National Journal of Multidisciplinary Research and Development
ISSN: 2455-9040
Impact Factor: RJIF 5.22
www.nationaljournals.com
Volume 3; Issue 1; January 2018; Page No. 965-967

A review of different methodologies for video steganography

Abhishek Saxena[1], Suraj Sharma[2]
[1] M. Tech. Scholar, Department of EC, Institute of Engineering and Technology, Alwar, Rajasthan, India
[2] Associate Professor, Department of EC, Institute of Engineering and Technology, Alwar, Rajasthan, India

Abstract
The Internet is the medium by which it's feasible to transfer information from one place to another place on very high speed. But it is really unsafe to transfer information across the internet. To sustain the privacy and to prevent an unauthorized person from secret information, steganography method is used. Steganography is a method to hide secret data. The secret data can be in the form of text, image, audio and video. These secret type data can be invisible in the text, image, audio and video. Hiding secret data in the video file is called as video steganography. In this paper, review on different video steganography methods is presented.

Keywords: video steganography, data hiding, encryption, PSNR

1. Introduction
At the present time, internet turns better source to transfer data, buying at the Internet, online railway booking, internet based money transfer and so more. But there is the requirement to assure data to avoid the interception by an unofficial hacker. Steganography is the process, which is applied to minimize these type of problem. The better reason for applying steganography is to keep privacy and to prevent it by an unauthorized person. The operation of steganography system is based on two elements- embedding efficiency and embedding payload. Embedding efficiency implies that how much information can be invisible in the cover file. Embedding payload means the capability of steganography scheme to hide maximum information with lower distortion. High embedding efficiency implies lowest distortion in cover file. It is generally difficult for unlicensed users to find the existence of data. Generally, embedding efficiency and embedding load are reciprocally proportional to each other. As we increment the implanting efficiency, embedding payload will decrease. It implies that as increase the capability of secret information it will decrement the quality of stego video.

2. Video steganography system
Few basic conditions which are essential to reading steganography system are given below-

A. **Original Data:** It works as a cover media in which secret information is enclosed.
B. **Secret Message:** It is the information which we're moving to cover in the original information.
C. **Keys:** A key is a value or a number. Embedding process and extraction process are both works on the same key.
D. **Stego Data:** It is the information got after implanting the secret data.

3. Related Work
In video steganography, video signals are utilized to hide secret data. The aim is to hide the heavy amount of secret data into the video files.

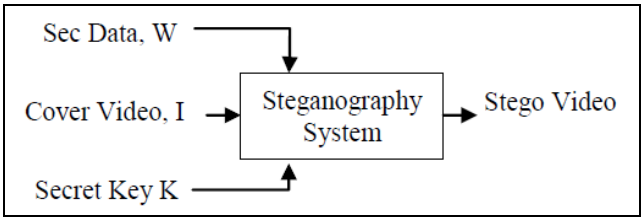

Fig 1: General block diagram of video steganography embedding algorithm

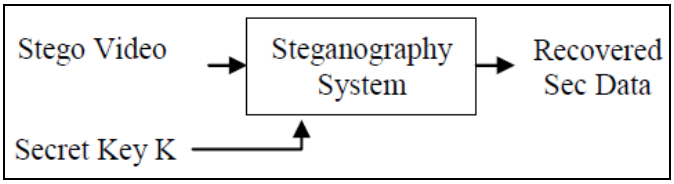

Fig 2: General block diagram of video steganography extraction algorithm

In this process, AVI file is applied as the carrier. Video files carrying audio frequency are divided into video and audio frames. Video frames are in the type of images, and hence image steganography is applied with video frames. As audio is separated or took out from video data file, it is an audio file and audio steganography is applied at audio files. As both audio and video frames applied as the carrier, capability of steganography is raised. The secret information could be image and audio or text. In this process, secret image and audio signals are covered in the video files. The advantage of these techniques are its robustness. It resists processes such as filtering, cropping, rotation and compression. The secret data is not found by the third party, hence the scheme is secure [2].
In 2016, Gopal Krishn Pandey and Mrs. Sameena Zafar gave a stegano graphic method for secure information hiding [3]. In this paper, least significant bit technique is applied for

information hiding. But LSB technique is not safe technique for data hiding. So, in this technique random frame selection method and pixel swapping method is applied to improve safty of this technique. In 2015, Anmol D Kulkarni and his co-operative research worker give a developed data security method, to hold quality of cover image and for decrease the size of video before transmission. In this paper, two stage techniques are applied to plant secret text data into a video clip. First level is image steganography by applying LSB technique. Second level is video steganography applying DCT method. The sizing of the video is modified after embedding technique. So lossless compressing method is applied. Advantages of this technique are increased information security, visual quality of stego video stays same and sizing of the final stego video is decreased for fast transmission.

Table 1: Comparison table for advantages and disadvantages

Author & year	Paper Title	Technique used	Advantage	Disadvantage
Ramadhan J. Mstafa and Khaled M. Elleithy, 2015	A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11)	Superior embedding payload of video steganography method	Visual quality of stego video is great and it can robust against Guassian and Impusive noises.	It is non robust enough against all attacks and LSB technique is open for more attacks.
Hemalatha, S.*, U. Dinesh Acharya and Renuka, A.,2016	High Capacity Video Steganography Technique in Transform Domain	Transform Domain	Robustness i.e. it resist processes like as filtering, cropping, rotation and compression	It does not have various protection parts
GopalKrishnPandey and Mrs. SameenaZafar, 2016	A Secure Data Hiding Technique Using Video Steganography	Combining of cryptology and Steganography.	Random frame choice, pixel swapping and encoding of content has been performed to increase the security.	This arrangement is difficult and output of stego video quality is low.
Anmol D Kulkarni, EstiBansal, Hole Rajashree B, JadhavRasika R, Lakshmi Madhuri, 2015	Improved Data Security Using Video Steganography	This paper suggests a two level operation, first level is image steganography by applying LSB technique and second level is video steganography applying DCT technique.	Increased data security, visual quality of stego video stays same and sizing of the final stego video is decreased for secured transmission.	
Ramadhan J. Mstafa and Khaled M. Elleithy	A Highly Secure Video Steganography using Hamming Code (7, 4)	Good video steganography method based principle of additive block code.	The planting area in all frame is at random chose and it will be the different from another frames to better the robustness.	As the capability of offered scheme increases up to 90 Kbits in every frame with the few degradation of visual quality.
ShyamalaA,and Raghu K,2016	A DWT-BCH code based Video Steganography by employing Variable bit length Algorithm	Variable bit based length methodology.	High PSNR value	
VaishaliB.Bhagat and Prof. Pravin Kulurkar, 2013	A Robust Audio and Video Steganographic Scheme	In this process, added to 4 LSB method are applied for secret information implanting in video file and parity bit encryption method is applied to embed secret data in audio file.	Combination of audio and video steganography makes the system more robust and secure.	
R. ShanthaKumari and Dr. S. Malliga, 2014	Video Steganography Using LSB Matching Revisited Algorithm	LSB Matching Revisited methodology	This technique is studied in conditions of both Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) calculation in between the original and steganographic images for each video frames.	Lack of security and low embedding rate.

In 2016, Shyamala A and Raghu K showed a variable bit length video steganography method [5]. To protect the secret information, it is firstly encrypted by BCH code. Then Discrete Wavelet Transform method is applied for image compression. The advantage of this technique is that it has high PSNR value. In 2015, Ramadhan J. Mstafa offered a high embedding payload of video steganography technique which is established on BCH coding [6]. The quantity of secret information in every video is roughly 6.12 Mbytes. The advantages of this technique are the good quality of stego video and it is robust versus Gaussian and Impulsive noises. Some negative points of this technique are, it is non robust sufficient for all attacks and LSB method is open for many attacks. In 2013, Vaishali B. Bhagat and Prof. Pravin Kulurkar presented a robust based audio and video stegano graphic method [7]. In this technique, 4 Bit LSB technique is applied

for secret information planting in the video file and parity bit encrypting method is applied to plant secret data in the audio file. Combining of audio and video steganography provide the system further robust and secure. In 2014, R. Shantha Kumari and Dr. S. Malliga suggested video steganography applying LSB Matching Revisited (LSBMR) method [8]. LSB Matching Revisited (LSBMR) method takes the planting regions according to the sizing of the secret message and the difference in between two serial pixels of a cover image. For less implanting rates, just sharper edge regions are applied while keeping smoother regions unchanged. In this technique, LSB Matching Revisited technique is applied to plant the secret message into the video. This technique is examined in both cases Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE). Disadvantages of this technique are low embedding rate and security. Ramadhan J. Mstafa and Khaled M. Elleithy suggested a secure video steganography method which is supported the principle of linear block code [9]. In this technique, nine uncompressed video sequences are applied as cover information and binary image logo using as a secret message. The pixel's location of cover videos and a secret message are randomly taped by applying a secret key to better system's security. To further improve the security, the result of the encrypted message will be X or with randomly generated values. Then the secret message is encrypted by using Hamming code (7, 4). The advantage of this technique is, it is robust the embedding area in every frame which is randomly chosen and it will be different from another frame for better the robustness. Security has been filled by more than one key to embed and extract the secret message.

4. Conclusion

The modern development of internet users gets increased the requirement for security of information. Steganography is the method which is applied for the security of information. Video steganography is applied for hiding the secret data (text, image, and video) in the video file. So this paper gives the different methods of video steganography.

5. References

1. Metev SM, Veiko VP. Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
2. KedarNath Choudry1, Aakash Wanjari2, A Survey Paper on Video Steganography.
3. Navdeep Ghotra, Aashdeep Singh, Kamal Gupta. A Review on Various Approaches for Video Digital Steganography.
4. Gopal Krishna Pandey1, Mrs. Sameena Zafar2. A Secure Data Hiding Technique Using Video Steganography.
5. Anmol Kulkarni D, Esti Bansal, Hole Rajashree B, Jadhav Rasika R, Lakshmi Madhuri. Improved Data Security Using Video Steganography.
6. Shyamala A, Raghu K. A DWT-BCH code based Video Steganography by employing Variable bit length Algorithm.
7. Ramadhan Mstafa J, Khaled Elleithy M. A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11).
8. Vaishali Bhagat B, Prof. Pravin Kulurkar. A Robust Audio and Video Steganographic Scheme.
9. Shanthakumari R, Dr. Malliga S. Video Steganography Using LSB Matching Revisited Algorithm.
10. Ramadhan Mstafa J, Khaled Elleithy M. A Highly Secure Video Steganography using Hamming Code (7, 4).