Hiding The Message Using Cryptography In Video Steganography

Reena Bansal , Dr. Neelendra Badal

Abstract : These instructions give you In modern world Internet is an important medium to transfer the information or data (text, image, video, audio) from one place to another place. But sometime hackers on internet can access the important or personal data of anyone; they can modify or can misuse the valuable information. To make the data safe and secure over the internet we have two different techniques Cryptography and Steganography. Cryptography is the process to convert the original information into unreadable form. And Steganography is science of hiding the secret information. This secret information can be hidden in the text, image, video and audio. To save the important information from the hackers on internet we are hiding the encrypted information in video.

Index Terms: Cryptography, Video Steganography, AES, Data Security, Data Integrity. Vedio Secuirity

1. INTRODUCTION

Today communication is like a basic need for all the human being. As we know that internet communication is the fastest way of data transfer . But the security is an important issue for internet data. Data security means protecting the data from the unwanted or unauthorized access of internet users. Now a day's data security has gained more attention due to the massive internet users. In order to provide the security to the data of internet there are many techniques like Cryptography, Steganography and watermarking. Cryptography is the process to convert the original message or data into unreadable form for the unauthorized user. Steganography is the process to hide the important or secret message into another media like text, image, audio and video files, in such a way that a third person cannot sense the presence of secret message. Watermarking. Cryptography is an essential information security tool. It provides Confidentiality, Authentication, Data Integrity and Non-repudiation. In cryptography the existence of the encrypted message or data is see able to the world. To hide the secret data or message in some other media without leaving the evidence of data alteration steganographic techniques can be useful. In steganography, only the sender and the receiver know the existence of the message. In present scenario steganographic technologies are very popular. Characteristics of steganography are Capacity, Robustness, Undetectable, Invisibility and Security. So the only use of Cryptography is not a sufficient solution for data security over the entrusted medium like Internet. The solution is based on the combination of two most popular techniques cryptography and steganography in providing the security to the data or message over the internet. By bringing together steganography and cryptography one can bringing out superior security to the data.[1],[2], [3]

- *Hindustan Aeronautics Limited School, Korwa, Amethi, UP India*
- *[e-mail:1bansalrina@yahoo.co.in]*
- *Kamla Nehru Institute of Technology, Sultanpur, UP, India*
- *[e-mail:2 n_badal@knit.ac.in]*

2 LITERATURE SURVEY

For studying the concept of video steganography, we have surveyed the various papers of different authors. In this section we are going to describe the relevant research papers of different authors. In [1] author is describing the characteristics of Steganography, to make the system more secure these characteristics plays a very important role. In this paper author is hiding the text using the S-Tool. S-Tools are a steganography application which can hide Word files, Text files, PDF Documents and Excel Sheets. In [2] author provide the review of different papers in a table form, this paper is very helpful to understand the different algorithms with their advantages and disadvantages. In [3] this paper, two stage processes is used to embed secret text data into the videoclip. First stage is image steganography by using LSB method. Second stage is video steganography using DCT algorithm. Lossless compression technique is also used. Enhanced security and fast transmission are the main advantages of this work. In[4] paper , modified 4LSB algorithm is used for the secret data embedding in video file and parity bit encoding algorithm is used to embed secret information in audio file. This combination makes the system more secure. In [5] paper author combines the idea of video steganography, cryptography and compressed technique which provide the enhanced security. The RC4 is used for encryption of compressed message and 4LSB method is used to conceal the processed text inside the cover media. With compression security is enhanced. In [6] author proposed the method for replacing one or two or three LSB of each pixel in video frame and apply the Advanced Encryption Standard (AES). It becomes very difficult for intruder to guess that an image is hidden in the video as individual frames are very difficult to analyze in a video. In [7] author dealt with three main seganography challenges: capacity, imperceptibility and secuirity. This achieved by hybrid data hiding scheme in corporate LSB technique with a key permutation method. In [8] author developed the modified AES algorithm to provide the enhanced security to the data. Experimental results and Theoretical analysis proved that this AES technique provide high speed as well as less transfer of data over the unsecured channels. The through study has been implemented in the research work itself. In [9] author gave a different concept by using a new approach of hiding image in video. The algorithm replace 1 LSB of each pixel in video frame. It becomes very difficult for a intruder to guess that an image is hidden in the

video as individual frame are difficult to analyze in a video running at 30 frame per second.

3 PROBLEM IDENTIFICATION

In present scenario hackers are more active and smart to hack the secret message or data. Because of the advancement of technology and easily availability of information hackers are becoming more intelligent to retrieve the secret data, to change the data or to damage the data. We have many ways to protect the secret data from the hackers but the problem is complexity and cost of the different solutions. Hence we need a solution which should provide the good security with minimum implementation cost to design and reduced complexity to implement easily.

4 PORPOSED SYSTEM

In the proposed system we are combining video steganography and encryption technique to make a highly secure system for the confidential data. This highly secure system is very difficult to break for the hacker to get the secret data. Significant growth of video over internet had made it a popular choice for Steganography. Video Steganography is famous due to high spatial and redundancy. Due to availability of large number of frames secret data can be easily hide inside the video. Digital video contains a set of frames (images) which are played back at fixed frame rates based on the video standard. Digital video quality depends on frames per second(fps), number of pixels in frame and frame size. Every image in a video called a frame which contains number of pixels having three or four colour combinations like RGB or CMYK. [4]

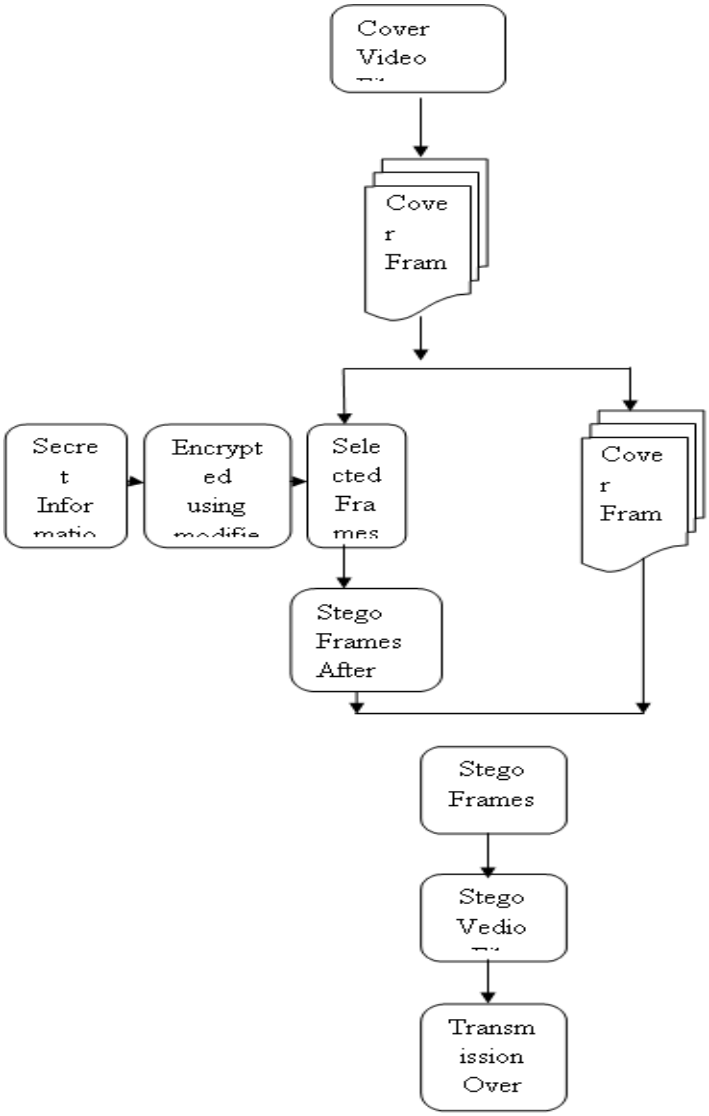

Figure1:-*At Sender Side*

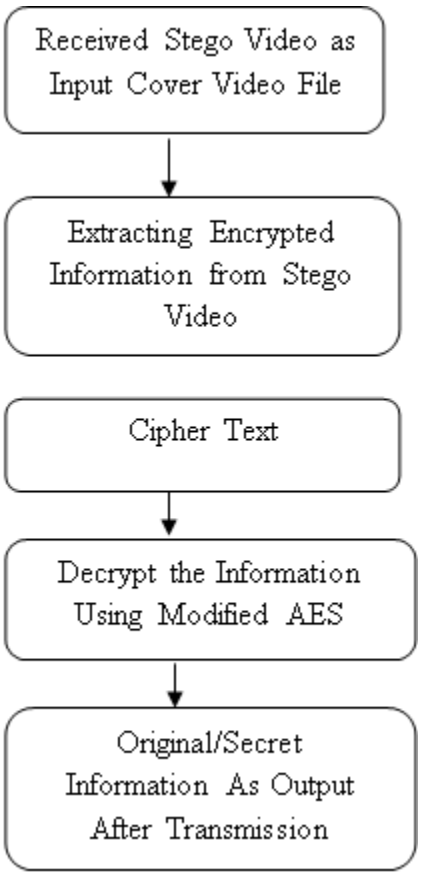

Figure2:-*At Receiver Side*

We use digital video for Steganography because of the weakness in the Human Visual System (HVS) which has a low sensitivity in random pattern changes. Because of this the secret messages can be hiding into the cover video. In this proposed system first stage will execute at the sender side where the secret data or message has encrypted by using the modified AES encryption algorithm. Now the encrypted message or data will be embedded into the video frames. Now at this time we have the stego video to send over the any communication system. At the receiver side the stego video will be converted to the frames, after extracting encrypted data or message decryption will be applied to get the original data or message. [5] Before embedding the text into video, text must be converted into the binary pattern first. The conversion of text into binary form can be done with the help of ASCII code. In ASCII code every letter, digit, and miscellaneous symbols are represented in unique seven bit binary codes. After converting the text or image into the binary form the steganography algorithm can be implemented to embed the data into video frame. [6]

5 METHODOLOGY IMPLEMENTED:

The main objective of the proposed system is to provide the double layer of security to the secret data. First layer is made of cryptography which makes the secret data unreadable to the third party. And second layer is made of steganography which hides the data from third party during the transmission of the data over the internet.

6 MODIFIED AES:

AES means Advanced Encryption Standard, the more popular and widely adopted symmetric encryption algorithm. AES is publicly accessible and also open cipher approved by the National Security Agency for the purpose of top secret information. The features of AES are as follows:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. Each step in key size requires only two additional rounds. In present day cryptography, AES is widely adopted and supported in both hardware and software. [7] In our proposed system we are using modified AES algorithm with the increase number of rounds (Nr) to 16 for the encryption and decryption process, which results in more security to the system.

7 LSB EMBEDDING METHOD:

Spatial Domain Method basically deals with hiding information in pixels of video frames. The most popular method of steganography is Least Significant Bit Method (LSB) due to its high embedding capacity, less embedding complexity and ease in implementationLeast Significant Bit is the best method for data hiding. Because of its simplicity in implementation LSB is commonly used approach to develop the steganography system. Like all other steganographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colours that the embedding creates. The proposed system is written in Java, compatibility over multiple operating systems and over different hardware not an issue. The idea behind the proposed design is to design a good, efficient, simple and low cost system for secret data transmission over the internet. [8]

SENDER SIDE ALGORITHM:
STEP1: INPUT THE SECRET MESSAGE
STEP2: ENCRYPTION WITH MODIFIED AES
STEP3: SPLIT THE VIDEO INTO THE FRAMES
STEP4: EMBEDDING WITH LSB METHOD
STEP5: STEGO VIDEO
STEP6: TRANSMISSION OVER THE INTERNET

RECEIVER SIDE ALGORITHM:
STEP1: INPUT STEGO VIDEO
STEP2: SPLIT THE VIDEO INTO THE FRAMES
STEP3: EXTRACTION OF ENCRYPTED MESSAGE
STEP4: DECRYPT THE MESSAGE
STEP5: ORIGINAL MESSAGE

8 RESULT ANALYSIS:

The performance of steganography system depends on two factors:- Embedding Efficiency and Embedding Payload. Embedding efficiency means amount of data that can be hidden in the cover file. And embedding payload means capacity of steganography system to hide data with less distortion. In our proposed system we worked on to maintain the quality of video with minimum distortion after embedding the secret data. We combined the two powerful techniques to provide the more secure way of data transmission. The proposed system has many advantages like simple without any complexity, more secure because of modified AES, and quality of video is also good. [9], [10-16]

9 FUTURE WORK:

In our proposed system we are hiding the data without any compression technique. We avoid the compression technique to make the system simple means a system without any complexity because there are some issues with compression techniques like speed and file size. Speed : The uncompressing process not only uses memory but also use processor time. The process is slow and is a disadvantage when we are trying to access a file quickly. Size: In some situations compression cannot make file smaller. Resulting file can be a larger in size than original file. So in the future we have to work on limitations of compression technique to make the system more simple and safe. [10-16] in part by a grant from XYZ.

REFERENCES

[1] Gursukhmani and Sugandha, “Case Study of Hiding a Text using Video Steganography”, International Journal of Science and Engineering Research, 2017.

[2] Pratidnya, Varsha, and Mayuri,”A Review Paper on Video Steganography”, International Advanced Research Journal in Science, Engineering and Technology, 2016.

[3] Anmol D Kulkarni, Esti Bansal, Hole Rajashree B, Jdhav Rasika R, Lakshmi Madhuri, “ Improved Data Security Using Video Steganography”.

[4] Vaishali B Bhagat and Prof. Pravin Kulurkar, “ A Robust Audio and Video Steganographic Scheme”.

[5] Swetha V, Liji L Dominic and Ambikadevi Amma T, ” Compress-Encrypt Video Steganography”, International Journal for Innovative Research in Science and Technology, 2015.

[6] Hemant Gupta, Setu Chaturvedi, “Video Steganography through LSB Based Hybrid Approach”, International Journal of Computer Science and Network Security 2014.

[7] Marghny Mohamed, “Data Hiding by LSB Substitution using Genetic Optimal Key Permutation “, International Arab Journal of E- Technology”, 2011.

[8] Puneet Kumar, Shashi B. Rana, “ Development of Modified AES Algorithm for Data Security”, Optik, Volume 127, Issue 4, February 2016.

[9] Saurabh Singh, “Hiding Images to Video”, International Journal of Engineering Science and Technology, 2010.

[10] Punita Meelu, “AES Asymmetric Key Cryptographic System”, International Journal of Information Technology and Knowledge Management, 2011.

[11] Pritish Bhautmage, Amutha, Ashish, ”Advanced Video Steganography Algorithm”, international Journal of Engineering Research and Applications, 2013.

[12] Niels Provos and Peter Honeyman, “Hide and Seek: An Introduction to Steganography”, University of Michigan, IEEE 2003.

[13] Daniela Stanescu, Mircea Stratulat, Voicu Groza, Joana Ghergulescu and Daniel Borca, "Steganography in YUVcolor space", IEEE International Workshop on Robotic and Sensors Environments (ROSE 2007), Ottawa-Canada, pp.1-4, October 2007.

[14] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al - Qershi, "Image Steganography Techniques: an Overview", International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (3): 2012.

[15] Saurabh Singh, Anurag Jain, “An enhanced text to image encryption using RGB Substitution and AES”, IEEE, 2013.

[16] Metaliya Viral. G, Deepak Kumar Jain, “A Real Time Approach for Secure Transmission of Text using Video Cryptography”, IEEE ,2014,Central Electronics Engineering Research Institute, Pilani, Rajasthan.

[17] Ashish T. Bhole and Rachna Patel, —Steganography over Video File using Random Byte Hiding and LSB Technique, International Conference on Computational Intelligence and Computing Research, pp. 189-194, 2012 IEEE.

[18] Sutaone, M.S.; Khandare, Image based Steganography using LSB insertion techniquell, IET, 2008.