ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

An approach to video steganography using novel substitution technique

Akash Agrawal[1], D. A. Borikar[2]

Research Scholar, Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India [1]

Assistant Professor, Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India [2]

Abstract: The secure communication is very necessary in today's world as various valuable information is shared over the network. So there is a possibility that this information can be hacked by attackers. Therefore to keep the information secure many algorithms of steganography and information hiding have been proposed. But at the same time many powerful steganographic analysis software programs are there which can retrieve the valuable secret information that has been embedded in the carrier files.These steganographic algorithms are detected by steganalytical detectors because of the lack of security and embedding efficiency.So to overcome such issue a secure video steganography technique is propose in this paper which is based on the principle of LSB substitution which cannot be easily detected by steganalytical detectors and also will provide high embedding payload with high embedding efficiency.

Keywords: Video Steganography, LSB Substitution, Cryptography, Hamming code, Digital watermarking.

I. INTRODUCTION

Now a dayhigh speed internet is used by various people for the communication purpose. The important messages are exchanged by various parties over the internet and also their valuable information is shared over it. So to keep the information secure various information hiding techniques are used. In information hiding cryptography is a technique which comes first in mind. Earlier in old days the cryptography was used to keep message secret. Cryptography is the technique of protecting the contents of a message by converting it to some encrypted format using different methods and then decrypted using the decryption methods. Various cryptographic techniques are proposed over the years. But the problem with cryptography is that one can know that a message has been encrypted. So the message can be obtain by the intruder. To overcome such an issue steganography came into existence where the message in hidden in some other medium and communicated.

Steganography is a field related toimage processing and information hiding. Image processing is a form of signal processing having an image as input and output will be an image or a set of characteristics or attributes related to the image. Information hiding is a technique to protect the embedded message against detection and also to prevent the removal of hidden data**.** The key concept behind steganography is that the message to be transmitted is not detectable to the normal eye. One more term related to information hiding is digital watermarking. Digital watermarking is mainly used for the copyright protection of the electronic product [1].

Steganography is a term which comes from the Greek word meaning covered writing [2]. The steganography is defined as the hiding of a message within another medium so that the presence of the hidden message remains unnoticeable. Steganography conceals existence of message in some another medium such as text, audio, image, video. Every medium has its own advantage but image and video steganography are very much effective as they can carry a large amount of data and can keep the data more secure.

In text steganography number of tabs, white spaces, capital letters *etc.* are used to achieve information hiding. In audio steganography audio is taken as a carrier for information hiding. Audio steganography uses digital audio formats such as CIF, Pal, AVI, MPEG etc.for steganography purpose.When the cover object is taken as an image in steganography it is known as image steganography. Normally, in image steganography the focus is on pixel intensities which are used to hide the information. Video Steganography is a technique to hide any kind of files or information into digital video format. Video is nothing but the combination of pictures which is used as carrier for hidden information. Various Substitution techniques such as LSB Substitution etc. can be used to hide the information in each of the images in the video, which is not noticeable by the human visual system. Video steganography uses video formats such as H.264, Mp4, MPEG, AVI etc [3] [4].

The two main factors that every steganography system should look upon are embedding efficiency and embedding payload. The steganography scheme should have a high embedding efficiency which guaranties a good quality of stego data and also ensures that a less amount of carrier data is going to be changed. Any obvious distortion in the stego data will increase the probability of the attacker's suspicion and the secret information can be easily detected by some of the steganalysis tools. These kinds of schemes are difficult to be detected by the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue xx, Xxxxx2014

steganalytical detectors. So the security of the steganography scheme is depending directly on the embedding efficiency. Secondly, the high embedding payload means that host data contain a large capacity of carrying secret information in it. The two factors embedding efficiency and embedding payload have a type of contradiction. Increasing efficiency may cause the capacity of embedding to have a low payload. So such a steganographic system should be designed which have both embedding efficiency and embedding payload.

II. LITERATURE REVIEW

Morkel.T, et.al, [5] have proposed an overview of image steganography, its uses and techniques. The paper attempts to identify the requirements of a good steganographic algorithm and briefly reflect on steganographic techniques that can be more suitable for applications. Author has concluded that all the major image file formats have different methods of hiding messages, with different ability respectively. Author has also specified that if one technique lacks in payload capacity the other lacks in robustness. So there is need of a steganographic system including both payload capacity and robustness.

Nagham Hamid, et.al.[6]Focuses on the use of an image file as a carrier, and they have presented the taxonomy of current stenographic techniques for image files. These techniques are analysed and discussed not only in terms of their ability to hide information in image files but also according to how much information can be hidden, and the ability towards different image processing attacks.

Video steganography [7] is used to hide a secret video stream in cover video stream. Each frame of secret video is broken into individual components and then converted into 8-bit binary values and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. To enhance more security each bit of secret frames is stored in cover frames following a pattern BGRRGBGR. Experimental results show that there is no visual distortion in host video stream and the quality of recovered secret video stream is also acceptable in practical.

An Improved LSB based Steganography technique for images [8] by Manu Devi and Sharma provides better information security for hiding secret information in images. The technique involves improved steganography method for embedding secret message bit in least significant byte of non-adjacent and random pixel locations in edges of images and 1-3-4 LSBs of red, green and blue components of randomly selected pixels across soft areas. The proposed technique ensures that the eavesdroppers will not have any suspicion that message bits are hidden in the image and standard steganography detection methods can not estimate the length of the secret message correctly. The aforesaid work details the use of grayscale bitmaps as cover images.

A secure video steganography algorithm based on the principle of linear block code by Ramadan Mustafa provides a better option for video steganography [9]. In the propose system for cover data nine uncompressed video sequences were used while for secret message a binary image logo was used. The pixel positions of both cover videos and a secret message are randomly chosen by using a private key to improve the system's security. After that the secret message is encoded by applying Hamming code (7, 4) before the embedding process to make the message more secure. The obtained result of the encoded message then is added to random generated values by using XOR function. The message is then embedded into the cover video frames. The embedding area in each frame is randomly selected and it is different from other frames which are applied to improve the robustness of system. In addition, the algorithm also has a high embedding efficiency which is demonstrated by the experimental results. In case of the system's quality, the Pick Signal to Noise Ratio (PSNR) of stego videos are above 51 decibel (db.), which is almost close to the original video quality. In the propose algorithm the embedding payload is also acceptable, which is 16 Kbits of data that can be embed in each video frame and it can go up to 90 Kbits without much degrading of the stego video's quality.

A data hiding scheme by Nadeem Akhtar [10] is based on a module-based substitution method with lossless secret data compression with some improvements to reduce the difference between cover and stego image pixel values. In the scheme user can hide text, image or audio file as secret data in cover image file. The author also involves method such as Modulus and shifting operations with compression logic for hiding secret data. When cover image and secret data is selected for hiding then firstly secret data is processed and then it is hidden in the cover image. Data values lies in the range of 0 to 255 then the scheme convert these decimal values into 8-bit binary numbers then these 8-bits are divided into 4-bits to convert it into nibbles.

An adaptive least significant bit spatial domain embedding method also has been proposed previously [11]. In this method an image pixel ranges from (0-255) is divided and stego-key is generated from it. The private stego-key which is generated has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The demerit of the method is to hide extra bits of signature with hidden message. The method is also modifying the blue color of the RGB color image to provide a better security for information hiding. The proposed method is expected to achieve high embedding capacity and also to provide security of hidden message.

III. PROPOSED WORK

A Video steganographic scheme which uses an uncompressed video stream based on the frames as still images has been proposed. For the data substitution purpose a novel LSB technique is used in which RGB

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue xx, Xxxxx2014

colour scheme is exploited. This scheme can be helpful in embedding large amount of data in host frame. It can also overcome the standard LSB substitution problem of making a heap of colour difference between original and reconstructed image. While for enhancing the security even more the hamming code (7,4) technique is used before embedding the secret data in cover data. This will not let the steganalytical detectors to extract the secret data efficiently. The propose scheme includes two phase; the first will be data embedding phase and second will be data extracting phase. In first phase the stego video along with secret data will be generated. While in Second phase the secret data will be extracted from the stego video.

A. *Data Embedding Phase*

Data embedding is a process of hiding a secret message inside host data by embedding it using different data substitution technique. The purpose of this phase is to create a stego video with almost same quality as original video, so that the existence of secret message inside a stego video should not be suspected. The fig (1) gives the detail explanation of the steps involved while making a stego video. The key will be used while embedding the data the same key will be required for extraction phase also. So this is also one of the security aspect provided in the scheme so that only intended recipient should get the secret message.

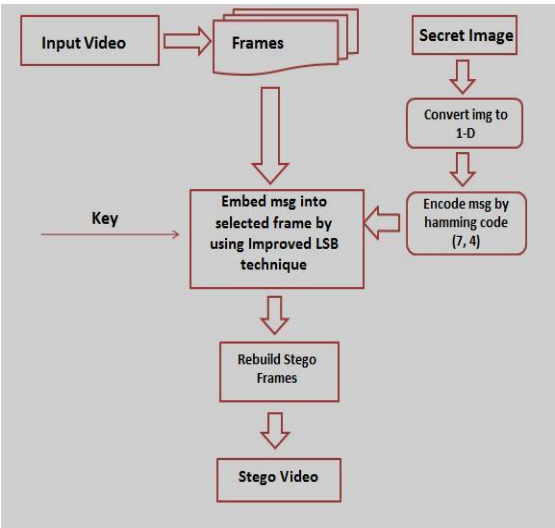

Fig 1: Block Diagram For data embedding phase

B. *Data Extracting Phase*

Data extracting is a process of retrieving the secret message from the stego videos by using the same technique used for embedding reversely. The secret message embedded with video is securely extracted in this phase. The fig (2) gives detail explanation of nearly all the steps used in the scheme for extracting secret image from cover video. The Method used while embedding is used reversely for getting the secret data. The phase should extract the image with almost same quality as an original secret image.

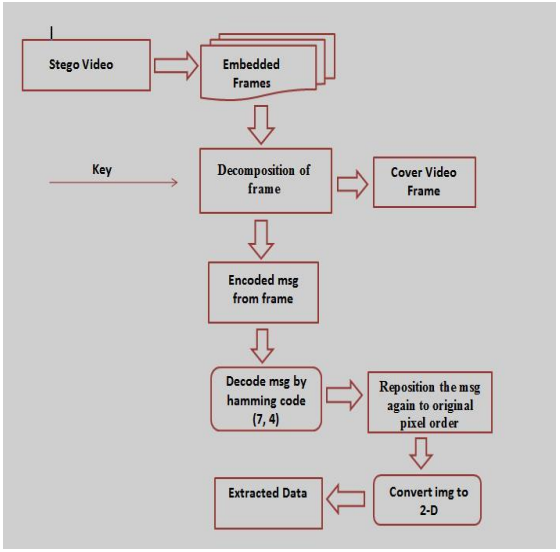

Fig 2: Block Diagram For data extracting phase

IV. CONCLUSION

The paper provides an overview of the existing steganographic system which intends the need of a better system with high embedding payload along with high embedding efficiency. So by studying the existing stenographic system a secure video stenographic system is proposed in this paper which is expected to carry a large amount of secret data and also can retrieve secret image having almost same psnr value as original secret image has.

ACKNOWLEDGMENT

The authors are grateful to the Head, Computer Science and Engineering Department and the Principal, Shri Ramdeobaba College of Engineering and Management for providing adequate facilities to conduct a research. Authors are thankful to the faculty members of Computer Science and Engineering Department for their support and cooperation during this work.

REFERENCES

[1]. Ingemar J. Cox Matthew L. Miller Jeffrey A. Bloom Jessica and Fridrich Ton Kalker, *Digital Watermarking and Steganography* (Second edition) Morgan Kaufmann, 2008.

[2]. Birgit Pfitzmann, Information hiding terminology, *InProceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350,1996.*

[3]. Rakhi and Suresh Gawande, A Review on steganography methods,*International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 10, October 2013.*

[4]. VipulaMadhukarWajgade and Dr. Suresh Kumar, Enhancing Data Security Using Video Steganography, *International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April 2013.*

[5]. Morkel.T, J.H.P. Eloff and M.S. Olivier, An Overview of Image Steganography, *Fifth Annual Information Security South Africa Conference , Sandton, South Africa, 2005.*

[6]. Nagham Hamid, AbidYahya, R. Badlishah Ahmad and Osamah M. Al-Qershi, Image Steganography Techniques: An Overview, *International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : 2012*

[7]. Pooja Yadav, Nishchol Mishra and Sanjeev Sharma, A Secure Video Steganography with Encryption Based on LSB Technique,

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue xx, Xxxxx2014

2013 IEEE International Conference on Computational Intelligence and Computing Research.

[8]. Manu Devi and Nidhi Sharma, Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images, *Engineering and Computational Sciences (RAECS),March 2014 IEEE.*

[9]. Ramadhan J. Mstafa and Khaled M. Elleithy , A Highly Secure Video Steganography using Hamming Code (7, 4) , *Systems, Applications and Technology Conference (LISAT), IEEE 2014.*

[10]. Nadeem Akhtar, AmbreenBano and FarazIslam ,An Improved Module Based Substitution Steganography Method, *International Conference on Communication Systems and Network Technologies IEEE 978-1-4799-3070-8/2014.*

[11]. Y. K. Jain and R. R. Ahirwal, A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys, *International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.*

BIOGRAPHIES

Akash Agrawalearned his B.E degree in computer science and engineering in 2013 from SGBAU Amravati University, Amravati (India). He is a pursuing Masters in Technology in Computer Science and Engineering from Shri Ramdeobaba College of Engineering and Management, Nagpur-440013. His areas of interest include Image Processing, Information hiding.

Dilipkumar A. Borikarearned his B. E. (Computer Technology) degree and M.B.A. (Finance and Marketing) in 1998 and 2001 respectively, from RTM Nagpur University, Nagpur (India). He obtained M. Tech. (Information Technology) from the School of Information Technology, Indian Institute of Technology, Kharagpur, West Bengal, India in 2009. He was awarded with Institute Silver Medal of IIT Kharagpur for 2009.

He has been in academics for over 14 years and is currently working as Assistant Professor in Computer Science and Engineering at Shri Ramdeobaba College of Engineering and Management, Nagpur.

He has published 07 technical papers in international conferences and journals. He is a life member of ISTE, New Delhi. His research interest includes information processing, access control and security, soft computing, image processing, and multidimensional databases.