Combining Cryptography and Steganography for Data Hiding in Videos

Anju Lukose[1], Akhil K Saji[2], Ansa Alex[3], Remy Raju[4], Rincy Roy Oommen[5]
[1,2,3,4]*B.Tech Student, Mount Zion College of Engineering, Kadammanitta, Kerala, India*
[5]*Assistant Professor, Department of Computer Science and Engineering, Mount Zion College of Engineering, Kadammanitta, Kerala, India*

***Abstract*- Steganography and cryptography is used together to add multiple layers security. Cryptography is a cryptographic technique and which is used to encrypt the visual information. Cryptography is used in data hiding, secure the images, colored image, multimedia and other fields. Steganography is the method of hiding secret data into another data so that it is even more secured. In steganography the secret messages embed in a harmless looking cover such as a digital image file, then the image is transmitted. For encrypt and decrypt the data we can use the cryptography method. The data are converted into some other gibberish form, and then the encrypted data are transmitted. Now a days we have seen a rapid growth of communications security and the antonymous person gain access to secret information for the data communication experts. Cryptography and Steganography are the widely used techniques to overcome this threat. LSB method is used to hide the encrypted message into videos. This project is to improve a new method of hiding secret messages into video, the space of representing the characters.**

Index Terms- Cryptography, Steganography, Cover video, Stego-video, Secret message, Data hiding, LSB method

I. INTRODUCTION

Digital information and data are transferred over the internet and securing sensitive messages need to discover and developed more often than ever before, new technologies for protecting and securing the sensitive messages needs to realize and develop. That is why cryptography and steganography methods is always exposed to attacks by Steganalysis, so we need to develop and look for new modes. Cryptography and Steganography are widely used techniques to handle the information in order to cipher or hide their existence respectively. Steganography is used to hides the existence of communication. In another way, cryptography is the enciphering and deciphering of data and information with a secret code so it didn't understood. The Steganography hides the message so it cannot seen. Although, cryptography systems can be classified into symmetric-key systems and that use a single key, both the sender and the receiver have and public-key systems that use two keys, a public key known to everybody and a private key that only the recipient of messages uses. However, steganography is most useful when the use of cryptography is illegal. Where cryptography and strong encryption are barred, steganography can avoid such policies to pass the message secretly. However, steganography and cryptography is only differ in the way they are judged. In Cryptography it is fails when the "enemy" is able to access the content of the cipher message, while steganography fails when the "enemy" detects that means there is a secret message present in the steganographic medium. The combination of these two methods helps to enhance the security of the data embedded. It will satisfy the requirements such as capacity, security, and robustness for secure data transmission over an open channel.

Data extraction can be done in encrypted domain or decrypted domain for adapting to different application scenarios. Furthermore even after the completion of encryption and data embedding the video file size can be strictly preserved. Thus the objective is to provide security for our data by hiding into encrypted video streams. This project proposes an authentication algorithm which uses cryptography to provide security for data. Cryptography schema is one of the most secure techniques for privacy and security and it allows the encryption of secret video or data by transferring it into the secure share and the decryption method is performed without any

computation devices. Steganography apply in various fields such as military and industrial applications. Lossless steganography techniques are used for secure and successful transmission of information from sender to receiver. Steganography is helps to hiding secret message in digital files.

II. RELATED WORKS

A. Advanced steganography algorithm using encrypted secret message: by Joyshree Nath and Asoke Nath.

In the work the authors have introduced a new method for hiding any encrypted secret message inside a cover file. For encrypting secret message the authors have used new algorithm as well as for hiding secret message we have used a method. These two methods are proposed by Nath and Asoke Nath. In MSA method we have modified the idea of Play fair method into a new platform where we can encrypt or decrypt any file. Here the authors introduced a new randomization method for generating the randomized key matrix to encrypt plain text file and to decrypt cipher text file. They are also introduced a new algorithm for encrypting the plain text multiple times. In this method it totally dependent on the random text key which is to be supplied by the user.

B. *A detailed look of audio steganography techniques using lsb and genetic algorithm approach: by Gunjan Nehru and Puja Dhar*

The various techniques of audio steganography using different algorithm is like genetic algorithm approach and LSB approach. In steganography method, the message used to hide secret message is called host message or cover message. Once the contents of the cover message are modified, then resultant message is known as stego message. On the other hand, stego message is combination of host message and secret message. Audio steganography requires a text or audio secret message and which helps to be embedded within a cover audio message. Due to presence of redundancy, the cover audio message before steganography, stego-message after steganography will contain the same for information hiding.

III. EXISTING SYSTEM

Combining cryptography and steganography for data hiding in images is the existing system. The primary purpose of this paper is to improve a new method of hiding secret messages in the image, possibly by combining steganography and cryptography. A new encoding technique is employed so as to lower the area of representing the characters. LSB methodology is employed to cover the encrypted message into pictures. PSNR and MSE are used for measure the standard of images; the results showed that the projected methodology provides higher results than straightforward LSB with higher PSNR lower MSE. Even though every ways provide security, this study proposes to mix each cryptography and steganography ways into one system so as to supply robust security, by exploitation 2 levels of data encryption .After the data encryption done, the cipher text will hide inside the image using an LSB steganographic technique. The new encryption technique used five spaces to represent each character in the message and five pixels to conceal each character in the image. A new methodology of embedded secret message into image; it's combined between cryptography and steganography so as to produce higher capability, robustness, and security. The algorithm is designed based LSB (Least Significant Bit) method to hide encrypted message into image.

IV. PROPOSED SYSTEM

Here we propose a new method of embedded secret message video; it is combined between cryptography and steganography in order to provide higher capacity, robustness, and security. The proposed algorithm is designed based LSB (Least Significant Bit) method to hide encrypted message into video. A secret data is being embedded inside a digital video to produce the stego video by using data embedding technique. When stego object is produced then, video file is protected by a user defined password which provides an additional security and it will be send via some public communications channel to receiver. The extracting process is simply the reverse of the embedding process. The receiver should be decode the stego object to view the secret message by applying an extracting algorithm or a technique. A digital video contains a set of frames that means digital images which are played back at fixed frame rates that are based on the video standards. An image

is a collection of pixels and each pixel is a mixture of three primary colors RGB (Red, Green and Blue). Pixels in the image are show row by row horizontally.

A pictorial description of the proposed scheme which combined concepts of cryptography and steganography is shown in Figure 1.

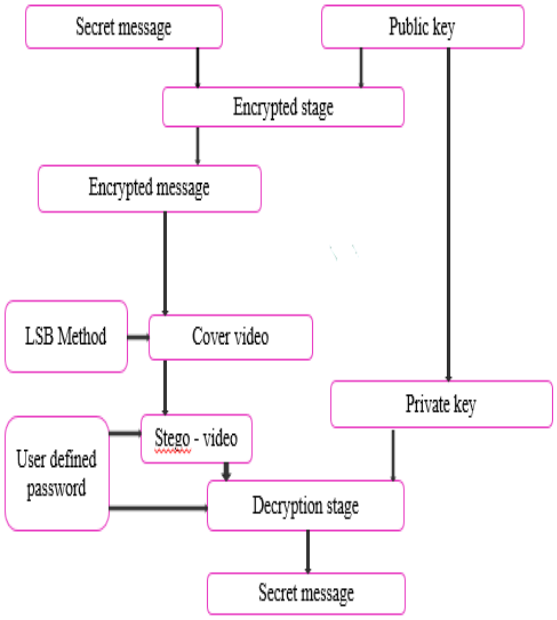

Fig1: The general flowchart of proposed scheme

A. Frame Extraction:

Consider we have 2 or more frames that are extracted from the video

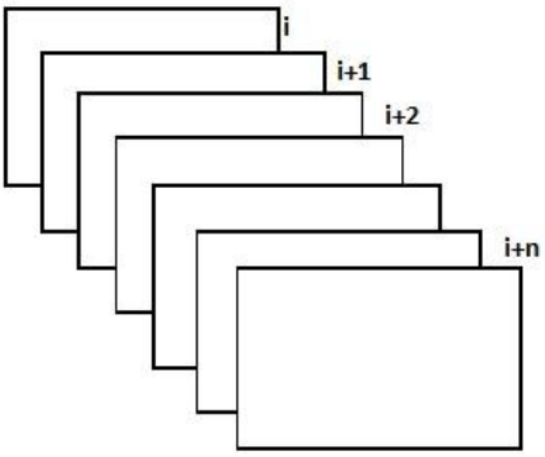

Fig 2: Video frames

Embedding and extracting technique of encrypted message is given below

A. Algorithm of Embedding

Step 1: Input video object file.
Step 2: Read required encrypted message of the video.
Step 3: Split the video into frames.
Step 4: Find LSB bits of pixel in the frame.
Step 5: get the position for embedding encrypted message into frames
Step 6: Regenerate video frames.
Step 7: Give user defined key to the regenerated video

B. Algorithm of Extracting

Step 1: Input stego video file.
Step 2: Apply user defined key.
Step 3: Read required message from the stego-video.
Step 4: Split the video into frames.
Step 5: Find LSB bits of frame.
Step 6: Obtain the position of the encrypted message i.e., embedded bits.
Step 7: Regenerate video frames.

V. Least Significant Bit (LSB) Technique

Data is hided in video file with the assistance of least significant bit (LSB) formula. LSB writing technique has the advantage of low computational quality and extremely high watermark channel bit rate. By this system, least significant bits of the individual pixels of carrier files are changed with the message bits.

The following example illustrates the method.

There are three adjacent pixels (nine bytes) with the following RGB encoding:

Fig 3: LSB method

If the 9 bits of data 100000001 are to hidden, these 9 bit are overlayed over the LSB of the 9 bytes above.

VI. CONCLUSION

There are various kinds of steganography techniques are offered to cover information in video however LSB substitution is a simple technique. The above

mentioned approach relies on the analysis to cover message into video (AVI) which provides a robust and secure way of data transmission. The proposed embedded video steganography has many advantages like user friendliness, simple and successful process of embedding secret message with more security. Successful process of embedding secret message for more security. With the growth in digital media, data security has become a major concern. Mere steganography is not a good solution to secrecy nor is mere encryption but a combination of both provide a powerful tool which enables people to communicate without possible eavesdroppers even knowing there's a kind of communication within the first place.

In this project, we have presented two levels of security for communicating secret information. Firstly, encrypted message is embedded into video and then video file is protected by using a password which provides an additional security. Video steganography proves to be more efficient than other stenographic methods with the amount of data that can be embedded in it. The text is encrypted prior embedding in the video thus increasing the security of information. Since the text is embedded by modifying only the least significant bit, no much change in the intensity of the image is noticeable.

ACKNOWLEDGEMENT

The authors would like to thank everyone for having given us this opportunity to conduct this study. We would also like to thank Mount Zion College of Engineering and APJ Abdul Kalam Technological University for giving us this platform.

REFERENCES

[1] Rajyaguru, M. H., Combination of Cryptography and Steganography With Rapidly Changing Keys, International Journal of Emerging Technology and Advanced Engineering, Vol.2,No.10, 2012, pp. 329-332.

[2] Manoj, I. V. S., Cryptography and Steganography. International Journal of Computer Applications (0975–8887), Vol.1, No.12, 2010, pp. 63-68

[3] Sherekar, S. S., Thakare, V. M., and Jain, S., Critical Review of Perceptual Models for Data Authentication, Emerging Trends in Engineering and Technology (ICETET) 2nd International Conference, 2009, pp. 323-329.IEEE.

[4] Usha, S., Kumar, G. A. S., and Boopathybagan , K., A secure triple level encryption method using cryptography and steganography , Computer Science and Network Technology (ICCSNT), International Conference, Vol.2,No.2.11, 2011pp. 1017-1020.IEEE.

[5] Bharti,P., and Soni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganograph, International Journal of Computer Applications,Vol.58,No.18,2012, pp1

[6] Marwaha.P, Visual cryptographic steganography in images, Computing, Communication and Networking Technologies (ICCCNT), International Conference, 2010, pp1-6. IEEE.

[7] Umamaheswari, M., Sivasubramanian, S. and S. Pandiarajan S., Analysis of Different Steganographic Algorithms for Secured Data Hiding, IJCSNS International Journal of Computer Science and Network Security, Vol.10,No.8, 2010, pp 154-160.

[8] Kandar. S and Maiti. A., Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number, International Journal of Computer Applications (0975 –8887) Vol.19, No.4, 2011, pp 35-40.

[9] Bairai, A. K., ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security,ISSN 2078-5828 (Print), ISSN 2218-5224 (Online), Vol.01,No.2,2011, pp 37-41, Manuscript Code: 110112.