Digital Video Steganography Using LSB Technique

M. VENKATA SAI TARUN[1], K. VENKATESHWARA RAO[2], M. NAGA MAHESH[3], N. SRIKANTH REDDY[4], M. VENKATESH[5]

[1, 2, 3, 4, 5] *Department of Electronics and Communication Engineering, Vasireddy Venkatadri Institute of Technology, Nambur, Guntur, Andhra Pradesh, India*

Abstract- ***The use of digital media such as Text, Image and Video is increasing day by day. This leads to need for security of digital media to prevent unauthorized access. One of the security technique we can use is Steganography. The process of hiding required data in any type of digital content is known as Steganography. Steganography is derived from a word Steganos , means hidden or covered and root graph indicates to write. In case of Cryptography the data can be hidden is encrypted and was transmitted. In this type of cases the risk of third party access is high. While in the steganography the encrypted content was hidden in cover source which makes it difficult for third party access.***

Indexed Terms- ***Cryptography, Encrypted content, Third party access, steganography***

I. INTRODUCTION

Steganography is one of the art of secret communication. Its function is to hide the very presence of communication as opposed to cryptography its goal is to make communication unintelligible to those who do not possess the right keys. Digital photos, audio files, videos, and other important computer files which contain perceptually irrelevant or redundant data was used as covers or carriers which was used to hide the secret messages.

II. BASIC MODEL

The below figure illustrates simple representation of the embedding and extracting process in the steganography. In figure shown below, secret message that we want to send is embedded inside a digital video to produces stego video with the help of data embedding algorithm. When the stego object was produced then, it will sent a data via some public communications channel to the receiver. The extracting process that was been takes place here is simply the reverse operation of the embedding process. The receiver must decode the stego object to view that secret message by applying an extracting algorithm.

Figure a: Structure of Steganography System

III. LSB SUBSTITUTION TECHNIQUE

A. Introduction to LSB

Maintenance of secrecy for digital information when it was being communicated from one place to another place over the Internet is a heavy task in present days. Given the knowing amount of minute computation power available and certain known limitations of the encryption techniques it is not more difficult to start attacks on those cipher-text. An ideal steganography method embeds the message containing confidential formation into a carrier image with virtually imperceptible modification of the image. Adaptive steganography comes closer to this ideal since it exploits the natural variations in the different pixel intensities of a cover image to hidden the confidential information.

The one of the main objective of steganography is a technique of embedding an additional data into form of the digital contents, which can be undetectable to the users. Here we are investigating various coding, detecting, and embedding techniques. The thought

behind the LSB algorithm is to insert the bits of the hidden information into the least significant bits to the pixels. As one of the application field of embedding data in to a digital multi-media source become broaden, various terms can used by different teams of researchers, which includes steganography, digital watermarking, and other data hiding techniques. This paper introduces a innovative, principle approaches to detect least significant bit (LSB). Steganography which was used in digital signals such as picture and sound. It is clearly shown that the total length of hidden data embedded in the bits (LSB) of a signal samples is can be estimated by taking relatively high precision. The recent steganalytic approach is interesting and works based on some statistics that are obtained from various measures of that particular sample pairs which are more sensitive to Least Significant Bit embed operation. On coming to resulting detection algorithm, it is fast and simple. To estimate the robustness of the proposed steganalytic design flow, bounds on those estimation errors were developed. Further, the vulnerability of this latest approach to possible attacks can be assessed, and here to counter measures also we suggested a detailed method that is presented along with results of project and its application on sample images.

B. Bits Replacement

The idea behind the Bits replacement algorithm is that to insert a bits of the hidden information into the bits (LSB) of the pixels.

Simplified Example with usage of 24-bit pixels:
1 pixel:
Insert 101:
(00100111 11101001 11001000)
(00100111 11101000 11001001)
Red green blue

Simplified Example with an 8-bit pixel:
1 pixel:
(00 01 10 11)
White red green blue
Insert 0011:
(00 00 11 11)
White white blue blue

C. Advantage

The major advantage of the Least Significant Bits algorithm is it is easy and quick. There has also been steganography software development which works around Least Significant Bit these color alterations occurs via palette manipulation. Least Significant Bits insertion is a method that also works efficient with gray scale pictures.

IV. BITS SUBSTITUTION

The most frequently used steganography method is the technique of Least Significant Bits substitution. In gray level images, each and every pixel consists of 8 bits of data. One pixel can has capacity to display 28=256 variations. The weighting configuration of an 8-bit number is shown in below figure.

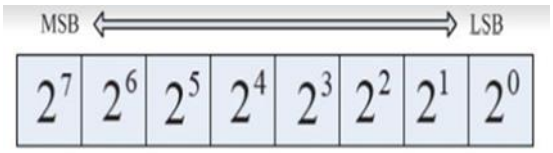

Figure b: Weighting of an 8- Bit Pixel

The basic concept of Least Significant Bit substitution can be embed the confidential information at the right most bits which means bits with the smallest weighting so that the embedding procedure does not completely affect the original pixel values greatly. The mathematical representation for Least Significant Bit method is: x represents the i the pixel value of the stego image, i x represents those values of the original cover image, and i m represents the decimal value of the i th block in confidential data. The number of Least Significant Bits can be substituted and it can be denoted with a letter k. Extraction process is to copy the k-rightmost bits directly without use of external bits

Therefore, a simple permutation of the extracted i m gives us the original secured data. This method is easy and straightforward. However, when the capacity is greatly increased, the image quality decreases a lot and hence a suspected stego-image results.

Furthermore, the confidential data might be easily stolen by simply extracting the k-rightmost bits directly

V. RESULTS

Step 1: input video and required Text file to hide in the video are given as shown in below figure

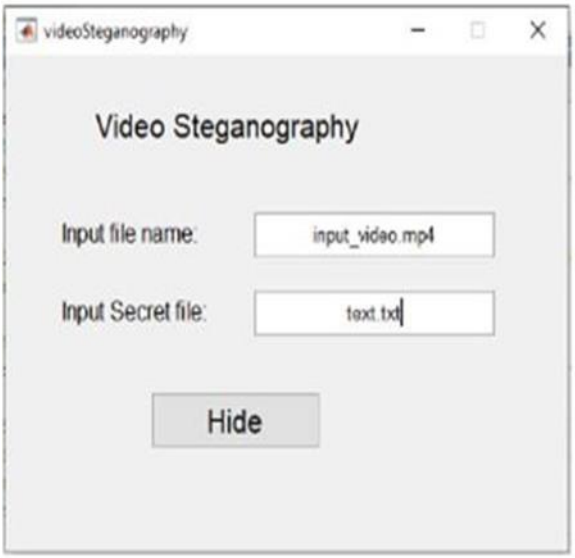

Figure c: Giving Input

Step 2: Press hide to create an output video in which the required text is hidden and a key file is generated .A message of Data Hided Successfully appears in the pop up window as shown below

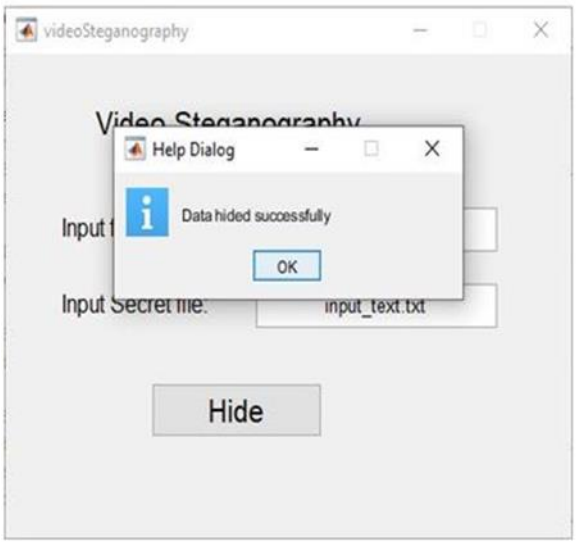

Figure d: Message Hidden Successfully

Step 3: Enter key.txt file generated in provided field and click on Retrieve to extract hidden text from the output.avi videos then a message of Data Retrieved Successfully appears as shown in below figure

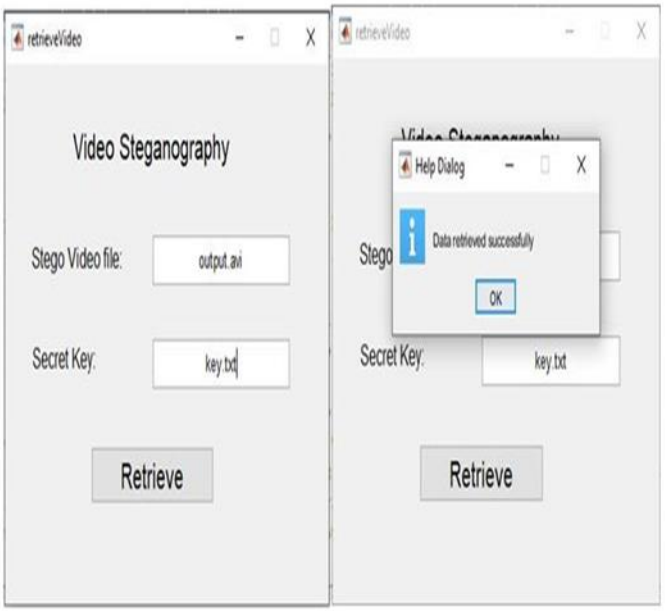

Figure e : Message Retrivel

Step 4: As shown below the data retrieved from video appears at separate file 'x.txt. As shown below. The data in 'input.txt' file represents given input and data in 'x.txt. File represents output

Figure f: Comparing Input and Output

VI. FUTURE WORK

We can increase security by using cryptographic algorithms for secret data used in video steganography

using LSB technique.

CONCLUSION

The project presented that encryption of compressed video bit streams and hiding privacy information to protect videos during transmission or cloud storage. Bits replacement method was used to embed secret message bits with compressed bit streams to prevent the video from tampering. In order to adapt to different application scenarios, data extraction was done either in the encrypted domain or in the decrypted domain to recover original data without any loss.

ACKNOWLEDGMENT

We whole-heartedly thank our project guide Prof. M. Venkatesh, assistant proffessor, department of Electronics and Communication Engineering for the precious guidance and invaluable suggestions which helped us a lot in making our project successful.

REFERENCES

[1] W. J. Lu, A. Varna, and M. Wu, “Secure video processing: Problems and challenges,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[2] B. Zhao, W. D. Kou, and H. Li, “Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol,” Inf. Sci., vol. 180, no. 23, pp. 4672–4684, 2010.

[3] W. Puech, M. Chaumont, and O. Strauss, “A reversible data hiding method for encrypted images,” Proc. SPIE, vol. 6819, pp. 68191E-1–68191E-9, Jan2008.

[4] W. Hong, T. S. Chen, and H. Y. Wu, “An improved reversible data hiding in encrypted images using side match,” IEEE Signal Process. Lett., vol. 19, no.

[5] Kamred Udham Singh Int. Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 5(Version 1), May 2014, pp.105-108

[6] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, “Reversible data hiding in encrypted images by reserving room before encryption,” IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.