Color Image Steganography using LSB

Ch. Rajesh Babu[1], G. V. Jagannath[2], B. Dinesh Manikantha[3], G. Narasimha Srivatsasa[4], Ch. Billy Paul[5]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Godavari Institute of Engineering and Technology (A), Rajahmundry, Andhra Pradesh, India

[2,3,4,5] UG Scholar, Department of Electronics and Communication Engineering, Godavari Institute of Engineering and Technology (A), Rajahmundry, Andhra Pradesh, India

Abstract: As the technology growing the risk of sharing important information also became a hefty task without being attacked by any external malware, virus or hacker. As information is power so therefore care must be taken while transmitting the data over the internet. So certain security measures should be taken while transmitting the data. One of the methods that provides the security is Steganography. It is an art of hiding the data over a cover. It allows no one to suspect the existence other the sender and recipient. This is very efficient technique because of the simplicity and undetectable. Here using the Least Significant Bit technique for hiding the information. Which divide the image into different color components Red, Green, Blue. To embed the data into these components, so the data can be easily retrieved.

Keywords: Steganography, Color image, Least Significant Bit (LSB), Edge, Components

DOI of the Article: https://doi.org/10.46501/GIETEC14

Available online at: https://ijmtst.com/icetee2021.html

As per UGC guidelines an electronic bar code is provided to seure your paper

To Cite this Article: Ch. Rajesh Babu; G. V. Jagannath; B. Dinesh Manikantha; G. Narasimha Srivatsasa and Ch. Billy Paul. Face Color Image Steganography using LSB. *International Journal for Modern Trends in Science and Technology* 2021, *7*, pp. 77-81. https://doi.org/10.46501/GIETEC14

Article Info. Received: 18 May 2021; Accepted: 25 June 2021; Published: 30 June 2021

INTRODUCTION

In this Digital World the security of the data should be given the main importance as data is the most confidential thing in this digital era. Data send over the internet should be accessed only by the receiver of the information but no one else should access the data it will be misled the information or the data can be used for wrong purposes so the data should be sent by using certain security measures. Steganography is one of that kind where the data is concealed inside some other data like an image, video or audio file. So, it is undetectable by the external user about the data hidden in the image, video or audio. Here we using the image or hiding the data so that the data will be hidden under the cover of the image and the data will be accessed only by the sender and receiver by using certain algorithms here the least significant bit algorithm is used to hide the data.

The data that is hidden can be of any format but the cover is an image and there will be no change in the image after hiding the data and before hiding the data so that the unauthenticated. There are several steganography techniques which are of different levels of security.

LITERATURE SURVEY

The previous analysis, methods and discussions are analyzed here. The word image Steganography states that the image is used as a mask for hiding the data over the image cover so that the image data is divided into components or edges and the data is embedded into the different components of the image. So, data will be undetectable or unpredictable by the unauthenticated user. The Word Steganography is combination of two words mainly ' Stegano 'and 'Grapy 'which means the 'Covered' and 'Writing' respectively.

Steganography is not the new technology it is used from our ancestors to transfer the message by hiding it. At the time of 400 BC in Greece to send a message by shaving the hair of a soldier and then tattoo the message on the head. Then let the hair grow and after reaching the receiver the hair will be shaved again and the message will be shared to the receiver. Later wax is used to send the message by writing the message on a wooden block and applying wax to that wooden block and make it to be appear as a tablet. So, that there will be no doubt on the message transformation and the message will be transmitted

Steganography is used for both the legal and illegal purposes. The legal activities aim to hide the data from the third party such that the information sharing among the military services. The data is transmitted in a coded form so maintain secrecy between the sender and the receiver only. The illegal form of transmission is also there to harm the country, its people and other important things.

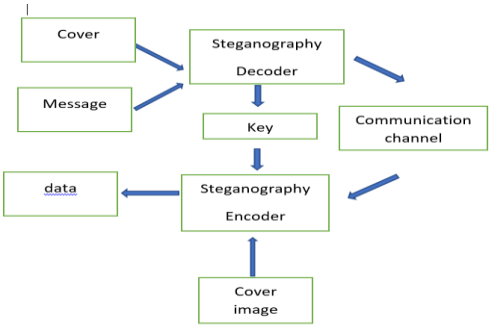

Figure 1: Block Diagram of the Color image Steganography

TYPES OF STEGANOGRAPHY

Steganography can be implemented using various cover forms. The steganography type depends upon the type of the cover file used for hiding the data. The cover file may be of any format like image, audio, video, text and protocol. The steganography techniques can be classified as follows

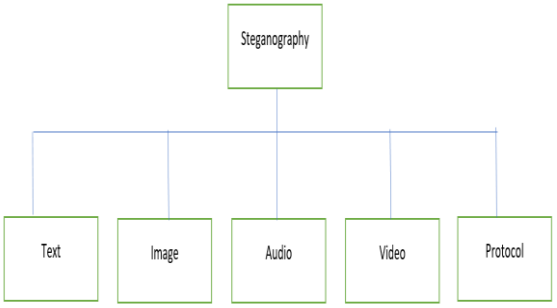

Figure 2: Classification of Steganography types

3.1 - Text Steganography:

In text steganography the cover file would be in the text format and the message data will be also in the text format. Text steganography also involves number of lines, white spaces, capital letters

3.2 - Image Steganography:

In image steganography the image is used as a cover object. It allows to store huge bits of data under the cover of the image. The image steganography is most widely used steganography technique.

3.3 - Audio Steganography:

It uses digital sound as the cover image for hiding the data in it. It can be of different forms .mp3, .wav, .au etc. It hides more amount data as image steganography technique.

3.4 - Video Steganography:

In this video is used as a media to cover the data. Here the data is embedded in the form of video frames.

3.5 - Protocol Steganography:

This is coming into existence in the recent days where the network layer protocol I.e., Tcp/IP protocol is used for hiding the data and this is not restricted to only this layer. Thesetransmit the information over the network by using the network layer.

EXISTING METHODS

There are mainly "Six" types of methods that exists to perform Steganography technique. Those methods are listed below.

4.1 Transformation Domain Method
4.2 Embedding Method
4.3 Spectrum Method
4.4 Statistical Method
4.5 Distortion Method
4.6 Filtering Method

Let us discuss briefly about each and every method in detail. Let's get into the explanation.

4.1- Transformation Domain:

The hiding of information in this domain is more complex when it compared to remaining methods that are present to perform steganography.

This method is further divided into three types, those are listed below.

1.Discrete Fourier Transform.
2.Discrete Wavelet Transform.
3.Discrete Cosine Transform.

4.2 - Embedding Method:

Robust algorithm with codec standards was used in this "embedding method". This embedded information will not effect the sequence of video.

4.3 - Spectrum Method:

In this method a secret data was spread over the wide band width frequency.

4.4 - Statistical Method:

By changing the properties of cover the message was embedded. In this way the method was performed to get steganography. The modification was done only when message bit size is "1", otherwise no modifications was done.

4.5 - Filtering Method:

A duplicate image was created to hide the data. In this method we use watermarking technique to integrate the image. In this method there is no fear of distortion.

4.6 - Distortion Method:

In this method, we distort the signal to store the secrete data.

PROPOSED METHODLOGY:

Our Proposed methodology is the Lease significant bit technique. Where the last bit of the each pixel in the image is replaced with the binary value of the hidden data.

Each pixel in the image is divided into three categories namely Red, Green and Blue whose values are lying in between the range of 0 to 255, it can be also called as a 8-bit values. Let us take an example to show how this techniques works. If you want to store the message 'hi' into image of 4*4 pixels having the below pixel values:

[(224, 13, 89), (145, 1, 54), (79, 34, 15), (16, 54, 23), (156, 61, 88), (63, 30, 17), (1, 55, 19), (99, 81, 66), (219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)]

Using the ASCI values first we will get the ASCI values of the message and then we convert that into the binary data format: 0110100 0110101.Now, we have to iterate the data over the pixel values one by one, after converting the data into binary, we have to replace the last significant bit with the message bit (e.g., 225 is 11100001, we have to replace the last bit in the pixel , the bit in the right (1) with the first data bit (0) and so on). This will change the pixel values by+1 or -1 which is not a noticeable change. After modifying the values the image pixels will be.

[(223, 14, 90), (144, 2, 54), (78, 35, 15), (16, 54, 24), (155, 61, 87), (63, 30, 17), (1, 55, 19), (98, 82, 67), (218, 77, 90), (68, 38, 51), (18, 201, 34), (24, 53, 191)]

The reason behind using the LSB methodology can be easily defined using below image.

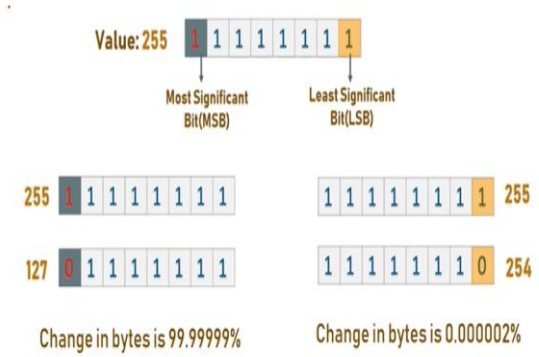

Figure 3: Proposed Methodology

So as to not alter the look of the image largely we are going to use the Least Significant Bit Methodology.

5.1 - Snippets of using proposed Methodology in real time

The first image shows about the encoding done to an original image, where the secret data is embedded into the image, this is known as stego image. The input fields to this are the original image, secret message, special symbol to terminate the message. Following is the image that gives a clear cut picture of what is described here.

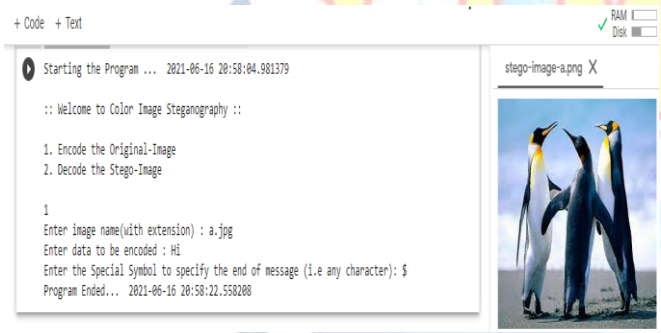

Figure 4: Encoding Process

As we have seen the converted image beside the output in the image, now we can retrieve the data in it using the decode function, the following image shown below shows the output of the retrieved data from an encoded image.

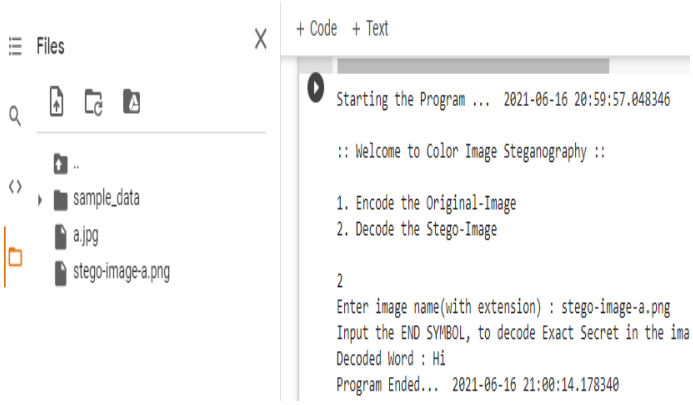

Figure 5: Decoding Process

EVALUTION CRITERIA FOR IMAGE STEGANOGRAPHY

There are several algorithms for performing steganography each technique is efficient in a particular way. It is hard to see a technique that follows all the criteria. A technique may be good result in one criterion have very less efficient in other. There are certain factors for evaluating the steganography technique. They are:

6.1 - Security:

As security is main concern for using the Steganography. So, the technique should satisfy several transforms like attacks, cropping, slicing etc.

6.2 - Independent of file format:

As there are different file formats in image so it will confuse about the format of the image a good steganography technique should be chosen so that it can able to hide data in any format of the file.

6.3 - Invisibility:

The invisibility factor of the steganography means it cannot be noticeable by the human visual system if it is done any tampering and it is noticeable then it is not an efficient technique for the steganography.

6.4 - Temper Resistance:

Temper resistance means the survival capacity of the technique even when there is an attempt to modify the data. Computation complexity is the process of hiding and extracting so that it should be as low as possible.

6.5 - Payload Capacity:

Payload capacity means hiding a huge amount of data behind the file chosen. A good steganography technique will have high payload capacity and it can be represented as bits per pixel.

CONCLUSION

The proposed method is very efficient and effective way of the data transmission.By using the proposed method, we can able to retrieve 100% of the given original data without any loss. There are lot of Steganography techniques available but the proposed method will provide the better results and for hiding large amount of data (message) we have to choose suitable image. The data or message embedded in various types of images of various size can be recovered easily by using this technique.

There is no need to send any special key along with the information the receiver has to know the length of the message data. The proposed method is more secure as

the threshold value which is selected dynamically is acts as a key between the sender and the receiver. As, the image changes the threshold value also changes.

REFERENCES

[1] **SABYASACHI KAMILA, RATNAKIRTI ROY AND SUVAMOY CHANGDER**"A DWT based steganography scheme with image block partitioning" at Noida, India, IEEE 2015

[2] **SATOSHI WATANABE, KAZUKI MURAKAMI, TOMOYA FURUKAWA AND QIANGFU ZHAO**"Steganalysis of JPEG image-based steganography with support vector machine" at Shanghai, China, IEEE 2016

[3] E. T. Lin and E. J. Delp, "A Review of Data Hiding in Digital Images," West Lafayette, 2001.

[4] M.V. Khandare and M. S. Sutaone," image based steganography using LSB insertion technique " 2008 IET International Conference on Wireless, Mobile and Multimedia Networks

[5] Jia Liu,Yan Ke, Zhuo Zhangand Jun Li"Recent Advances of Image Steganography with Generative Adversarial Networks" at IEEE 2020