International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-5 Issue-1, October 2015

Novel Approach to Secure Data Transmission using Video

Nikita Lemos, Kavita Sonawane, Bidisha Roy

Abstract—Internet is being widely used for transmitting sensitive data. The data transferred online is prone to attacks. This paper presents a novel technique where steganography and cryptography are clubbed together to get achieve dual level security. Steganography hides the existence of data and cryptography scrambles the data and makes it difficult to interpret it even if the attacker gets hold of the data. Since videos are used widely today and are a popular on social media we have used video as a cover to the hide the secret data Text data is stored in video frames. The data is subjected to steganography and cryptography which are simple and novel techniques and then stored in the video frames using a random fashion using simple linear probing techniques.

Index Terms—Steganography, cryptography, cover, security threats

I. INTRODUCTION

In todays digitalized world, the Internet serves as an important role for data transmission. There are high chances of confidential data being stolen, modified or destroyed since it's a worlwide and easily available medium [1]. Therefore protecting sensitive data becomes a major issue in order to prevent damage from happening.

In steganography secret message is the data that the sender wishes to remain confidential and can be text, images, audio, video, or any other data that can be represented by a stream of bits. The cover is the medium in which the message is embedded and serves to hide the presence of the message. The message embedding technique is strongly dependent on the structure of the cover. Cryptography deals with scrambling the contents of the secret data but it is known that some kind of data is being transmitted , the existence of data is not hidden [2]. Cryptography and setganography as individual techniques are prone to attacks [3]. Each of them has their own unique advantage so if they are clubbed together advantages of both can be used to secure the secret data being sent using a suitable cover. The proposed technique combines simple and novel cryptography and steganography techniques to hide the data in video frames. The frame selection is done randomly on the basis of a linear probing technique. An overview is presented in section II. The section III describes the proposed methodology.

Manuscript published on 30 October 2015.
***** Correspondence Author (s)
Nikita Lemos, Department of Computer Engineering, Xavier Institute of Engineering, Mumbai (Maharashtra). India.
Kavita Sonawane, Department of Computer Engineering, St. Francis Institute of Technology, Mumbai (Maharashtra). India.
Bidisha Roy, Department of Computer Engineering, St. Francis Institute of Technology, Mumbai (Maharashtra). India.

Section IV bdescribes about the algorithmic view and results. Section V depicts about the performance evaluation and section VI describes the future work.

II. OVERVIEW

The technique proposed in the paper is a novel technique since it combines cryptography and steganography as uses video as a cover medium to transmit the video. The crypto-stego techniques used are simple but the combination is unique hence less prone to attacks. Human perceptibility is an key point for transmission of the video in a secure manner and accurate retrieval of the secret message that is being passed [4].These two goals if satisfied it can be said that the goal to transmit data secretly is achieved.

III. PROPOSED SYSTEM

This section gives a general idea of the proposed work. In the latter half of this section we focus on a simple technique that has been implemented [5].

Step 1- Secret data (i.e. text in our case) is used as an input to the system

Step 2- Cryptography (encryption) technique is applied to the secret data, which results in scrambled data

Step3- The scrambled data is broken into chunks and steganography technique is applied to it in order to hide the data in the video frames

Step4- Linear probing is applied to store the data in a random fashion.

Step5- The cover video which is a stego-crypto video containing the secret message is sent across the communication channel

Step6-Extraction technique is applied to the stego-crypto video on the receiver's end where in the cover video is obtained and the steganography message is extracted using the frame selection logic and integrated

Step7-The message is descrambled and the receiver finally receives the secret message.

A. Senders side

The secret data that has to be hidden in the video is alphanumeric in this case. The data undergoes three phases, cryptography, frame selection and steganography. Cryptography is a means to scramble the data. Symmetric key is also taken as an input along with the secret data. The text data is subjected to hashing first. The data is divided in chunks depending upon the size this is done dynamically. A random key value is generated and the chunks of the data are arranged as per the key value thus disordering it.

After this a simple scrambling technique is used over the disordered data. Where in the data is stored in a matrix fashion Frame selection is done with the help of linear probing. A user defined mod value is obtained and its mod is obtained against the number of frames in the video. The value obtained is the frame in which the data will be stored. Data is stored with the help of lsb technique which is modified as rgb values are considered while storing the data. The frame is subjected to dwt and stego-crypto video is sent across any medium of communication.

B. Receivers side

The receiver receives a crypto-stego video, from which the data has to be extracted. The receiver has to agree upon the same symmetric key and mod value which the sender has decided. At the receivers end the reverse process of inverse transform is applied by locating the frame and the scrambled data is retrieved inverse hashing and scrambling is applied to obtain the text secret message.

IV. ALGORITHMIC VIEW AND RESULTS

The implemented technique is a simple but novel technique on the lines of the proposed system. The software used is Matlab 2013 is and the video format used is avi, the secret message is stored in .txt format. Symmetric key is used as an added level of security on the senders and the receiver's side after the sender selects the text to be embedded as a secret data the sender has to enter a key as well as on the receivers side the the data can be decrypted with the same symmetric key. Fig.1 gives an example of the symmetric key.

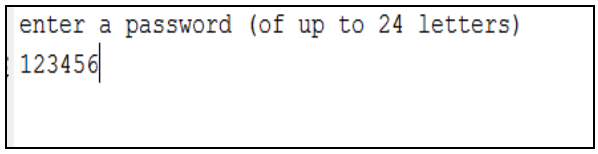

Fig.1 Sender enters the symmetric key

The stego crypto video containing the secret data is transferred over a communication channel,

Fig.1 focuses on the fact that the secret data decrypted at the receivers end after the symmetric key is entered by the receiver.

Fig. 2 shows and extracted and erconsturcted encoded frame.

Fig.2 Reconstructed frame

Visual perceptibility is of highest importance for the success of secure transmission using video. The Fig.3 displays a frame before and after the data has being embedded along with its histograms. The two different histograms of the same frame show evidently that data has been incorporated in the frame. The frame achieves good level of visual perceptibility since to the human eye the visual difference is not noticeable. But the resolution of the frames is not the same. The Signal noise ration ratio is 35.1263 dB and efficiency 0.9999.

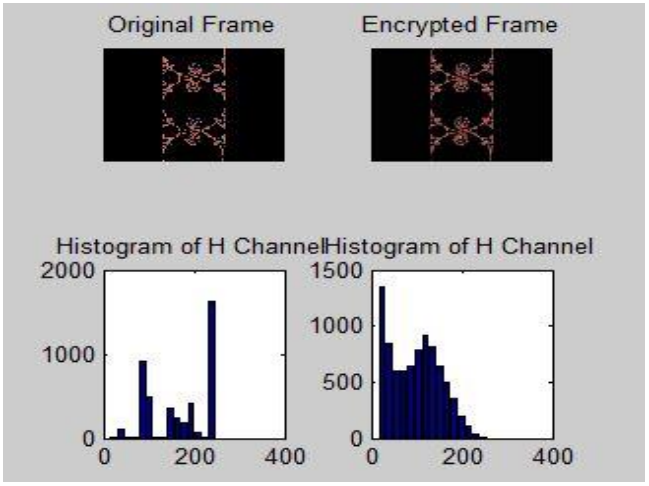

Fig.3 Comparison based on histogram

V. PERFORMANCE EVALUATION

A. Less computational time

The proposed system contains a frame selection logic which uses an index, hence retrieval of the secret data from the stego-crypto video becomes easy and fast.

B. Highly secure

Dual level of security is obtained by the use of steganography as well as cryptography. In addition to it there is a frame selection logic used which embeds the data in random frames, which becomes difficult to gauge.

C. High availability

Videos are used widely across many social networking sites and applications. Thus the usage of video will not arouse any suspicion since they are commonly used these days. Confidential data can such as banking or military information can be transmitted across an unsecure communication channel too, since it won't gross attention.

VI. CONCLUSION AND FUTURE WORK

In this paper a simple and novel technique was used to send data in a secure manner over a video. In future various video formats can be used and multiple simple and novel combination of crypto-stego techniques can be used.

REFERENCES

1. Petitcolas, F.A.P.: "Introduction to Information Hiding". In: Katzenbeisser, S and Petitcolas, F.A.P (ed.) (2000) Information hiding Techniques for Steganography and Digital Watermarking. Norwood: Artech House, INC.
2. Ashish T. Bhole, Rachna Patel, "Design and Implementation of Steganography Over Video File", The Indian Journal of Technical Education, Special Issue for NCEVT' 12, pp. 69-72, April 2012.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

3. Natarajan Meghanathan, Lopamudra Nayak, “Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio And Video Cover Media”, International Journal of Network Security and its Applications (IJNSA),Vol.2, No.1,pp. 43-55, January 2010.
4. R. Balaji and G. Naveen,” Secure Data Transmission Using Video Steganography”, Electro/Information Technology IEEE International Conference , 2011
5. Nikita lemos, Kavita sonawane and Bidisha Roy,”Secure data transmission using video”, Eight International Conference on Contemporary Computing (IC3) IEEE ,2015