A Review Paper on Video Steganography

Ms. Pratidnya Sapate[1], Ms. Varsha Patil[2], Ms. Mayuri Pardeshi[3], Prof. Arjun Nichal[4]

BE Student, Electronics & Telecommunication Engineering, AITRC, Vita, India[1,2,3]

Assistant Professor, Electronics & Telecommunication Engineering, AITRC, Vita, India[4]

Abstract: Internet is the media due to which it is possible to transfer data from one place to another place with very high speed. But it is very risky to transfer data over internet. Hence to maintain privacy and to prevent an unauthorized person from extracting information steganography technique is used. Steganography is the science of hiding secret information. The secret information is in the form of text, image, audio and video. This secret information can be hidden in the text, image, audio and video. Hiding secret information in video file is called as video steganography. In this paper, review on various video steganography techniques is presented.

Keywords: Video steganography, Data Hiding, Encryption, PSNR

I. INTRODUCTION

This Now days, internet become major source to transfer information, online shopping, online rail reservation, online money transfer, online payment. But there is need to secure information in order to avoid the interception from an unauthorized interceptor. Steganography is the technique which is used to minimize this problem. The major reason for using steganography is to maintain privacy and to prevent an unauthorized person from extracting information. The performance of steganography system is depending on two factors- embedding efficiency and embedding payload.

Embedding efficiency means amount of data can be hidden in the cover file. Embedding payload means capacity of steganography system to hide as much data with less distortion. High embedding efficiency means least distortion in cover file hence it is very difficult to unauthorized users to determine existence of data. Generally, embedding efficiency and embedding payload are inversely proportional to each other. When we increase the embedding efficiency, embedding payload will decrease. That means if we have to increase the capacity of secret data it will decrease the quality of stego video.

II. VIDEO STEGANOGRAPHY SYSTEM

Some common terms which are necessary to understand steganography system are as follows-

Original Data: It act as a cover media in which secret data is embedded.

Secret message: It is the data which we are going to hide in the original data.

Keys: A key is a value or a number. Embedding process and extraction process are both operates on the key.

Stego Data: It is the data obtained after embedding the secret information.

III. RELATED WORK

In video steganography, video signals are used to hide secret information. The objective is to hide large amount of secret data in video files.

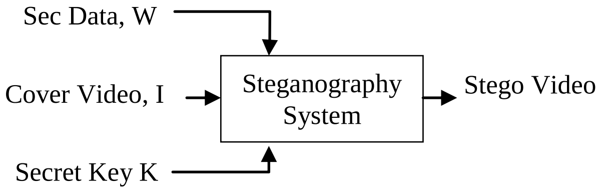

Fig 1. General Block Diagram of Video steganography Embedding algorithm

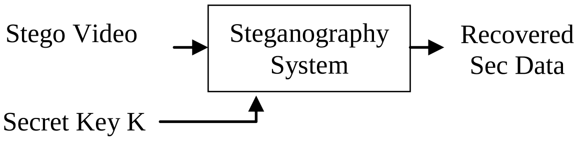

Fig 2. General Block Diagram of Video steganography Extraction algorithm

In this method, AVI file is used as carrier. Video files containing audio are separated into video and audio frames. Video frames are in the form of images, and hence image steganography is used on video frames. When audio is separated from or extracted from video files, it is like an audio file and hence audio steganography is used on audio files. Since both audio and video frames used as carrier, capacity of steganography is increased. The secret data can be image and audio or text. In this method, secret image and audio signals are hidden in the video files. Advantage of this method is its robustness. It resists operations such as filtering, cropping, rotation and compression. The hidden information is not detected by third party, hence the system is secure. [2]

In 2016, Gopal Krishn Pandey and Mrs. Sameena Zafar presented a steganographic algorithm for secure data hiding. [3] In this paper, least significant bit method is used for data hiding. But LSB method is not secure method for data hiding. Therefore, in this method random frame selection algorithm and pixel swapping algorithm is used to improve security of this method.

TABLE I REVIEW OF ALL PAPERS

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)	High embedding payload of video steganography algorithm	Visual quality of stego video is high and it is robust against Guassian and Impusive noises.	It is non robust enough against all attacks and LSB algorithm is susceptible to many 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 operations such as filtering, cropping, rotation and compression	It doesn’t have various protection levels
Gopal Krishn Pandey and Mrs. Sameena Zafar, 2016	A Secure Data Hiding Technique Using Video Steganography	Combination of cryptography and Steganography.	Random frame selection, pixel swapping and encryption of message has been done to enhance the security.	This system is complex as well as output or stego video quality is low.
Anmol D Kulkarni, Esti Bansal, Hole Rajashree B, Jadhav Rasika R, Lakshmi Madhuri, 2015	Improved Data Security Using Video Steganography	This paper proposes a two stage process, first stage is image steganography by using LSB method and second stage is video steganography using DCT algorithm.	Enhanced data security, visual quality of stego video remains unchanged and size of the final stego video is reduced for fast transmission.	----
Ramadhan J. Mstafa and Khaled M. Elleithy	A Highly Secure Video Steganography using Hamming Code (7, 4)	Secure video steganography algorithm based on the principle of linear block code.	The embedding area in each frame is randomly selected and it will be different from other frames to improve the robustness.	When the capacity of proposed scheme increases up to 90 Kbits in each frame with the some degradation of visual quality.
Shyamala A,and Raghu K,2016	A DWT-BCH code based Video Steganography by employing Variable bit length Algorithm	Variable bit length algorithm	High PSNR value	----
Vaishali B.Bhagat and Prof.Pravin Kulurkar,2013	A Robust Audio and Video Steganographic Scheme	In this method, modified 4LSB algorithm is used for secret data embedding in video file and parity bit encoding algorithm is used to embed secret information in audio file.	Combination of audio and video steganography makes the system more robust and secure.	----

DOI 10.17148/IARJSET.2016.31238

R. Shantha Kumari and Dr. S. Malliga, 2014	Video Steganography Using LSB Matching Revisited Algorithm	LSB Matching Revisited Algorithm	This method is analyzed in terms of both Peak Signal to Noise Ratio (PSNR) compared to the original cover video as well as Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames.	Lack of security and low embedding rate

In 2015, Anmol D Kulkarni and his co-operative researcher presented an improved data security algorithm, to maintain quality of cover image and to reduce the size of video brfore transmission. [4]In this paper, two stage processes is used to embed secret text data into a video clip. First stage is image steganography by using LSB method. Second stage is video steganography using DCT algorithm. The size of the video is increased after embedding process hence lossless compression technique is used. Advantages of this method are enhanced data security, visual quality of stego video remains unchanged and size of the final stego video is reduced for fast transmission.

In 2016, Shyamala A and Raghu K presented a variable bit length video steganography algorithm. [5] To protect the secret data, it is first encoded by BCH code. Then Discrete Wavelet Transform technique is used for image compression. Advantage of this method is that it has high PSNR value.

In 2015, Ramadhan J. Mstafa proposed a high embedding payload of video steganography algorithm based on BCH coding.[6] The amount of secret data in each video is approximately 6.12 Mbytes. The advantages of this method are visual quality of stego video is high and it is robust against Gaussian and Impulsive noises. Disadvantages of this method are, it is non robust enough against all attacks and LSB algorithm is susceptible to many attacks.

In 2013, Vaishali B. Bhagat and Prof. Pravin Kulurkar proposed a robust audio and video steganographic scheme.[7] In this method, modified 4LSB algorithm is used for secret data embedding in video file and parity bit encoding algorithm is used to embed secret information in audio file.Combination of audio and video steganography makes the system more robust and secure.

In 2014, R. Shanthakumari and Dr. S. Malliga proposed video steganography using LSB Matching Revisited (LSBMR) algorithm. [8] LSB Matching Revisited (LSBMR) algorithm selects the embedding regions according to the size of secret message and difference between two consecutive pixels in cover image. For lower embedding rates, only sharper edge regions are used while keep smoother regions as they are. In this method, LSB Matching Revisited algorithm is used to embed the secret message into the video. This method is analyzed in terms of both Peak Signal to Noise Ratio (PSNR) as well as Mean Square Error (MSE). Disadvantages of this method are lack ofsecurity and low embedding rate.

Ramadhan J. Mstafa and Khaled M. Elleithy proposed a secure video steganography algorithm based on the principle of linear block code. [9] In this method, nine uncompressed video sequences are used as cover data and binary image logo as a secret message. The pixel's position of both cover videos and a secret message are randomly recorded by using a private key to improve system's security. To improve security, the result of the encoded message will be Xord with random generated values. Then the secret message is encoded by applying Hamming code (7, 4). Advantage of this method is, it is robust i.e. the embedding area in each frame is randomly selected and it will be different from other frames to improve the robustness. Security has been satisfied by having more than one key to embed and extract the secret message.

IV. CONCLUSION

The recent growth of internet users has increased the need for protection of data. Steganography is the technique used for protection of data. Video steganography is used for hiding the secret information (text, image and video) in video file. So this paper presents the various techniques of video steganography.

REFERENCES

[1] S. M. Metev and V. P. Veiko, Laser Assisted Microtechnology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] Kedar Nath 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 Krishn Pandey1, Mrs. Sameena Zafar2,"A Secure Data Hiding Technique Using Video Steganography"

[5] Anmol D Kulkarni, Esti Bansal, Hole Rajashree B, Jadhav Rasika R, Lakshmi Madhuri, "Improved Data Security Using Video Steganography"

DOI 10.17148/IARJSET.2016.31238

[6] Shyamala A,and Raghu K "A DWT-BCH code based Video Steganography by employing Variable bit length Algorithm"

[7] Ramadhan J. Mstafa and Khaled M. Elleithy, "A High Payload Video Steganography Algorithm in DWT Domain Based on BCH Codes (15, 11)"

[8] Vaishali B.Bhagat and Prof.Pravin Kulurkar, "A Robust Audio and Video SteganographicScheme"

[9] R.Shanthakumari and Dr.S. Malliga, "Video Steganography Using LSB Matching Revisited Algorithm"

[10] Ramadhan J. Mstafa and Khaled M. Elleithy, "A Highly Secure Video Steganography using Hamming Code (7, 4)"

BIOGRAPHIES

Ms. Pratidnya Sapate Pursuing her BE in Electronics & Telecommunication from AITRC vita. Her area of interest is Image Processing and Embedded system.

Ms. Varsha Patil Pursuing her BE in Electronics & Telecommunication from AITRC vita. Her area of interest is Image Processing and Embedded system.

Ms. Mayuri Pardeshi Pursuing her BE in Electronics & Telecommunication from AITRC vita. Her area of interest is Image Processing and Embedded system.

Prof. Arjun Nichal Received his M.tech degree from Walchand college of Engg, Sangli in 2012. Pursuing Ph.D. from Shivaji University Kolhapur. Working as a assistant professor in AITRC vita. His area of interest is image processing, embedded system. Published one E- book and 17 international journal papers.

DOI 10.17148/IARJSET.2016.31238