

Video Steganography by LSB Substitution Using Different Polynomial Equations

A. Swathi¹, Dr. S.A.K Jilani, Ph.D²

¹(M.tech Student, ²Professor,) Electronics and communication Engineering, Madanapalli Institute of Technology and science

Abstract:

Video Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements. The least significant bit (LSB) insertion is an important approach for embedding information in a carrier file. Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit. In this project, a data hiding scheme will be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation.

Keywords: least significant bit, Steganography

1. Introduction:

Currently, internet and digital media are getting more and more popularity. So, requirement of secure transmission of data also increased. For this reason various good techniques are proposed and already taken into practice. In this project, we use the steganography process for the secure data transmission from the sender to receiver through the internet.

2. Steganography Introduction:

Steganography is the process of secretly embedding information inside a data source without changing its perceptual quality. Steganography comes from the Greek word *steganos* which literally means “covered” and *graphia* which means “writing”, i.e. covered writing. The most common use of steganography is to hide a file inside another file.

Generally, in data hiding, the actual information is not maintained in its original format. The format is converted into an alternative equivalent multimedia files like images, video or audio. Which in turn is being hidden within another object[7].

3. Block diagram:

The basic block diagram representation for steganography mechanism is shown in the below figure.

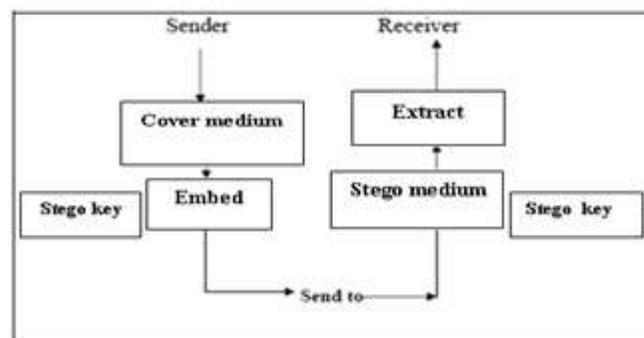


Fig 3. 1: Steganography mechanism

3.1 Block Diagram Explanation:

The above figure shows a simple representation of the generic embedding and extraction process in steganography. In this example, a secret data is being embedded inside a cover image to produce the stego image. A key is often needed in the embedding process. The embedding procedure is done by the sender by using the proper stego key. The recipient can Extract the stego cover image in order to view the secret data by using the same key used by the sender. The stego image should look almost identical to the cover image.

4. Least Significant Bit Insertion Method:

Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover video. Video is converted into a number of frames, and then convert each frame in to an image[6]. After that, the Least Significant Bit (in other words the 8 bit) of some or all of the bytes inside an image is changed to a bit of each of the Red, Green and Blue colour components can be used, since they are each represented by a byte. In other words one can store 3 bit in each pixel. An 800 x 600 pixel image can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. We implemented our project such that it can accept and video of any size.

For example a grid for 3 pixels of a 24 bit image can be as follows:

```
(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)
```

When the letter A, which binary representation is 01000001 and is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

```
(00101100 00011101 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)
```

Although the letter was embedded into the first 8 bytes of the grid, only the 2 highlighted bits need to be changed according to the embedded message. On average only half of the bit in an image will need to be modified to hide a secret message using the maximum cover size.

First we read the original video signal and text. We have to embed the text into the video signal. Then we have to convert the text data into the binary format. Binary conversion is done by taking the ASCII

Value of the character and converting those ASCII values into binary format. We take the binary representation of samples of cover signal and we insert the binary representation of text into that cover signal

The LSB bits of video signals are replaced by the binary bits of data and this encoded signal is called stego signal is ready for transmission through internet. For the steganography the important video format is Audio Video Interleave (AVI). The message which we want to hide is converted into ASCII and then converted into its binary representation with each word consist of 8bits. These bits are substituted in the Least Significant Bits of binary representation of each image ample. Suppose if we want to hide letter A (01000001) in LSBs of binary signal.

Here the polynomial equations are used to find the location of insertion of message binary bit in the video file. Below process shows finding the location by using polynomial equations. After finding the location in audio file Least Significant Bits are replaced as below process.

Y=X	M1=3X+5	M2=2X+5
123	if X=1 → M1= 8	M2=7
124	X=2 → M1= 11	M2=9
126	:	:
128	:	:
135	X=10 → M1= 35	M2=25
144		
135	-----→ 10111000 -----→ 10111000	
156		11111110 AND operation by 254 th bit
173		-----
192		10111000
203		1 OR operation by message bit
257		-----
269		10111001
288		

If the message is **mits.**, ASCII(m)-129 → (10000001)
 If we get same locations by two polynomials
 Then 2 will be added to location.
 M1=22 M2=22 then M=22+2=24

```
01110001 10011000 11001000 00110110
10001101 11000111 01010011 10100011
```

becomes

```
01110000 10011001 11001000 00110110
10001100 11000110 01010010 10100011
```

5. Flow Chart for encoding:

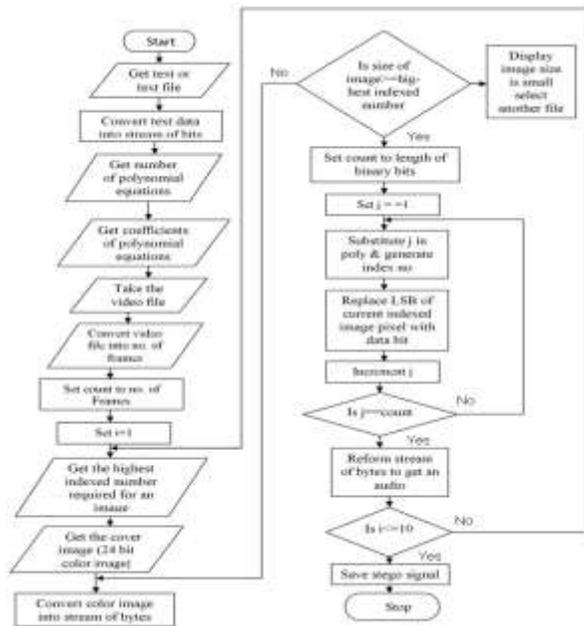


Fig 5.1 : Flow chart for encoding

Description about Encoding:

First we will take the original video and text file in which we have to embed into original image. Then we have to convert the video file into number of frames, we consider each frame as an image. Here we set the counter value to frames. Then we have convert the text data into binary format. Binary conversion is done by taking the ASCII value of each character and converting those ASCII values into binary format. We are going to set the counter value to the length of the binary message, so that the loop repeats that much times. The LSB bit of the image pixel is replaced by the binary data. This encoded image called as stego video is ready for transmission through the internet.

5.1 Flow Chart for decoding:

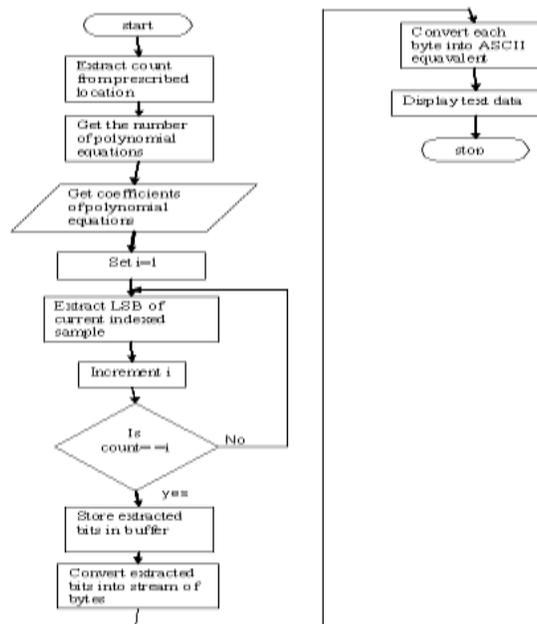


Fig 5.2 : Flow chart for Decoding

Description about Decoding:

First we take the LSB encoded image. We will set the counter to the length of the binary data. Then we will extract the binary data from the LSB encoded image by extracting the LSB bits of the image pixels. In order to form the text file from the binary data we have to group all the binary bits.



Cover Video



Stego Video

Description:

By observing the above two figures we can simply say that both stego and cover videos are identically equal.

6. Conclusion:

There are many kinds of steganography techniques are available among them hiding data in video by LSB substitution is a simple method. Here the information will be embedded based on the stego key. Key is used in the form of polynomial equations with different coefficients. By using this the capacity of embedding bits into the cover image can be increased.

References

- [1] Ping Wah Wong and Edward J. Delp, editors. Security and Watermarking of Multimedia Contents, volume 3657. Society of Photooptical Instrumentation Engineers, 1999.
- [2] Ping Wah Wong and Edward J. Delp, editors. Security and Watermarking of Multimedia Contents II, volume 3971. Society of Photo-optical Instrumentation Engineers, 2000.
- [3] W. Bender, D. Gruhl, N. Morimoto, A. Lu: Techniques for data hiding, IBM SYSTEMS JOURNAL, VOL 35, NOS 3&4, 1996
- [4] R. Anderson, F. Petitcolas: On the limits of the steganography, IEEE Journal Selected Areas in Communications, VOL .16, NO. 4, MAY 1998.
- [5] FABIEN A. P. PETITCOLAS, ROSS J. ANDERSON, AND MARKUS G. KUHN, Information Hiding—A Survey, PROCEEDINGS OF THE IEEE, VOL. 87, NO. 7, JULY 1999.
- [6] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs: Implementation of LSB Steganography and Its Evaluation for Various Bits, 2001.
- [7] NedeljkoCvejic, TapioSeppben: Increasing the capacity of LSB-based video steganography, IEEE 2002.
- [8] Dr D Mukhopadhyay, A Mukherjee, S Ghosh, S Biswas, P Chakarborty: An Approach for Message Hiding using Substitution Techniques and video Steganography, IEEE 2005.
- [9] Zhou Lin-na, Liu Cui-qing, Ping Xi-jian, Wang Yun-he: Information Hiding Method in Digital Audio Signal Based on Perfect Codes, Information Hiding and Multimedia Signal Processing, IEEE 2006.