International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 02 | Feb-2016 www.irjet.net p-ISSN: 2395-0072

An Infallible Method to Transfer Confidential Data using Delta Steganography.

Ms. Kajal Prakash Kamble[1], Ms. Swapnali Vasant Khabale[2], Mr. Ankush Shahu Morale[3], Prof. Chadrashekhar Shankar Shinde[4].

[1] *Department of Computer Science and Engineering, Dr. J. J. Magdum College of Engineering, Jaysingpur, India. kajalkamble157@gmail.com*

[2] *Department of Computer Science and Engineering, Dr. J. J. Magdum College of Engineering, Jaysingpur, India. swapnalikhabale28@gmail.com*

[3] *Department of Computer Science and Engineering, Dr. J. J. Magdum College of Engineering, Jaysingpur, India. moraleankush99@gmail.com*

[4] *Department of Computer Science and Engineering, Dr. J. J. Magdum College of Engineering, Jaysingpur, India. csshinde7769@rediffmail.com*

Abstract

In the Steganography is secret writing or hiding fact that communication taking place, by hiding secret information inside image. The scope of project is implementation of steganography tools for information includes any type of information file and image file and path where user want to retrieve the information file. For hiding information in image, their exist large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this paper reduce the text in R, G and B planes in separately and data embedded in random manner. This proposed system uses different keys used for embedding and extraction of the secret data, where key used for embedding message and used for extraction of data. This method shows good high capacity, security, Robustness. Image steganography is a technique that provides a safe way to the secret embedded data to the target user. To hide the secret data in the images various techniques are proposed by the researchers, some are complex and other produce good results.

Keywords—**Delta Compression, Embedding, Encryption Extraction, RGB, LSB, Steganography.**

1. INTRODUCTION

Steganography is a type of cryptography in which the secret message is hidden in a digital picture, video or audio file. Steganography differs from Cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, whereas steganography focuses on keeping the very existence of the message secret. The main goal of steganography is to provide secret and robust communication. There are two more concepts are mixed with steganography: cryptography and watermarking. Cryptography is technique encodes information in such way that nobody can read it, except the person who holds the key. Watermarking is process of hiding digital information through carrier signal. Steganography is about hiding the message so that intermediate person cannot see message. The basic structure of Steganography is made of three components:

i. The Carrier image,
ii. The secret message,
iii. The secret key.

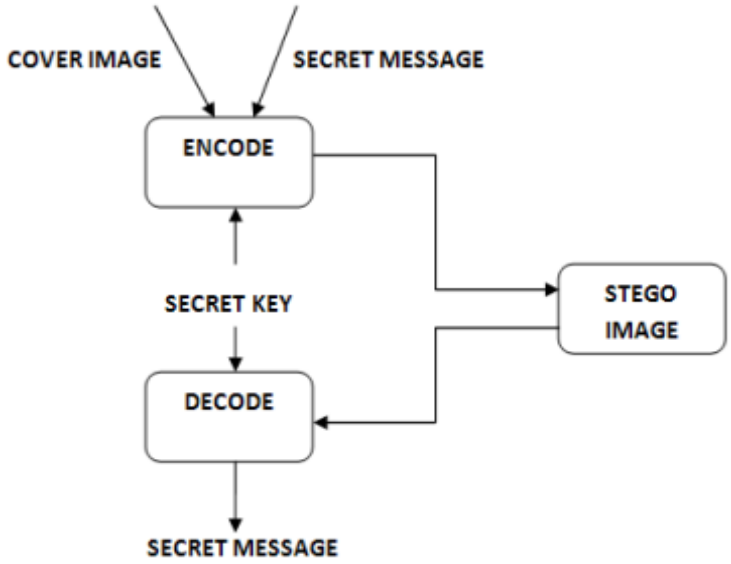


Fig-1: Steganography operation

The steganography can done through different carriers that is we can classify steganography into four different types,

1.1 Text steganography

In this technique of steganography, the secret data is embedded in text form by altering certain properties of text document. This technique is not widely used. Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of the internet and different types of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

1.2 Audio steganography

In this technique of steganography, the secret data is embedded in the audio form.

1.3 Image steganogarphy

In this technique of steganography, the secret data is embedded in the image. This is achieved by adjusting the pixel values. Images are the used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego-image unauthenticated persons can only notice the transmission of an image but can't see the existence of the hidden message.

1.4 Video steganography

In this secret data is embedded in video form.

1.5 Protocol steganography

The term protocol steganography is to embedding information within network protocol such as TCP/IP. We hide information in the header of TCP/IP packet in some fields that can be either optional or are never used.

2. IMAGE STEGANOGRAPHY

2.1 Image definition

This project is developed for hiding information in any image file. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap. An image map is file containing information that associates different locations on a specified image with hypertext links. This numeric representation forms a grid and the individual points are referred to as pixels (picture element). Grayscale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color are represented by 8 bits. Thus in one given pixel, there can be 256 different quantities of red, green and blue.

The scope of the project is implementation of steganography tools for hiding information includes any type of information file and image files and the path where the user wants to save Image and extruded file. User needs to run the application. The user has two tab options as encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file. The basic terminologies used in image steganography system are cover image, secret message, the secret key and embedded algorithm. The cover message is the carrier of message such as text, image, audio, video or some other digital media. The secret message is the information which is needed to be hidden in digital media. The embedding algorithm is the way that embeds secret information in cover image.

2.2 Image compression

In images there are two types of compression: lossy compression and lossless compression. In Lossless compression, with lossless compression, every single bit of data that was originally in the file remains after the file is uncompressed. All of the information is completely restored. The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and BMP (bitmap file). Lossy compression reduces a file by permanently eliminating certain information, especially redundant information. When the file is uncompressed, only a part of the original information is still there. In this case the resulting image is expected to be something similar to the original image, but not the same as the original. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group).

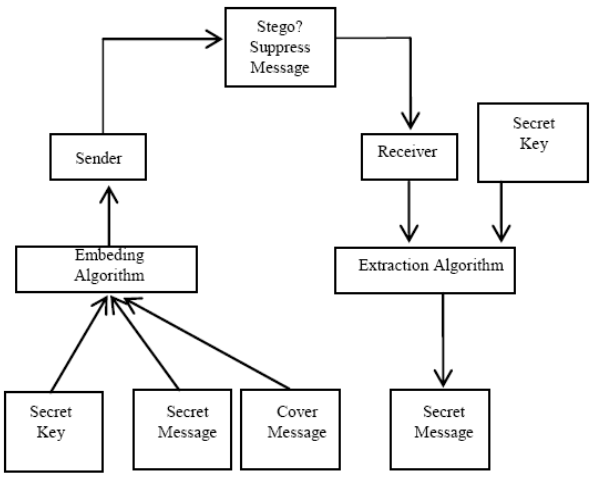


Fig-2: General Steganographic Approach

3. COMPERATIVE STUDY OF IMAGE ENCODING TECHNIQUE

3.1 LSB Steganography

Least Significant Bit (LSB) approach was basically carried out to hide text in images in which the last bit of every pixel of the image is replaced with the information. The simplest and most common type of steganography is LSB. In this method the messages are embedded into cover image by replacing the least significant bits of the image directly. The hiding capacity can be increased by using up to 4 least significant bits in each pixel which is also quite hard to detect.

The one's bit of a byte is used to encode the hidden information. Suppose we want to encode the letter S (ASCII 65 or binary 01010011) in the following 8 bytes of a carrier file.

Table-1: Original RGB pixel value

Pixel/Color	RED	GREEN	BLUE
Pixel 0	00100111	11101001	11001000
Pixel1	00100111	11001000	11101001
Pixel 2	11001000	00100111	11101001

After inserting S into above sequence the embed image look like this

Table-2: Replacing least pixel of RGB with binary of S

Pixel/Color	RED	GREEN	BLUE
Pixel 0	0010011**0**	1110100**1**	1100100**0**
Pixel1	0010011**1**	1100100**0**	1110100**0**
Pixel 2	1100100**1**	0010011**1**	11101001

Least Significant Bit (LSB) insertion is a common simple approach to embedding information in a cover file. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 bit BMP‟s or possibly another image format such as GIF.

Unfortunately it is vulnerable to even a slight image manipulation. Converting an image from a format like GIF or BMP which reconstructs the original message exactly. But while using format like JPEG, which does not reconstruct back the original message, and could destroy the information hidden in the LSB's. Even though LSB provide security it is not robust. Another variation of the LSB would be randomization in which the secret message is spread out among the cover image in a random manner and a secret key is used for providing security. The secret key is shared only between the sender and receiver.

The purpose of the key is to generate pseudorandom numbers, which will identify where and in what order the hidden message is laid out. Sensitive to any kind of filtering, Hackers can destruct the messages by removing or zeroing the LSB. While removing the LSB it will not affects the quality and it is not identified by the end user. So the content could be destroyed. After the converting our information in secret code or encrypted form we need to patch that data in the image. We use least significant bit for the patching of data because of following reason.

a. Because the intensity of image is only change by 1 or 0 after hiding the information.
b. Change in intensity is either 0 or 1 because the change at last bit .e.g.

11111000 ⟶ 11111001

Steps to insert data into carrier image:

a. Take an input image.
b. Find out the pixel values.
c. Select the pixel on which we want to insert data.

This process of selection of pixel is done as users choice he may choose pixel continuous or alternate or at a fixed distance insert the data values in pixels.

The change is only one bit so that the intensity of image is not effected too much and we can easily transfer the data.

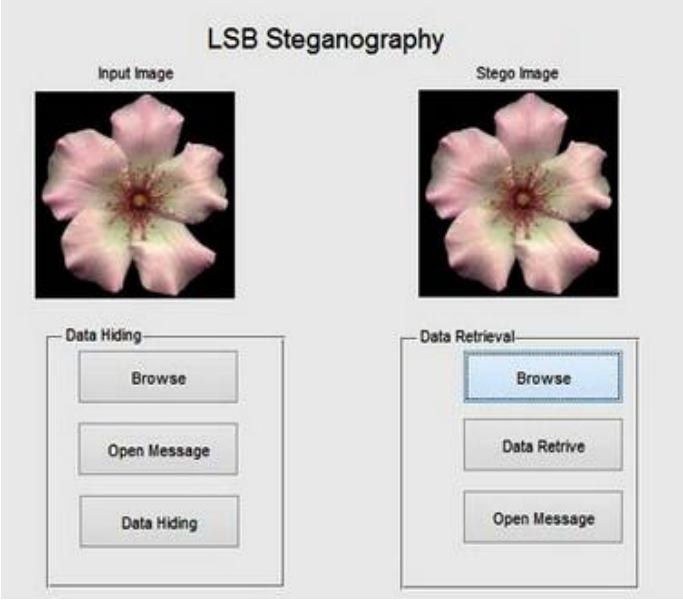


Fig-3: Cover image **Fig-4:** Stego image

Advantages:-

1. Degradation of the original image is not easy.
2. Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages:-

1. LSB technique cannot support to the JPEG image file format.
2. It is lossy compression technique.

3.2 RGB Steganography

The RGB technique is basically an extension of the LSB which is quite vulnerable. A Digital image is an array of numbers that represent light intensities at various points or pixels. Digital computer images can be normally stored as 24-bit (RGB) or 8-bit (Grayscale) files. A 24-bit file can be quite large however it provides more space for hiding information. As we know all colors are essentially a combination of three primary colors: red, green, and blue. Every primary color is represented by one byte that is every pixel represents a combination of (R,G,B). Along with this variable bit steganography technique is also used in RGB based steganography.

Delta Compression: In order to reduce the space consumption and to increase the efficiency of data transfers, delta compression techniques are widely used in the computer networks and in the data storage systems. These delta compression techniques make use of compression which accepts reference source file and the target files as its two inputs. The notations F' denotes secret file, F is reference file and ΔF is delta file. The delta creator locates and copies the difference between the target and source file, comparing only these differences as a delta shown in figure 5.

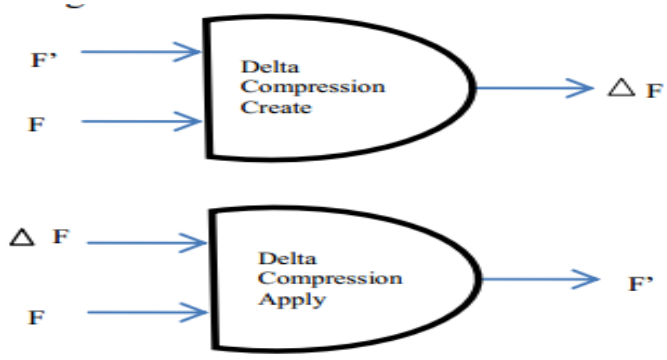
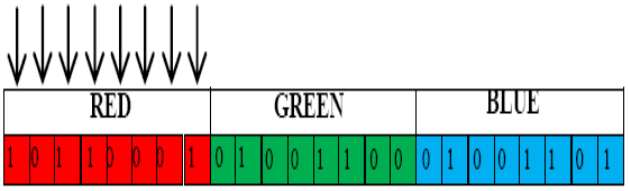


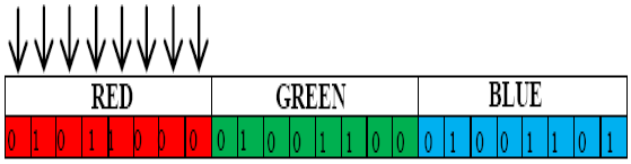
Fig.5: Delta Compression.

Size (ΔF-F') << Size (F')

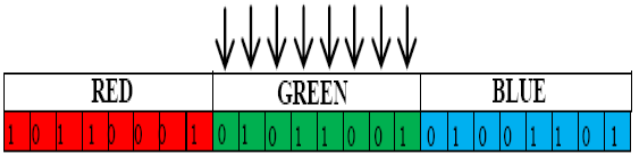
Instead of hiding the data in least significant bits of the RGB components of a pixel, we in this algorithm, would be hiding data as shown below: - Let the data to be hidden is word "ABC"
ASCII code of A= 65 and corresponding binary is 01000001.
ASCII code of B= 66 and corresponding binary is 01000010.
ASCII code of C= 67 and corresponding binary is 01000011.
Let the first pixels RGB component be: -
Red component is replaced with binary of 65 i.e. A.
Original Red Component



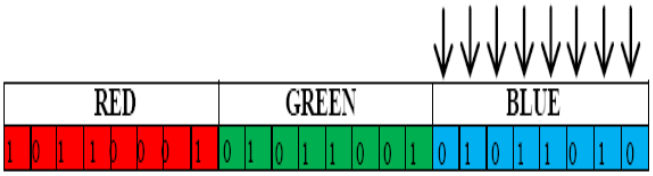
Red component is replaced with the binary of 88, i.e. X.



Replace the green component in the same pixel with binary of 89 i.e. Y.



Replace the blue component in the same pixel with binary of 90 i.e. Z.



And process continues.

The proposed embedding technique.
Inputs:-Secret text, secret key, cover image.
Output:-Delta file.
Begin

1. Select the Secret Text, call ASCII code generation function.
2. Select an image, Find number of pixels, Convert its RGB components, and calculate number of bits in text file.
3. If calculated bits is less than or equal to number of RGB Components, then

Start iteration
Displace red component of first pixel with ASCII value of first character.
Displace green component of first pixel with second character.
Displace blue component of first pixel with third character and store RGB component values. Select next pixel and reiteration until character get empty.
End iteration

4. Accept secret key and call encryption.
5. Call delta creator and save delta file.

Else
Error, image is of low resolution.
End

Proposed extraction technique.
Inputs:-Reference image, Secret key, Delta file.
Output:-Secret text.
Begin

1. Select delta file.
2. Provide secret key and reference image, and then call extraction function.
3. Display secret message.

End

Image after embedding of data using modulus RGB Steganography technique.

Fig-3: Cover image

Fig.4: Stego image

Advantages:-

1. High security.
2. lossless compression technique.
3. It is used in the hiding, not the information but the password to that information.
4. It can be applied differently in video, audio files.
5. It can be done faster with varying number of software's using different algorithm.

Table-3: Comparison of different file sizes

Sl. no	Reference image size	Text file size	Stego image size	Delta file size
1	1569KB	18KB	1519KB	191KB
2	1569KB	36KB	1701KB	323KB
3	586KB	20KB	1812KB	220KB
4	3761KB	36KB	3761KB	389KB

Table-4: Comparison of LSB and RGB with Different image file formats

Image file	**.JPEG**	**.BMP**	**.GIF**
LSB	Lossy compression	Lossless compression	Lossless compression
RGB	Lossy compression	Lossy compression	Lossless compression
Embedding	Done	Done	Done
Extraction	Done	Done	Done

4. CONCLUSION

Steganography is an effective way to hide sensitive information. In this paper we have used the LSB Technique and RGB Technique on images to obtain secure stego-image. Our results indicate that the RGB using secret key is better than simple LSB insertion in case of lossless compression. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel .It is also more difficult to identify by hackers when compared with LSB method. Hence it is more advantageous over the LSB method for use of steganography.