ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

LSB Approach in Video Steganography

Nikita N. Pawar[1], S.S.Gadekar[2], P.R.Thorat [3]

PG Student, Department of Electronics & Telecommunication Engineering, Shreeyash College of Engineering and Technology, Aurangabad, India[1]

Assistant Professor, Department of Electronics & Telecommunication Engineering, Shreeyash College of Engineering and Technology, Aurangabad, India[2]

Professor, Department of Electronics & Telecommunication Engineering, Shreeyash College of Engineering and Technology, Aurangabad, India[3]

ABSTRACT: now a day's use of digital dataincluding voice, text, image, and video is very popular and become a necessary. Transferring private digital data through internet is having very risk. To protect data from the hackers or cyber criminals over internet, steganography is best solution, which should not only encrypt the data into another form but also hides its presence. This system provides the video steganography to provide the security to digital data.

KEYWORDS: Digital Data, Hackers, Cyber Criminals, Steganography, Encrypt, Security.

I. INTRODUCTION

Now a day's transferring data from one user to another user over internet is not safe because of hackers or cyber criminals and created new challenges for sending a message in a safe and secure way. Steganography provides the security to the data. Steganography is a Greek word, combination of Steganos means "covered, concealed, or protected" and graphein meaning "writing", and provides way of secret communication [1, 2]. Steganography provides a way that only the sender and intended recipient of a message. The main aim of stego-system is to reduce any suspicion that a third party may have over occurring communication [3]. There are four type of steganography namely Text, Image, Audio/Video and Protocol, as shown in the figure 1[1]. Steganography is way in which sender and the recipient is able to detect the message, following general formula explain the process of steganographic, the cover_medium is the file in which is used to hide the hidden_data and stego_key is used to encrypt message. Stego_medium is the encrypted file contains same type of file name of cover_medium [4].

cover_medium + hidden data + stego_key = stego_medium

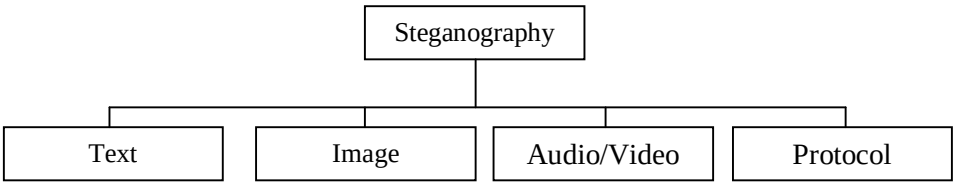

Figure 1 Different categories of steganography [1]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

II. COMPARISON BETWEEN STEGANOGRAPHY, CRYPTOGRAPHY AND WATERMARKING

In a Steganography only the sender and the intended recipient is able to detect the message sent through it [4]. Cryptographyand steganography try to protect data and when combine both approaches together to increase thesecurity level of the system. While watermarking is another technology, it is similar to steganography, but lies ondifferent goals and philosophies.Table 1 shows a comparison between steganography, cryptography and watermarking [2].

Table 1 Comparison between steganography, cryptography and watermarking [2]

	Steganography	Cryptography	Watermarking
Goal	Conceal the existence of the communications	Hide the contents of the communications	Protect the embedded content against intentional attacks for destruction or removal
Perceptual invisibility	Must Exist	Doesn't Exist	Application dependent
Signature size	Large	Large	Application dependent
Signature structure	May Change	Must Change	Doesn't Change
Use of key	Optional	Necessary	Optional
Output	Stego-file	Cipher text	Watermarked file
Goal fails when	Secret message existence is detected	Cipher text is decrypted	Watermark is changed or removed
Challenges	Perceptual transparency, Hiding capacity and robustness	Robustness	Robustness

III. LITERATURE SURVEY

Video steganography is a technique in which ew can hide any kind of file into a video. Figure 2 shows the different types of video steganography.

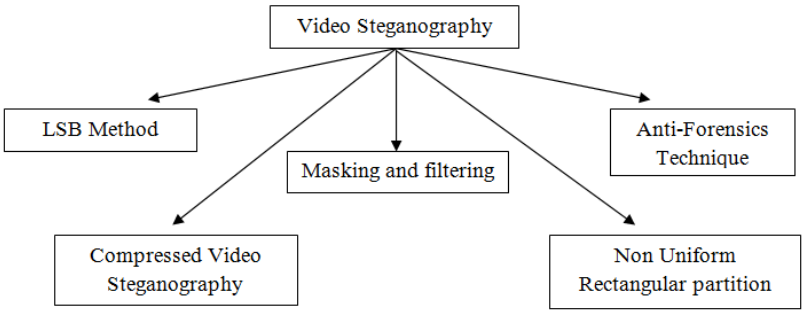

Figure 2 Types of Video steganography

KamredUdham Singh [5] present video based Steganography by using least significant bit (LSB) insertion technique. In this system, it change LSB of video file with the information bits and also system focus on hiding information in specific frames of the video and in specific position of the frame by LSB substitution. This system provides to hide message into video images (AVI). S. Suma Christal Mary M.E [6] proposes a real-time hiding of information by using

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

compressed video secure steganography (CVSS) algorithm in audio steganography. In this proposed system to adjust the embedding strategy and capacity new criteria employing statistical invisibility of contiguous frames is used, indirectly it improve the security.Sherly A P and Amritha P P [7] proposed Compressed Video Steganographic scheme in which to enlarge the capacity of the hiddensecret information and to provide an imperceptible stego-image for human vision. Tri-way pixel-value differencing (TPVD) is used for embedding.Prof. D.J.Bonde et al. [8] proposed g Anti forensics techniques for Audio and video steganography, in which Forbidden Zone Data Hiding(FZDH) is used for image steganography and for Audio Steganography phase Coding algorithm was used.

IV. METHODOLOGY

Inthis project for encryption, cover video and data together creates a stego video and for decryption this stego video is again decomposed and the frames are assembled to separate the data and the cover video. Here we are using LSB (Least Significant Bits) method to encrypt the stego video. In this project the cover and data both are in terms of video (.mp4) format.HMM (Hidden Markov Model) is used to select the frames instead of selecting any random number of frames to hide the data. Figure 2 a and b shows the Encryption and Decryption of Stego video respectively

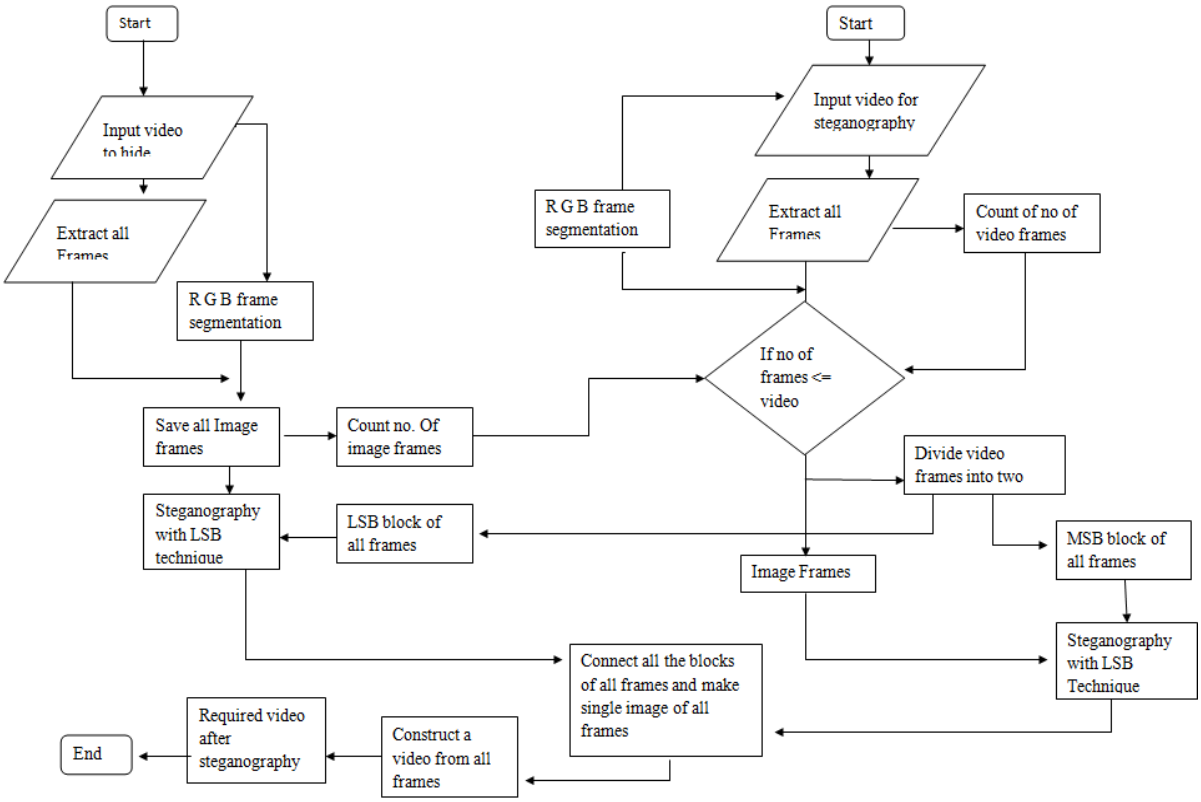

Figure 2a Encryption of Video

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

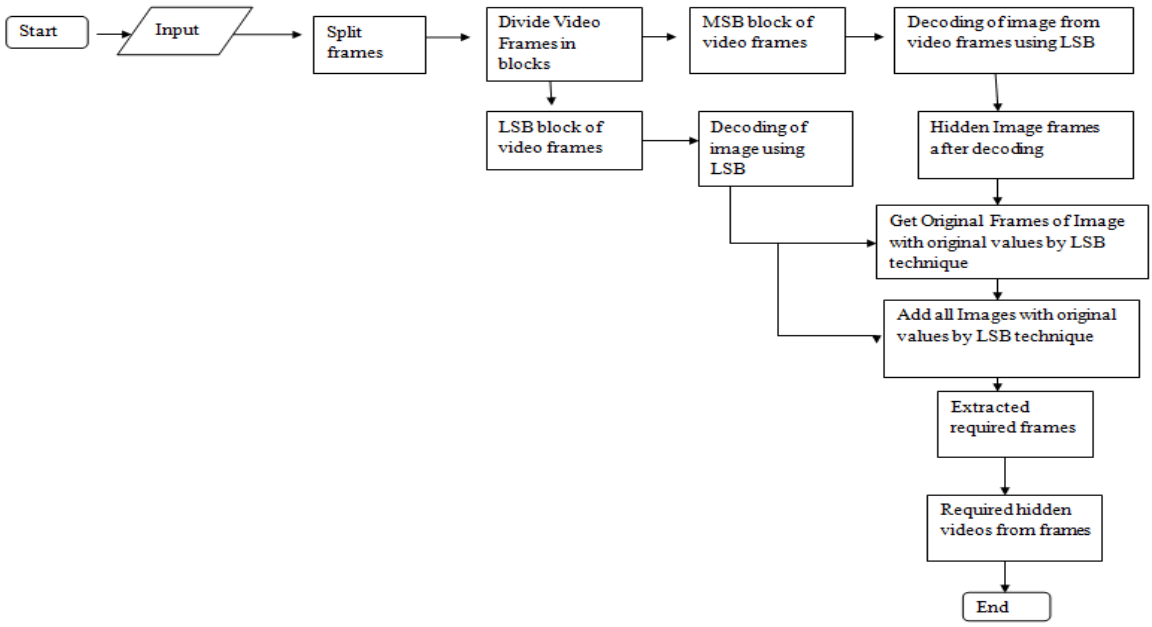

Figure 2b Decryption of Stego video

V. RESULT AND DISCUSSION

The table2 shows file size and time required to encrypt and decrypt the data according to the file size. The very first cover file is of 908 kb and the target file which is to be hidden is of 247 kb. The process of decomposition of frames is taken place. After Process it took 12-16 seconds to generate the stego video which is of 908 kb in size, same as cover video. At the time of decryption of stego video, it tool around 23-27 seconds.In second case, cover file size is 670 kb and target file size is of 35 kb which is small compared to first case. Because of this, generating stego video took only 2-5 seconds having size 670 kb. Decryption of stego video is done in 10-12 sec.

In third case, cover video size and target video size, both are more compared to above cases. This took 10-12 seconds to generate stego video and 24-28 sec to decrypt.If we see closely in fourth case, the target file size is more compared t cover file but still the program is able to generate the stego file. Beside the time taken by this case is more compared to above cases to generate stego video. But at the time of decryption, as the cover file is small decryption is done in 11-16 seconds.All above studies shows that the time is the major factor which is totally dependent on the file size of cover and target file. The study shows that if the cover files size is more than target file it will take around 10-15 seconds to generate stego video. And if the target file is more than cover file size the time taken is more. Decryption is also totally depending upon the size of stego video.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 12, December 2018

Table 2 Output analysis

Sl. No.	Cover file size (kb)	Target file size (kb)	Stego file size (kb)	Approx time taken to process file (sec)	Approx time taken to decrypt file (sec)	Process completed
1	908	247	908	6-10	23-27	✓
2	670	35	670	2-5	10-12	✓
3	908	670	908	10-12	24-28	✓
4	670	908	670	21-25	11-16	✓

VI. CONCLUSION

Steganography is the technique that provides confidential communication between two users. In this paper, main techniques of image and video steganography are discussed. Each steganography technique must satisfy the three main objectives (imperceptibility, capacity and robustness). In case of video steganography, wavelet transforms based techniques are more robust. Also the combination of LSB and wavelet transform can improve the performance of the steganographic system. LSB based techniques results are also good and can be improved by combining this technique with artificial intelligence, fuzzy logic neural network. Steganography is the fast growing and upcoming field and has a great scope for research and development.

REFERENCES

[1] Abhinav Thakur, Harbinder Singh and ShikhaSharda, "Different Techniques of Image and Video Steganography: A Review", RIEECE, Volume 2, Spl. Issue 2, 2015.
[2] Mennatallah M. Sadek&Amal S. Khalifa&Mostafa G. M. Mostafa, "Video steganography: a comprehensive review", Springer, 2014.
[3] Thomas Sloan and Julio Hernandez-Castro, "Forensic analysis of video steganography tools", PeerJComput. Sci, 2017.
[4] ShivaniKhosla and ParamjeetKaur, "Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Applications, Volume 95, No. 20, June 2014.
[5]KamredUdham Singh, "Video Steganography: Text Hiding in Video by LSB Substitution", Int. Journal of Engineering Research and Applications, Vol. 4, Issue 5(Version 1), May 2014, pp.105-108.
[6] S. Suma Christal Mary M.E, "Improved Protection in Video Steganography Used Compressed Video Bitstreams", International Journal on Computer Science and Engineering, Vol. 02, No. 03, 2010, 764-766.
[7]Sherly A P and Amritha P P, "A Compressed Video Steganography using TPVD",International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010.
[8] Prof. D.J.Bonde, ShindeGovind Narayan, SalunkheVaishaliPandharinath,Shete Puja Pandurang and ShindeRupeshTanaji, "Application of Data hiding using Anti-Forensic Technique", International Research Journal of Engineering and Technology (IRJET), Volume: 03, Issue: 03, Mar-2016.