RANDOMIZED LEAST SIGNIFICANT BIT(LSB) EMBEDDING IMAGE STEGANOGRAPHY WITH ADVANCED ENCRYPTION STANDARD(AES) ALGORITHM

Team Details

1. G M S Padmini (20EG105415)
2. B Vaishnavi (20EG105406)
3. CH Shreya (20EG105407)

Project Supervisor

Dr. K Madhuri
Associate Professor

Introduction

- The **"Randomized Least Significant Bit(LSB) Embedding Image Steganography with Advanced Encryption Standard (AES)"** project is a combination of Image Steganography and AES Encryption technique.
- The developing environment is **Python 3.11** and **Command prompt.**
- It allows confidential information to be securely hidden within digital images, ensuring privacy and confidentiality during data transmission.
- The applications span various domains, including secure communication, digital forensics, privacy protection,etc.
- By embedding messages within images using **Randomized Least Significant Bit (LSB)** manipulation and ensuring further layer of security with AES encryption, this project offers a solution for secret communication while preserving the visual integrity of the images.

Literature

Sl.no	Author (s)	Method	Advantages	Disadvantages
1	Adit Pabbi, Rakshit Malhotra, Manikandan K	Implementation of LSB Steganography with AES Algorithm Using GUI - 2021	Enhanced Security, Covert Communication	Less security compared to the proposed method.
2	Utsav Sheth, Shiva Saxena	Image Steganography Using AES Encryption, Least Significant Nibble and Java - 2016	Graphical user interface, Comprehensive libraries	Limited to lower nibble, Lossy compression limitations
3	C. Lalengmawia, A. Bhattacharya	Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data by embedding the position of pixels randomly - 2016	Increased security, dynamic embedding, comparative analysis	Lack of specific details, Potential impact on image quality

4	Masumeh Damrudi, Kamal Jadidy Aval	Image Steganography using LSB and encrypted message with AES, and other hybrid algorithms by considering the factors PSNR, MSE - 2019	Concealment of the message, Increased resistance to the attack	Increased complexity.
5	Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial and Brendan Halloran	Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research - 2019	Secure image transmission, availability of digital images	Limited Embedding capacity, Impact on image quality.

Problem Statement

Conventional methods of data transmission often lack the desired level of privacy, making sensitive information vulnerable to interception. These methods of sending data can be intercepted or compromised, posing a risk to sensitive information and are subjected to brute force attacks.

This fusion of steganography and encryption methods aims to create a seamless and secure channel for transmitting confidential information without arousing suspicion by also ensuring the integrity and to avoid brute force attacks. Steganalysis is not easily detected.

Objective

- The solution for the above problem is the proposed method -

  "To Design and implement a steganography system that combines Randomized Least Significant Bit (LSB) Embedding by encrypting the text message with Advanced Encryption Standard algorithm (AES - 256) for secure communication in digital environments."

- The parameters which are considered for the project evaluation are:

  → Preserving the visual quality and integrity of the images.

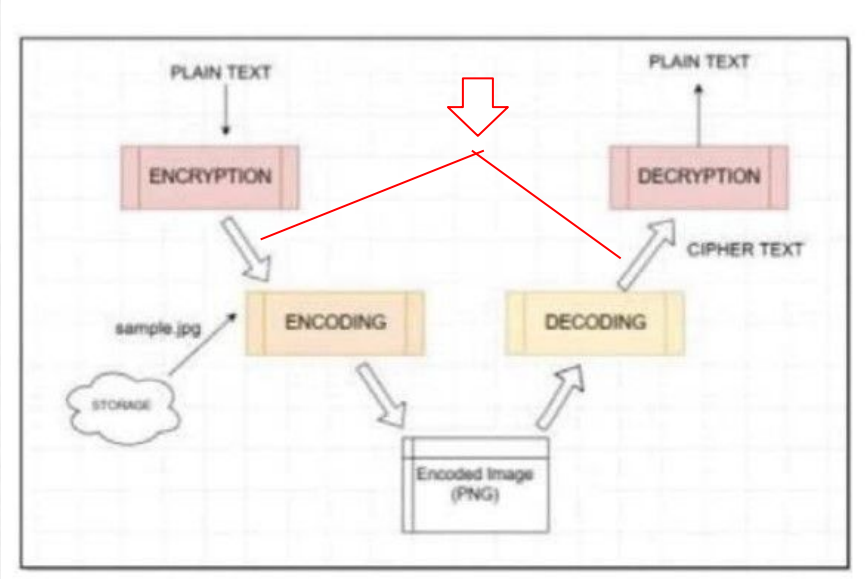
  → Security enhancement using AES- 256 encryption by proper key management.

Proposed Method

- The proposed method is **"Randomized Least Significant Bit (LSB) Embedded Steganography with Advanced Encryption Standard(AES) Algorithm".**

This methodology consists of :

- AES Encryption.
- Shuffling the bits.
- LSB Encoding.
- LSB Decoding.
- Unshuffling the bits.
- AES Decryption.



INPUTS: Image
Message
Password.

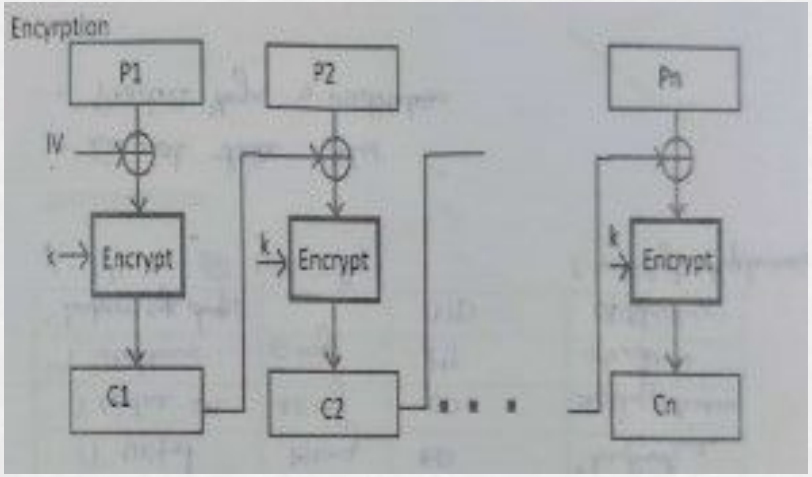
Proposed Method

- ➔ Firstly, check if the image is in **RGB mode**, if not we need to convert it.
- ➔ The provided password must be of at least **12 characters.**
- ➔ With the given password, we will do Password Key Derivation where we use SHA-256 to get 256 bit key hash value which is used as encryption key for AES Encryption.

AES ENCRYPTION:

AES algorithm is used in Cipher Block Chaining (CBC) mode which takes Derived Key and Initialization Vector (IV) as inputs.
An initialization vector (IV) is an arbitrary number that can be used with a secret key for data encryption.
Initialization vector, XOR operation adds extra layer of security to use CBC mode.
Derived Key is 256 bit length.
AES works on 128 bit length fixed length block so the message is divided into 128 bit length blocks.

Proposed Method



→ **CBC Mode**

The final cipher text is obtained is in the form of bytes where we need to convert the message to individual bits by keeping them in the form of a list.

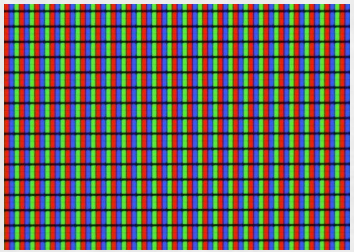
SHUFFLING THE BITS:

Shuffled Index**:** (i + 8) % length (message bits) where i= index of the bit.

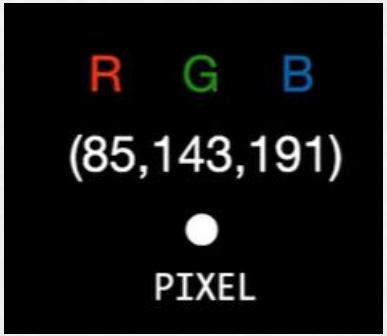
Proposed Method

LSB ENCODING:

- Header Text is encoded along with the cipher text.
- Header Text is is a predefined string that is used as a marker or identifier at the beginning of the hidden message.
- The length of the Header Text is 12 characters - "**M6nMjy5THr2J**". Its purpose is to distinguish between the header (marker) and the actual encrypted message within the image.
- The header is shared among the Sender and Receiver.
- When decoding an image, the code checks whether the header text is present at the beginning of the decoded data. If it is not found or does not match the expected header text, the code considers the data invalid. This helps to ensure the integrity of the encoded message.

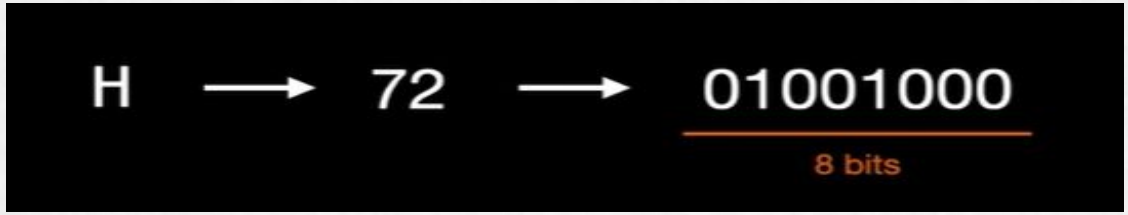


The image is made up of pixels

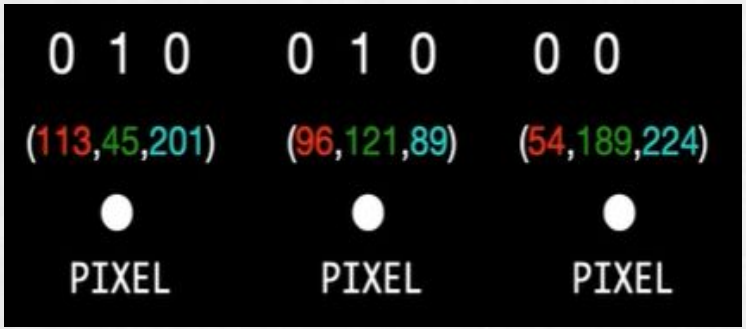


Each pixel has 3 colours - Red, Green and Blue

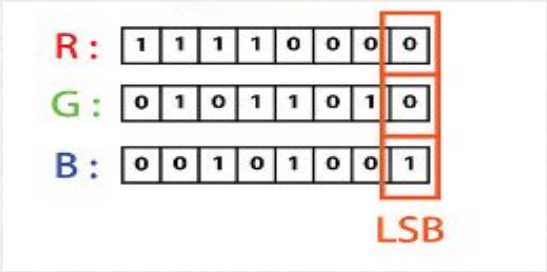
For example, in the steganography process, if the message bit to encode is "H" then the procedure is as follows:



Each character is converted to the corresponding ASCII value and converted to 8 bits.



Each character needs 3 pixels to encode it

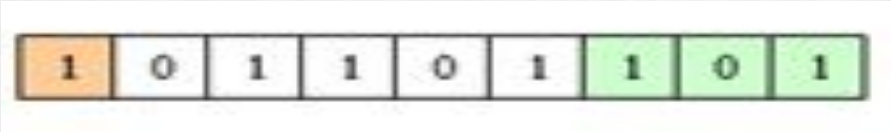


LSB in each colour of the pixel

Proposed Method

1	0	0	1	0	1	0	1

→ Message bits



→ 3 Pixels RGB Colours LSB

- ➔ If the message bit is ‘0’ then value of LSB of the colour of pixel must be ‘0’
- ➔ If the message bit is ‘1’ then value of LSB of the colour of pixel must be ‘1’
- ➔ 9th bit is called as **“STATUS BIT”.** (3rd pixel’s blue LSB)
- ➔ 9th bit should be ‘0’ if the message continues or make it as ‘1’ if the message ends with that character.

LSB DECODING:

The code iterates through the pixel data of the encoded image. For each pixel, it reads the least significant bits (LSB) of the RGB values.

Proposed Method

UNSHUFFLING THE BITS:

Unshuffled Index**:** (i - 8) % length(message bits) where i= index of the bit.

AES DECRYPTION:

- ➔ This process takes the same key used for encryption.
- ➔ It extracts the IV from the beginning of the data and uses it to initialize.
- ➔ The decrypted data is then unpadded to remove the padding bits which are added during encryption.
- ➔ The bits are converted into bytes which in turn is converted to ASCII Text and the corresponding original message is obtained.

Project Status

S.No	Functionality	Status (Completed /in-progress/Not started)
01	AES Encryption of the message .	Completed
02	Padding the message bits.	Inprogress
03	Shuffling and Unshuffling the bits	Inprogress
04	Image loading and conversion	Completed
05	Header insertion and validation.	Not Started
06	Encoding of the message by Randomized LSB Embedding	Not Started
07	Decoding of the message by randomized LSB Embedding	Not Started
08	AES Decryption of the message	Not Started
09	Removing the padded bits	Not Started
10	Error handling and management	Not Started

References

1. IEEE Paper – Implementation of Least Significant Bit Image Steganography with Advanced Encryption Standard
   (URL: https://ieeexplore.ieee.org/document/9396884)
2. IEEE Paper - Image Steganography Using AES Encryption, Least Significant Nibble and Java
   (URL: https://ieeexplore.ieee.org/document/7754272)
3. IEEE Paper - Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data by embedding the position of pixels randomly
   (URL: https://ieeexplore.ieee.org/document/7569552)
4. Paper - Image Steganography using Advanced Encryption Standard for implantation of Audio/Video Data by embedding the position of pixels randomly
   (URL: https://www.ijet.org/wp-content/uploads/papers/v8i6S3/F10330986S319
5. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research - 2019
   (URL:https://www.sciencedirect.com/science/article/abs/pii/S0925231218312591)
6. Hide your secret messages in image video
   (URL:https://www.youtube.com/watch?v=_KX8ORUA_98&list=WL&index=15&t=215s)