
Welcome
Lets Get Started

P P SAVANI UNIVERSITY

School of Engineering

Image Steganography

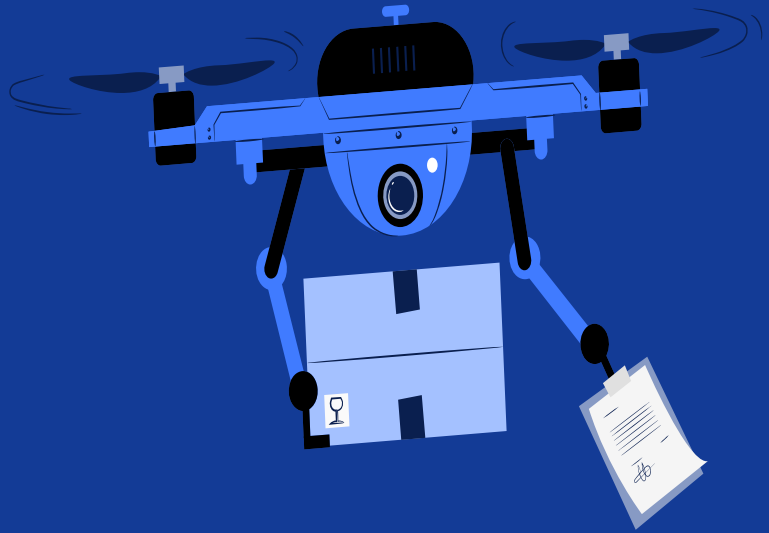
Present By
Keyur Finaviya - 17SE02CE015
Dhruv Gandhi - 17SE02CE017
Mansi Hirpara - 17SE02CE020

Supervised By:
Ms. Bannishiskha Banerjee

P P SAVANI UNIVERSITY
School of Engineering

Outline

- Introduction
- Application
- Objective
- Literature
- Proposed System (Demo)
- Analysis
- Conclusion
- Future Work
- Reference



Introduction

What is Steganography ?

- Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection, the secret data is then extracted at its destination.

- The different methods of Steganography are:
  - Text Based Steganography
  - Image Based Steganography
  - Audio Based Steganography
  - Video Based Steganography

Introduction

What is Image Based Steganography ?

- Image Steganography refers to the process of hiding data within an image file.
- The image selected for this purpose is called the cover-image and the image obtained after steganography is called the stego-image.

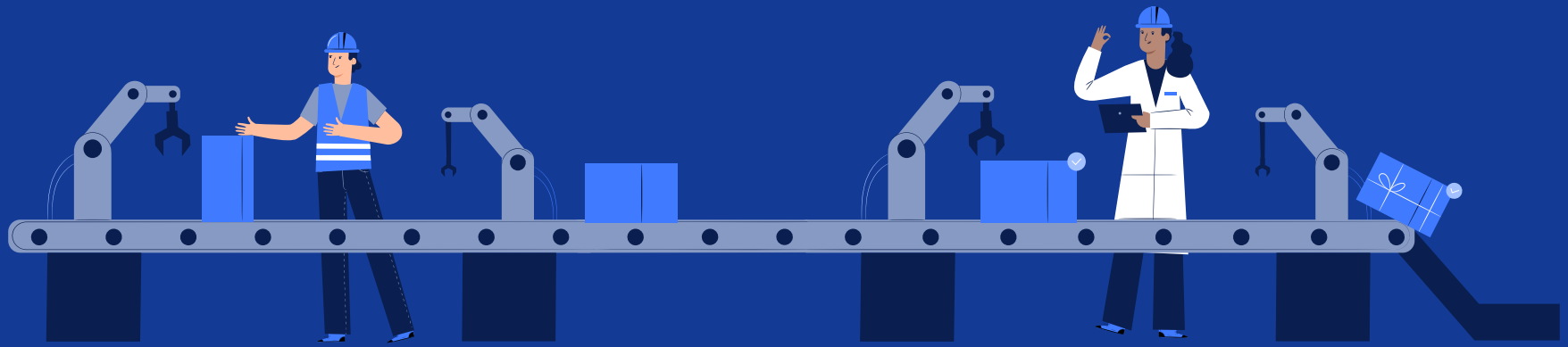
Fig. 1 Basic Image Steganography

Application

- Secure Private Files and Documents.
- Hide Passwords and Encryption Keys.
- Transport Highly Private Documents between International Governments.
- Transmit message/data without revealing the existence of available message

Objective

- To hide a secret message within an object. It will be done in such a way that the presence of message is not visible.



Literature

- Image Based Steganography can be performed using two methods :
  - Least Significant Bit (LSB) Method
  - Discrete Cosine Transform Method

- In this application we make use of the Least Significant Bit (LSB) Method

Literature

LSB Method

- The most common and popular method of modern day steganography is to make use of LSB of picture's pixel information.
- This technique works best when the file is longer than the message file and if image is grayscale.
- When applying LSB techniques to each byte of a 24 bit image, three bits can be encoded into each pixel.

Literature

How LSB Method is embedded Data

Read Input

- Extract Pixels From Cover Image
- Extract Characters From Text
- Extract Characters From Key

Embed Data in image

- Choose Pixels and Place characters from Stego Key in Pixels.
- Add Terminal Symbol indicating end of key.
- Insert characters from the message in the pixels.

Stego Image Ready

Literature

How LSB Method is Extracted Data

Extract Lsbs

- Extract Least Significant Bits from Pixels Of Stego Image

Extract Key

- Read key in Image, till the occurrence the entered of Termination character.
- If retrieved key matches the entered key, extract data from the

Extract Message

- Read Characters from the LSBs of the Image Pixels
- Combine all extracted characters, to form original message.

Literature

Example:

We can use images to hide things if we replace the last bit of every color's byte with a bit from the message.

Message A-01000001

Image with 3 pixels

Pixel 1: 11111000 11001001 00000011

Pixel 2: 11111000 11001001 00000011

Pixel 3: 11111000 11001001 00000011

Literature

Now we hide our message in the image.
Message: 01000001

Image with 3 pixels

Pixel 1: 11111000 11001001 00000010

Pixel 2: 11111000 11001000 00000010

Pixel 3: 11111000 11001001 00000011

New image:

Literature

P P SAVANI UNIVERSITY
School of Engineering

- AES

- AES is an encryption standard chosen by the National Institute of Standards and Technology(NIST), USA to protect classified information. It has been accepted world wide as a desirable algorithm to encrypt sensitive data.

- It is a block cipher which operates on block size of 128 bits for both encrypting as well as decrypting.

- Each Round performs same operations.

Literature

- AES Working

- AES basically repeats 4 major functions to encrypt data. It takes 128 bit block of data and a key[layman's term password] and gives a cipher text as output.

- The functions are:
  I. Sub Bytes
  II. Shift Rows
  III. Mix Columns
  IV. Add Key

Literature

P P SAVANI UNIVERSITY
School of Engineering

- AES Working

- The number of rounds performed by the algorithm strictly depends on the size of key.
- The following table gives overview of no. Of rounds performed with the input of varying key lengths:
- Key Size(in bits) Rounds
  128.....10
  192.....12
  256.....14
- The larger the number of keys the more secure will be the data. The time taken by s/w to encrypt will increase with no. of rounds.

Literature

- AES Working

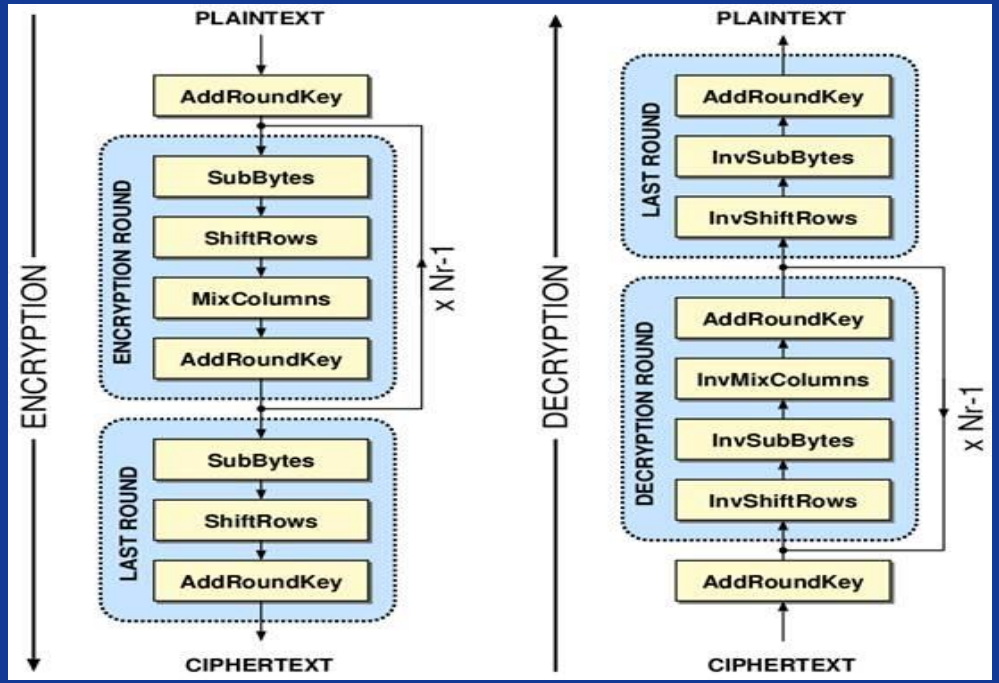


Fig. 2 AES Simple Encryption and Decryption

Proposed System (Demo)

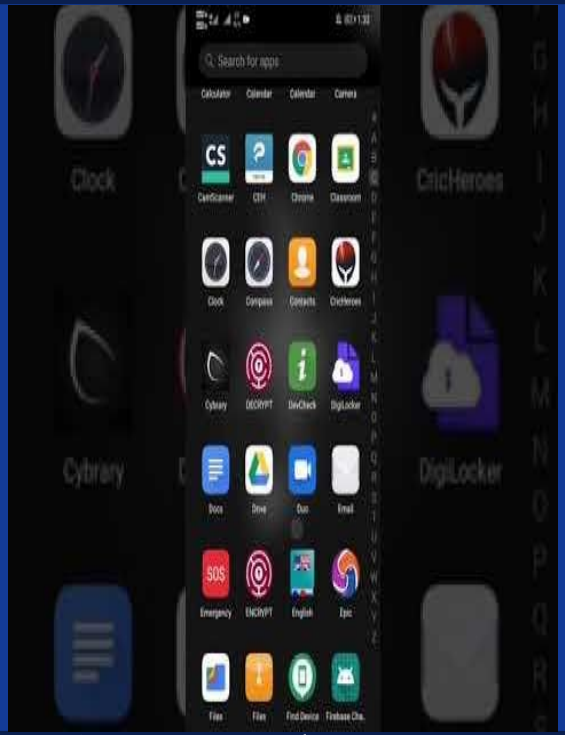


Fig. 3 Proposed system Demo

Analysis

- In this project we mainly concentrated on embedding the data into an image. We have designed the steganography application which embedded the data into the image.
- Normally, after embedding the data into the image, the image may lose its resolution. In the proposed approach, the image remains unchanged in its resolution as well in size.
- The speed of embedding the data into the image is also high in the proposed approach such that the image is protected and the data to the destination is sent securely.
- There are many steganography algorithms available like JSteg, F5 and LSB algorithms.
- We have used the Least Significant Bit algorithm in designing the steganography application because LSB algorithm works efficiently when we consider bit map images .bmp files. The speed of embedding is also high when using LSB compared to the JSteg algorithm.

Conclusion

- In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet.

- Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information un- intended to him.

- So Hiding a message with steganography methods reduces the chance of a message being detected or hack.

Future Work

- In Future we are going to embed this system in chat application as we discussed in present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination.
- We can see that so many fake images are share in chat. So to we use image steganography as origin finder.
- For that we will store **use-id** in stego image so that we can find out easily.

References

- https://www.geeksforgeeks.org/image-steganography-in-cryptography/
- https://searchsecurity.techtarget.com/definition/steganography
- https://lyra-kdf.net/guide-rise-fall-5-best-key-encryption-algorithms/
- https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm
- https://www.irjet.net/archives/V5/i4/IRJET-V5I4337.pdf

P P SAVANI UNIVERSITY
School of Engineering

Thank You So Much