Scientific Journal of Impact Factor(SJIF): 3.134

e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 5, May -2015

Video Steganography : An Approach To Hide Text And Image Data using sequential coding.

Khushbu Sahu[1] and Utkarsh Sharma[2]

[1]*ME (communication), Shri Shankaracharya Technical Campus, khushbusahu.20@gmail.com*
[2]*Department of Electronics & Telecommunication, Shri Shankaracharya Technical Campus, utkarsh.sharma004@gmail.com*

Abstract — *Steganography refers to data or a file that has been hide within a digital image, video or audio file. If someone views the article during which the data is hidden within, he or she is going to haven't any indication that there's any hidden data that the person won't try and decode the data. Steganography is employed to cover the messages within alternative harmless messages during a means that doesn't permit any enemy to even sense that there's a second secret message present whereas the aim of computer forensics is that it provides security from covert communication handling digital information and covert communication channel. In this paper we tend to used video as cover media for concealment(hide) the secret message or images. Steganography are often divided into Text Steganography, Image Steganography, Audio/Video Steganography. Need of concealing info from intruders has been around since ancient times. Today Digital media is obtaining advanced like text, image, audio, video etc. In this paper, we propose a secure video steganography algorithm using sequential encoding/decoding process. To keep up the secrecy of data, totally different ways of concealing are evolved. One amongst them is Steganography, which suggests concealing data underneath another data while not noticeable modification in cover data. The experimental result shows the cover video and steganography video having no perceptual difference. In this paper, PSNR and MSE of the cover video frame and stego video frame is compared and histogram is almost identical.*

Keywords- *Steganography; Video Steganography; Covert Communication; Concealment; Secret Message.*

I. INTRODUCTION

The Steganography, Cryptography and Digital Watermarking techniques may be used to get security and privacy of information. The steganography is that the art of concealment information within another information like cover medium by applying totally different steganographic techniques. Recently Video Steganography has become a boon for providing large amount of information to be transferred secretly. Video is just a sequence of images; therefore a lot of area is on the market in between for concealing data. In proposed scheme video steganography is used to hide a secret video stream in cover video stream. every frame of secret video are broken into individual parts then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames are hidden within the least important little bit of every frames using ordered encoding of cover video.

Steganography may be a methodology of concealment secret messages in a cover object whereas communication takes place between sender and receiver. Security of confidential information has perpetually been a significant issue from the past times to the present time. With the development of pc and expanding its use in several areas of life and work, the problem of information security has become more and more necessary. One in all the grounds mentioned in information security is the exchange of data through the cover media. Today, totally different ways like cryptography, steganography, coding, etc are used. The strategy of steganography is among the ways that have received attention in recent years. The goal of steganography is to hide data within the different cover media so different person won't notice the presence of the data.

II. CLASSIFICATION OF STEGANOGRAPHY

A. Text steganography:

Text steganography will involve something from ever-changing the format of an existing text, to ever-changing words within a text, to generating random character sequences or using context-free grammars to generate readable texts [1]. Text steganography is believed to be the trickiest as a result of deficiency of redundant data that is present in image, audio or a video file. The structure of text documents is identical with what we have a tendency to observe, whereas in different varieties of documents like in image, the structure of document is completely different from what we have a tendency to observe. Therefore, in such documents, we will hide data by introducing modifications within the structure of the document without creating a notable change within the concerned output [2]. Imperceptible changes are often created to a picture or an audio file, but, in text files, even an extra letter or punctuation are often marked by a casual reader [3]. Storing text file need less memory and it's quicker moreover as easier communication makes it preferred to different varieties of steganographic strategies. Text steganography are often loosely classified into 3 types: Format based, Random and statistical generation, Linguistic methods.

B. Audio steganography:

Watermarking of audio signals is more difficult compared to the watermarking of pictures or video sequences, because of wider dynamic range of the HAS compared with human visual system (HVS) [5]. The HAS perceives sounds over a variety of power bigger than 109:1 and a variety of frequencies bigger than 103:1. The sensitivity of the has to the additive white gaussian noise (AWGN) is high as well; this noise in a sound file is detected as low as seventy decibel below close level [4]. When taking audio as a carrier for info concealing it's referred to as audio steganography. it's become terribly important medium because of voice over ip (VOIP) popularity. Audio steganography uses digital audio formats like WAVE, MIDI, AVI MPEG or etc for steganography [5].

C. Image steganography:

Taking the cover object as image in steganography is called as image steganography. Generally, during this method pixel intensities used to conceal the data. Image steganography is technique of data concealing into cover-image and generates a stego-image [6]. This stego-image then sent to the other party by known medium, wherever the third party doesn't apprehend that this stego-image has hidden message. After receiving stego-image hidden message will merely be extracted with or without stego-key (depending on embedding algorithm) by the receiving end [7]. Output of embedding algorithm may be a stego-image that merely sent to extracting algorithm, wherever extracted algorithm unhides the message from stego-image.

D. Video steganography:

Video Steganography is a technique to hide any kind of files into a carrying Video file [8]. the use of the video based Steganography will be more eligible than other multimedia files, due to its size and memory needs. the least significant bit (LSB) insertion is a crucial approach for embedding info in a carrier file; Least significant bit (LSB) insertion technique operates on LSB bit of the media file to cover the data bit [9]. During this project, an information concealment theme is developed to cover the data in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. Video (combination of pictures) is used as carrier for hidden info. Usually discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) that is employed to cover the data in every of the images within the video, that isn't noticeable by the human eye [10]. Video steganography uses like H.264, Mp4, MPEG, AVI or alternative video formats.

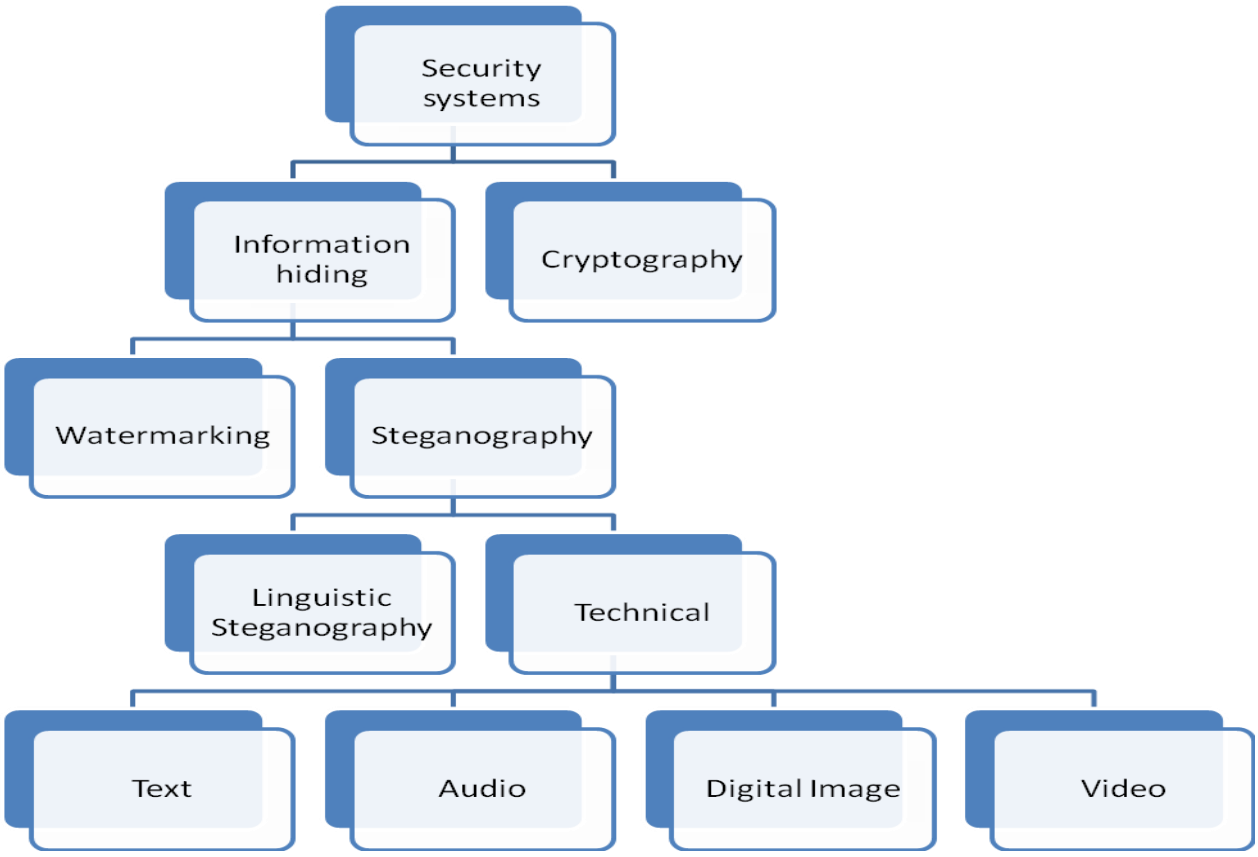


Figure 1. Steganography in Security Domain

III. SEQUENTIAL ENCODING/DECODING

Sequential encoding/decoding:

Message data is Encoded/Decoded from some starting point, typically usually upper left pixel and therefore the data is Encoded/Decoded in a set identical pattern or outline, unremarkably to adjacent pixels. And it's easy to implement. It may also observe Message Size Directly and simply Detected using histogram Analysis. Usually enforced using counters; slows recovery process. Repeatable encoding methodology decreases effectiveness of any encoding Techniques.

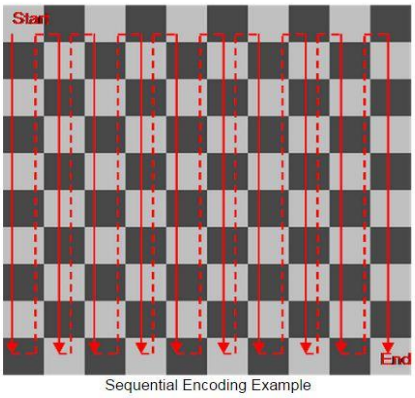
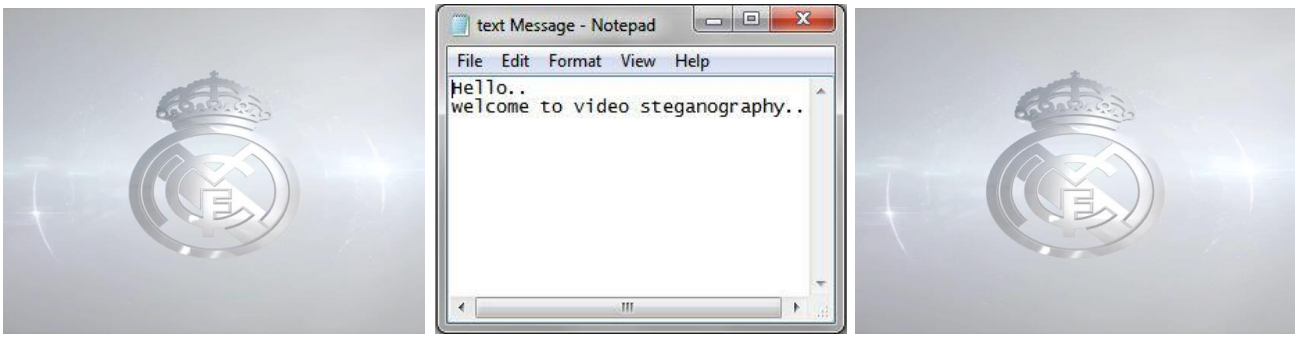


Figure 2. Example Of Sequential Encoding

IV. Result

In this project, a message i.e. an image/text is hidden in a frame of the video. The proposed algorithm is tested against ''1.mp4'',''2.mp4'' and ''3.mp4'' as cover video. The output video ''myfile1.avi'', ''myfile2.avi'' and ''myfile3.avi'' are the stego video of their respective cover videos. The figures below show the frames of the cover video and the frames of the stego video in which the message has been embedded. The output shows absolutely no perceptual differences between the cover video and the stego video.

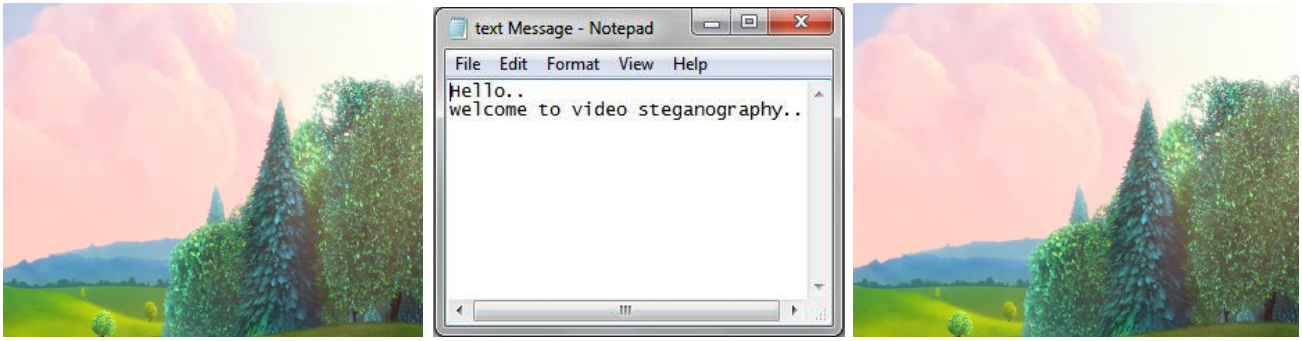


(a) 50th frame of cover video *(b) embedded text message* *(c) 50th frame of stego video*

Figure 3. Frame number 50 of the cover video '1.mp4', embedded text message and stego video 'Myfile1.avi'.

(a) 100th frame of cover video *(b) embedded image message* *(c) 100th frame of stego video*

Figure 4. Frame number 100 of the cover video '1.mp4', embedded image message and stego video 'Myfile1.avi'.

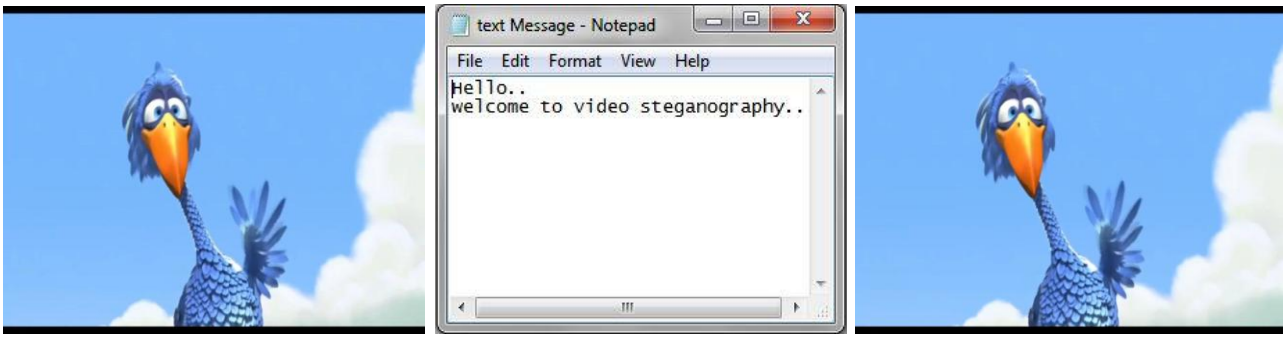


(a) 150th frame of cover video *(b) embedded text message* *(c) 150th frame of stego video*

Figure 5. Frame number 150 of the cover video '2.mp4', embedded text message and stego video 'Myfile2.avi'.

(a) 300th frame of cover video *(b) embedded image message* *(c) 300th frame of stego video*

Figure 6. Frame number 300 of the cover video '2.mp4', embedded image message and stego video 'Myfile2.avi'.



(a) 400th frame of cover video *(b) embedded text message* *(c) 400th frame of stego video*

Figure 7. Frame number 400 of the cover video '3.mp4', embedded text message and stego video 'Myfile3.avi'.

(a) 600th frame of cover video *(b) embedded image message* *(c) 600th frame of stego video*

Figure 8. Frame number 600 of the cover video '3.mp4', embedded image message and stego video 'Myfile3.avi'.

4.1 Peak Signal to Noise ratio (PSNR)

Peak Signal to Noise ratio (PSNR) is employed to work out what proportion similar the cover video frame and therefore the corresponding stego video frame are. Since PSNR determines the degree of similarity between the cover frame so the stego frame therefore higher the value of PSNR higher is that the result.

$$PSNR = 10. Log10 (R2 / MSE)$$

Where R is the maximum possible value of luminance. For an 8 – bit image value of R will be 255. PSNR is measured in decibels (dB).

4.2 Mean squared Error (MSE)

Mean squared Error (MSE) is employed to determine how much completely different the cover video frame and therefore the stego video frame are. This is often done by taking sum of difference between the corresponding pixel values of each the frames so dividing the sum by the size of the frame. Since MSE determines the degree of dissimilarities between cover frame and stego frame thus lower the value of MSE higher is that the result.

$$MSE = (\sum M, N [f(m,n) – F(m,n)]2) /M * N$$

Where R is the maximum possible value of luminance. For an 8 – bit image value of R will be 255. PSNR is measured in decibels (dB).

The MSE and PSNR values for the cover video frame and the stego video frame are shown in the following table:

Table 1. Result of quality evaluation of cover video frames and stego video frames.

Cover Video	Stego Video	Frame Number	MSE	PSNR (in dB)
1.mp4	Myfile1.avi	50	0.0154	66.2838
		100	0.0042	71.9255
2.mp4	Myfile2.avi	150	0.0068	69.8554
		300	0.0097	68.2752
3.mp4	Myfile3.avi	400	0.0036	72.6578
		600	0.0043	71.8062

4.3 Histogram difference

The following figure shows the comparison between the histograms of the frames of the cover video and stego video:

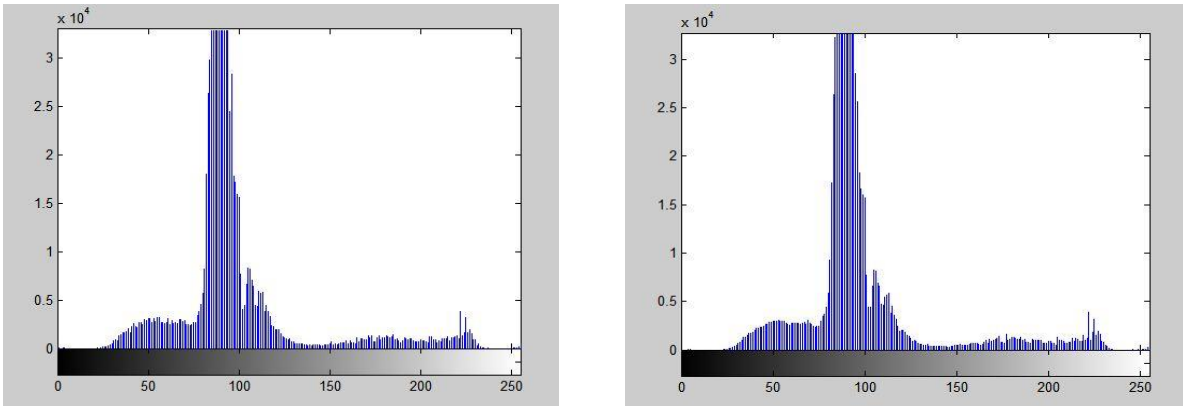


Figure 9. Histogram comparison of frame number 50 of cover file 1.mp4 and stego file Myfile1.avi

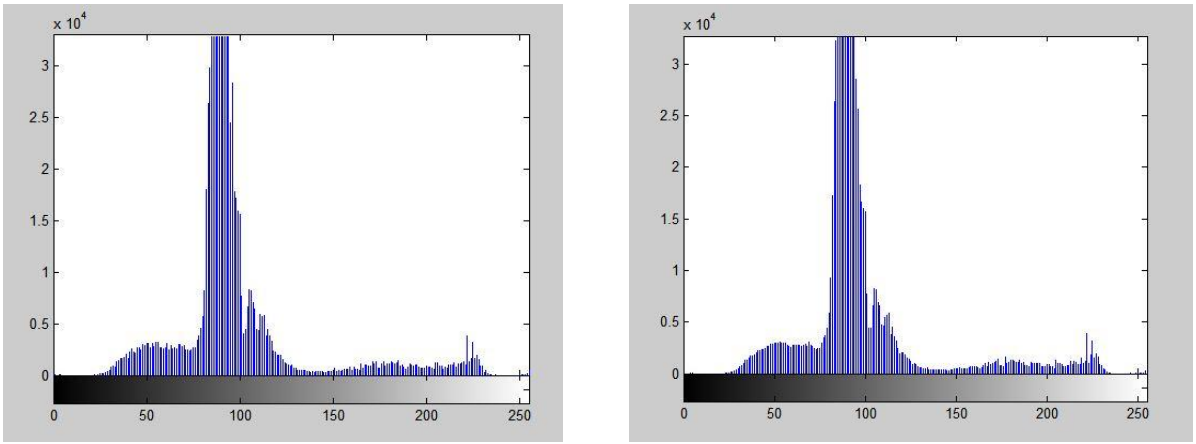


Figure 10. Histogram comparison of frame number 100 of cover file 1.mp4 and stego file Myfile1.avi

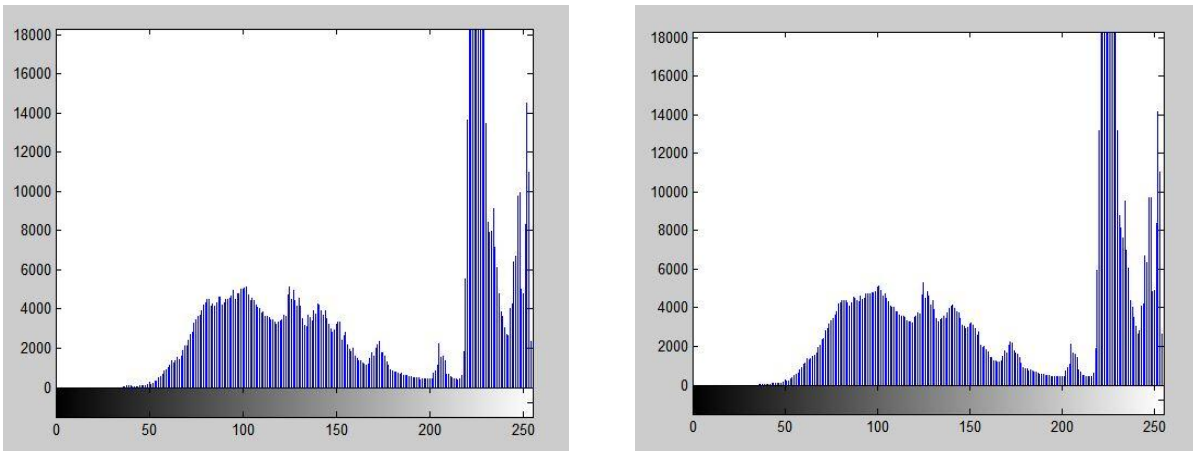


Figure 11. Histogram comparison of frame number 150 of cover file 2.mp4 and stego file Myfile2.avi

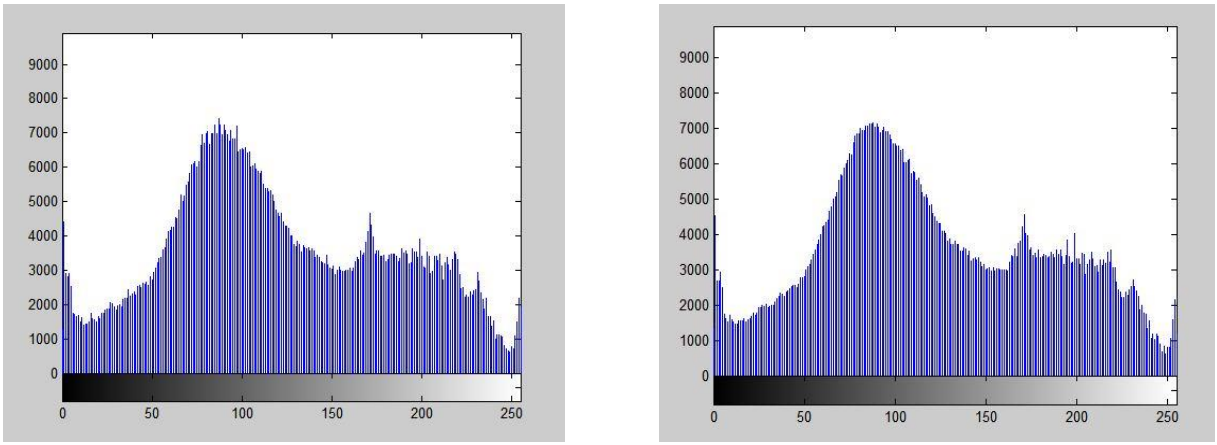


Figure 12. Histogram comparison of frame number 300 of cover file 2.mp4 and stego file Myfile2.avi

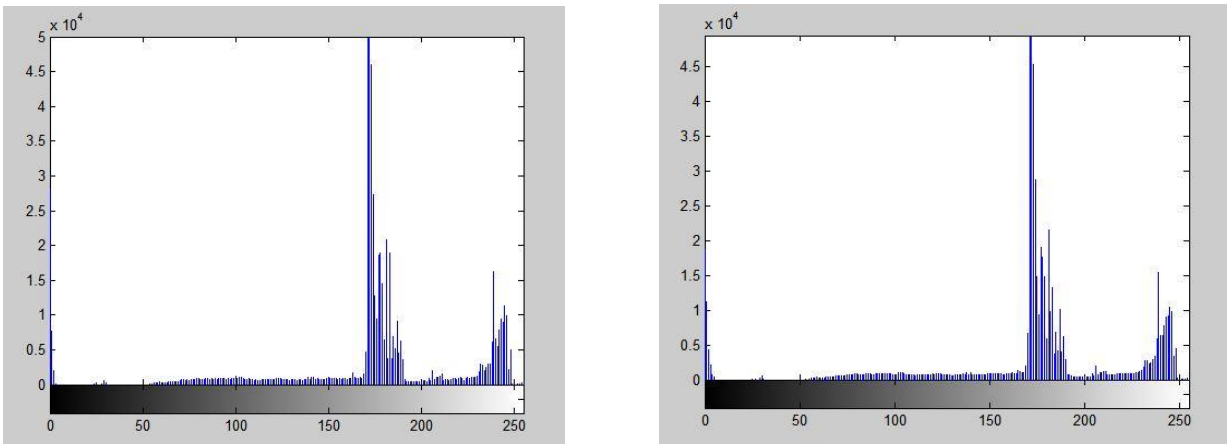


Figure 13. Histogram comparison of frame number 400 of cover file 3.mp4and stego file Myfile3.avi

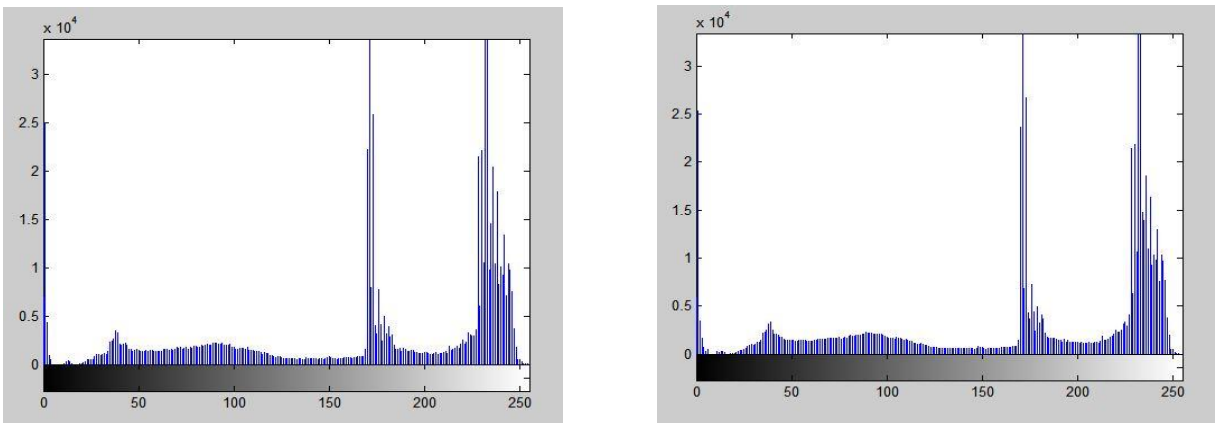


Figure 14. Histogram comparison of frame number 600 of cover file 3.mp4 and stego file Myfile3.avi

V. Conclusion

The objective of this paper is to hide a message in the form of an image or text in a video. In this paper, we are hiding message (i.e. an image/text) is hidden in a frame of the video that only sender and receiver knows. Furthermore, we are using a secret key shared between sender and receiver. This adds security to the system. We use sequential encoding system. Then the frame in which message is embedded is saved. For the decryption of the message, we'll do vice-versa process. The comparison between the histograms of the selected frame of the original video and stego video shows a little

changes because of embedded message i.e. text or image in it. The MSE and PSNR values for the cover video frame and the stego video frame are also shown which is good.

REFERENCES

[1] Mohsina Choudhury, Sarita Thapa, Prashant Kumar, "Digital Image Hiding using Superposition Method", Int.J.Computer Technology & Applications,Vol. 6 (1), pp. 121-126, Jan-Feb 2015.

[2] Ei Nyein Chan Wai and May Aye Khine, "Modified Linguistic Steganography Approach by Using Syntax Bank and Digital Signature", International Journal of Information and Education Technology, Vol. 1, No. 5, pp. 410-415, December 2011

[3] Abhishek Koluguri , Sheikh Gouse, Dr. P. Bhaskara Reddy, " Text Steganography Methods and its Tools", International Journal of Advanced Scientific and Technical Research, Issue 4 volume 2,pp. 888-902 , March-April 2014

[4] NEDELJKO CVEJIC, "ALGORITHMS FOR AUDIO WATERMARKING AND STEGANOGRAPHY", Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu, 2004

[5] Tamanna , Prof Ashwani Sethi, "Steganography:A Review", International Journal of Research and Innovation in Computer Engineering (IJRICE), vol. 1(5), pp. 1-5, May 2015

[6] Alisha Arora, Mrs. Nirvair Neeru, Mrs. Taqdir, "IMAGE STEGANOGRAPHY TECHNIQUES: AN OVERVIEW ", International Journal For Technological Research In Engineering Vol. 1(9), pp. 924-929, May-2014

[7] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, pp. 113-124, May, 2013

[8] Deepak Kumar Sharma, AsthaGautam, "AN APPROACH TO HIDE DATA IN VIDEO USING STEGANOGRAPHY"IJRET: International Journal of Research in Engineering and Technology, Vol. 3(4), pp. 164-168, Apr-2014

[9] Jayshree D. Kularkar, Sonal Honale, "ENHANCING VISUAL DATA SECURITY WITH USER AUTHENTICATION", IORD Journal of Science & Technology, Vol. 2(2), PP. 77-82, JAN –FEB 2015

[10] Randeepika Samagh, Shailja Rani, "Data Hiding using Image Steganography", International Journal of Emerging Trends in Engineering and Development Issue 5, Vol. 3, pp. 123-129, April.-May. 2015

