High Security Video Steganography

Putti DeepthiChandan, Dr. M. Narayana

Abstract- Video Steganography is a technique to hide any kind of files into a carrying video file. Textual data is hidden in red, green, blue components separately in specific frames of the carrier video file. The least significant bit insertion method is an important and simple approach for embedding textual information in the carrier video file. If the location of the pixel exceeds the size of the video-image, choose the pixel location within the boundary of the video-images. The specific location of the pixel is chosen by using pseudo random equations. This method protects messages as it is passed in innocuous content like image. Using Video Steganography, we can hide large number of characters when compared to Image Steganography. Video Steganography provides high security in hiding maximum number of characters as the video consists of many images.

Keywords- Cryptography, Frame, Least Significant Bit, Pseudo Random Equations, Text, Video –Image, Video Steganography.

1 INTRODUCTION

Steganography is an ancient art of conveying messages in a secret way that only receiver knows the existence of message [1]. Steganography comes from the Greek word, steganos which literally means "covered" and graphia means "writing" ,i.e, "covered writing"[2].

The concept of steganography has for thousands of years .The Greek used to pass secret information by writing in wax covered tablet, the secret message was written on the tablet, and the tablet was written on the tablet was given covered with the wax [3]. Another technique was to shave a messenger's head, tattoo a message or an image on the bald head and let hair grow again so that tattoo could not be seen .Shaving the head again revealed the tattoo. The use of invisible ink was also used extensively used but the invisible secret message gets revealed when heated. Then the image files are used to hide messages. But, image files are not the only carriers [9]. Secret information can be hidden in computer image files (JPEG, GIF, BMP), audio files (MP3) [10] or even text files.

Traditionally, Steganography [11] is based on hiding secret information in image files. Lately, there has been a growing interest in implementing steganographic techniques to video files and the audio files .The advantage of using video files in hiding information is to be added security against hackers[4].The main aim of Steganography is to hide information in the other wrap media so that other persons will not observe the existence of information.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as document file, image file. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and the colour of every 77th pixel to correspond to a letter in the alphabet, looking for it is unlikely to notice it.

With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. Making use of the Internet secret information hidden in the carrier can be transmitted quickly, secretly and securely [12].

1.1 Comparison of Steganography and Cryptography

Steganography and Cryptography are closely related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the cipher text. In steganography, comparisons may be made between cover- media, the stega - media and the possible portions of the message. The end result in cryptography is the cipher-text, while the end result in steganography is the stego-media. The message in steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

1.2 Combination of Steganography and Cryptography

Those who seek the ultimate in private communication can combine encryption and steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. In some situations, sending an encrypted will cause suspicion while an invisible message will not do so. Both methods can be combined to produce better security. For the proposed system, steganography alone can produce better security.

The advantage of steganography over cryptography alone that message don't attract to them self [5].

Steganography is implemented in different fields such as military and industrial applications [4] and it is also applicable in espionage, intelligent services and to add copyright information [14].

2 REQUIREMENTS OF HIDING INFORMATION DIGITALLY

There are many different protocols and embedding techniques that enable us to hide data in a given object. However, all of the protocols and techniques must satisfy a

number of requirements so that steganography can be applied correctly.

The following is a list of main requirements that steganography techniques must satisfy:

a) The integrity of the hidden information after it has been embedded inside the stego object must be correct.

b) The stego object must remain unchanged to the naked eye.

c) In watermarking, changes in the stego object must have no effect on the watermark.

d) Finally, we always assume that the attacker knows that there is hidden information inside the stego object.

3 PROPOSED SYSTEM

This paper focuses on Video Steganography. Motion of images/ frames is a video. We extract a specific frame from that video and convert to digital image. Digital images are the most popular cover objects compared to text.
To a computer, image is a collection of numbers which represent the light intensities in different areas of the image. The individual numbers are called pixels [13]. These pixels are represented horizontally row by row. Gray images use 8 bits to represent each pixel and have 256 different shades, where as color images use 24 bits as it uses three primary colors: red, green and blue. Thus, each pixel has 256 shades of each color component represented using 8 bits. So using color images we can hide large amount of information.The proposed system is based on video steganography for hiding data in the video-image, retrieving the hidden information from the video using least significant bit modification method. Though least significant bit modification method is used in many of the existing systems, it provides an efficient method for hiding the data in the video file and sending it to the destination securely. The existing systems difficulty in choosing the key and more encodes-decode time consumption. The proposed system provides easy way of implementation in hiding data in video file when compared to other video steganographic techniques.

3.1 Hiding Data in Red, Green, Blue Components Separately

The proposed system is based on the video steganography for hiding text in the video-image by separating red, blue, green components.

As an example, imagine "hiding" the characters "WMC"
W is hidden in red video-image
M is hidden in green video-image
C is hidden in blue video-image

3.2 Pseudo Random Equation

Here, the pseudo random equations are used to find the location of insertion message binary bit in the video file. After finding the location in video file, Least Significant Bits are replaced.

If the location of the pixel exceeds the size of the video-image, choose the pixel location within the boundary of the video-images. The specific location of the pixel is chosen by using pseudo random equations.

3.3 Least Significant Bit Modification

The Least Significant Bit modification is used in this system to conceal the textual data in the video file. The main advantage of LSB coding method is high security with low computational complexity [5].

Every character, digit, symbol has its own ASCII value.
Example, the ASCII value of 'E' is 69.

As an example, let the pixel value at the specific location be 164.
Binary value of 164 is 10100100.

Letter 'E' is represented in ASCII format as a binary string 1000101.

Case 1: If '1'has to be inserted at the pixel location then Bit-or with
(00000001).

(10100100)

(00000001)

(10100101)

The binary value of 165 is 10100101. We find minor change in the pixel value. But, the change in the pixel value is undetectable to the human vision.

Case 2: If '0'has to be inserted at the pixel location then Bit-and with (11111110).

(10100100)

(11111110)

(10100100)

The binary value of 164 is 10100100. We find no change in the pixel value.

The same process is repeated to all the bits. Thus, letter 'E' is stored.

3.4 Implementation:

Locations where the text to be hidden

L(1,3)	L(2,4)	L(2,6)	L(4,4)	L(4,7)	L(5,2)	L(6,6)

Values at that location

145	164	134	33	242	152	193

Binary equivalents of the values

10010001	10100100	10000110	100001	11110010	10011000	11000001

ASCII value 'E'=1000101

1	0	0	0	1	0	1

Inserting 'E' at the random locations with the LSB of the pixels.

NC	NC	NC	+1	+1	NC	NC

Values at the locations after inserting 'E'

145	164	134	34	243	152	193

*NC=No Change

L(1,3), L(2,4),L(2,6), L(4,4), L(4,7), L(5,2), L(6,6) are the location of the randomly selected pixels.

L (1, 3) represents 1st row, 3rd column of the image.

L (2, 4) represents 2nd row, 4th column of the image.

L (2, 6) represents 2nd row, 6th column of the image.

L (4, 4) represents 4th row, 4th column of the image.

L (4, 7) represents 4th row, 7th column of the image.

L (5, 2) represents 5th row, 2nd column of the image.

L (6, 6) represents 6th row, 6th column of the image.

3.5 Retrieval of the Text from the Image

Stego Image Pixel Values

145	164	134	34	243	152	193

Bit and with 00000001 to the above pixel values, we get

1	0	0	0	1	0	1

ASCII value of 'E' is 1000101.Hence, the retrieved data is 'E'.

4 RESULTS AND DISCUSSIONS

From the following figures, we can notice that there are indistinguishable changes between the original video-image and the stego video-image. The results obtained during the experiment have invisible changes to the human vision.

Fig. 1. Represents the original video-image with red, green, blue components separated and Fig. 2. Represents the original video-image with red, green, blue components separated. Both figures are identically equal.

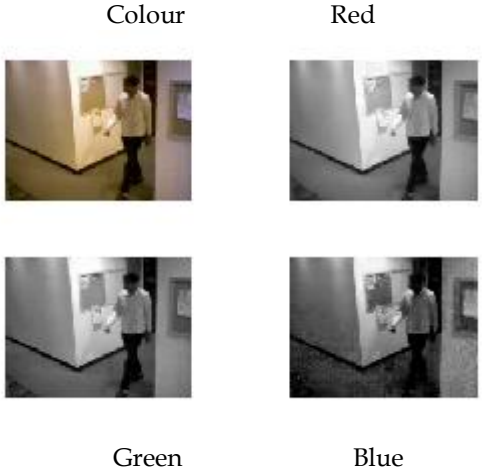

Fig. 1. Original video-image with red, green, blue components separated.

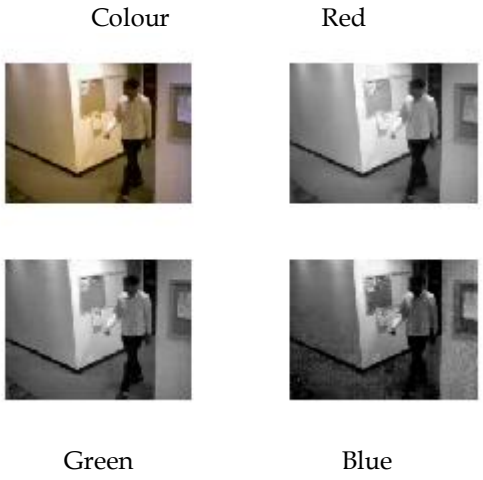

Fig. 2. Stego video-image with red, green, blue components separated

At the transmitter section, the characters are inserted such that the first three characters in R, G, B planes respectively and so on using pseudo random equation.

At the receiver section, the corresponding characters are retrieved from the R, G, and B planes using same pseudo random equation employed at the transmitter section.

With advent of separating red, green, blue components of each frame and selecting the pixels randomly using pseudo random equations makes the system highly robust.

In Image steganography, it is possible detect the existence of the data by finding the difference between the original image and the stego image.
Using video steganography, it is impossible to detect the existence of the data because, frames are in motion.

As the number of characters increases, the performance of the system gets down in terms of speed.

TABLE 1
NUMBER OF CHARACTERS PER FRAME VS TIME IN CLOCK

Number of characters	Time in clock
3	0.4668
6	0.7570
9	1.1365

But, the actual aim of the proposed system is to hide the information and send the data securely to the destination, the speed is compensated.

If number of characters per frame =3 then the elapsed time is 0.4668 Seconds.

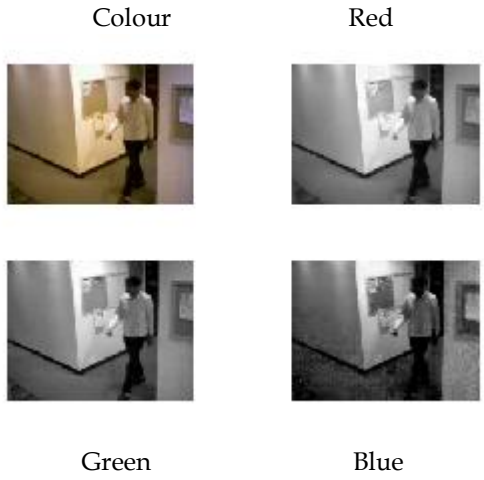

Fig. 3. Stego video-image with number of characters per frame=3.

If number of characters per frame =6 then the elapsed time is 0.7570 Seconds.

Fig. 4. Stego video-image with number of characters per frame =6.

If number of characters per frame =9 then the elapsed time is 1.1365 Seconds.

Fig. 5. Stego video-image with number of characters per frame =9

.

Though the number of characters increases, there are undetectable changes in the above video-images. Using Video steganography, we can hide large number of characters when compared to Image steganography. Video steganography provides high security in hiding maximum number of characters as the video consists of many images.

TABLE 2
RETRIEVAL OF DATA AT THE RECEIVER END

Number of characters per frame	Time in clock(in seconds)	Characters embedded	Characters retrieved
3	0.4668	WMC	WMC
6	0.7570	WMCWMC	WMCWMC
9	1.1365	WMCWMCWMC	WMCWMCWMC

The proposed system has the following advantages.

1. Messages do not attract attention to themselves.
2. The task of detecting and disabling information is highly impossible.
3. Protects both messages and communicating parties as it is passed in innocuous content like image.
4. Slight changes to colour values make the presence of secret data undetectable.

4 CONCLUSION AND FURTHER SCOPE

There are many kinds of steganography techniques available .Among them, hiding data in the video-image by least significant bit method. Here, the information is embedded is based on the pseudo random equations. Characters are embedded in red, green, blue components of the video-image making the system highly secured.

The alterations between the original video-image and the stego video-image are not visible to the human eye. Though the number of characters increases, there are undetectable changes to the human eye.

Using Video steganography, we can hide large number of characters when compared to Image steganography. Video steganography provides high security in hiding maximum number of characters as the video consists of many images.

Further diverse work on video steganography should be carried out. First of all, work should focus on the further development and improvement of the proposals presented so far. With the current knowledge on the video steganography, we can see the need to build a real and secure system that allows hidden data transmission.

REFERENCES

[1] Behrouz A.Forouzan, Debdeep Mukhopadhyay, Cryptography and Network Security, 2nd Edition.

[2] William Stallings, Cryptography and Network security: Principle and Practice, 2000, PE.

[3] Niels Provos and peter Honey man, "Hide and Seek: An introduction to Steganography ", University of Michigan, IEEE 2003.

[4] S. Suma Christal Mary/IJCSE, "Improved Protection in Video Steganography used compressed Video Bit streams ", PSN college of engg & technology, Vol.02, NO.03, 2010, 764-766.

[5] Mr.Chintan Mahant, "Steganography and Steganalysis: Different Approaches for Information Hiding ", ISSN: 2278-0181, Vol.1 Issue 10, December 2012.

[6] A. Swathi, Dr.S.A.K Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", (ijceronline. com) Vol.2 Issue .5.

[7] Sutaone, M. S., Khandre, "Image Based Steganography Using LSB insertion technique", IET, 2008.

[8] Yao wang, Joem Ostermann and Ya-quin zhang, Video Processing and Communication

[9] Kharazzi, M., Sencar, H.T., and Memon, W. (2004) Image Steganography: Concepts and Practice. In WSPC lecture notes series.

[10] Mazdak Zamani, Azizah A. Manf, and Shahidan Abdullah, "A Genetic Algorithm Based Approach for Audio Steganography" Waset 2009.

[11] Mohammad Shirali-Shahreza, "A New method for real time Steganography", ICSP 2006 Proceedings of IEEE.

[12] Shashikala Channalli et al / International Journal on Computer Science and Engineering Vol.1 (3), 2009, 137-141.

[13] Gonzaleze and Woods, Digital Image Processing, 3rd ed., Pearson.

[14] Mark Burgess, John Weil, Principles of Network and Systems Administration