NEIL GOGTE INSTITUTE OF TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

INTEGRATING CRYPTOGRAPHY AND STEGANOGRAPHY FOR ROBUST DATA PROTECTION IN IMAGES

Presented By:

Godda Rushendar Reddy	245321733154
K. Sathwika	245321733318
Sury Supriya	245321733319

Under the Guidance
Of

Dr. R.Srilakshmi
Assistant Professor

CONTENTS

1. Introduction
2. Existing System

    2.1 Disadvantages

3. Proposed System

    3.1 Advantages

4. System Architecture
5. Modules
6. Software Requirements
7. UML diagrams
8. Results
9. Conclusion & Future Scope
10. References

INTRODUCTION

Overview of the project

- In today's digital age, protecting sensitive information from unauthorized access and tampering is crucial, especially when transmitted through unsecured channels.
- To address this challenge, the integration of cryptography and steganography has emerged as a powerful solution for securing data.
- Cryptography, using encryption algorithms like AES, RSA, and Diffie-Hellman, ensures data confidentiality, integrity, and authentication. Steganography specifically through techniques like Least Significant Bit (LSB), allows for embedding encrypted data within images, making it less detectable.

Problem Statement

- The problem at hand is the increasing demand for stronger data protection in digital communication.
- Existing cryptographic methods may not be sufficient to meet this demand, leading to the need for innovative solutions. 'Crystography' is introduced as a blend of cryptography and steganography to enhance information security by covertly embedding encrypted data within images, a common medium of communication.
- This problem statement emphasizes the necessity of such innovative approaches in safeguarding sensitive information in the digital data exchange landscape.

LITERATURE SURVEY / EXISTING SYSTEM

Existing Systems:

● In existing systems for information security, Standard encryption algorithms like AES, RSA and Deffie-helman are commonly used for cryptography to provide confidentiality, integrity, and authentication of data.

● For steganography, the Least Significant Bit (LSB) technique is one of the most common methods used to hide data within other media, such as images or audio files, without apparent changes to the cover medium.

CONT..

Limitations:

- WorkLow robustness against compression or noise.
- Vulnerable to statistical steganalysis.
- Lack of integration between cryptography and steganography.
- Poor adaptability across image formats and sizes.
- Limited GUI or real-time usability.

PROPOSED SYSTEM

- The proposed system integrates cryptography and steganography to enhance data protection within digital images. Initially, a symmetric key cryptographic algorithm encrypts the secret message using a private key KKK generated by a key generation algorithm.

- Subsequently, the encrypted message (ciphertext) is embedded into a cover image using the 3-3-2 Least Significant Bit (LSB) insertion method.

- This technique distributes the ciphertext bits across the red, green, and blue channels of the image in a 3-3-2 pattern, effectively concealing the data while maintaining image quality.

- To retrieve the hidden message, the process is reversed: the stego image is analyzed to extract the embedded bits, which are then decrypted using the private key KKK to recover the original secret message.

CONT..

Key Innovations & Improvements

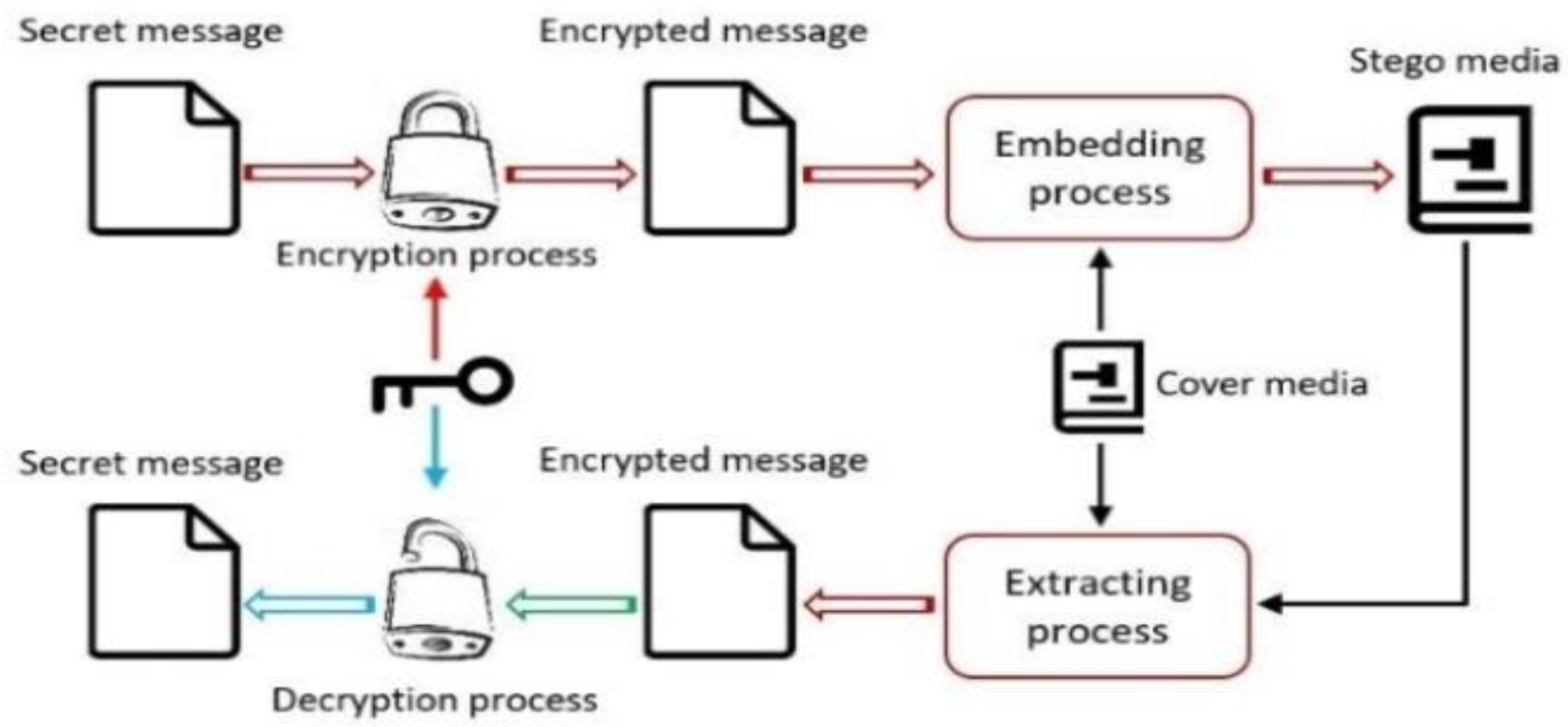
- **Crystography:** Combines cryptography and steganography into a unified technique called "crystography" to enhance data security.
- **Dynamic Private Key Generation:** Introduces a method to generate private keys dynamically based on random character positions in the message, increasing unpredictability.
- **Metadata Embedding within Image:** Embeds encryption metadata into the last row of the image, enabling self-contained stego images that do not require external key files.

CONT..

Objectives of the Project

- To enhance data security by integrating twopowerful techniques-cryptography and steganography-into a unified approach called crystography.
- To encrypt the user’s message using a custom symmetric key cryptographic algorithm with a dynamically generated private key.
- To embed the encrypted message into an image using a novel 3-3-2 LSB (Least Significant Bit) steganographic technique that leverages human visual limitations to ensure imperceptibility.
- To provide a user-friendly software tool with GUI features using Python and Tkinter that facilitates.

SYSTEM ARCHITECTURE



CONT..

Private Key generation algorithm

1. Find the length n of the string.

2. Generate a random number between 1 to n.

3. Go to the r*th* character of the string.

4. Get the ASCII value for the r*th* character and generate the 8-bit equivalent binary value.

5. Select the 4-digit key (value must be greater than or equal to (1000)2 or 8) as K from the first 4 bits of the binary value. If the condition is not satisfied then move for the next 4 bits and do the same check again.

6 .If K is not found from the previous steps, then repeat the same process from step 1 to step 5.

CONT..

Encryption Algorithm

1. Generate the ASCII value of all the letters.
2. Divide all the values with K.
3. Store the quotient as 4 MSB bits and remainder as 4 LSB bits. Represent both quotient and remainder in 4-bit binary representation.
4. Reverse all the 8-bit binary number(s).
5. Now the resultant binary set of numbers after the above operations is the secret encrypted cipher text, ready to use for the second step.

CONT..

Decryption Algorithm

1. Reverse all the 8-bit numbers of H.
2. Multiply 4 MSB bits of all the ciphertext by the Key K.
3. Add 4 LSB bits of the cipher text with the result produced in the previous step.
4. If the result produced in the previous step is not an 8-bit number we need to make it an 8-bit number by adding 0s (Zeros) in the left hand side.
5. All the numbers in 8 bits become the original text i.e. The Plain Text or Secret data.

MODULES

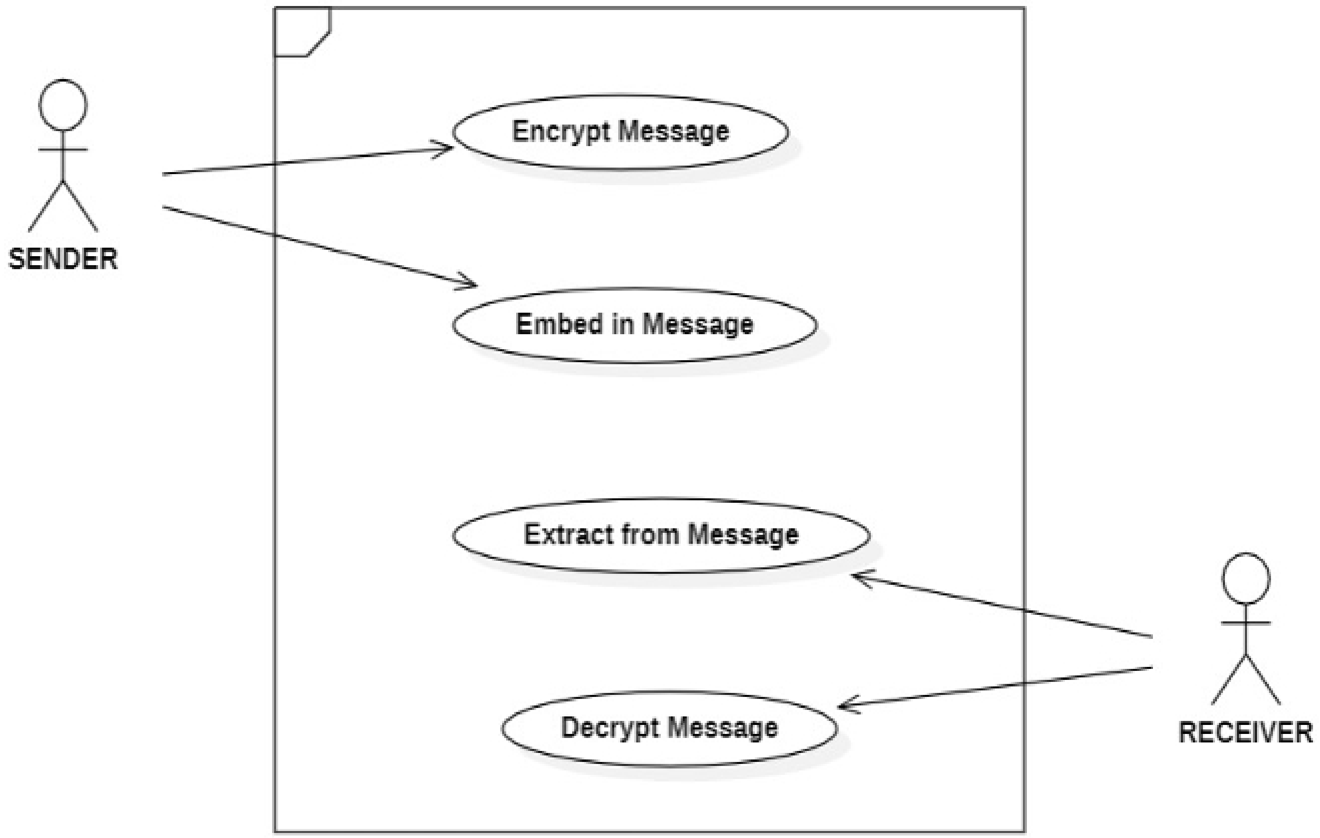
Technology/Method	Description	Limitations/Challenges
AES (Advanced Encryption Standard)	Symmetric key encryption for secure data transmission	Key management and detection risks if used without concealment
RSA (Rivest–Shamir–Adleman)	Public-key cryptographic algorithm	Computationally expensive and vulnerable if not combined with concealment
Diffie-Hellman	Key exchange protocol for secure communication	Does not encrypt messages directly; vulnerable to man-in-the-middle attacks
LSB Steganography	Embeds data in Least Significant Bits of images/audio	Easily detectable through statistical analysis; lacks robustness against compression or image manipulation
Basic LSB Patterns	Standard embedding in fixed LSB positions	Predictable, making it susceptible to steganalysis

SOFTWARE REQUIREMENTS

Libraries and Frameworks used:

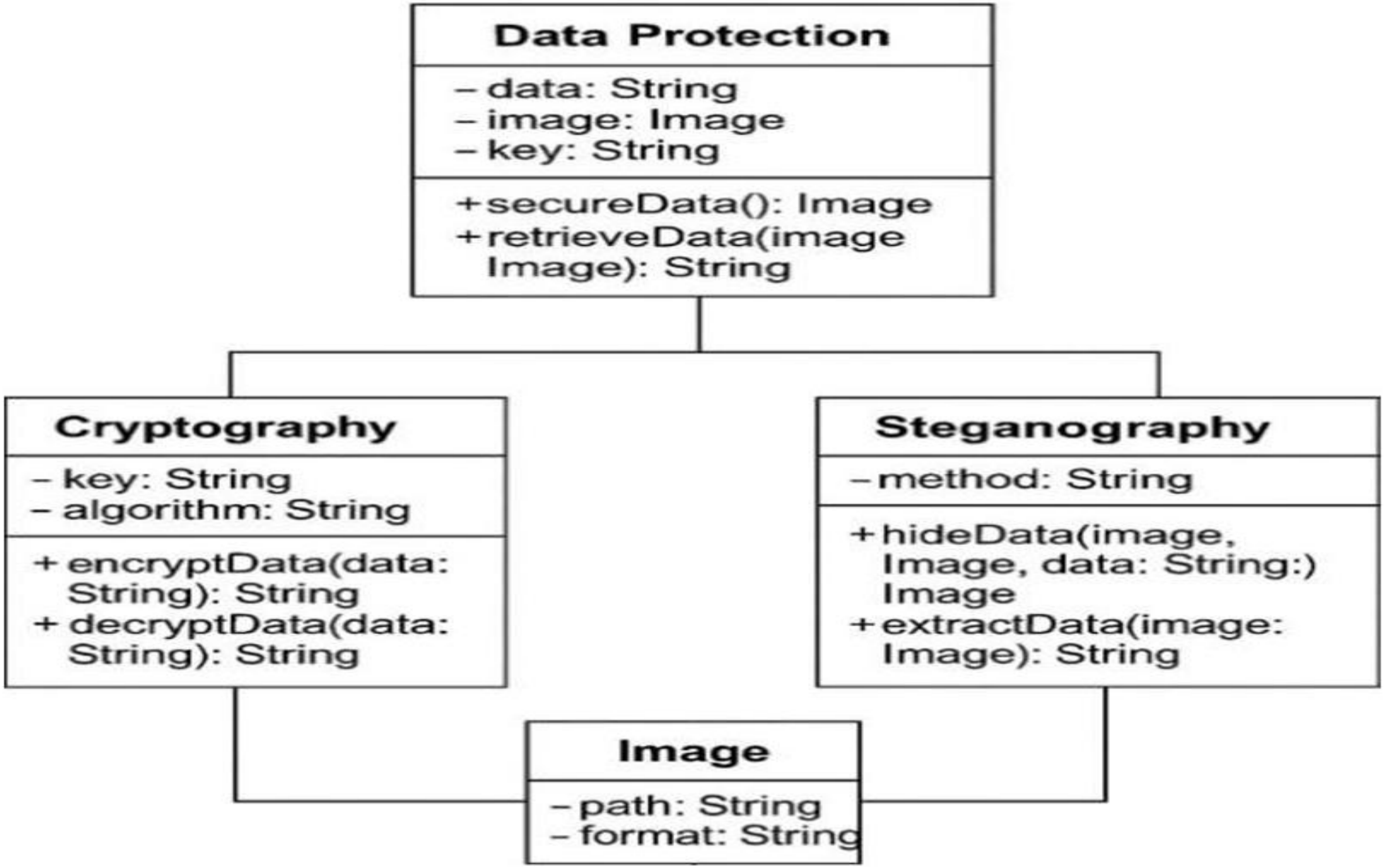
- Tkinter
- PIL(Python Imaging Library)
- Python
- Hashlib
- Pathlib
- os
- Random
- Numpy

UML DIAGRAMS



Use Case Diagram

CONT..



Data Protection

– data: String
– image: Image
– key: String

+secureData(): Image
+retrieveData(image Image): String

Cryptography

– key: String
– algorithm: String

+ encryptData(data: String): String
+ decryptData(data: String): String

Steganography

– method: String

+ hideData(image, Image, data: String:) Image
+ extractData(image: Image): String

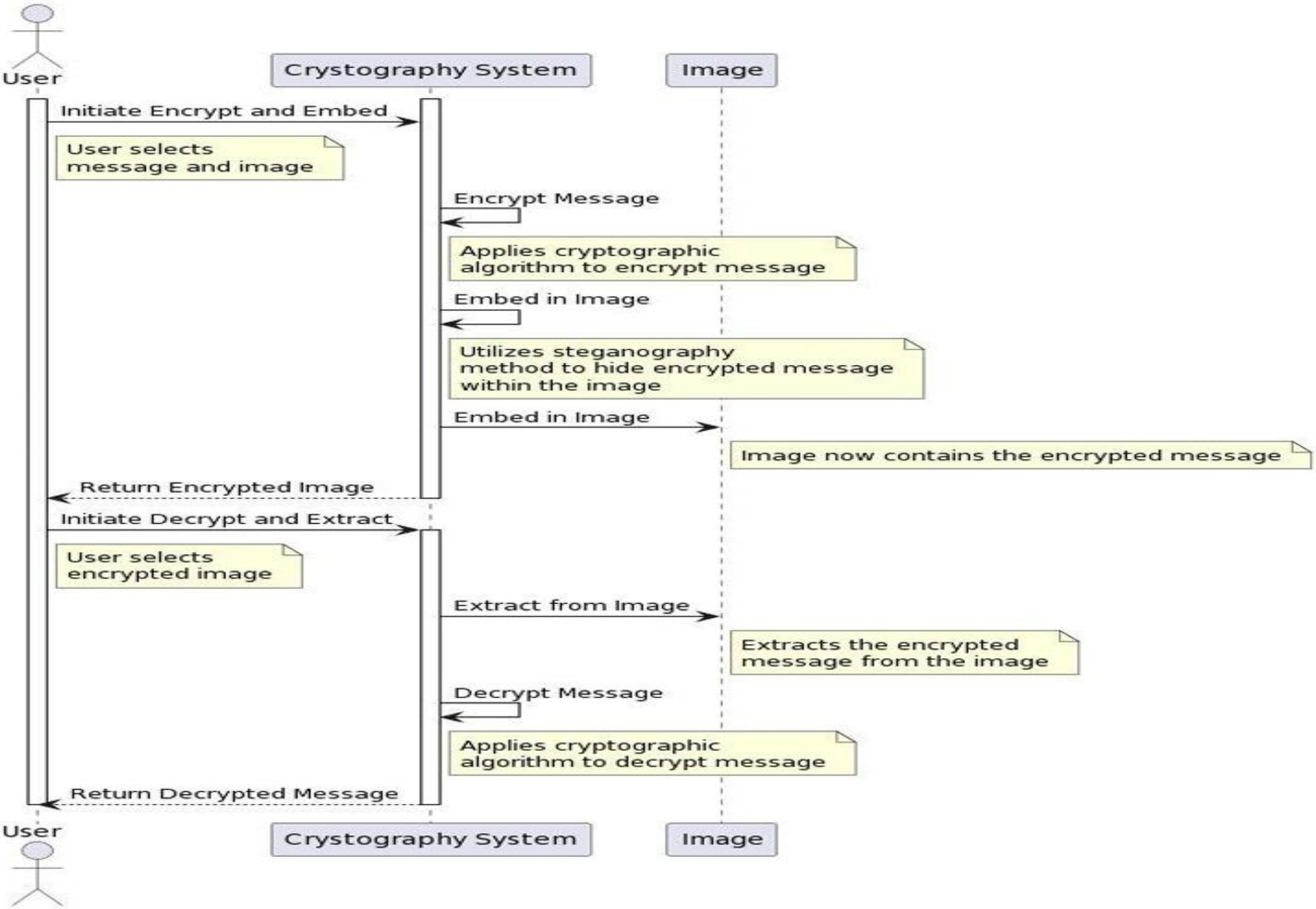
Image

– path: String
– format: String

Class Diagram

CONT..

Sequence diagram



User

Crystography System

Image

Initiate Encrypt and Embed

User selects
message and image

Encrypt Message

Applies cryptographic
algorithm to encrypt message

Embed in Image

Utilizes steganography
method to hide encrypted message
within the image

Embed in Image

Image now contains the encrypted message

Return Encrypted Image

Initiate Decrypt and Extract

User selects
encrypted image

Extract from Image

Extracts the encrypted
message from the image

Decrypt Message

Applies cryptographic
algorithm to decrypt message

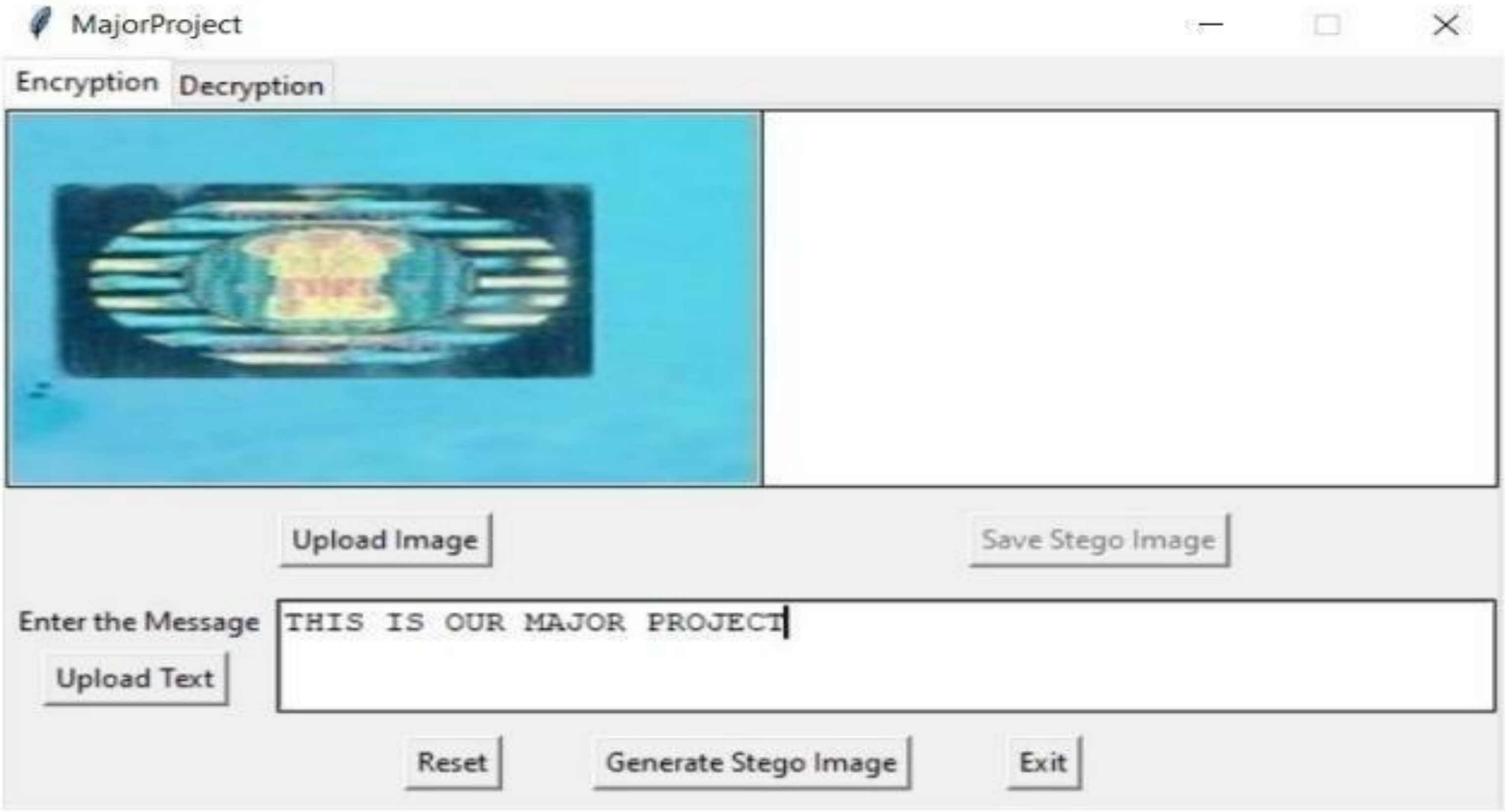
Return Decrypted Message

User

Crystography System

Image

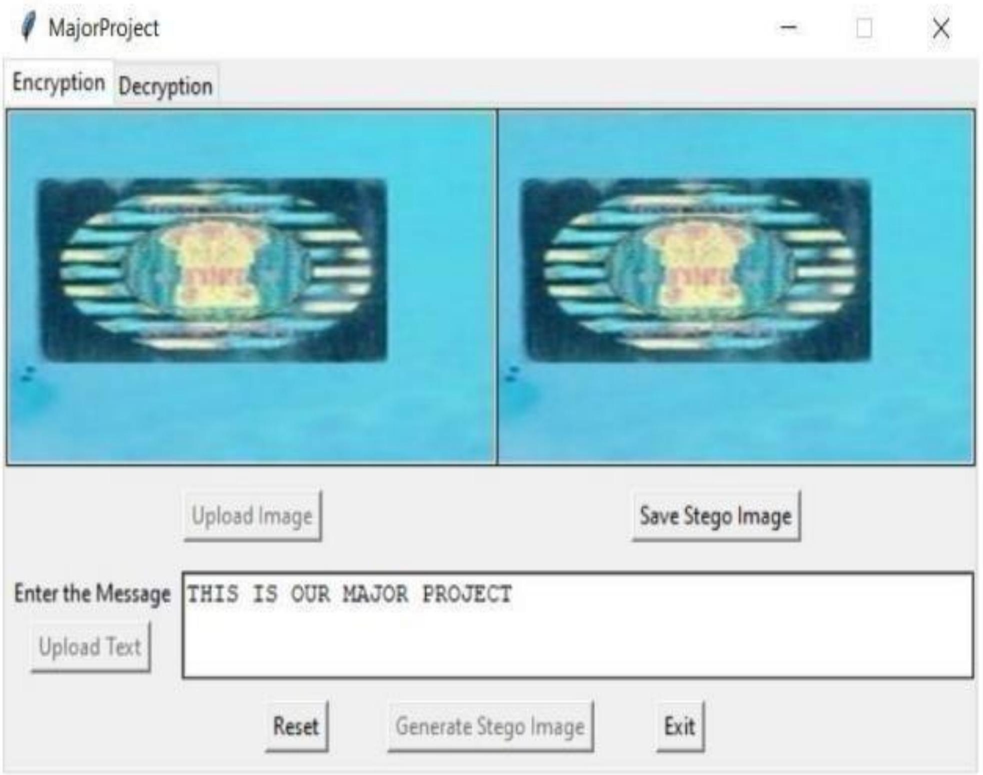
RESULTS



Enter the Message THIS IS OUR MAJOR PROJECT

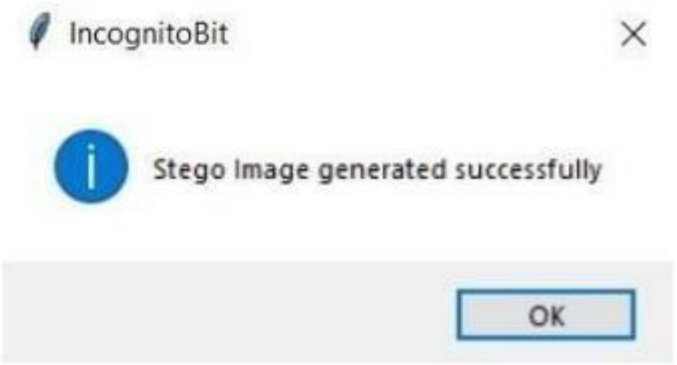
Uploading the image and text

CONT..



Enter the Message: THIS IS OUR MAJOR PROJECT

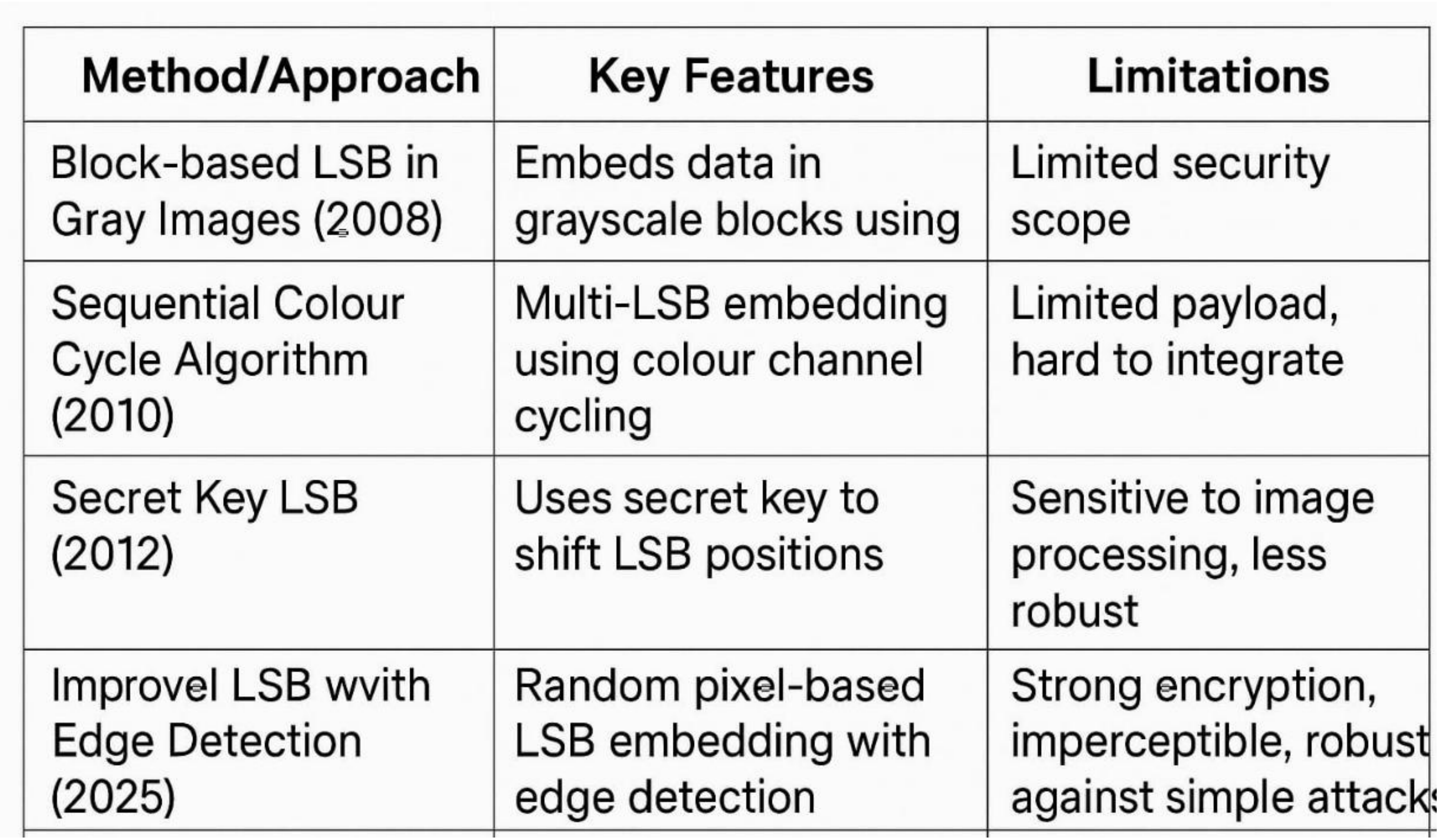
Encrypting and storing message within the image



Stego Image generated successfully

Generating Stego image

CONT..



Method/Approach	Key Features	Limitations
Block-based LSB in Gray Images (2008)	Embeds data in grayscale blocks using	Limited security scope
Sequential Colour Cycle Algorithm (2010)	Multi-LSB embedding using colour channel cycling	Limited payload, hard to integrate
Secret Key LSB (2012)	Uses secret key to shift LSB positions	Sensitive to image processing, less robust
Improvel LSB wvith Edge Detection (2025)	Random pixel-based LSB embedding with edge detection	Strong encryption, imperceptible, robust against simple attacks

Comparison of methods

CONCLUSION AND FUTURE SCOPE

Conclusion

- The proposed technique is a highly secure technique for embedding messages into images. Also, the symmetric key cryptographic algorithm used in this approach is very strong as it uses 8 bits key and a complex enciphering algorithm.
- It is almost computationally infeasible to retrieve the original message with a plain text attack.
- This technique also results in less distortion in an image after embedding. It has high PSNR (Peak Signal to Noise Ratio), less MSE (Minimum Squared Error), and it is imperceptible.
- This technique is also better than conventional LSB steganography. In this way, the system was strengthened using the LSB approach to provide a means of secure communication.

CONT..

Future Scope

- A strong cryptosystem can be built from the proposed method.
- A stronger cryptographic technique can be applied with the proposed steganographic technique in order to increase the security.
- Instead of single or double level; multilevel encryption can be applied with this technique to make the proposed method more secure.

REFERENCES

[1] S. M. Masud Karim, M. S. Rahman and M. I. Hossain, "A new approach for LSB based image steganography using secret key," 14th International Conference on Computer and Information Technology (ICCIT 2011), 10.1109/ICCITechn.2011.6164800. Dhaka, Bangladesh, 2011, pp. 286-291, doi:

[2] Al-Taani, Ahmad & Al - Issa, Mohammed. (2008). A new approach for data hiding in gray-level images. 48-53.

[3] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2015, pp. 1-4, doi: 10.1109/ICECCT.2015.7226122.

[4] Farhan, Hamid & Alwan, Zena. (2018). Improved method using a two Exclusive-OR to binary image in RGB color image steganography.

[5] Zena Ahmed and M. Hamid Mohammed Farhan, “Secure Watermark Image Steganography by Pixel Indicator Based on Randomization”, JMAUC, vol. 4, no. 2, pp. 101-110, Dec. 2012.

[6] S. Goyal, M. Ramaiya and D. Dubey, "Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images," 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, India, 2015, pp. 1120-1124, doi: 10.1109/CICN.2015.220.

[7] Por, Yee & Beh Mei Yin, Delina & Ang, T.F. & Ong, Simying. (2013). An enhanced mechanism for image steganography using sequential color cycle Algorithm. International Arab Journal of Information Technology. 10.

CONT..

[[8] G. R., Manjula & Danti, Ajit. (2015). A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain. International Journal of Security, Privacy and Trust Management. 4. 10.5121/ijsptm.2015.4102.

[9] Pramanik, Sabyasachi & Singh, R & Ghosh, Ramkrishna. (2019). A new encrypted method in image steganography. 1412-1419. 10.11591/ijeecs.v13.i3.pp1412-1419.

[10] R. S. Phadte and R. Dhanaraj, "Enhanced blend of image steganography and cryptography," 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2017, pp. 230-235, doi: 10.1109/ICCMC.2017.8282682.

ANY QUESTIONS?

THANK YOU