Steganography in Video Files

Shahd Abdul-Rhman Hasso

**Department of Software Engineering, College of Computer Sciences and Math.,
University of Mosul / Mosul, Iraq**

Abstract

This paper proposed a new technique for hiding in video files, Secret message has been hidden as number of bits after converts every frame of image colored bit to its value as 24 bit. The result video show high capacity and there is no suspicion of the existence of secret text.

The result video show no change when played after embedding process, the receiver need the length of text that will send in secret locations within video file to know the number of bits embedded in every frame and width number of image in frame.

Mean Square Error (*MSE)* and Peak Signal to Noise Ratio (*PSNR*) are used to measure the performance of the work and the result is that, the MSE , is decreased ,the PSNR is increased when increase the number of bits embedded and when the size of video file is increased.

Keywords*; steganography*, *video steganography*

1. Introduction

In today's world internet increase the communication speed to send receive data so digital communication is overtaking other means of communication. But with many advantages their some disadvantages and one of main issue is data security. When highly confidential data send through the insecure environment then there is chance that the data may be lost, tempered or modified by some intruders so there is many ways to overcome this and one of them is steganography [1].

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 [2].

Steganography rather focuses on making it extremely difficult to tell whether a secret message exists at all or not. If an unauthorized third party is able to say with high confidence that a file contains a secret message, then steganography has failed. There are many reasons why steganography is used. Mainly it insures the possibility of sending secret messages even under monitored conditions. There are many different ways of sending messages to people without anyone else knowing the message exist [3].

2. Related work

In [4] Cruz Jason Paul et.al. ,(2012), proposed the design and implementation of a steganographic protocol and a suite of tools that can automatically analyze a flash video (FLV) format and effectively hide information within it for application in a digital records environment, the automated FLV analysis software also generates Excel files that record some of the parameters (i.e., the type, sizes, and timestamps of the metadata, video, and audio tags) for further analysis. The creation of the automated FLV analysis software was a vital part in this study, When video or audio tags were removed in whole, including the tag type, body size, timestamp, extended timestamp, streamed, the actual data, and the previous tag size, the modified FLV played the entire length but with distortions on the corresponding timestamp of the removed tags. Even though the FLV format did not contain conflicts, actual data was missing at a specific point in time throughout the duration of the video.

In [5] Lee Yunjung (2013), in which it is fit for streaming video data to hide information related in copyright and authentication of video data. Secret information is encrypted by session key generated with symmetric key by pseudo-random number; shared by sender and receiver, To share the secret key with video streaming server and customer, the server encrypts the secret key with customer's public key and sends it to customer. Customer requests video streaming service through wired or wireless communication like Internet, Wi-Fi or cellular channel to the server of video streaming service provider. Then, the server authenticates the customer, and creates session key used in transmitting stego video data. Then, it sends encrypted session key with customer's public key and retrieves appropriate video file from the video file database, and embeds secret messages like copyright or ownership information into cover media, video file, by steganographic manner. After that, it sends the stego video file where secret messages are inserted. While stego video file is received, the customer, if needs, extracts hidden messages from stego video file received and replays transmitted the video file (stego video file). Used LSB inserting method for secure and faster steganographic data embedding and extracting in streaming situation.

In [6] Jenifer K et.al., (2014), used the LSB approach along with the Masking-Filtering and Transformations techniques to hide the secret image or any other file Cover frame is the Frame image that is selected from the carrier video file. It can be any type of video files. The secret image is the selected personal image and it may any other file which can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Stego-key, which ensures that only recipient who knows the corresponding decoding key, will be able to extract the image from a cover-frame of carrier video file. The cover-frame with the secretly

embedded image is then called the Embedded Stegano-Image Recovering image from embedded Stegano-image requires the cover-frame itself and a corresponding decoding key if a stego-key was used during the encoding process.

In [7] Selvigrija P. and Ramya E. (2015), used Dual Steganography (cryptography and steganography) concept has been applied to secure the original videos from unauthorized person by embedding the original video inside another video. Both the videos are converted into frames first. After that, the individual frames of original video are sampled with the frames of another video. After completing the sampling process, the output frames are combined to obtain the encrypted video. Each frame of the secrete video are encrypted using Arnold Transformation Method. The Arnold Transformation, Discrete Wavelet Transform and Alpha Blend method has been introduced in hiding Secrete Video inside Video. The three important algorithms used for secrete video encryption; image decomposition and image embedding are the Arnold Transformation, Discrete Wavelet Transform and an Alpha Blend method respectively. The encryption of the image takes place using the Arnold Transformation. After encryption of image frames, the scrambled frames and cover frames are decomposed using DWT method and embedded using an Alpha Blend method. Finally, Stego frames will be produced. Later, the Stego Frames are combined to obtain a Stego Video.

When in [8] Sangareswari S. and Aruna V. (2015), said each frame consisting of three channel of RGB. After collecting the frame we perform DCT (8x8 block) on any channel (say Rchannel) of the frames and embed the secret information bits in selected higher order coefficients. Each frame is processed by 8x8 Inverse DCT block processing and combined to get mp4 video with hided message. Decoding is done in reverse process of encoding. First each frame is extracted from the created MP4 stego video, then perform 8x8 DCT block processing on the channel where secret information was embedded earlier. Finally the secret bit information's are extracted by subtracting from original DCT block processed values.

3. Video Steganography

Video Steganography is a technique to hide any kind of files into a carrying Video file. The separation of video into audio and images or frames results in the efficient method for data hiding. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques, because of its size and memory requirements [9] [2].

Video is a sequence of still images. Steganographic data embedding in video is very similar to images. However, there are many differences between data hiding in images and video. One of the important differences is the size of the carrier media. Since video contain higher capacity than a still image, more secret messages can be embedded in the video file [5].

4. The New Proposed Algorithm

As we mentioned, we can send a secret message by embedding it in video frames according to number of bits per 24 bit, the new method consist of two levels: embedding and extracting level

Embedding level

The embedding level consists of the following steps:

1-Read the video file any type and isolate audio from video frames, every frame will be three dimensional matrixes. The first is red content, second is the green and third is the blue color content.

2-convert every frame content into two dimensional 24 bit image frame:

Blue content (8 bit)	Green content (8 bit)	Red content (8 bit)

3- Read the text file, converts its content to binary.

4-Embed the length of text file after represented in 16 bit length in secret location (stego_key1) in any frames.

5-Distribute the text bits in all frames according to the length of text.

6- Embed the bit text using stego_key2 (width, height), when height is the first position. . Next values of height will depended on the length of text.

7-Represent the results of 24 bit carrier secret message to three dimensional matrixes red content, green and blue content.

8-Finally, store the video frames and audio to video file and send the video to the receiver. Figure (1) shows the flow chart of the embedding level for the proposed method.

Extracting level

The retrieving level is as follows:

1-Read the video file and isolate audio from video frames.

2- Convert frame contents to 24 representations

3-Retrive the length of text from stego_key1.

4-From stego_key2 you know the width and first height position. Next values of height will depended on the length of text.

5- Finally, convert the bit text to equals in character.

5. Result and Discussion

Steganography scheme is evaluated by imperceptibility and capacity. Imperceptibility is measurement whether the embedded data is imperceptible to the human eye and statistical analysis or not. The performance measures are used to measure the imperceptibility of the proposed method is

Peak Signal to Noise Ratio (PSNR) and Mean Square error (MSE) are calculated by the equations:

$$MSE = \frac{1}{MN}\sum\sum(Output\_frame - input\_frame)^2 \quad .....(1)$$

$$PSNR = 10\log 10\left[\frac{\max value}{\frac{1}{MN}\sum\sum(Output\_frame - input\_frame)^2}\right] \quad .....(2)$$

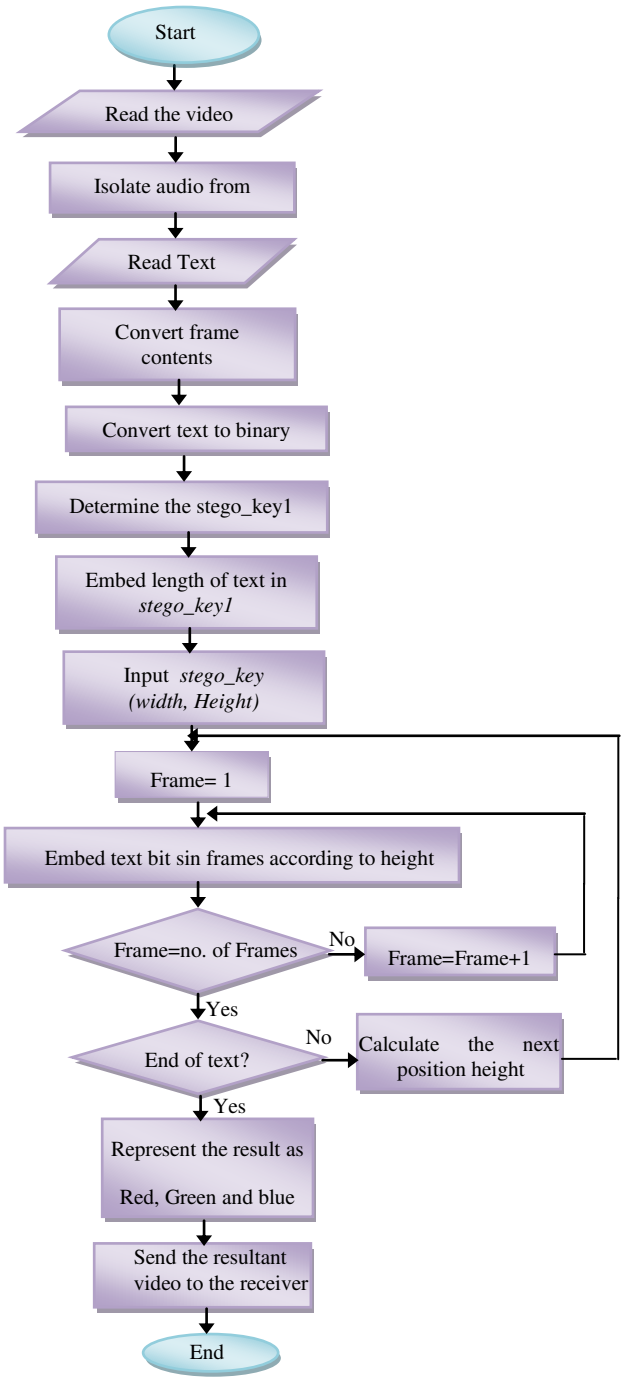

Figure (1) flow chart of the embedding level of the proposed method

Many types of video applied to this method and check the performance measures of frames, the performance measures are calculated according to video file size. We calculate performance measures for every frame then find the average of frames. Table (1) shows the results of the proposed method for text (2590) bytes, Table (2) shows the result of the proposed method for text (5180), and Table (3) shows the results for (10300) bytes. These tables show that the efficient of hiding is increased when increasing the number of frames and the number of bits embedded per 24 bit. The changes of frames are unnoticeable after play the video.

Table (1): THE PERFORMANCE MEASURES OF THE PROPOSED METHODWHEN TEXT LENGTH IS 2590 Byte

File no.	No. of Frames	Size of Frame	10 /24bit		16 /24bit	
			MSE	*PSNR*	*MSE*	*PSNR*
File1	40	240*320	0.0147	67.0132	0.0087	68.8595
File2	44	480*640	0.0078	70.9662	0.0064	72.0266
File3	126	240*320	0.0015	76.6547	0.0011	78.8390
File 4	248	400*400	0.0003	84.0493	0.0001	85.9667

Table (2): THE PERFORMANCE MEASURES OF THE PROPOSED METHODWHEN TEXT LENGTH IS 5180 Byte

File no.	No. of Frames	Size of Frame	10 /24bit		16 /24bit	
			MSE	PSNR	MSE	PSNR
File1	40	240*320	0.0299	63.7679	0.0140	66.7332
File2	44	480*640	0.0090	69.0009	0.0067	70.0944
File3	126	240*320	0.0030	73.5146	0.0024	75.3422
File 4	248	400*400	0.0006	80.7848	0.0003	82.8456

Table (3): THE PERFORMANCE MEASURES OF THE PROPOSED METHODWHEN TEXT LENGTH IS 10300 Byte

File no.	No. of frames	Size of Frame	10 /24bit		16 /24bit	
			MSE	PSNR	MSE	PSNR
File 1	40	240*320	0.0615	60.9643	0.0234	64.4882
File 2	44	480*640	0.0161	66.4471	0.0133	67.3992
File 3	126	240x320	0.0075	69.5269	0.0054	71.2016
File 4	248	400*400	0.0012	78.2099	0.0006	80.0443

6. Conclusions

Through the application of the proposed method we obtain the following:

1. The increase of text length will not affect the original video.
2. The increase the number of bits embedded per 24 bit will enable the user to send large text without noticeable changes in video.
3. The efficiency of proposed method is increased when increase the size video file, because of the text more distributed in video as a result the changes is not focus in one frame.

REFERENCES

[1] Kaushik Koumal , Sangwan Suman, "State of Art Techniques in Video Steganography", Proceedings of National Conference on Innovative Trends in Computer Science Engineering (ITCSE-2015) held at BRCMCET, Bahal on 4th April 2015.

[2] Swathi A. , K Jilani S.A., "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5 September| 2012 .pp:1620-1623.

[3] Jaheel Hamdan Lateef and Beiji Zou, "A Novel Approach of Combing Steganography Algorithms", INTERNATIONAL JOURNAL ON SMART SENSING AND INTELLIGENT SYSTEMS VOL. 8, NO. 1, MARCH 2015.

[4] Cruz Jason Paul, Libatique Nathaniel Joseph and Tangonan Gregory , "Steganography and Data Hiding in Flash Video (FLV)", 2012, TENCON 2012 1569632023.

[5] Lee Yunjung , ",Streaming Video Service Model using Secure Steganographic Method ", International Journal of Security and Its Applications Vol.7, No.6 (2013), pp.79-88 http://dx.doi.org/10.14257/ijsia.2013.7.6.08 ISSN: 1738-9976 IJSIA Copyright ⓒ 2013 SERSC .

[6] Jenifer K. Steffy , Yogaraj G., Rajalakshmi , K., " LSB Approach for Video Steganography to Embed Image", K. Steffy Jenifer et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 319-322.

[7] Selvigrija P. and Ramya E., " Dual Steganography for Hiding Video in Video", INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY VOLUME 3 ISSUE 3 – MARCH 2015 – ISSN: 2349 – 9303.

[8] Sangareswari S. and Aruna V. , " Application of image hiding in mp4-video using steganography technique", International Journal of Electrical, Computing Engineering and Communication (IJECC) Vol. 1, Issue. 2, April – 2015 ISSN (Online): 2394-8310.

[9] Joshi Jayashri , Choudhary Mithilesh, Tiwari Vikash, Bhagasara Suraj, "A Review on Data Security Using Video Steganography", International Journal of Advanced Research in lectrical, Electronics and Instrumentation Engineering Vol. 4, Issue 5, May 2015.

AUTHOR: Mrs. Shahd A. R. Hasso (M Sc.) is currently a lecturer at Mosul University/ College of Computer Science and Mathematics/ Software Engineering Department. She received B.Sc. degree in Computer Science from University of Mosul in 1998 and M.Sc. degree from University of Mosul in 2003. Her research interests and activity are in data security, data strutures, network security, information hiding. Now, she teaches data security undergraduate students.