely.

Scalability:

Scalability Analysis: Assess how well the encryption scheme performs with larger images and datasets.

Usability:

User Experience (UX) Evaluation: Gather feedback from users to assess the system's ease of use and user-friendliness.

Compliance:

Regulatory Compliance: Ensure that the encryption scheme complies with relevant data protection and privacy regulations, depending on the application.

Documentation:

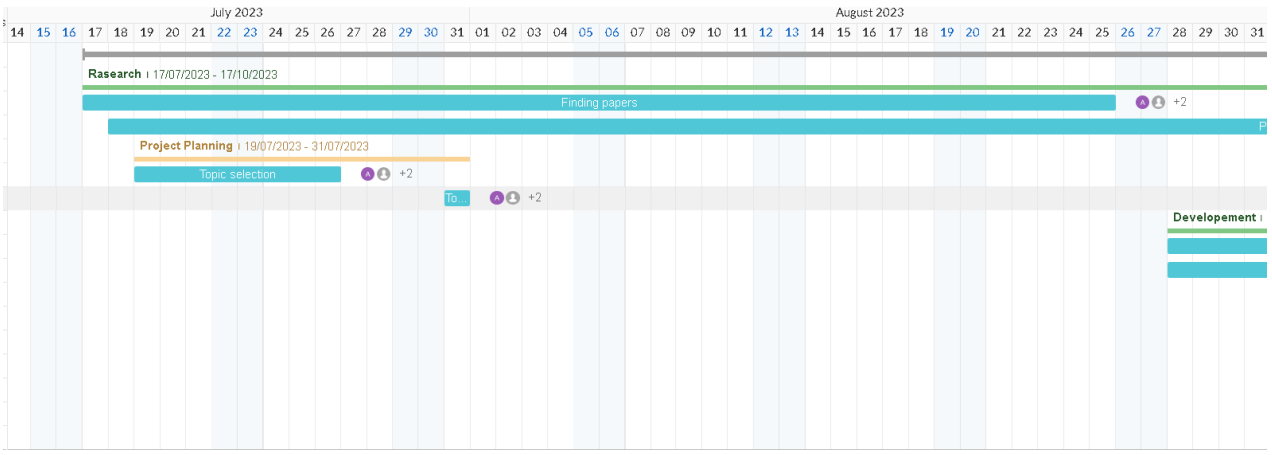
Documentation Quality: Ensure that the project documentation is clear, comprehensive, and well-organized for users and developers.

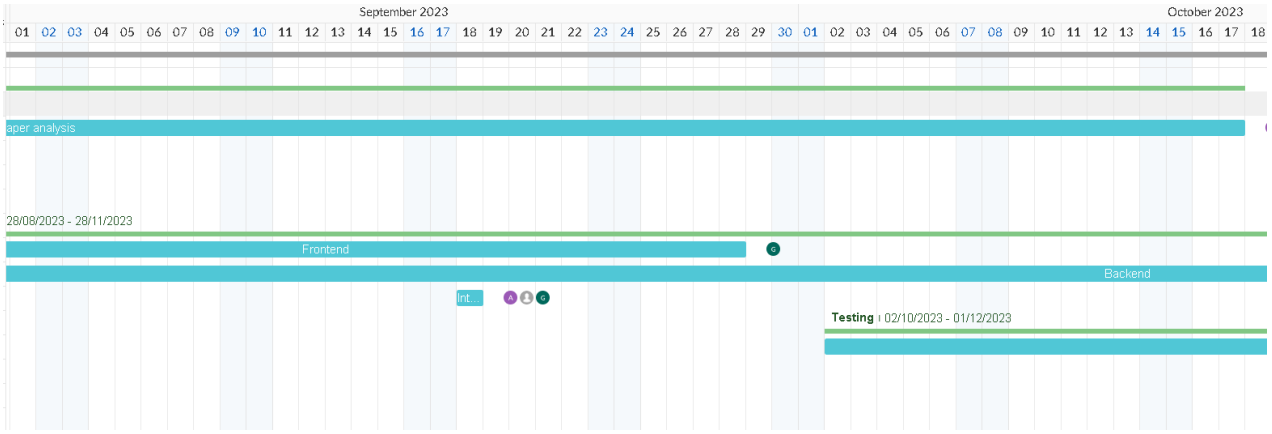
Testing:

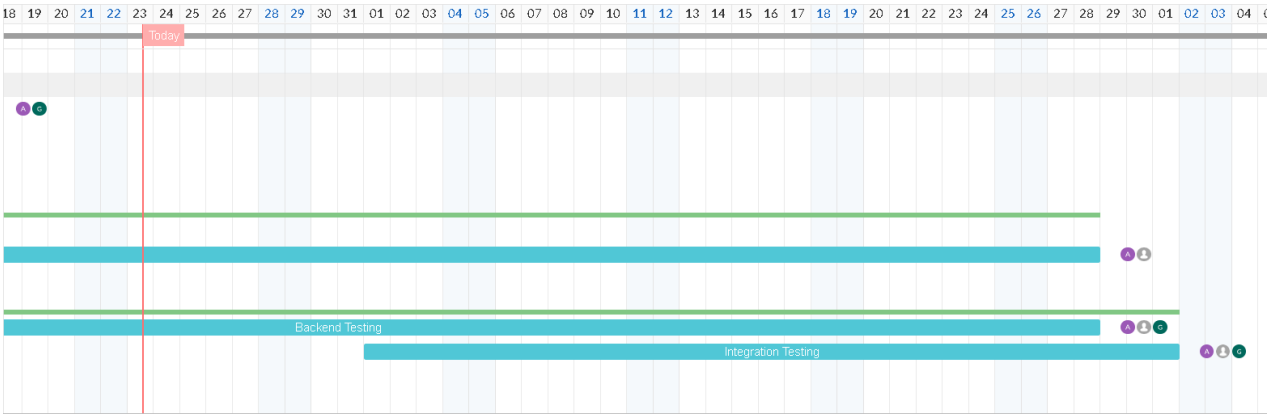
Testing and Validation: Perform extensive testing and validation, including unit testing, integration testing, and system testing, to identify and address potential issues.

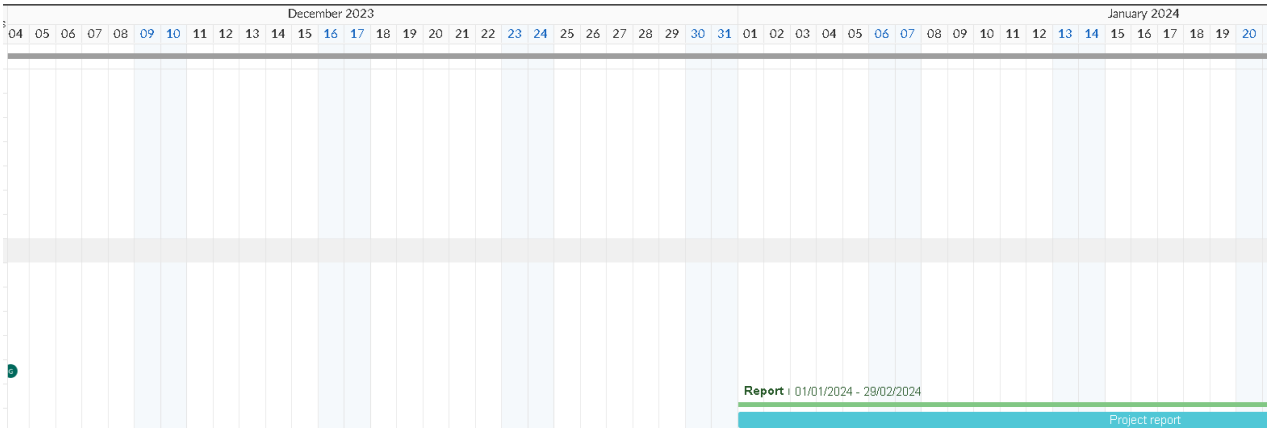
CHAPTER 7

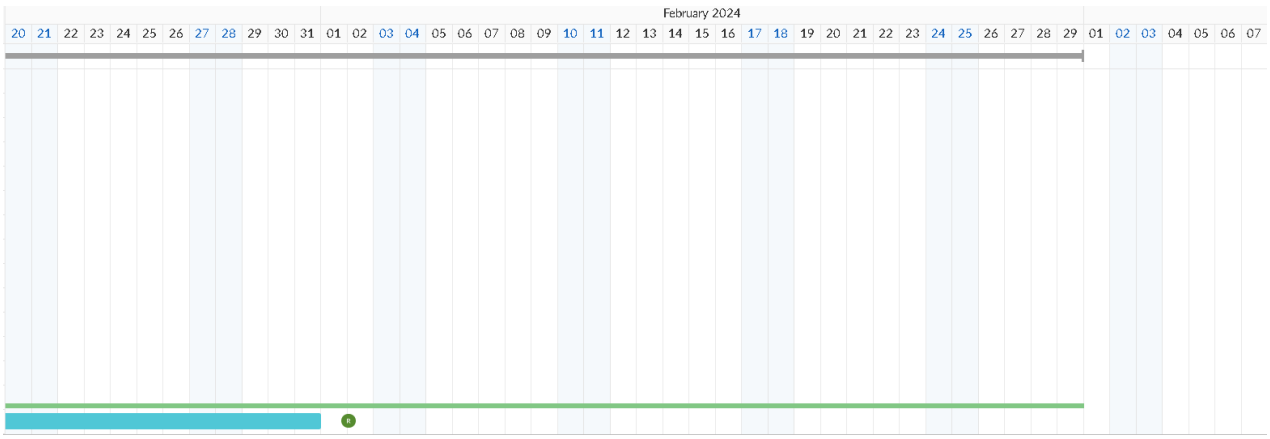
Gantt Chart








December 2023
January 2024
04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20
Report : 01/01/2024 - 29/02/2024
Project report


February 2024
20 21 22 23 24 25 26 27 28 29 30 31 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 01 02 03 04 05 06 07

CHAPTER 8

References

[1] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[2] Q. Cun, X. Tong, Z. Wang, and M. Zhang, "Selective image encryption method based on dynamic DNA coding and new chaotic map," *Optik (Stuttg)*, vol. 243, Oct. 2021, doi: 10.1016/j.ijleo.2021.167286.

[3] J. Zhang and D. Huo, "Image encryption algorithm based on quantum chaotic map and DNA coding," *Multimed Tools Appl*, vol. 78, no. 11, pp. 15605–15621, Jun. 2019, doi: 10.1007/s11042-018-6973-6.

[4] J. C. Dagadu, J. P. Li, and E. O. Aboagye, "Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion," *Wirel Pers Commun*, vol. 108, no. 1, pp. 591–612, Sep. 2019, doi: 10.1007/s11277-019-06420-z.

[5] A. Jain and N. Rajpal, "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," *Multimed Tools Appl*, vol. 75, no. 10, pp. 5455–5472, May 2016, doi: 10.1007/s11042-015-2515-7.

[6] L. Liu, Q. Zhang, and X. Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map," *Computers and Electrical Engineering*, vol. 38, no. 5, pp. 1240–1248, 2012, doi: 10.1016/j.compeleceng.2012.02.007.

[7] P. Mishra, C. Bhaya, A. K. Pal, and A. K. Singh, "A medical image cryptosystem using bit-level diffusion with DNA coding," *J Ambient Intell Humaniz Comput*, vol. 14, no. 3, pp. 1731–1752, Mar. 2023, doi: 10.1007/s12652-021-03410-7.

[8] S. Patel, V. Thanikaiselvan, D. Pelusi, B. Nagaraj, R. Arunkumar, and R. Amirtharajan, "Colour image encryption based on customized neural network and DNA encoding," *Neural Comput Appl*, vol. 33, no. 21, pp. 14533–14550, Nov. 2021, doi: 10.1007/s00521-021-06096-2.