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 random coding

Khushbu Sahu[1] and Utkarsh Sharma[2]

[1]*ME (communication), Shri Shankaracharya Technical Campus,*
[2]*Department of Electronics & Telecommunication, Shri Shankaracharya Technical Campus,*

Abstract *— Steganography refers to a file or info that has been concel (hide) within, video/audio file or a digital image. Steganography is employed to cover the messages within different harmless messages during a in a that doesn't allow 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 managing digital information and covert communication channel. In this paper we tend to used video as cover media for concealment(hide) the secret message i.e text or images and we use random encoding/decoding process. For additional security, we used the random encoding/decoding process. Steganography is divided into Text Steganography, Image Steganography, Audio/Video Steganography. The experimental result shows that the original cover video and stego video are visually almost identical i.e. there's no perceptual difference between the 2 videos. In this paper we have a tendency to also analyze the histogram of the frames of the cover video & stego video, which doesnot show much difference.*

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

I. INTRODUCTION

Steganography is that the art of sending hidden messages in an exceedingly specific means that nobody will the exception of the sender and also the receiver suspects the existence of a message. The word steganography virtually suggests that covered writing as derived from Greek. The goal of steganography is to hide the existence of the info from a 3rd party. A correct data concealment method ought to contain many needs like imperceptibility, robustness, capacity and Security. In steganography, an information message is hidden (embedded) inside a cover signal. The output of the embedder is named a stego signal. After transmission, recording and other signal process which can contaminate and deform the stego signal, the embedded message is retrieved using the suitable stego key within the block known as extractor. The carrier of steganography is a picture, text, audio or a video file. Most of the steganography systems are developed so as to insert an, image or in audio file in a carrier file.

Steganography these days, however, is considerably more sophisticated, permitting a user to hide large amounts of data within image and audio files. These sorts of steganography typically are utilized in conjunction so the data is doubly protected; 1st it's encrypted and so hidden so that an human has to 1st find the data (an typically difficult task in and of itself) and so decrypt it [1]. During this paper, a security thesis is projected that imposes the thought of secrecy over privacy for messages in varied formats. Classification of the steganography are :

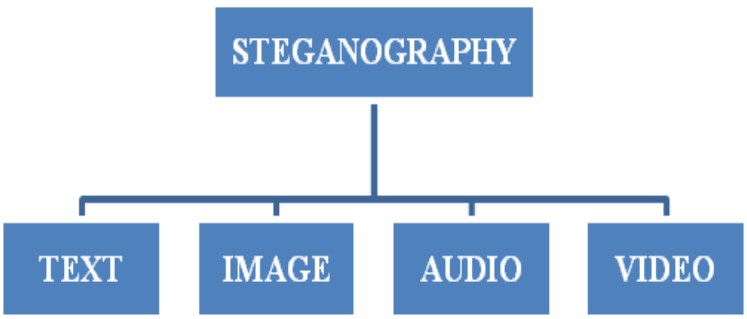


Figure 1. Classification Of Steganography

II. HISTORY

The conception of message concealment isn't new – it's been around for hundreds of years. A Greek shaven the head of a slave, wrote a message, then waited for the hair to grow back before causing the slave to his destination.[4] Steganography (in the form of invisible ink) was employed by Washington within the Revolutionary War. Prior to the civil war, quilts were sewed with special patterns to inform escaping slaves that direction to travel and what to try and do. During WWI there was a cable the read, "Father is dead." Suspecting a hidden which means, the censor modified it to "Father is deceased" that caused the reply, "Is Father dead or deceased?"[2].

During WWII chess by mail was prohibited, problem puzzles examined, stamps were removed and replaced by ones of equal price. In the 1980's, a number of Margaret Thatcher's cabinet documents were leaked to the press. She ordered that the word processors being employed by government workers, encrypt their identity within the word spacing of the documents [2]. It is believed that steganography was initial practiced throughout the Golden Age in greece [3]. An ancient greek record describes the practice of melting wax off wax tablets used for writing messages then inscribing a message within the underlying wood [4]. The wax was then reapplied to the wood, giving the looks of a brand new, unused tablet. The ensuing tablets may be innocently transported without anyone suspecting the presence of a message below the wax.

Federal Bureau of Investigation Director J. Edgar Hoover stated as "the enemy's masterpiece of undercover work. In a picture the scale of a written amount having the clarity of standard-sized written pages are the microdots. The message wasn't hidden, nor encrypted. It had been with great care little on not draw attention to itself. Besides being therefore small, microdots allowable the transmission of huge amounts of information as well as drawings and pictures. the utilization of Invisible inks is Another common style of invisible writing . Such inks were used with abundant success as recently as WW-II. a totally different message written between the lines it might contain in a letter. Early in WW-II steganographic technology consisted completely solely of invisible inks. Common sources for invisible inks are milk, vinegar, fruit juices [5]. once heated All of those are darken.

III. METHODOLOGY

3.1 Random Encoding/decoding

Pseudo-Random Number Generator Initialized, usually no set starting point. Message Data is then Encoded/Decoded based upon the pixel location determined by Random Number Generator normally no set pattern. No set Encoding/Decoding Pattern for Histogram Analysis to Detect. It has Quicker Recovery Rate generally implemented by Pre-Defining encoding pattern; more efficient for recovery process. Message size is very difficult to estimate. Disadvantage is that it is Detectable using varying sized windows and localized Histogram Analysis.

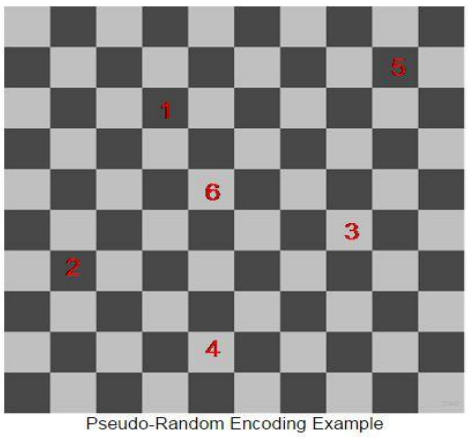


Figure 2. Example Of Random Encoding/decoding

3.1.1 Random encoding process:

Firstly take an input or cover video. From the frames of the video, we'll select 1 video frame for embedding or hiding a message i.e. text or image. One secret key is used which is shared between sender and reciver only. This will add more security to the entire system. We use random encoding in this system. Then the frame in which message is embedded (or hidden) is saved. And we get the stego video.

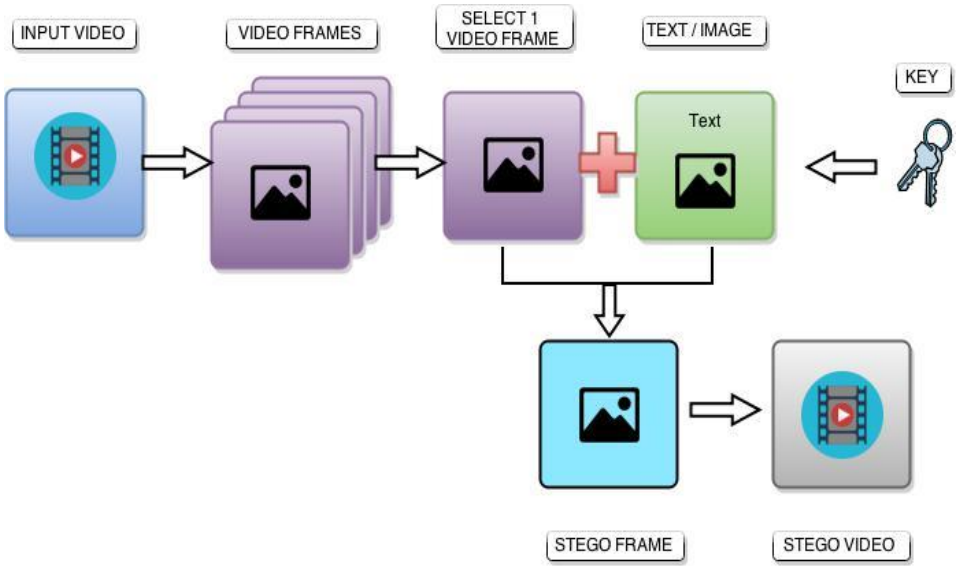


Figure 3. Random encoding process

3.1.2 Random decoding process:

For the decoding process, the stego video is used. The stego frame is extracted from the stego video. The extracted stego frame is decrypted using random decoding process in this system. The same secret key is used which is shared between the sender and the receiver only. From the decrypted stego frame the message (i.e. text or image) is extracted. Then the original input is retrieved.

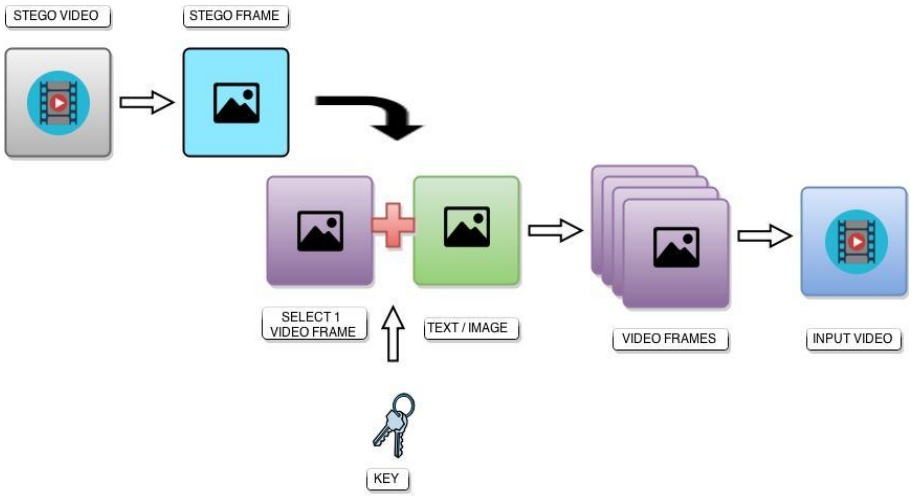


Figure 4. Random decoding process

3.2 Applications of steganography

- ✓ To have secure secret communications wherever cryptographical encoding strategies aren't accessible.
- ✓ To possess secure secret communication wherever robust cryptography is not possible[1].
- ✓ In some cases, as an example in military applications, even the data that 2 parties communicate may be of enormous importance.
- ✓ The health care, and particularly medical imaging systems, could greatly take pleasure in info concealing techniques.
- ✓ A popular application of watermarking techniques is to supply a proof of possession of digital information by embedding copyright statements into video or image digital merchandise[6].
- ✓ Automatic observance and tracking of copy-write material on net. (For example, a robot searches the online for marked material and thereby identifies potential contraband problems.)

- ✓ Automatic audit of radio transmissions: (A robot will "listen" to a station and appearance for marks, that indicate that a selected piece of music, or advertizement , has been broadcast.)[6].
- ✓ Information augmentation - to add info for the advantage of the general public.
- ✓ Fingerprinting applications (in order to differentiate distributed data)

IV. RESULT

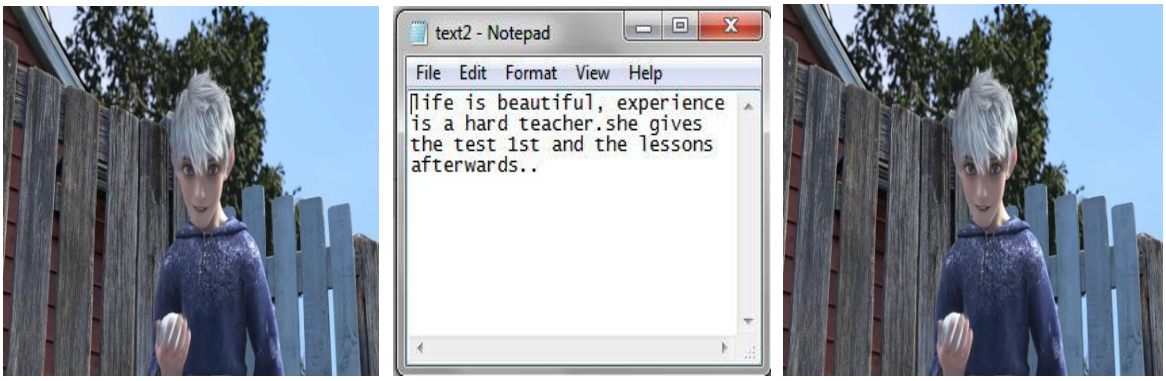
In this project, a message i.e. an image/text is hidden in a frame of the cover video. The proposed algorithm is tested against "blue umbrella.mp4", "rotg.mp4" and "sandman.mp4" as cover video. The output video "myfile1.avi", "myfile2.avi" and "myfile3.avi" are the stego video of their respective cover 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) 200th frame of cover video *(b) embedded text message* *(c) 200th frame of stego video*

Figure 5. Frame number 200 of the cover video 'blue umbrella.mp4', embedded text message and stego video 'Myfile1.avi'.

(a) 460th frame of cover video *(b) embedded image message* *(c) 460th frame of stego video*

Figure 6. Frame number 460 of the cover video 'blue umbrella.mp4', embedded image message and stego video 'Myfile1.avi'.



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

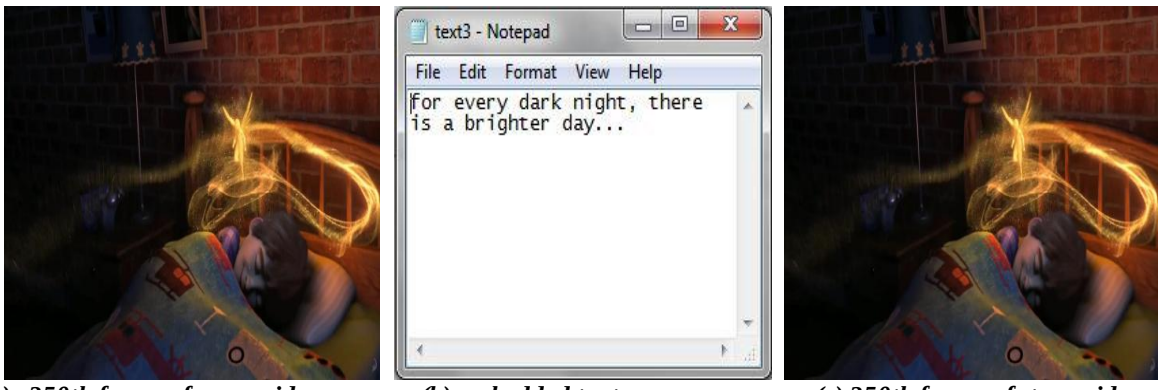
Figure 7. Frame number 50 of the cover video 'rotg.mp4', embedded text message and stego video 'Myfile2.avi'.

(a) 350th frame of cover video *(b) embedded image message* *(c) 350th frame of stego video*

Figure 8. Frame number 350 of the cover video 'rotg.mp4', embedded image message and stego video 'Myfile2.avi'.

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

Figure 9. Frame number 100 of the cover video 'sandman.mp4', embedded image message and stego video 'Myfile3.avi'.



(a) 350th frame of cover video *(b) embedded text message* *(c) 350th frame of stego video*

Figure 10. Frame number 350 of the cover video 'sandman.mp4', embedded text message and stego video 'Myfile3.avi'.

4.1 Peak Signal to Noise ratio (PSNR)

Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation [7]. 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 is easily defined via the mean squared error (MSE).

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

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)

The mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated [8]. Mean squared Error (MSE) is employed to determine how the stego video frame and the cover video frame are different [9]. 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)
Blue umbrella.mp4	Myfile1.avi	200	0.0032	73.1562
		460	0.0038	72.3688
rotg.mp4	Myfile2.avi	50	0.0087	68.7667
		350	0.0060	70.3763
sandman.mp4	Myfile3.avi	100	0.0041	72.0519
		350	0.0052	71.0390

4.3 Histogram difference

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

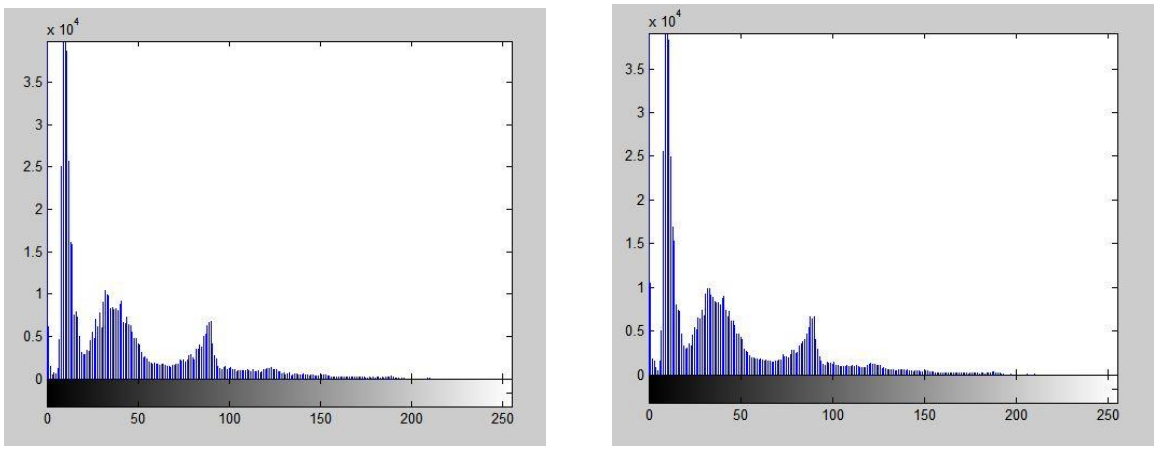


Figure 11. Histogram comparison of frame number 200 of cover file blue umbrella.mp4 and stego file Myfile1.avi'

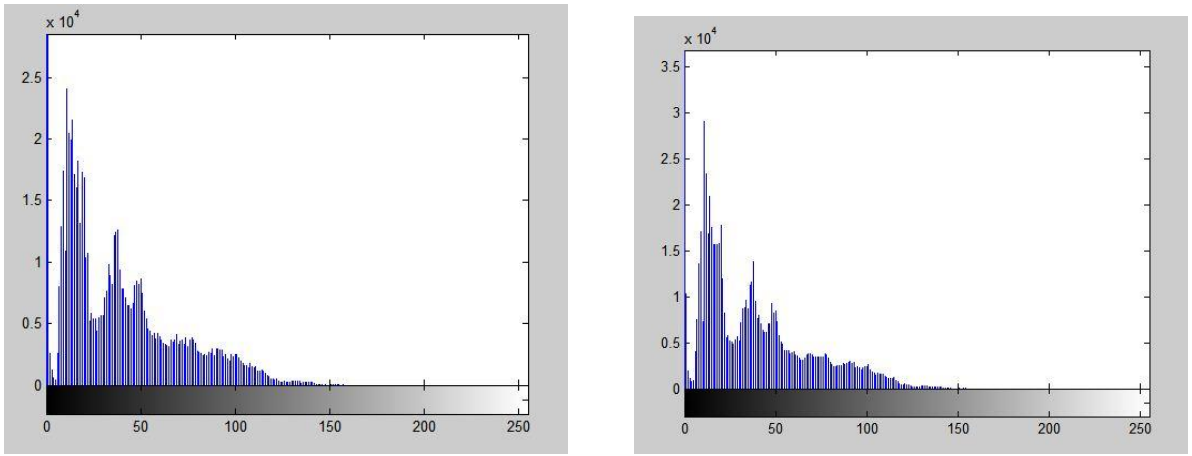


Figure 12. Histogram comparison of frame number 460 of cover file blue umbrella.mp4 and stego file Myfile1.avi'

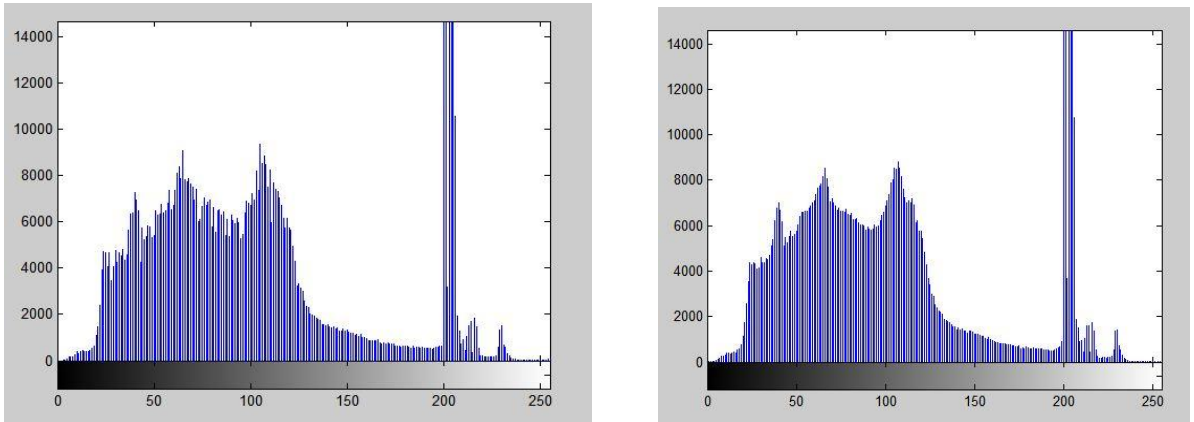


Figure 13. Histogram comparison of frame number 50 of cover file rotg.mp4 and stego file Myfile2.avi'

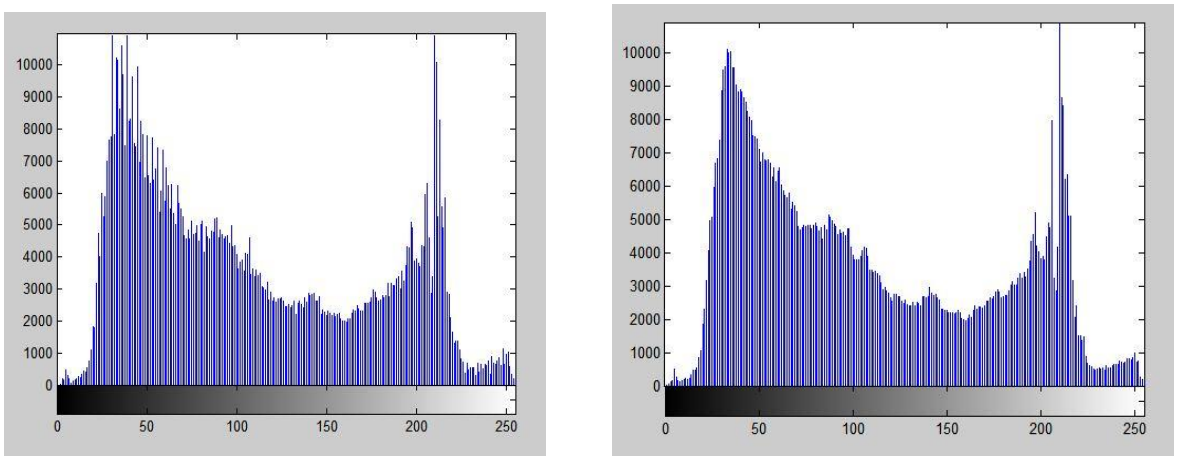


Figure 14. Histogram comparison of frame number 350 of cover file rotg.mp4 and stego file Myfile2.avi'

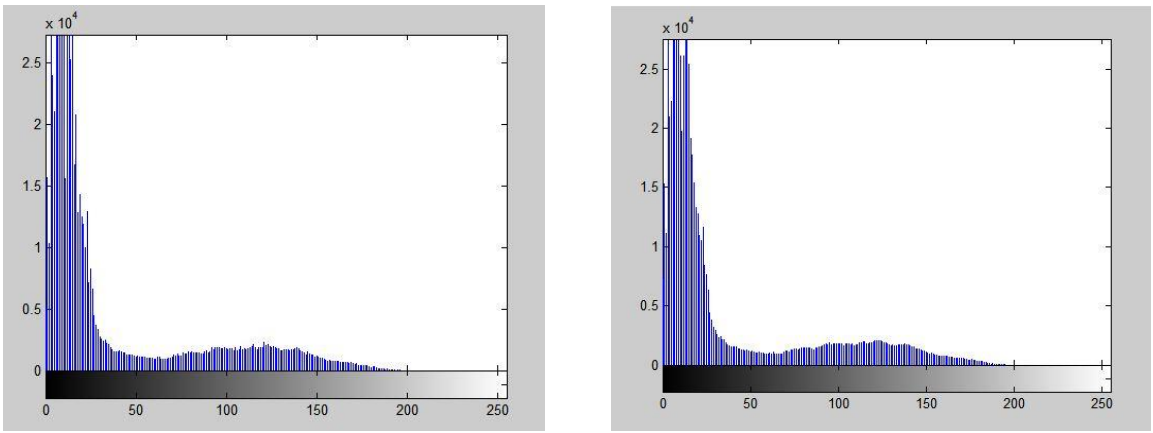


Figure 15. Histogram comparison of frame number 100 of cover file sandman.mp4and stego file Myfile3.avi'

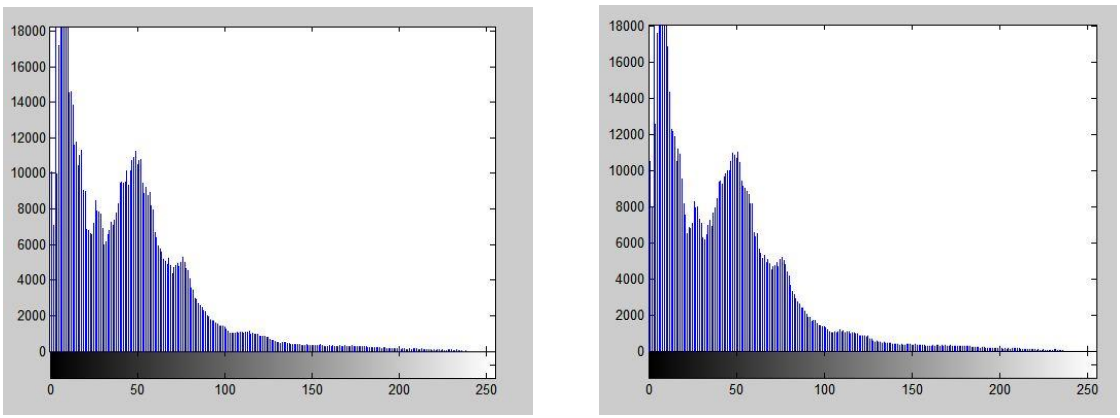


Figure 16. Histogram comparison of frame number 350 of cover file sandman.mp4 and stego file Myfile3.avi

The comparison between the histograms of the original video and stego video shows a little changes because of embedded message i.e. text or image in it.

V. CONCLUSION

The objective of this paper is to hide a message i.e. an image or text in a video using random encoding/decoding. In this paper, we are hiding a message (i.e. an image/text), which is hidden in a video frame that only sender and receiver knows. In addition, between sender and receiver we are sharing a secret key. This will add more security to the system. We use random encoding system. Then the frame in which the message is embedded is saved. For the decryption of the message, we'll do vice-versa process. The MSE and PSNR values for the cover video frame and the stego video frame

are also shown. The comparison between the histograms of the selected video frame of the original video and stego video doesn't show visually much difference, shows only a little changes because of embedded message i.e. text or image in it. So the method proposed in this paper is more efficient.

REFERENCES

[1] Urmila Kumari, Saroj Hiranwal, "Data Hiding in Gray-Scale Images by LSB Method using IWT with Lifting Scheme", International Journal on Recent and Innovation Trends in Computing and Communication, Vol.1(10), pp. 782 – 792, October 2013.

[2] http://www.cs.utsa.edu/~jortiz/CS4953/Lecture%20Notes/L01-Introduction%20to%20Steganography.ppt

[3] Donovan ArtzDigital Steganography: Hiding Data within Data, IEEE INTERNET COMPUTING, pp. 75-80, MAY-JUNE 2001.

[4] Vidhya P.M and Dr. Varghese Paul, "HIDE and SEEK-A Survey", International Conference on Security and Authentication, pp. 144- 148, 2014.

[5] R.M. Goudar, Pankaj Joshi, "INFORMATION SECURITY THROUGH STEGANOGRAPHY USING TCP/IP HEADER FIELDS", International Journal Of Next Generation Computer Applications, Vol.1(4), pp. 1-3, December 2012.

[6] http://www.fi.muni.cz/usr/gruska/crypto04/CHAPTER%2013%20%20Steganography%20and%20Watermarking.ppt

[7] http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

[8] http://en.wikipedia.org/wiki/Mean_squared_error

[9] Yunjung Lee, "Streaming Video Service Model using Secure Steganographic Method", International Journal of Security and Its Applications Vol.7(6), pp.79-88, 2013.

[10] 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.

[11] 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

[12] 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

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

[14] 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

[15] 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

[16] 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

[17] 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

[18] 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

[19] 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

