” FINAL PROJECT REPORT”

IMAGE STEGANOGRAPHY

Riddhi Tamakuwala (1226810171)

Abhinav Nathari (1225973205)

IFT520 Advanced Information System Security

Department of Information Technology, Arizona State University

Dr. Jim Helm

Nov 29th,2022

TABLE OF CONTENTS

ABSTRACT 2

INTRODUCTION 3

Problem Statement: 6

Significance of Study: 6

Objective: 7

DESIGN PROCESS 8

Requirements: 13

Hardware requirements 14

Software requirements 14

Scope 15

DEVELOPMENT PROCESS 16

Tools 17

Technical Description of Project: 21

TESTING AND RESULT 25

SUMMARY AND CONCLUSIONS 28

REFERENCES 31

APPENDIX 32

ABSTRACT

Steganography is the art and science of delivering covert communications so that only the sender and intended receiver are aware of their existence and content. Steganography is the practice of concealing information without modifying it in other information. The art of concealing a message within a multimedia block is what it is. Today, attacks, abuse, and illegal access to information are major concerns, making the protection of documents on digital media a top issue. Information is frequently stored via digital photographs. There are several different methods for concealing sensitive information in photographs. Some applications can need complete secrecy, while others may call for the concealment of big secret messages.

This project report aims to provide an overview of picture steganography, including its applications and methods. It also tries to define what makes a good steganography algorithm and makes a quick assessment of which steganographic methods are better suited for specific uses. Image steganography is the practice of concealing information, such as text, pictures, or audio recordings, together within image or video file. The current study intends to use spatial domain steganography for one picture with another image. Only a suitable decoding procedure can reveal this secret information. The photos are encrypted and decrypted using python and tkinter program.

Keywords*:* Substitution, Least Significant bit, Cryptography, Steganalysis, Steganography

INTRODUCTION

The word Steganography is derived from the Greek words – steganos (meaning hidden or covered) and the graph (meaning to write). Steganography is the practice of hiding a file, image, or video within another file, message, image, or video. Steganography can also be referred to as the technique of hiding secret data within an ordinary, non-secret, file, or message to avoid detection; the secret data is then extracted at its destination . Data masking is critical in many applications. The basic approaches for hobbyists, hidden data transit, user privacy, and so forth are: Steganography and Cryptography. Steganography is a straightforward security approach. In general, three approaches are employed to conceal information: steganography, cryptography, and watermarking. All knowledge to be concealed is encrypted using certain procedures in cryptography; this information is commonly acknowledged to be coded since the data seems nonsensical. Steganography conceals information; this is often unnoticeable since the adding functional does not seem aberrant, i.e. their presence is invisible by sight. Steganalysis is the detecting of secret message.

Steganography is of different types:

1. Text steganography
2. Image steganography
3. Audio steganography
4. Video steganography

The basic premise of hiding data is to embed a secret message in another cover object that may or may not be of any consequence, such that the data encryption eventually displays just the cover

data. As a result, unless adequate decryption is applied, it cannot readily be discovered as holding concealed information. The most frequent method was evaluated is the LSB substitution method.

The least significant bit (LSB) technique is a common and straightforward method for encoding data in a cover file.

Steganography employs the LSB substitution approach. That is, because every picture contains three components (RGB). This pixel data is encoded and saved in one byte. The initial bits of each pixel's data can be adjusted to store the concealed text. The preliminary requirement that the information to be stored be less or equal in size towards the picture used it to hide the content. A spatial domain approach based on LSB. However, this is susceptible to chopping and noise. The MSB (most significant bits) of the concealed message picture are saved inside the LSB (least significant bits) of the picture used as the cover image in this approach.

It is well understood that pixels in a picture are stored as bits. The luminosity of each pixel in a grayscale picture is represented in binary number (1byte). Similarly, each pixel in a color (RGB-red, green, blue) picture needs bit (8bits for each layer). When the LSB bit is changed, the human vision (HVS) cannot perceive changes in the color or luminosity of a pixel. This one is psycho-visual redundancy because it may be utilized to store records in these bits while seeing no significant difference in the image.

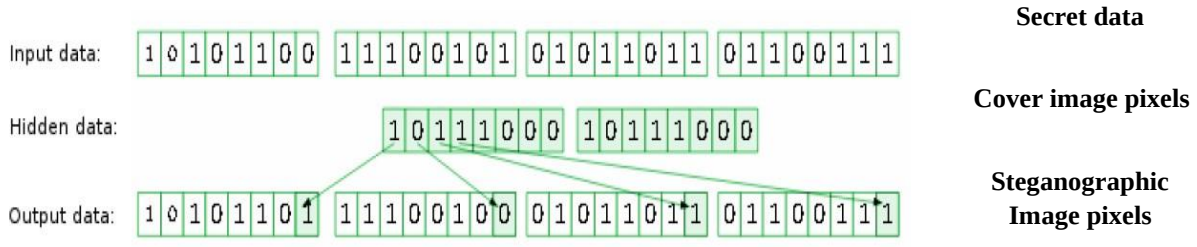


Fig 1 Pixel Representation

- **Cryptography** and **steganography** are both methods used to hide or protect secret data. However, they differ in the respect that cryptography makes the **data unreadable**, or **hides the *meaning* of the data**, while steganography hides the ***existence*** of the data.
- **Cryptography** is like writing a letter in a secret language: people can read it but won't understand what it means. However, the existence of a (probably secret) message would be obvious to anyone who sees the letter, and if someone either knows or figures out your secret language, then your message can easily be read.
- If you were to use ***steganography*** in the same situation, you would hide the letter inside a pair of socks that you would be gifting to the intended recipient of the letter. Only the intended recipient knows what to look for, and finds the message hidden in them.
- The use of **Steganography** can be combined with encryption as an extra step for hiding or protecting data.
- **Cryptography** is often used to supplement the security offered by steganography. **Cryptography** algorithms are used to encrypt secret data before embedding it into cover files.
- **Cryptography** can be used as extra layer of security even over the existence of file i.e., **Steganography**
- In watermarking applications, the message includes data that is often used for copyright protection, such as owner identification and a digital time stamp. To individually identify each user of the data set, the owner of the data set embeds a serial number within the data set. Due to the addition of copyright information, any unlawful use of the data set may now be linked back to the user. Steganography is a method of securely communicating a secret message to a recipient while

concealing it within the host data set and making its existence undetectable. The host data set is intentionally contaminated, but invisibly, so that it cannot be seen by information analysis.

Problem Statement:

How can one send a message secretly to the destination. Using steganography, information can be hidden in carriers such as images, audio files, text files, videos, and data transmissions. Image Steganography is the process of hiding information which can be text, image, or video inside a cover image. The secret information is hidden in a way that it not visible to the human eyes.

Significance of Study:

The goal was to examine information concealing strategies that might assist users in disseminating information to the intended recipients while avoiding detection by other computer users (intruders or attackers) when engaging in routine organizational duties.

When users want to keep information from someone who might not have permission to view it, they confront their largest barrier. By concealing and encrypting information using pictures and keys, respectively, this study aims to understand how steganography, an information hiding technique, aids in solving the issues they confront. It also tests and evaluates the usefulness, validity, and usability of various strategies.

In digital media, steganography is a method of information concealment. It differs from cryptography in that no one can discover the presence of the information. However, by applying steganography, another individual is even rendered unable to comprehend the existence of information.

Participating in the online revolution increases people's awareness of steganography. Steganography is the practice of hiding a message from being discovered. The message is hidden from being found utilizing a variety of covert communication techniques, such as steganography.

Objective:

Steganography aims to facilitate clandestine communication. The hider message transmitted by the stego-media must thus not be understandable to humans to comply with a key criterion of this steganography technology. The other purpose of steganography is to prevent suspicion of a hidden message from being raised. This kind of information concealment has lately grown in significance in a variety of application areas.

The goal of this project is to: Create a security tool based on steganography methods.

To investigate data-hiding methods utilizing this project's encryption module.

To extract methods for obtaining confidential information using a decryption module.

When encryption is not allowed, steganography is sometimes utilized. Steganography is also frequently used in conjunction with encryption. Regardless of whether the encrypted file is cracked, the concealed message will not be visible since steganography may still be used to hide information in an encrypted file.

Steganography is the more advanced kind of encryption when the user is unaware that secret information is being encrypted. If a user accidentally suspects that information exists, there is no method for them to obtain it.

DESIGN PROCESS

As the image depicts, both cover file(X) and secret message(M) are fed into steganographic encoder as input. Steganographic Encoder function, f(X,M,K) embeds the secret message into a cover file . The result of a Steganography Object looks very similar to your cover file, with no visible changes. This completes encoding. To retrieve the secret message, Steganography Object is fed into Steganographic Decoder.

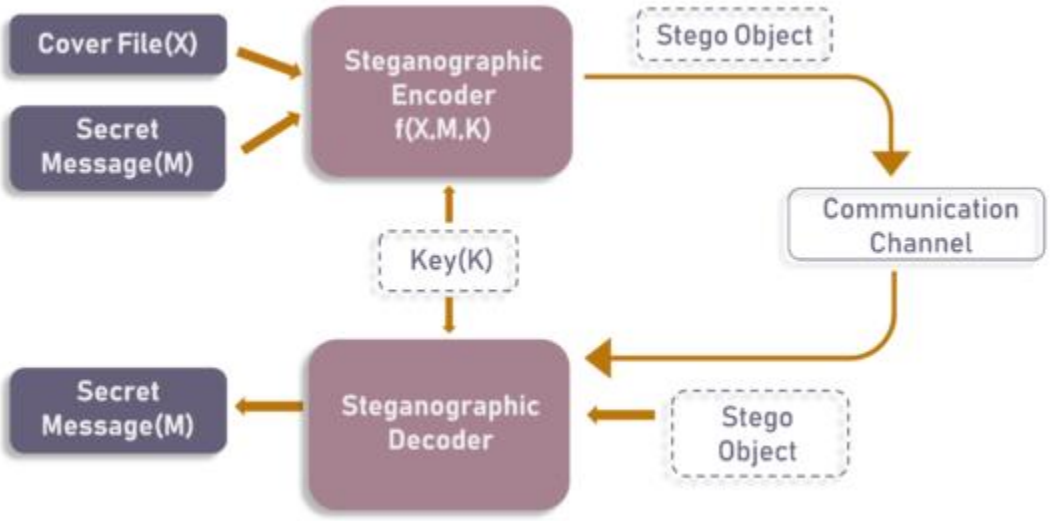


Fig 2 Steganographic Model

Encryption phase

The "Encryption phase" uses two types of files for encryption purpose. One is the secret file which is to be transmitted securely, and the other is a carrier file such as image. In the encryption phase the data is embedded into the image.

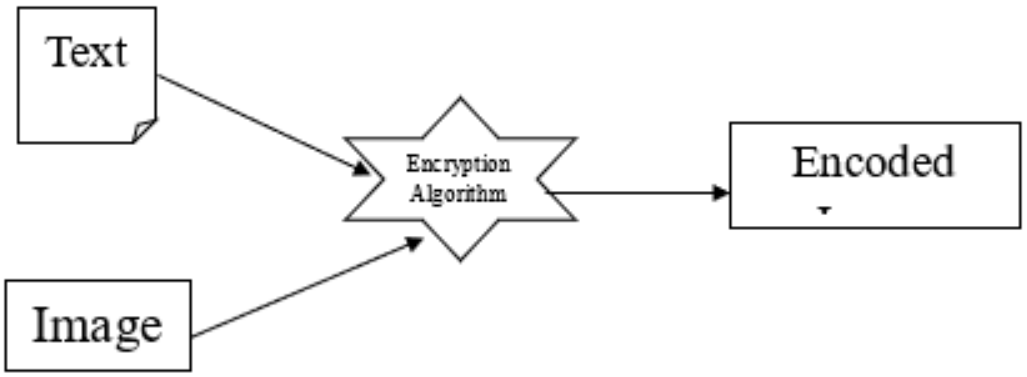


Fig 3 Encryption process

The algorithm for encryption of data into image follows following steps:

1. The value of counter is set to zero initially which interprets the position of pointer in the array.
2. Loading of image and Set each pixel to (0,0,0) or (255,255,255) according to the value of the LSB.
3. Moving on we assume two parameters R and K,where

   R represents the least significant bit for the selected pixel in terms with red.

   K represents the bit for message after converted into ASCII.
4. The XOR operation is performed on R and K to determine which bits need to be changed.

   If XOR == 1,LSB of green would be replaced.

XOR == 0 , LSB of blue would be replaced.

5. After replacing,again the counter value is increased by 1 so in order to move to the next letter of the data.
6. The same cycle repeats until the pointer reached delimeter or the end of the message given.

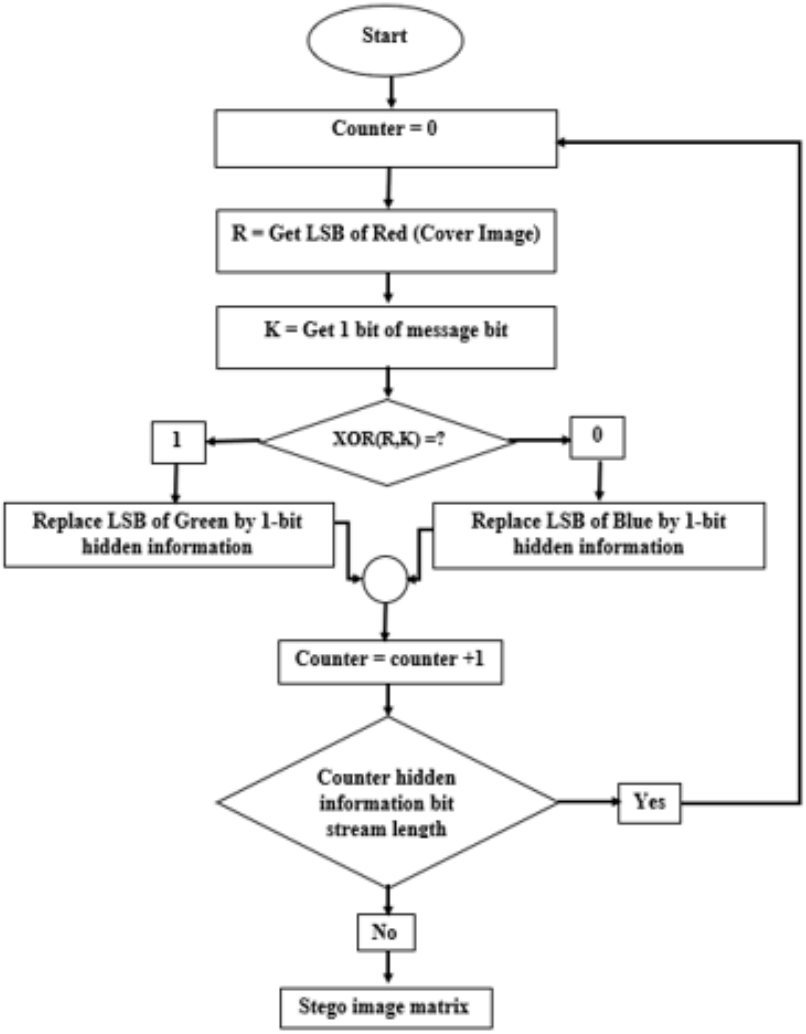


Fig 4 Encryption algorithm

Decryption phase

The Decryption phase is reverse to encryption phase. In decryption phase, the carrier image in which the data is hidden is given as an input file. decryption section uses the "Least Significant bit Algorithm" (LSB) by which the encoded bits in the image is decoded and turns to its original state and gives the output as a text document.

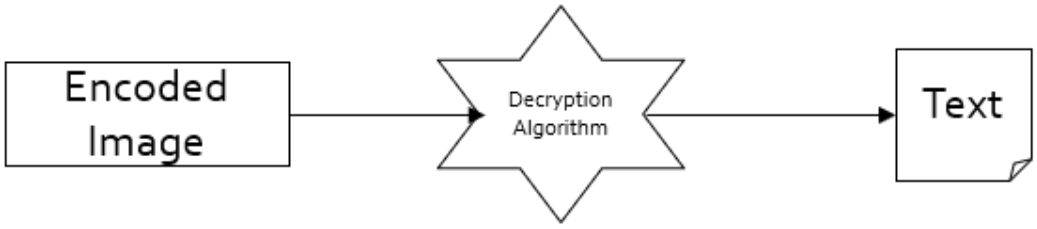


Fig 5 Decryption process

Lets see the procedure for decytion of image to get the desired data :

1. The value of counter is set to zero initially which interprets the position of pointer in the array.
2. Set each pixel to (0,0,0) or (255,255,255) according to the value of the LSB
3. Moving on we assume two parameters R and K,where

   R represents the least significant bit for the selected pixel in terms with red.

   K represents the bit for message after converted into ASCII.
4. The XOR operation is performed on R and K to determine which bits need to be picked.

   If XOR == 1,LSB of green would be extracted.

   XOR == 0 , LSB of blue would be extracted.

5. After extracting,again the counter value is increased by 1 so in order to work on to the next letter of the hidden data in the image
6. The same cycle repeats until the pointer reached delimeter or the end of the image bites given.

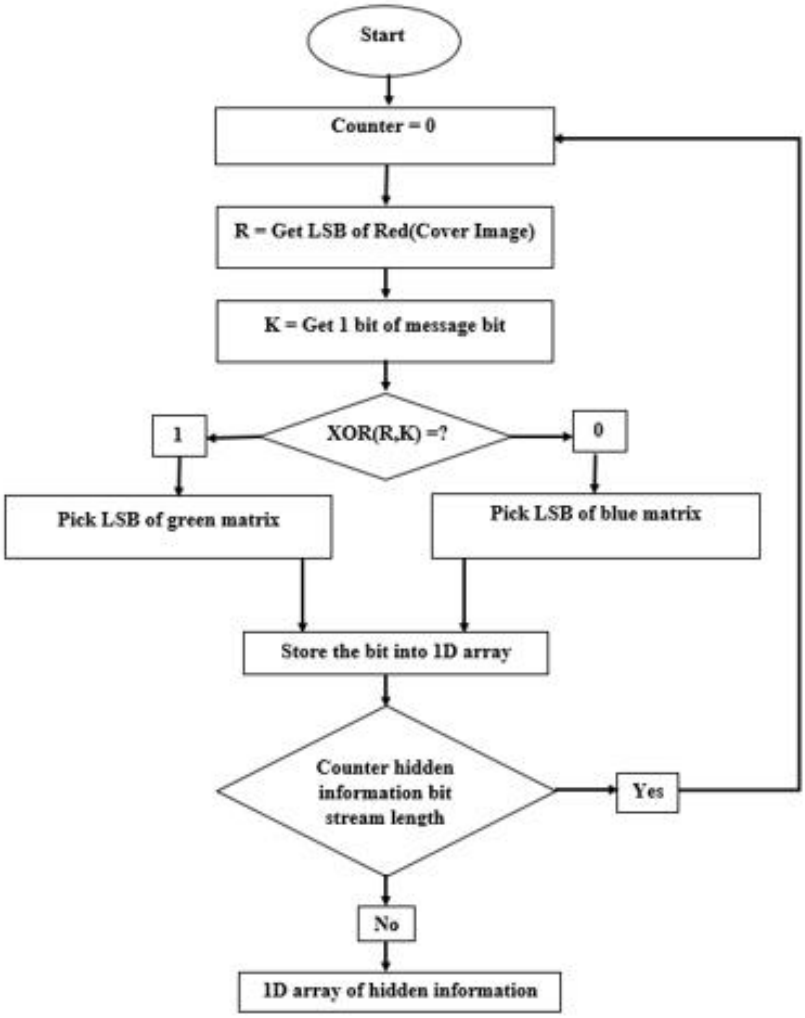


Fig 6 Decryption algorithm

Requirements:

Steganography has various requirements, which are as follows:

Because the power of steganography depends in its capacity to be undetected by the human sight, the obscurity of an image steganography algorithm is the initial and order requirement. The objective is that a picture may be shown to have been tampered with, and the technique is negotiated.

Payload capacity: Despite watermarking, which required only a minimal set of copyright notice to be embedded, steganography aimed to covert communication and hence required significant installation capacity.

Robustness against statistical assaults: Quantitative steganalysis is the process of discovering hidden data by using statistical tests on picture data. When integrating data, certain steganographic techniques leave a ‘signature' that may be easily discovered through data methods.

While it may be possible to avoid detection by a warden, a steganographic technique must not produce a statistically significant mark on the image.

Robustness against image manipulation: When a stego picture is connected via trusted systems, the image can be transformed by an active warden in an attempt to remove concealed information.

Photoshopping or rotating a picture before this reaches its destination is an example of image manipulation. These actions can destroy the concealed message depending on how the message is placed. It is preferable for steganalysis algorithms to be resistant to malicious or random picture modifications.

Independent of file format: It may appear strange if just one kind of file format is always linked between two parties while various other picture file formats are utilized on the Internet.

As a result, robust steganographic algorithms may embed data in any form of file. This also tackles the problem of not constantly being able to find the perfect picture at the right time and in the right format.

Unsuspicious files: Such situation reflects several steganographic method characteristics that can produce in pictures that are not often used and can raise suspicion. An irregular size of the file, for instance, is one attribute of a picture that might lead to further inspection by a warden.

Hardware requirements

- A working laptop/computer
- Windows version 6 or more
- RAM: 6 GB or more

Software requirements

- Python version 3.6 or more
- Tkinter
- Windows command prompt
- Python libraries

Scope

This project is developed for hiding information in any image file. The scope of the project is to limit unauthorized access and provide better security during message transmission. To meet the requirements, the project uses the simple and basic approach of steganography. In this project, the proposed approach finds a suitable algorithm for embedding the data in an image using steganography which provides a better security pattern for sending messages through a network. For practically implementing the function of the discussed algorithms, python framework is used.

Technique is used for covert communication—hiding the presence of a transmission from a third party. Steganalysis is becoming increasingly important to members of the police departments, security, and army communities.

The project is being implemented with the following goals in mind:

- To conceal a signal or private message in a picture that serves as a cover medium by employing the LSB & fake random techniques.
- Our present effort is primarily motivated by the need to improve the PSNR of the stego picture (peak signal to noise ratio).

DEVELOPMENT PROCESS

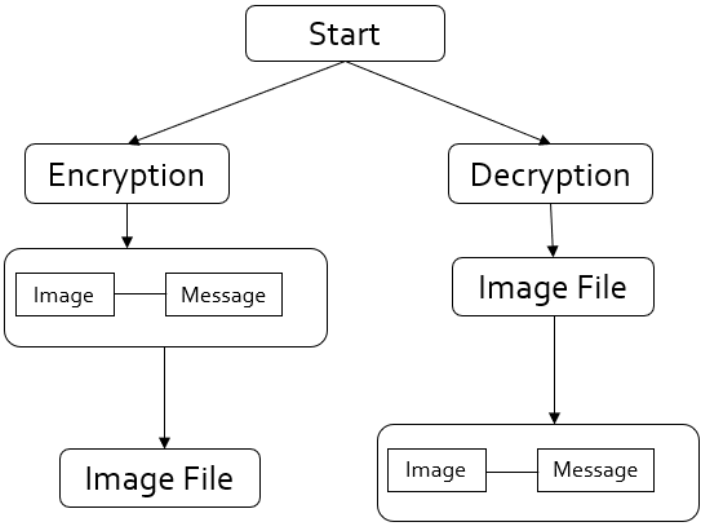


Fig 7 Block Diagram

The process flow of our project can be easily depicted from the diagram given. The user interacts with our application and selects and performs according to his need.

The user is having two choices:

1. ***Encode the image.***

   If he chooses to encode the image, he will need to do forementioned things:

   Upload the desired image.

   Enter the data which he wants to encrypt.

   After entering all the necessary details, just press the encode button.

   He will be further asked to enter the name with which he wishes to store his encoded file.

   A dialog box will appear showing the message successful if it's done.

2. ***Decode the image.***

If he chooses to alternative option that is decode the image, he will need to do forementioned things:

Upload the desired image.

After uploading the image, just press the decode button.

The user will get output as the data which is encrypted or concealed in the image.

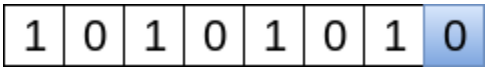
He will be further allowed to see the information of the image which is encrypted.

A dialog box will appear showing the message of the same on clicking “more info” button.

The project is being implemented with the following goals in mind: To conceal a signal or private message in a picture that serves as a cover medium by employing the LSB & fake random techniques. My present effort is primarily motivated by the need to improve the PSNR of the stego picture (peak signal to noise ratio).

Tools

- LSB algorithm is a classic Steganography method used to conceal the existence of secret data inside a “public” cover. The LSB or “Least Significant Bit”, in computing terms, represents the bit at the unit’s place in the binary representation of a number.
- For example, we can represent the decimal number 170 in binary notation as 10101010. As shown in the figure, the least significant bit, in this case, is 0.



- In the simplistic form, LSB algorithm replaces the LSB of each byte in the “carrier” data with one bit from the “secret” message.

- This concept is visualized in the diagram below.

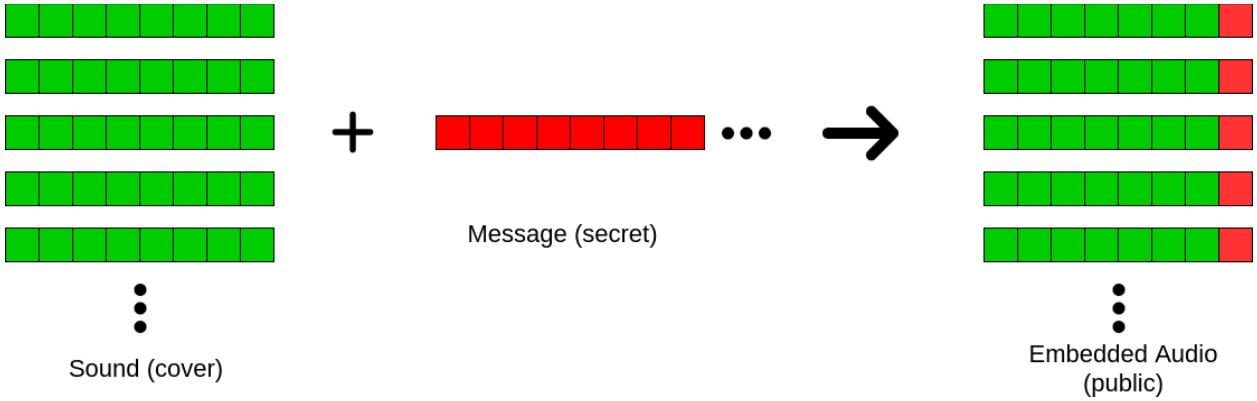


Fig 8 Concept of steganography

- The sender performs “embedding” of the bits of secret messages onto the carrier data byte-by-byte. Whereas the receiver performs the “extraction” procedure by reading LSB bits of each byte of received data, this way the receiver reconstructs the secret message.

- **Isn’t this corrupting the carrier signal?**

- Yes, but the main idea here is that we are trying to exploit the human perception of the integrity of the carrier signal. LSB steganography is very popular for Image Steganography, i.e., hiding secrets in images. And the change in LSB affects the color just so slightly that the change in color is not generally perceptible to the human eye. However, the human ear is more sensitive to slights changes in sound and hence the “noise” that we are adding would have a higher chance of being noticed. To overcome this problem of this trivial form of LSB algorithm, many researchers have suggested variants that increase robustness in the audio domain.

- **Text in Image, Image in Image** come under Image Steganography.

- Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used as a cover source because there are a huge number

of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image. Common approaches include:

- **Least Significant Bit Insertion**
- Masking and Filtering
- Redundant Pattern Encoding
- Encrypt and Scatter

Least Significant bit - instance

If we want to hide the data like "Aha!"

Then we convert the message "Aha!" into ASCII Code and then their equivalent binary code.

A=65 (01000001)

h=104(01101000)

a=97(01100001)

! =33(00100001)

- Each pixel contains three values which are Red, Green, Blue, these values range from 0 to 255, in other words, they are 8-bit values. [4] Let's take an example of how this technique works, suppose you want to hide the message "hi" into a 4x4 image which has the following pixel values:
- [(**225**, 12, 99), (**155**, 2, 50), (99, 51, 15), (15, 55, 22), (155, 61, 87), (63, 30, 17), (1, 55, 19), (99, 81, 66), (219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)]

- Using the ASCII Table, we can convert the secret message into decimal values and then into binary: 0110100 0110101.
- Now, we iterate over the pixel values one by one, after converting them to binary, we replace each least significant bit with that message bits sequentially
- e.g., 225 is 11100001, we replace the last bit, the bit in the right (1) with the first data bit (0) and so on.
- This will only modify the pixel values by +1 or -1 which is not noticeable at all.
- The resulting pixel values after performing LSBS is as shown below:[(**224**, 13, 99),(**154**, 3, 50),(98, 50, 15),(15, 54, 23),(154, 61, 87),(63, 30, 17),(1, 55, 19),(99, 81, 66),(219, 77, 91),(69, 39, 50),(18, 200, 33),(25, 54, 190)]

Technical Description of Project:

Steganography is a method for hiding a secret message inside (or occasionally on atop of) an otherwise open communication. You could have almost whatever you want as that object. In many cases of steganography nowadays, a text message is concealed behind a picture alternatively, by covertly inserting a phrase or script into an Excel or Word document. Steganography allows for both concealment and deception. It is a type of covert communication in which the messages are concealed through various mediums. It doesn't include key cryptography or data scrambling; thus, it isn't a type of cryptography. It is a technique for data hiding that may be applied in devious ways. In contrast to encryption, which is a field of study that normally supports privacy, steganography is a method that allows concealment and dishonesty. This project was created to mask data contained in any picture file. The extent of the project involves using steganography technologies for any sort of information may be masked. File and picture files, as well as the user's desired location to save the extruded file and image. This method was selected because this system additionally includes undetectability by any steganalysis instrument in addition to imperceptibility. With the help of this project, we will be able to convert the text data to the image securely. The encoded image will be same as the normal image no one will be able to identify that the image is encoded, and it has the information. In this project we will mainly target masking the data into the image. Firstly, we will be selecting the image for which we are willing to encode the data then we will be selecting the text or the information that we want to encrypt. After providing the information for which we want to encrypt the data we will be able to name the new encoded image and able to save the image. If we want to decrypt the image, we first must select the encrypted image to the tool and then we will be able to decrypt and read the data or the text information that was encrypted. The backend of the project is executed completely. The procedure for encryption

and decryption is running perfectly well. We have used python programming language for our execution of project.

Steganography, a technique for hiding hidden information in carriers including video, audio, digital images, and text, is used to protect online privacy. Picture steganography, or the incorporation of secret information into an image by changing the pixel values, produces a stegoimage. Steganography is an intriguing subject, in contrast to the routine encryption & that most systems administration of us deal with every day. Steganography is a secret communication method. The practical and theoretical limits of steganography have been examined. We will be printing out the development of its photo steganography method using the LSB refers to enable secure communication. When the message was embedded into the cover picture, a stego-key was referred to the system. This steganography program is designed to teach users how to use various picture formats to conceal different types of data inside them. The backend of our project is done and now we are working on the frontend of our project. This will help in giving a better representation of our work to various kinds of users. The website will make it easier for users to understand and interpret the website. It will allow them to encrypt and decrypt the image in a simpler way. They just need to upload the image in the desired location, following entering the text they wish to encrypt. On other hand, for decryption one needs to just upload the image with hidden message in it and expect the hidden text as desired output. His method incorporated security, capacity, and resilience, the three essential components of steganography that make it useful in covert communication and the hidden transmission of data through text files. Important files containing sensitive information can be stored on the server inside an encrypted manner, making it impossible for an intrusive party to get access to the original file while it is being transmitted. Steganography's main goal is to establish private connections in a way that is wholly

undetectable and to avoid creating doubt about the transfer of secret information. The goal is to stop people from believing that the concealed data even exists, not to stop them from interpreting the hidden data. If a steganography technique leads someone to question the carrier media, the technique has failed.

Steps used in LSB steganography:

a. ***Steps for hiding message image:***

1. Read the image to be used as cover image. Noise is added to make it easier to disguise changes due to embedding the message image.
2. Read the image to be sued as message image.
3. Separate the bit planes of each image.

As it is known that the LSB (least significant bit) plane contains the least information associated with any image, and the MSB (most significant bit) plane contains most of the shape, color information of an image.

It is generally ideal to replace up to 4 least bitplanes of the cover image, with the upper 4 bitplanes without revealing changes in the resultant image. Lesser number of bitplanes from the message image could be used, but the retrieved image would become distorted and loses information.

4. Replace the least 4 bitplanes of cover image with the 4 most significant bitplanes from message image.
5. Get the resultant Steganographic image by recombining these bitplanes.

b. ***Retrieving message image:***

1. Read the Steganographic image.
2. Extract the required number of bitplanes of the image.
3. Recombining the lower four bitplanes would give the retrieved message image.

TESTING AND RESULT

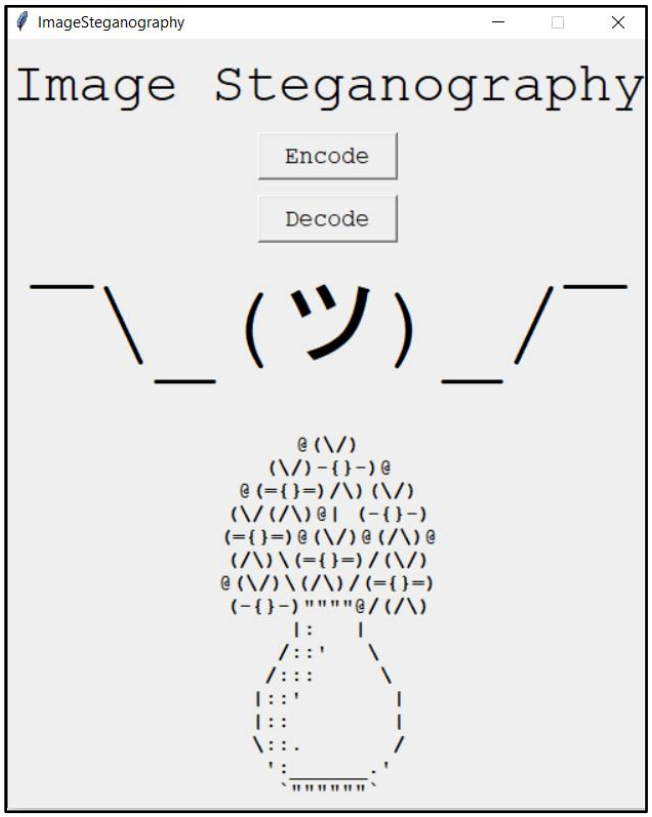


Fig 9 Home Page

On executing the generated exe file or running the python file in command prompt will lead you to the initial screen that is displayed above.

After clicking on encode or decode the various screen would be displayed. The first image below shows for encoding and second one shows for decryption.

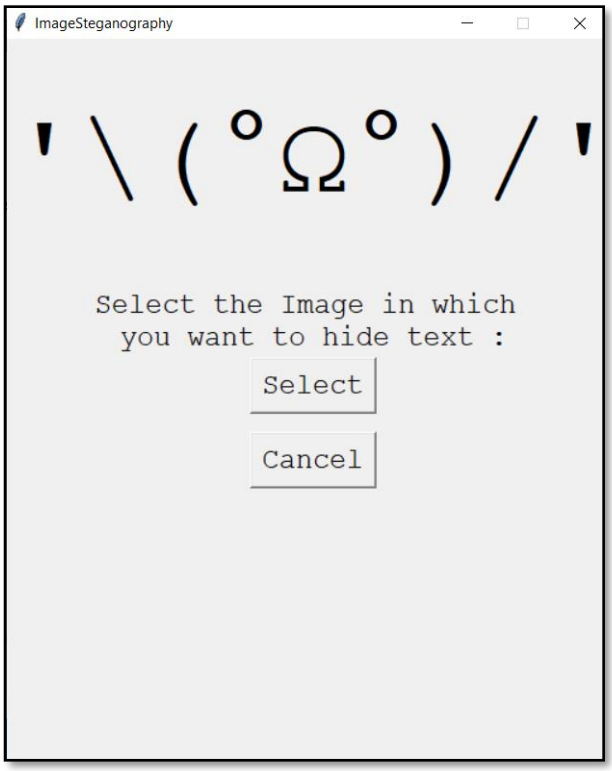


Fig 10 Encoding Page

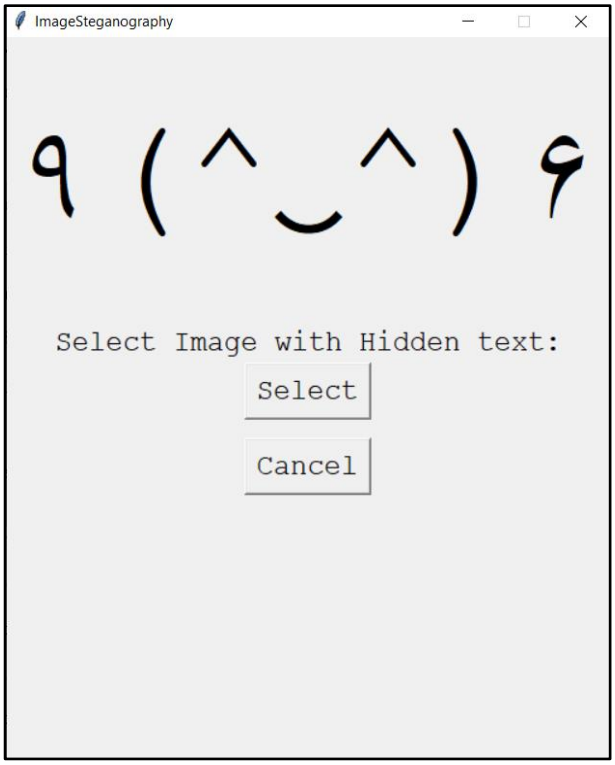


Fig 11 Decoding Page

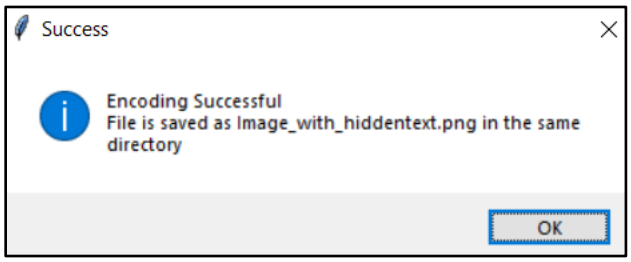


Fig 12 Encoding Success

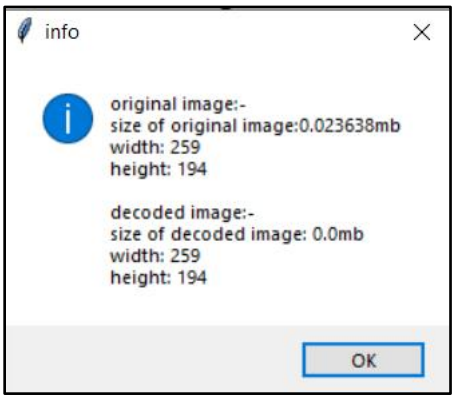


Fig 13 Image Information

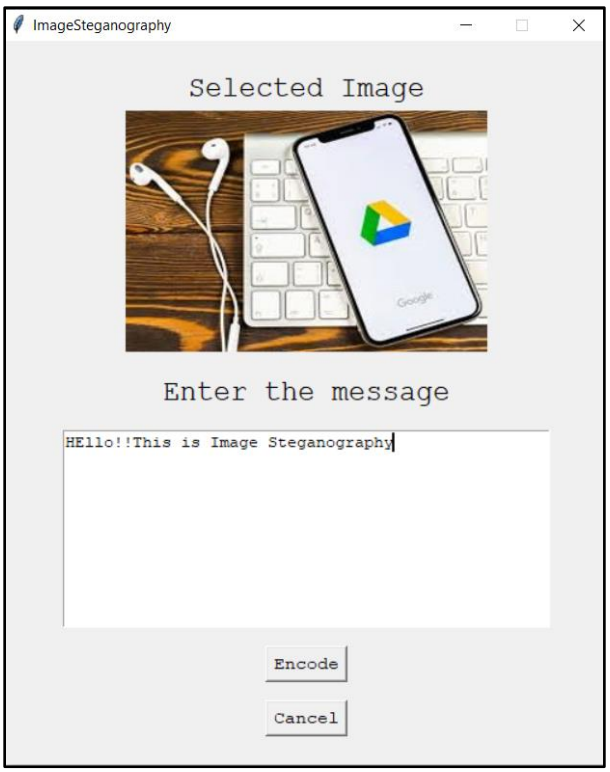


Fig 14 Encoding Result

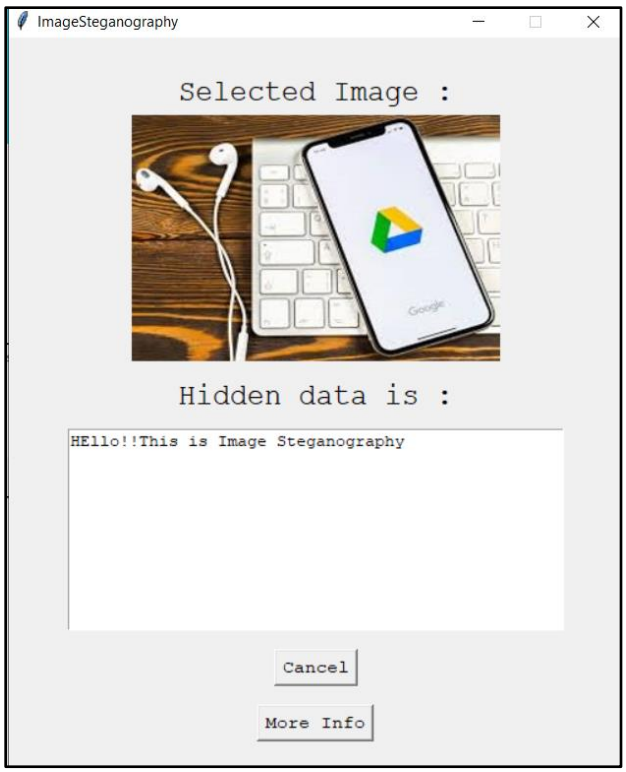


Fig 15 Decoding Result

SUMMARY AND CONCLUSIONS

It has been discovered that the results gained in data concealment using the LSB Substitution Steganographic approach are rather spectacular, as it makes use of the fact that each picture can be divided up into distinct bit-planes, each of which contains various levels of information. It should be emphasized that, as previously stated, this strategy is only useful for bitmap pictures because they use lossless compression techniques. In addition, greyscale photographs were utilized for demonstration in this research. However, this procedure may be expanded to be utilized for color pictures by performing bitplane slicing on each of the top four bitplanes of the messaging image, which are then placed inside the Rgb, planes of the cover picture, and extraction is performed similarly. In this project mainly concentrated on embedding the data into an image. We have designed a steganographic 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 as 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 steganographic algorithms available like JSteg, F5 and LSB algorithms. We have used the Least Significant Bit algorithm in designing the steganographic 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.
- In the present world, the data transfers using the internet are rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and businesspeople use it to transfer business documents, important information using internet.

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

The future work on this project is to improve the compression ratio of the image to the text. This project can be extended to a level that can be used for different types of formats like audio files, text files, videos in the future. The security using Least Significant Bit Algorithm is good, but we can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption.

In an effort to keep secrets hidden, steganography conveys information through coverings that appear innocent. The use and applications of digital picture steganography and its variants are expanding. People are looking at steganography as a way to get around laws banning strong encryption and cryptography and transmit communications discreetly. Steganography and Steganalysis will continuously create new strategies to oppose each other, just like with the other major achievements of the digital age: the conflict between cryptographers and cryptanalysis, security professionals and hackers, record labels and pirates.

The field of digital watermarking is likely to see steganographic techniques used most often soon. Digital watermarks offer a mechanism to identify the owners of these items, which is something content providers are anxious to safeguard against unauthorized dissemination of their intellectual works. Due to government claims that criminals utilize these methods to communicate, steganography may also be restricted by legislation.

It is also crucial to note that, while steganography was originally undetectable, with the numerous technologies now available, it is not only possible to detect its presence but also to retrieve it. For

example, basic approaches to determine whether a picture has been changed without the need of software or complicated tools include:

1. Image dimensions: When compared to the conventional image of same proportions, an Image steganography image has a much larger storage size. For example, if the original picture storage capacity is a few KBs, the Secret message image may be many MBs in size. This varies depending on the size and type of picture utilized.
2. Image noise: Especially compared to a standard image, a Steganographic image contains noise. This is why, at first, just a little amount of background noise is added toward the cover picture, so that the Image encryption image does not look too noisy in relation to the actual cover image.

However, this study focuses on LSB or spatial multiplexing steganography, certain information concerning transform domain approaches have been investigated and the fundamentals of these approaches have been addressed. As a result of the different publications and theories accessible, it has been discovered that transforming domain approaches outperform image pixels methods.

The following are some potential applications for steganography:

1.protecting network data in the event of a breach.

2.private conversations between peers.

3.Publishing private messages online to prevent transfer.

4.Including corrected audio or picture data if corrosion happens due to a bad connection or transmission.

REFERENCES

1. Team, D. F. (2022, March 16). Python image steganography - learn how to hide data in images. Data Flair. Retrieved November 29, 2022, from https://data-flair.training/blogs/python-image-steganography-project/
2. Eloise. "AP 186 Blog Reports: Image Types and Formats." AP 186 Blog Reports, 28 June 2011, jigglingatoms.blogspot.com/2011/06/image-types-and-formats.html. Accessed 8 Dec. 2015.
3. Dr Ekta Walia, Payal Jain and Navdeep. “An analysis of LSB & DCT based Steganography.” Global Journal of Computer Science and Technology, April2010. https://globaljournals.org/GJCST_Volume10/gjcst_vol10_issue_1_paper8.pdf
4. Image based steganography using Python. GeeksforGeeks. (2020, August 20). Retrieved November 29, 2022, from https://www.geeksforgeeks.org/image-based-steganography-using-python/

APPENDIX

GitHub Link:

https://github.com/Riddhi1213/IMAGE_STEGANOGRAPHY

Code:

For code kindly refer to attached zip file.