International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

Sequential and Random Encoding Techniques for Video Steganography

Ramyashree G R[1], Dr. Nataraj K R[2]

[1]*Student, VLSI and Embedded Systems, Dpt. of ECE, SJB Institute of Technology, Karnataka, India*
[2]*Professor and Head,Dpt. of ECE,SJB Institute of Technology, Karnataka, India*

Abstract -*In this competition world secret communication has become an essential part , hence in this paper we have discussed a video Steganographic technique by using the Audio Video Interleave (AVI) as the cover media, the video files are used as cover media due to their capacity of holding information in a large amount ,we have embedded the text message or the Image message in the video file using an Random encoding Technique and the sequential encoding techniques along with the encryption key using LSB(Least Significant Bit insertion) method , an extra layer of security is added by making the random key selection this makes it difficult to decode the hidden message for the unauthorized person , in order to decode the secreted text or the image message the recipient should have the prior knowledge of the encryption key used and the methodology used for secreting the information.*

Key Words:**Video steganography, Sequential Encoding, Encryption Key, Random encoding, Random Seed Value, Steganalysis, LSB insertion, Stego Video**

1. INTRODUCTION

With the development of computer and its uses as the part of communication in different areas of work in life has made an information security as a very important issue to be solved, one of the methods is security of the information by exchanging the information by using the cover media. There are different methods for hiding the information like cryptography, Steganography, coding and many more, the true intension of Steganographic technique is to secret the information in the cover media such that the unauthorized or the third person will never get to know the presence of the secret message in the cover media.

1.1 VIDEO STEGANOGRAPHY

Video Steganography is classified mainly into two types , one among the technique is to secret the information in an uncompressed video , after the insertion the video is compressed , as compared to first the second method is little complex where the secret message is embedded directly into the compressed video format , problem associated with the first technique is how effectively the impact of video compression is avoided on the embedded secret message

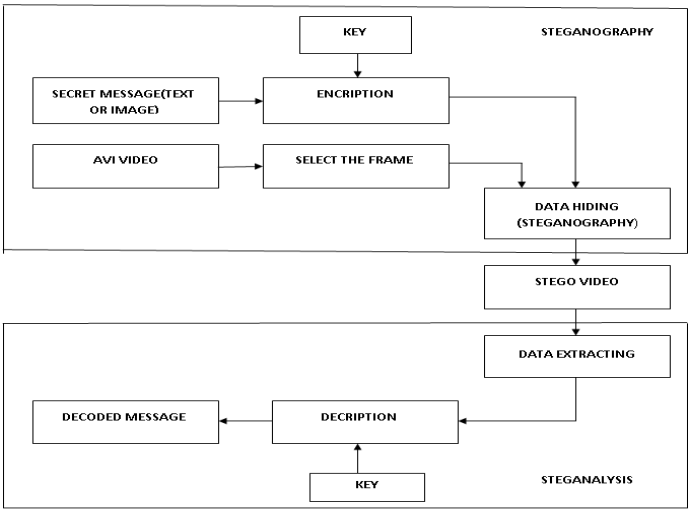

Fig-1. Basic block diagram of Video Steganography and Steganalysis

The video Steganography can be applied on the spatial domain and the frequency domain, some transformation algorithms are used in frequency domain using which the images are transformed into frequency components and the secret message is embedded into all these frequency components or in some frequency components, the secret message embedding can be done in block level or in the bit level. In the case of spatial domain the LSB (Least Significant Bit) insertion technique in most of the application, using this method the large amount of data can be inserted in a cover object .Video quality can be measured with the formal methods like expert observation or by PSNR metrics.

The main advantage of using Least Significant Insertion (LSB) technique is an unauthorized person or the third party will never get a clue that some

message is embedded in the video, since the changes made in the video is not susceptible by the Human Eyes.

2. IMPLEMENTATION

In this project the Least Significant Insertion methodology is used for secreting the image or the text message, message embedding is done using Random type of encoding or sequential encoding technique the most simplest among the other techniques are Least Significant bit insertion , i.e. inserting a single bit of message directly in to the bits of the cover media either in a very deterministic manner or in random fashion using random seed value as a reference .inserting the LSB bit in the cover results in the similar video where the changes made are not human perceptible differences.

2.1 ENCODING (STEGANOGRAPHY)

The Fig-2.1 flow chart below describes the fundamental flow of Steganographic technique, at the first step a raw (AVI) video into which the secret text message or image message is to be inserted is read, the frames of the video are extracted and one frame is selected by the user in which the message will be embedded

The secret message is encrypted using the encryption key which ranges from 0 to 255, the encrypted data is embedded into the extracted frame using either sequential or random encoding techniques , if the technique used is random encoding then a random seed value from 1-100 is used which provides the extra layer of protection

The pixel order of RGBBGRRG is chosen for encryption and the same order is repeated for all the pixels of the frame, the frame is put back in the video, the resultant video is known as the Stego video and the process is known as steganography.

2.2 STEGANALYSIS (DECODING)

Stego video is transmitted over the channel, the third person will not get any clue that there is a presence of secret message in the video even if third person find out the message presence, they cannot decode the message unless they know the encryption key and the technique used for the encoding and they must know the random seed value used during encoding process,

The intended recipient will have a prior knowledge of encryption key used and the random seed value using which the secret message is decoded without any loss.

The same is explained in the Fig-2.2.

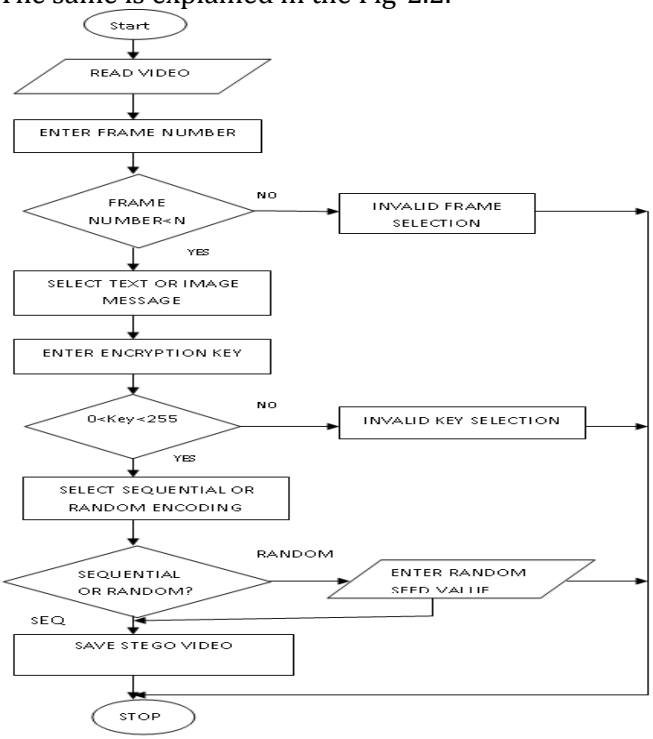

Fig-2.1. Flow chart of Steganographic Process

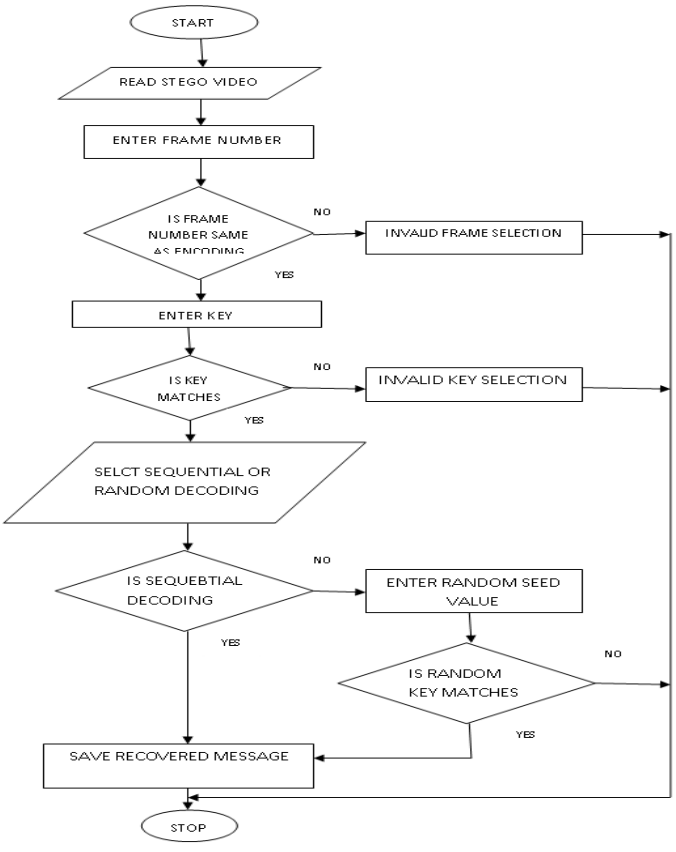

Fig-2.2. Flow chart of decoding(Steganalysis)

2.3 PERFORMANCE ANALYSIS

2.3.1 Objective quality assessment

These automated quality assessment techniques are based on mathematical and computational algorithms to measure the accuracy of the perceived image. Most of the recent objective quality assessment techniques are based on computing the quality of the image with the original image. Here we compare the accuracy of the cover image with the stegoimage using two techniques, i.e. Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

$$MSE = \frac{\sum_{M,N}[C(m,n)-S(m,n)]^2}{M \times N}$$

Where M and N are the rows and columns of the cover image respectively, C and S are the cover and stego image respectively

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

Where R is the dynamic range of pixel values(R=255 for gray scale images).PSNR gives the value infinity under one condition only; that is when the cover image is compared to itself.

Otherwise if the PSNR result is greater than 30 dB, then the human visual system would not be able to differentiate between the cover image and the stego image progressively. A PSNR value of less than 30 dB would indicate a human ability to notice the quality degradation.

By using the above equations and getting the number of pixels at each level from the histogram of the cover and stego image as show, we have

PSNR ≈ 78.4038

As we see the PSNR value is greater than 30 db which indicate that human visual system cannot differentiate between cover image and stego image.

2.3.2 HISTOGRAM ANALYSIS

To prevent the leakage of information to attackers it is important to ensure that encrypted and original secret image do not have any statistical similarities.

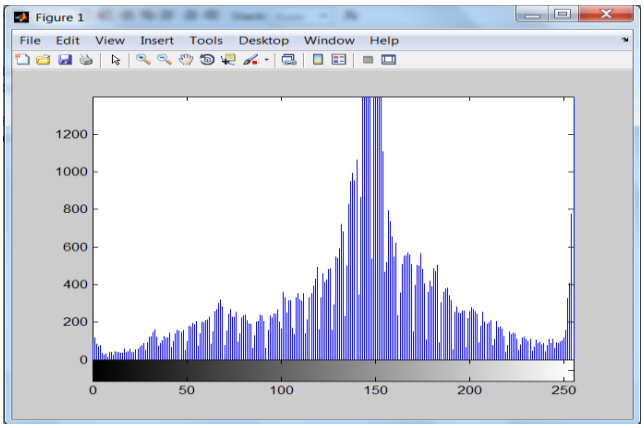

Fig 2.3.1. Histogram of original Image

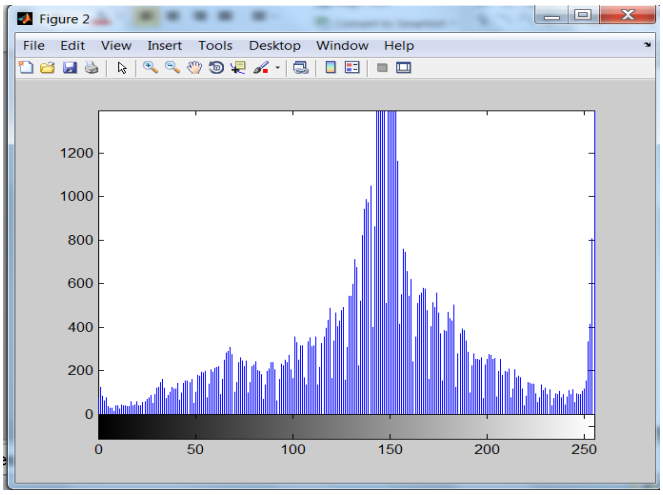

Fig 2.3.2. Histogram of Stego image

3. CONCLUSION

With the digital media growth Data Security has become one of the major concern and Steganography is one among those techniques used for the data security , in which an unauthorized person will never get to know the secret message presence , even if the third person predicts the presence of the secret message they cannot decode the message without knowing the technique of encoding and the encryption key due the presence of high layer of security, in this project video steganography is implemented for both text file message and the Image message , the stego video is generated and is visually inspected and compared with the original image and not much difference is found in both the videos

REFERENCES

[1] Yadav, P, Mishra, N, Sharma, S, " *A secure video steganography with encryption based on LSB technique*", IEEE International Conference on Digital Object Computational Intelligence and Computing Research (ICCIC), 2013 IEEE.

[2] Balaji, R,Naveen, G ," *Secure data transmission using video Steganography*", IEEE International Conference on Electro/Information Technology (EIT), 2011.

[3] Mozo, A.J, Obien, M.E,Rigor, C.J, Rayel, D.F, Chua, K.Tangonan.G," *Video steganography using Flash Video (FLV)*", Instrumentation and Measurement Technology Conference,IEEE 2009.

[4] Kelash, H.M,Abdel Wahab, O.F, Elshakankiry, O.A,El-sayed, H.S," *Hiding data in video sequences using steganography algorithms*" ICT Convergence (ICTC)2013.

[5] Munasinghe, A, Dharmaratne, A, De Zoysa, K, "*Video steganography*", International Conference on Advances in ICT for Emerging Regions (ICTer) 2013.

[6] Cruz.J.P, Libatique, N.J. Tangonan, G, " *Steganography and data hiding in flash video (FLV)*" TENCON 2012 - 2012 IEEE.

[7] Thakur, V.Saikia, M.,"*Hiding secret image in video*",International Conference on Intelligent Systems and Signal Processing (ISSP) , 2013.

[8] P.Paulpandi1, Dr.T.Meyyappan " *Hiding Messages Using Motion Vector Technique In Video Steganography*", International Journal of Engineering Trends and Technology- Volume3Issue3- 2012.

[9] A.Swathi 1, Dr. S.A.K Jilani," *Video Steganography by LSB Substitution Using Different Polynomial Equations*", International Journal Of Computational Engineering Research Vol. 2 Issue. 5.

[10] Ronak Doshi, Pratik Jain, Lalit Gupta,"*Steganography and Its Applications in Security*" International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012.

[11] Shashikala Channalli, Ajay Jadhav Steganography, *"An Art of Hiding Data",* International Journal on Computer Science and Engineering Vol.1(3), 2009.

[12] Ross J.Anderson,Fabien A.P.Petitcols" *On The limits of steganography*",IEEE Journal of Selected Areas in Communication,May 1998 .