Steganography "The Art Of Hiding Data"

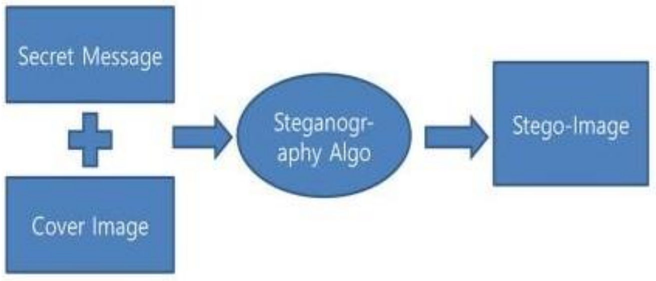
Vishnu kk[1], Prof. Vijay Swaroop A[2]
[1]Dept of iComputer Science and Engineering
[2]Asst. Professor, Dept of Computer Science and Engineering
[1, 2]Atria Institute Of Technology, BLR, KA, India

Abstract- *Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This project hides the message with in the image . For a more secure approach, the project it allows user to choose the bits for replacement instead of LSB replacement from the image. sender select the cover image with the secret text or text file and hide it in to the image with the bit replacement choice, it help to generate the secure stego image .the stego image is sent to the destination with the help of private or public communication network on the other side i.e. receiver. receiver download the stego image and using the software retrieve the secret text hidden in the stego image.*

Keywords- Steganography, LSB, Image, secret message, stego key, cover image, Techniques.

I. INTRODUCTION

STEGANOGRAPHY is a Greek word which means secret writing. The word steganos means secret and graphy means writing. Thus, Steganography is not only the art of hiding data but also the hiding fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of messages. An ancient example is, In history king used to shave the head of his most trusted slave and tattooed a message on it. After his hair was grown, the message was hidden. The purpose was to revolt against Persians. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data.In today's world, the communication is the basic necessity of every growing area.Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of data so that no one can detect its presence. In steganography the process of hiding information content inside any multimedia content like image , audio, video referred as a Embedding. For increasing confidentiality of communicating data both techniques may combined. The aim of steganography is to encrypt the data or hide the data over an image using steganographic technique and to know that algorithms in the context of quality of concealing and to describe their functionality in data security. We can limit the unauthorized access and provide better security.



II. LITERATURE SURVEY

Dipti Watni, Sonal Chawla, (October 2019) started "Comparitive evaluation of JPEG steganography", Images are available in different formats, out of which jpeg images is the most popular image format due to its small size.This paper also analysis's these algorithms based on the parameters of image steganography.Undetectability, robustness and embedding capacity.With the dependency on internet and smart gadgets, security of data has become a major concern.These images undergo lossy compression resulting in small sized images, but hiding data behind these images is a challenge. Many algorithms have been suggested till date. This paper intends to give understanding and evolution of different techniques for jpeg steganography. It summarizes various algorithms and techniques used in the past and in present. This paper also analysis's these algorithms based on the basic parameters of image steganography: Undetectability, robustness and embedding capacity.

Jun Tae Kim, Sangwon Kim, Keechoen Kim, (October 2019) started "A Study on improved JPEG steganography algorithm to prevent steganalysis", Video steganography is a data-hiding technology that inserts confidential messages intended to be hidden in video data at an unrecognizable level. Image steganography can be divided into spatial area techniques for inserting confidential data by manipulating the Last Significant Bit (LSB) of each image pixel and frequency domain techniques for manipulating the DCT (Discrete Cosine Transform) coefficients of images.JPEG (Joint Photographic Experts Group), which is used as the image loss compression standard, uses JPEG steganography techniques such as Jsteg, F3, F4, and F5 based on frequency domain techniques that manipulate DCT coefficients.

Neha Sharma, Usha Batra, (October 2017) started " A review on spatial domain technique based on image steganography", As we are moving towards a digital world with rapid strides and advancements in the field of communication of information with effective use of technology, it becomes mandatory that the communicable information is kept in an electronic format.In the paper, we are focusing on spatial domain image based steganography. The technique is scrutinized and argued in the terms of its payload capacity i.e., the ability to hide information, how much information can be hidden, and it robustness.

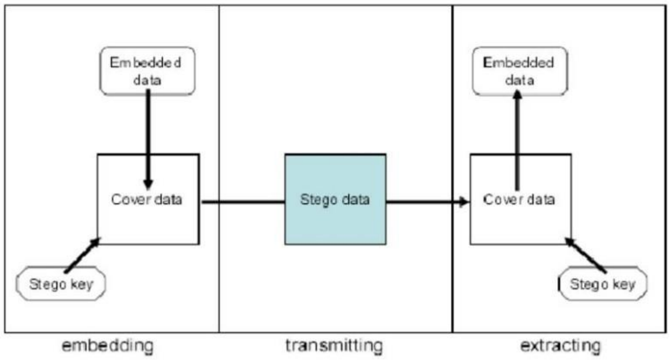
Nidhi Menon, Usha Batra, (December 2017), started " A survey on image steganography", In many areas security systems are very popular as the technologies are increasing day-by-day.Using encryption and steganography information security can be achieved. In today's world, cryptography is most often associated with scrambling plaintext into ciphertext, then back again. In the presence of third parties, it is a practice for secure communication.Its success depends on the secrecy of the action and if detected, the system will fail but security of data depends on the robustness of the applied algorithm.

Arnold Gabriel Benedict, (March 2019), started " Improved file security system using multiple image steganography", Steganography is the process of hiding a secret message within an ordinary message & extracting it at its destination.The data slicing ensures secure transmission of the vital data making it merely impossible for the intruder to decrypt the data without the encrypting details.

III. EXISTING SYSTEM

- Key oriented algorithms used were very bulky to manage as key handling must be done.
- For transmitting a file from one point to another, only encyrption was used which will not provide that much of security.
- Application used was only platform dependant.
- It supports either command mode or graphical mode.

IV. ARCHITECTURE DIAGRAM



The three main phases of the architecture diagram are Embedding, Transmitting and extracting.

1) EMBEDDING

Embedding means all the actual characters that are included with the file. In embedding algorithm the one file is a club or adds into another file. Initializes some parameters, which are used for subsequent data pre processing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message, then the data hiding is performed on the selected region. Embedding phase consists of Embedded data, Cover data and Stego key.

- Embedded data: Embedded Data is any extra information that we would like to record.
- Cover data: The data within an ordinary, non-secret file or message in an order to avoid detection.
- Stego key: This is the secret key used in the embedding process.

2) TRANSMITTING

In this process, the secret information is transmitted by hiding this behind a signal or image or video. Image stenography is another approach which utilizes an image for the secure transmission of data by hiding it behind a cover image. Steganography is done for secure transmission of data on network. Various phases for data steganography are described below. Phase 1 Select on cover image for data embedding cover image should be a color image containing red, green and blue pixels. Phase 2 In the second phase least significant bits and intermediate significant bits for implemented for the predictions of No. of least significant bits available in that according to pixel value. Phase 3 In this phase secret data is embedded into the LSB and ISB of cover images. Secret data that has to be embedding has been covert into cipher text that has to been generated by steganographic approaches.

3) EXTRACTING

First extract the side information, i.e., the block size and the threshold from the stego image. As we done exactly the same things in data embedding. The stego image is divided into blocks and the blocks are then rotated by random degrees based on the secret key. For extraction process applies the inverse support vector dimension on watermarked image. With the use of a secret key the decryption is done only. Then it transfers the YCbCr to RGB image, form and calculate the PSNR values of the original image and watermarked image. Extract the original and the watermark image. The quality of the image doesn't degrade while decompression. The human eyes can't detect easily. It provides the high security to the secret image that cannot alter by hackers or intruder easily. Extracting phase consists of Embedded data, Cover data and Stego key.

- Embedded data: Embedded Data is any extra information that we would like to record.
- Cover data: The data within an ordinary, non-secret file or message in an order to avoid detection.Cover image will be the original image with no hidden secrets. Image selected for the purpose of hiding is called cover image.
- Stego key: This is the secret key used in the embedding process.

V. PROPOSED SYSTEM

- Steganography is both securable and reliable.
- The application is platform independent.
- It supports both command mode and graphical mode.
- Provides interactive interface through which user can interact with different types of images,image sizes and text messages.
- To improve the quality of existing system, LSB algorithm is used.

IMAGE STEGANOGRAPHY

It is the technique of hiding the data within the image in such a way that prevents the unintended user from detecting the hidden messages or data.

Image Steganography Elements:

- **Cover medium:** It is an image that holds secret message.
- **The Secret Message:** It is a message to be transmitted. It can be plain text, image or any other data.
- **The Stego Key**: It is key used to hide the message.

Two types of compression techniques are:

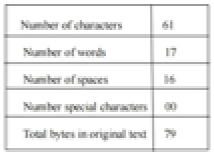
1. Lossy Compression

- They may not maintain original images integrity.
- It offers high compression.
- Ex: JPEG

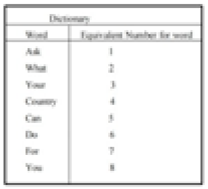
2. Lossless Compression

- They maintain the data exactly.
- The compression on lossless image has no effect on original image.
- Ex: BMP

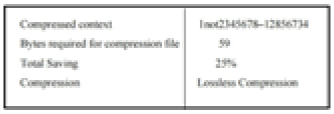
Ask not what your country can do for you – ask what you can do for your country



Number of characters	61
Number of words	17
Number of spaces	16
Number special characters	00
Total bytes in original text	79



Dictionary	
Word	Equivalent Number for word
Ask	1
What	2
Your	3
Country	4
Can	5
Do	6
For	7
You	8



Compressed context	1not2345678-12856734
Bytes required for compression file	59
Total Saving	25%
Compression	Lossless Compression

After applying lossless compression, the size of the original context is reduced from 79 bytes to 59 bytes.

● LSB ALGORITHM

The most popular technique used in image steganography. The easiest method to embed secret information within an image. The binary representation of the secret data are taken and LSB of each byte is overwritten within the image. Permits huge amount of secret information to be embedded.

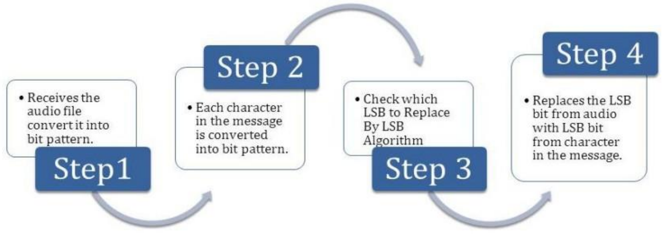

Step1
• Receives the audio file convert it into bit pattern.
Step 2
• Each character in the message is converted into bit pattern.
Step 3
• Check which LSB to Replace By LSB Algorithm
Step 4
• Replaces the LSB bit from audio with LSB bit from character in the message.

Figure: **STEPS IN LSB ALGORITHM**

LSB is called as Least Significant Bit. I the below figure 1 is denoted as Most Significant Bit 0 is denoted as Least Significant Bit. The easiest way to embed secret information within the cover file is called LSB insertion. In this technique, the binary representations of the secret data have been taken and the LSB of each byte is overwritten within the image. If 24-bit color images are used, then the quantity of modification will be small.

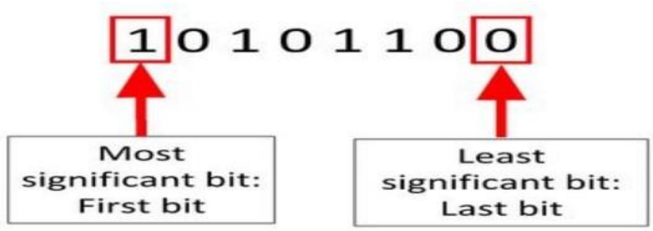
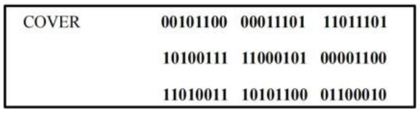

1 0 1 0 1 1 0 0
Most significant bit: First bit
Least significant bit: Last bit

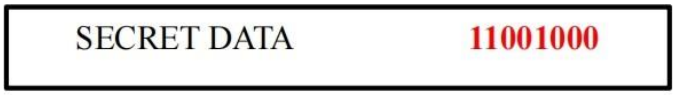
Figure: **MSB AND LSB**

Example for LSB Algorithm:



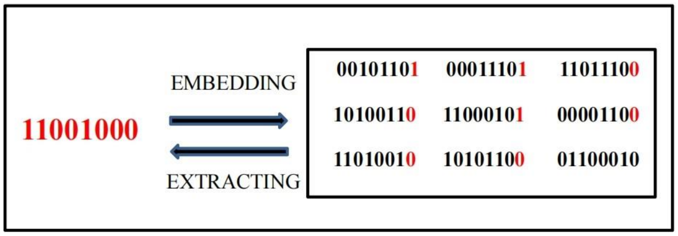
COVER	00101100	00011101	11011101
	10100111	11000101	00001100
	11010011	10101100	01100010

Above is the cover data that has to be sent from source to destination.



SECRET DATA 11001000

The secret data 11001000 has to be embedded within the cover data.



00101101	00011101	11011100
10100110	11000101	00001100
11010010	10101100	01100010

In the above figure, the secret data is embedded within the cover data. The red coloured digits in the above figure is the secret data. And also the data can be extracted back the secret data is obtained. This is a two way approach.

The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit- plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates.In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

VI. FUTURE WORK

- Future work on this topic is to improve the compression ratio of the image.
- It can be extended such that it can be used for the different types of images formats like .bmp, .jpeg etc.
- Combine both cryptography and steganography for additional security.

VII. ADVANTAGES

It is used in the way of hiding not the information but the password to reach the information. Confidential communication and secret data storing. Protection of data alteration. The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.

VIII. DISADVANTAGES

Password leakage may occur and it leads to the unauthorized access of data. If the technique is used in wrong way then this can be very dangerous. Huge number of data results in large file sizes. Image is distorted. Message easily lost if picture subject to compression such as JPEG. When properly implemented, steganography can be difficult to detect, but not impossible. Steganography detection can be used to prevent communication of malicious data.

IX. SCOPE

Hide passwords and Encryption Keys. Limit the unauthorized access and provide better security during image transmission. The approach finds the suitable algorithm for embedding the data in an image using steganography**.**

X. CONCLUSION

Steganography is in the nascent stage of development. LSB technique provide secure communication over the internet.

Hiding the message with steganography method reduces the chance of a message being detected. In this process the message which is hidden is invisible. Steganography is to create secrete communication, in addition to this crypto way of embedding gives us higher end of security. Even if the person gets both stego and cove image he needs key to retrieve the data, without the key one can't recover the data. The growth of modern communication needs a special means of security especially on computer network. As there appears a risk that the sensitive information transmitted might be intercepted or distorted by unintended observers for the openness of the internet. So it has resulted in an explosive growth in secure communication and information hiding. Moreover, the information hiding technique can be used extensively in applications like business, military, commercials, anti-criminal, digital forensic and so on. Steganography is the technique of secret communication which has received much attention. In this report image based steganography methods have been proposed to increase the performance of the data hiding techniques.

REFERENCES

[1] Dipti Watni, Sonal Chawla, “Comparitive evaluation of JPEG steganography” - 2019.

[2] Arnold Gabriel Benedict, “Improved file security system using multiple image steganography”-2019.

[3] Sangwon Kim, “A Study on improved JPEG steganography algorithm to prevent steganalysis”, Vol 22-0, 2019.

[4] Neha Sharma, Usha Batra, “A review on spatial domain technique based on image steganography” - 2017.

[5] Nidhi Menon, “A survey on image steganography” - 2017.