

**SEED PHRASE ENCRYPTION AND
DECRYPTION AND TEXT TO IMAGE
ENCODING OF OCTAL
REPRESENTATION**

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

By

**KARTHIK M (Reg .No – 40110557)
SHERLINE SHEELA A (Reg.No – 40111196)**



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING**

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

**Accredited with Grade “A++” by NAAC
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI - 600119**

NOVEMBER – 2023

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **KARTHIK M (Reg.No-40110557)** and **SHERLINE SHEELA A (Reg.No-40111196)** who carried out the project entitled "**SEED PHRASE ENCRYPTION AND DECRYPTION AND TEXT TO IMAGE ENCODING OF OCTAL REPRESENTATION**" under my supervision from November 2023 to April 2024.

Internal Guide

Dr. SREE KRISHNA M M.E., Ph.D.

HEAD OF THE DEPARTMENT
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Dr. L. LAKSHMANAN M.E., Ph.D.
Contact - 990 119

Submitted for Viva voce Examination held on 15.04.2024

of yonisha
15/4/24
Internal Examiner

15/4/24
External Examiner

DECLARATION

I, **Karthik M (Reg No- 40110557)**, hereby declare that the Project Phase-1 Report entitled “**SEED PHRASE ENCRYPTION AND DECRYPTION AND TEXT TO IMAGE ENCODING OF OCTAL REPRESENTATION**” done by me under the guidance of **Dr. Sreekrishna M.E., (Ph.D.)** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**.

A handwritten signature in black ink, appearing to read 'Karthik', is centered within a light gray rectangular box.

DATE:

PLACE: Chennai

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T.Sasikala M.E., Ph. D, Dean**, School of Computing, **Dr. L. Lakshmanan M.E., Ph.D.**, Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. Sreekrishna M.E., (Ph.D.)** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my phase-1 project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

This project outlines a comprehensive approach for the secure transformation of textual data into encrypted image format through the integration of the Advanced Encryption Standard (AES) algorithm and an intricate octal representation technique. The utilization of AES encryption ensures the protection and confidentiality of the textual content, enhancing the security measures against unauthorized access. By mapping octal digits to pixel values, the encrypted image construction becomes visually complex, further fortified by the introduction of "junk digits" to obscure the original data. A key feature of the project is the implementation of a specialized functionality that facilitates the seamless identification and decryption of the encrypted image within a collection of images, ensuring secure retrieval of the original text. This framework offers an effective solution for enhancing data security and privacy, catering to the increasing demand for safeguarding sensitive information in a digital environment. This abstract provides an overview of the combined approach involving seed phrase encryption and decryption, along with text-to-image encoding using octal representation. The integration of cryptographic security and innovative data representation techniques offers a versatile solution with broad applicability in secure communication, storage, and visual representation of data.

TABLE OF CONTENTS

Chapter No.	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	viii
1	INTRODUCTION	1
2	LITERATURE SURVEY	
	2.1 Inferences from Literature Survey	3
	2.2 Open problems in Existing System	5
3	REQUIREMENTS ANALYSIS	
	3.1 Feasibility Studies/Risk Analysis of the Project	7
	3.2 Software Requirements Specification Document	10
4	DESCRIPTION OF PROPOSED SYSTEM	
	4.1 Selected Methodology or process model	13
	4.2 Architecture / Overall Design of Proposed System	14
	4.3 Description of Software for Implementation and Testing plan of the Proposed Model/System	15
	4.4 Project Management Plan	17
	REFERENCES	19

LIST OF FIGURES

Figure No.	FIGURE NAME	Page No.
4.1.1	Encryption model	13
4.1.2	Decryption model	13
4.2.1	Architecture model	14

CHAPTER 1

INTRODUCTION

Seed Phrase Encryption and Decryption: In the landscape of cryptography, the concept of a "seed phrase" holds critical significance, acting as the foundational element for generating cryptographic keys. The proposed method for encrypting and decrypting the seed phrase emphasizes the paramount importance of preserving the confidentiality and integrity of this essential cryptographic component. Through a meticulously designed encryption process, the seed phrase is transformed into an indecipherable format, ensuring that it remains impervious to unauthorized access. The corresponding decryption operation serves as a reliable means of restoring the original seed phrase securely, thereby enabling authorized entities to access and utilize the cryptographic keys as needed. Notably, the robustness and efficiency of the encryption and decryption procedures are carefully crafted to withstand potential security breaches, reinforcing the overall protection of sensitive cryptographic data against various forms of malicious attacks.

Text-to-Image Encoding using Octal Representation: In the context of data representation, the conversion of textual information into visually comprehensible images represents a significant advancement in data visualization techniques. By incorporating the octal representation methodology, which operates within a base-8 numerical system, the proposed approach demonstrates a sophisticated means of encoding textual data into an image-based format. This intricate encoding process involves the mapping of individual characters or groups of characters from the text to their corresponding octal values. Subsequently, these designated octal values are meticulously translated into pixel values, culminating in the creation of a comprehensive and visually coherent representation of the original textual data. The utilization of the octal representation technique not only ensures the secure encapsulation of textual information within the resulting images but also fosters an intuitive and visually compelling medium for conveying complex data sets.

Integration and Synergy: The seamless integration of the seed phrase encryption and decryption mechanism with the octal-based text-to-image encoding strategy embodies a holistic and comprehensive approach to data security and representation. By harmonizing these two crucial components, the combined approach establishes a robust framework that not only safeguards the confidentiality of cryptographic keys but also facilitates the effective visualization and representation of intricate textual data. This synergistic fusion of cryptographic security and innovative data representation techniques contributes to the development of a versatile and adaptable solution with widespread applicability across diverse domains, including secure communication protocols, resilient data storage systems, and visually enhanced data presentation methodologies.

This comprehensive overview underscores the intrinsic value of the combined approach, emphasizing its profound implications for reinforcing data security, promoting effective communication, and enhancing the visual representation of sensitive information across various applications and use cases.

CHAPTER 2

LITERATURE SURVEY

2.1 INFERENCES FROM LITREATURE SURVEY

1. Ahmad Abusukhon, Shadi AlZu'bi , New Direction of Cryptography: A Review on Textto- Image Encryption Algorithms Based on RGB Color Value

This paper reviewed the works carried out in the direction of text encryption based on mapping a text into an image. The mapping process is based on the RGB color value. In this context, a comparison between various recent works is held based on various factors such as the encryption technique, on the fly/database storage, the use of standard algorithms and the use of block encryption algorithm.

2. B. Karthikeyan B. Bharathkumar G.Manikandan R. Seethalakshmi A Combination of RSA Algorithm with Image Steganography to Ensure Enhanced Encryption

In this work, a method that encrypts data embedded into an image in the proper manner was proposed. The entire process results in improved data security at a really highlevel. Four new levels of encrypting techniques to keep messages private were implemented in this work. The plaintext has been divided into odd-numbered lines and even numbered lines and two different encryption processes are performed on each of the parts. Finally, the encrypted plaintext is injected into an image. This technique can be used in defense, banking, and e-commerce sectors where it can produce good results by preventing attackers from attacking the data. The time consumed for the encryption process ismuch higher compared to other processes because four levels of encryption are being performed.

3. Dr. Himanshu Arora, Dr. Pramod Kumar Sharma ,Km Mitanshi, Aayush Choursia Enhanced Security of Digital Picture and Text Information with Hybrid Model of Hiding and Encryption Techniques

In this introduced hybrid model of hiding and encryption that is utilized to work on the security of the advanced picture and text. For hiding XOR procedure is used and for encryption reason AES calculation is utilized.. Utilizing proposed strategy give the multi-facet of insurance to the secret text information and secret picture. So utilizing the proposed procedure upgrades the security of digital picture and text information

4. K.Malathi R.Kavitha MKLiza Pixel based method for Text to Image Encryption

In this paper, an efficient way for transacting the text is proposed. The technique used is namely text to image encryption. The three concepts had provided an enhanced outcome by providing a required memory space, evaluate the text and then it produces a better description about it. This technique has provided a better security in transferring the text in the secure form.

5. Heidilyn V. Gamido¹ , Ariel M. Sison² , Ruji P. Medina³, Modified AES for Text and Image Encryption

The paper used bit permutation to replace the Mix Columns Transformation of AES to improve the efficiency of AES. The paper compared the performance of the standard and modified AES algorithm by encrypting text files and images. The two algorithms were evaluated based on their encryption time, CPU usage and avalanche effect. Based on the results, the modified AES has increased the efficiency of the standard AES as it has faster encryption time in text files and images. The modified AES also consumed lesser CPU usage than the standard AES. During the testing, the modified algorithm also produced higher avalanche effect. Therefore, the use of the bit permutation in modified AES increased the efficiency, level of security and overall performance of the algorithm in encrypting text files and images.

2.2 OPEN PROBLEMS IN EXISTING SYSTEM

Text to image encryption using RGB substitution is a specialized area that involves converting textual data into an image by manipulating the RGB components of pixels. Here are potential open problems and challenges in this domain:

1. Security and Cryptanalysis:

Analyzing the security of RGB substitution-based encryption against various cryptographic attacks, including statistical attacks, differential attacks, or other known vulnerabilities. Understanding the robustness of the technique is crucial.

2. Encryption Strength vs. Perceptual Integrity:

Balancing encryption strength with the perceptual integrity of the resulting image. Striking the right balance to ensure that the encrypted image retains meaningful visual information while maintaining a high level of security.

3. Key Management and Distribution:

Designing secure and efficient key management mechanisms for RGB substitution-based encryption. Addressing issues related to key generation, distribution, and protection against unauthorized access.

4. Adversarial Attacks and Steganalysis:

Investigating the vulnerability of the encrypted images to adversarial attacks and steganalysis. Enhancing the technique to be robust against attempts to detect or manipulate the hidden information.

5. Efficiency and Scalability:

Optimizing the encryption and decryption processes to be efficient and scalable, particularly for large-sized images and large volumes of textual data. Enhancing performance without compromising security.

6. Enhanced Embedding Capacity:

Increasing the embedding capacity to allow for more text to be securely embedded within an image while maintaining encryption strength and avoiding perceptual degradation.

7. Integration with Communication Protocols:

Integrating the RGB substitution encryption technique with existing communication protocols or platforms to enable secure text-to-image transmission over networks while maintaining compatibility and security.

8. Quantitative Metrics for Image Quality:

Developing standardized quantitative metrics to evaluate the quality of the resulting images in terms of information hiding capacity, visual fidelity, and resistance to attacks.

9. Real-Time Processing and Streaming:

Addressing the challenge of real-time processing and streaming of text-to-image encryption using RGB substitution, particularly for applications that require quick and continuous encryption and decryption.

10. Usability and User Experience:

Enhancing the user interface and experience for both encrypting and decrypting text into images and vice versa, ensuring a seamless and intuitive process for end-users.

11. Interoperability and Standardization:

Establishing standards or guidelines for text-to-image encryption using RGB substitution to promote interoperability and facilitate integration with various systems and applications.

Researchers and practitioners in this domain should actively explore and address these open problems to advance the field of text-to-image encryption using RGB substitution, ensuring a strong balance between security, efficiency, and usability. Collaboration and rigorous testing will be essential for making meaningful progress in this area.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 FEASIBILITY STUDIES/RISK ANALYSIS OF THE PROJECT

Analyzing the risks associated with the combined approach of seed phrase encryption and decryption, along with text-to-image encoding using octal representation, is essential for understanding potential vulnerabilities and ensuring a secure system. Here's a risk analysis of this combined approach:

1. Encryption Algorithm Weaknesses:

Risk: The encryption algorithm used for seed phrase encryption and octal representation encoding might have weaknesses, making it susceptible to various attacks, such as brute force, cryptanalysis, or known-plaintext attacks.

Mitigation: Employing well-established and thoroughly analyzed encryption algorithms, staying updated with cryptographic best practices, and continuously monitoring and adapting to new vulnerabilities can mitigate this risk.

2. Inadequate Key Management:

Risk: Weaknesses in key generation, storage, or distribution can compromise the entire encryption-decryption process, making it easier for attackers to decrypt the seed phrase or manipulate the encoded images.

Mitigation: Implementing secure key management practices, including strong key generation, secure storage, access controls, and periodic key updates, can mitigate this risk.

3. Adversarial Attacks on Image Encoding:

Risk: Adversarial attacks, such as input manipulation or model inversion, could potentially manipulate the encoded image, revealing sensitive information or compromising the integrity of the seed phrase.

Mitigation: Implementing robustness checks, using anti-adversarial techniques, and ensuring a secure encoding process can mitigate the risk of adversarial attacks.

4. Data Loss or Corruption:

Risk: Loss or corruption of the encoded images or encryption keys could result in the irreversible loss of seed phrases or make decryption impossible, leading to loss of access to critical data.

Mitigation: Implementing robust backup and recovery mechanisms, securely storing and managing data, and regularly validating data integrity can mitigate the risk of data loss or corruption.

5. Interoperability Issues:

Risk: Integration challenges or lack of compatibility with existing systems or applications could hinder the widespread adoption and usage of the combined approach.

Mitigation: Designing the system with interoperability in mind, following relevant standards, and conducting thorough integration testing can mitigate interoperability risks.

6. User Error or Negligence:

Risk: Human error, such as sharing encryption keys accidentally or mismanaging the seed phrase, can jeopardize the security of the encrypted data.

Mitigation: Providing user education, implementing user-friendly interfaces, and employing access controls and verification mechanisms can mitigate risks associated with user error or negligence.

7. Insufficient Encryption Strength:

Risk: If the encryption strength is insufficient, attackers may easily decrypt the seed phrase or reverse-engineer the original text from the octal representation.

Mitigation: Using strong encryption algorithms, appropriate key lengths, and periodic security assessments can mitigate the risk of insufficient encryption strength.

8. Privacy Violations during Image Transmission:

Risk: Transmitting images for text-to-image encoding may expose sensitive data, leading to potential privacy violations.

Mitigation: Implementing secure transmission protocols, encryption of transmitted data, and ensuring data privacy compliance can mitigate risks associated with image transmission.

Regular risk assessments, threat modeling, and security audits are crucial to identify, analyze, and mitigate risks effectively. Collaboration with security experts and adherence to best practices in cryptography and information security are essential to build a robust and secure system for this combined approach.

3.2 SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

To implement a system for seed phrase encryption and decryption, along with text-to-image encoding using octal representation, you will need a set of software components and tools. Below are the essential software requirements for this combined approach:

1. Programming Languages:

Python: A versatile and widely used programming language suitable for both cryptographic operations and image processing.

2. Cryptography Libraries:

Cryptography: A Python library that provides various cryptographic algorithms for encryption and decryption.

hashlib: A Python library for secure hashing.

PyCryptodome: A self-contained Python package of low-level cryptographic primitives.

3. Image Processing Libraries:

PIL (Python Imaging Library) or Pillow: Python libraries for opening, manipulating, and saving many different image file formats.

OpenCV: An open-source computer vision and machine learning library with functionalities for image manipulation and processing.

4. Machine Learning Libraries:

TensorFlow : Deep learning frameworks that can be used for training models to generate meaningful images from octal representations.

5. Web Framework:

To create a web application, web framework like Django, Flask, or React is used

6. Development Environment:

Visual Studio Code : Code editor or integrated development environment (IDE)

such for writing and managing your code.

7. Dependency Management:

pip: The package installer for Python. To install and manage dependencies.

8. Testing Frameworks:

Unittest (built-in) : Testing framework for writing and running tests to ensure the functionality and robustness of your code.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

For Seed Phrase Encryption and Decryption, several key steps must be implemented. Initially, a secure Seed Phrase Generation technique, employing the BIP-39 standard or similar cryptographic algorithms, should be adopted. Following this, a resilient Encryption Algorithm like AES (Advanced Encryption Standard) must be applied to safeguard the seed phrase. To ensure the protection of encryption keys, secure key management practices, including the use of hardware security modules (HSMs) or key management systems, should be implemented. Moreover, a well-designed Decryption Mechanism is crucial to securely retrieve the original seed phrase using the appropriate decryption key, incorporating secure protocols to restrict access to authorized users only.

For the Text to Image Encoding of Octal Representation, the process involves first converting the input text into its octal representation through ASCII encoding or Unicode encoding. Subsequently, an Image Encoding Algorithm must be devised to accurately map these octal values to pixel values in an image, considering parameters such as image resolution, color depth, and pixel arrangement. Utilizing the encoded pixel values, an image can be generated in formats such as JPEG, PNG, or BMP, with necessary security measures like data integrity checks, watermarking, and encryption to safeguard the encoded image against unauthorized access and tampering.

Regarding System Integration and User Interface, an intuitive and user-friendly interface should be developed to facilitate user interactions with the system. This interface would allow users to input seed phrases, perform data encryption and decryption, and convert text to images seamlessly. Additionally, seamless functionality within the system necessitates the integration of the seed phrase encryption and decryption module with the text-to-image encoding module, ensuring a cohesive and unified user experience.

4.1 SELECTED METHODOLOGY OR PROCESS MODEL

ENCRYPTION:

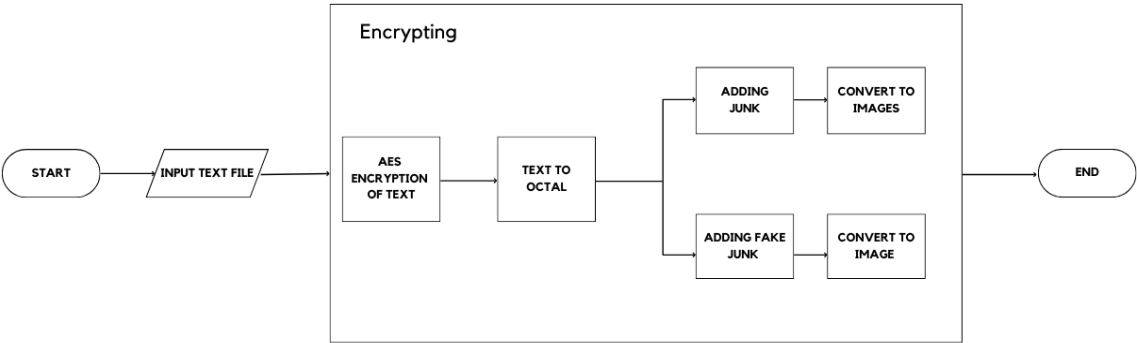


Fig.4.1.1 Encryption Model

DECRYPTION:

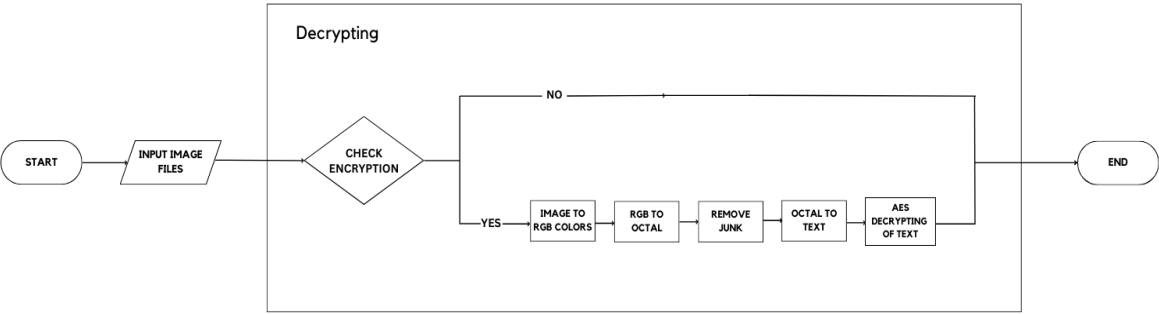


Fig.4.1.2 Decryption Model

4.2 ARCHITECTURE / OVERALL DESIGN OF PROPOSED SYSTEM

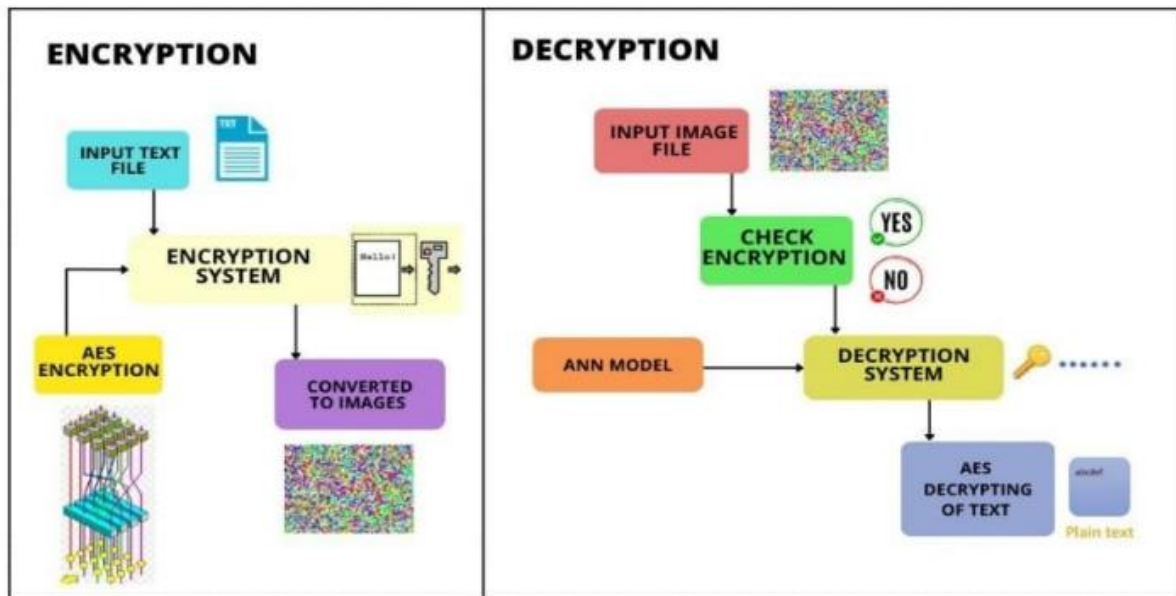


Fig.4.2.1 System Architecture

4.3 DESCRIPTION OF SOFTWARE FOR IMPLEMENTATION AND TESTING PLAN OF THE PROPOSED MODEL/SYSTEM

FRONT END TOOLS	React, CSS
BACK END TOOLS	Python-Flask
MARKUP LANGUAGES	HTML
SCRIPTING LANGUAGES	JavaScript, Python
IDE	Visual Studio Code

React, CSS - The project requires a front-end framework to create a responsive and interactive user interface. React is a popular JavaScript library that allows for easy component-based development, and CSS is used to style and design the components.

Python-Flask - The project requires a back-end framework to handle server-side processing and to interact with databases. Python-Flask is a lightweight and efficient framework that is easy to use and provides a lot of flexibility.

HTML - The project requires HTML to structure and display content on the front-end. HTML is the standard markup language for creating web pages and provides the necessary structure for displaying content.

Javascript, Python - The project requires both JavaScript and Python for various tasks. JavaScript is used for client-side scripting and interactivity, while Python is used for server-side processing, database handling, and other tasks.

Visual Studio Code - The project requires an integrated development environment (IDE) to develop and test the code. Visual Studio Code is a popular and powerful IDE that provides a range of features, including debugging, syntax highlighting, and Git integration. It is also highly customizable and supports many programming languages.

4.4 PROJECT MANAGEMENT PLAN

1. Project Overview:

- **Project Title:** Seed Phrase Encryption and Decryption & Text to Image Encoding of Octal Representation
- **Project Duration:** 06/2023 – 12/2023

2. Project Objectives:

- Develop a secure and efficient seed phrase encryption and decryption mechanism.
- Implement a robust text-to-image encoding process for octal representation.
- Ensure seamless integration of the two functionalities for enhanced data security.
- Conduct rigorous testing to guarantee the reliability and performance of the system.

3. Scope and Deliverables:

- **Seed Phrase Encryption and Decryption:**
 - Algorithm Design
 - Code Implementation
 - Encryption Testing
 - Decryption Testing
 - Documentation
- **Text to Image Encoding of Octal Representation:**
 - Encoding Algorithm Design
 - Image Generation Functionality
 - Integration Testing
 - Performance Testing
 - Documentation
- **Integration of Functionalities:**
 - Comprehensive Testing
 - Bug Fixing
 - Documentation

4. Risk Management:

- **Data Security Risks:** Mitigate the risk of data breaches during encryption and transmission.
- **Integration Challenges:** Anticipate potential issues during the integration of encryption and image encoding modules.
- **Resource Constraints:** Ensure sufficient resources are available throughout the project duration.

5. Communication Plan:

- To discuss progress, issues, and upcoming tasks.
- Immediate communication in case of critical issues or roadblocks.

6. Quality Assurance:

- Regular testing at each stage of development.

7. Project Closure:

- Final documentation and report preparation.

CONCLUSION

This project management plan aims to provide a structured approach for the successful execution of the Seed Phrase Encryption and Decryption & Text to Image Encoding of Octal Representation project. Regular monitoring, evaluation, and communication are crucial to ensure that the project progresses smoothly within the specified time and budget constraints.

REFERENCES:

1. Ahmad Abusukhon, Shadi AlZu'bi , New Direction of Cryptography: A Review on Text to- Image Encryption Algorithms Based on RGB Color Value, 2020 Seventh International Conference on Software Defined Systems (SDS) UTC from IEEE Xplore.
2. B. Karthikeyan B. Bharathkumar G.Manikandan R. Seethalakshmi A Combination of RSA Algorithm with Image Steganography to Ensure Enhanced Encryption Proceedings of the Second International Conference on Electronics and Renewable Systems (ICEARS-2023) IEEE Explore.
3. Dr. Himanshu Arora, Dr. Pramod Kumar Sharma ,Km Mitanshi, Aayush Choursia Enhanced Security of Digital Picture and Text Information with Hybrid Model of Hiding and Encryption Techniques (ICSCDS-2022) IEEE Xplore.
4. K.Malathi R.Kavitha MKLiza Pixel based method for Text to Image Encryption Fourth International Conference on Electronics, Communication and Aerospace Technology (ICECA-2020) IEEE Xplore.
5. Heidilyn V. Gamido¹ , Ariel M. Sison² , Ruji P. Medina³, Modified AES for Text and Image Encryption, 2020 Institute of Advanced Engineering and Science. Indonesian Journal of Electrical Engineering and Computer Science.
6. Amal Joshy,Amitha Baby K X, Padma S, Fasila K A, Text to Image Encryption Technique using RGB Substitution and AES ,2017 UTC from IEEE Xplore.
7. Flevina Jonese D'souza, Dakshata Panchal, Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach 2017 International Conference on Computing, Communication and Automation (ICCCA2017) UTC from IEEE Xplore.
8. Daniel F. García, Performance Evaluation of Advanced Encryption Standard Algorithm, 2021 Second International Conference UTC from IEEE Xplore.
9. Dodis, Yevgeniy, et al. "Key-insulated symmetric key cryptography and mitigating attacks against cryptographic cloud software." Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. ACM, 2012.
10. M Arun, S.MohamedAzarudeen and T.N. Nivek, AES based Text to Pixel Encryption using Color Code Conversion by Modulo Arithmetic, International Journal of Recent Research in Science, Engineering and Technology Vol. 1, Issue 3, June 2015.

11. Z. Musliyana, T. Y. Arif and R. Munadi, "Security Enhancement of Advanced Encryption Standard (AES) using Time-Based Dynamic Key Generation," ARPN Journal of Engineering and Applied Sciences, vol.10, October 2015.