ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Video Steganography through RC4 Cryptography with Random Sequence of Data Hiding

Sapna

M.Tech Student, Dept. of E.C.E., Seth Jai Parkash Mukand Lal Institute of Engineering and Technology, Radaur, Yamuna Nagar, India.

ABSTRACT: Now a day's security of confidential information is a vital problem due to the rapid development of internet and multimedia technology. Every user demands their data to be delivering to the intended receiver without any interference. Various methods have been investigated and developed from recent time to accomplish the goal of information hiding and to protect the personal data from unauthorized user. Steganography is one of such method .In this paper we propose a video based steganography because of large memory requirement of video. We deal about the concealing of text data in video frames. Before embedding process, secret data is encrypted by using a RC4 cryptographic algorithm and then the encrypted data is embedded in randomly selected frames. For this an index is created for frames to embed encrypted data in random manners and next frames are selected randomly on the basis of random sequence for addition of data. By doing this we achieve security in two terms, first by encrypting the data and second due to random addition of data in frames. The proposed approach increase the security level and make difficult for the attacker to find hidden information from the randomly frames. Security level is very high in randomly addition of data as compare to addition of data in frames in sequential manner. The effectiveness of the proposed method has been estimated by analyzing Mean square error (MSE) Peak Signal to Noise Ratio (PSNR) and image fidelity (IF). Experimental results show that the proposed algorithm provides high security, imperceptibility, very efficient and high capacity.

KEYWORDS: Video steganography, cryptography, data hiding, random sequence, secret communication.

I. INTRODUCTION

There is rapid improvement of the internet and telecommunication techniques in past few years. Computers and information technology (IT) touch nearly every aspects of modern life. With the enhancement in Information Technology, there is also increase in some evil technique like data are attacked and manipulated by unauthorized person. Interference in confidential information is increasing day by day through attacker. To ensure the security of the data, people are paying attention towards the data hiding concept with innovative solutions to protect data from various attack like hacker, cracker, trojan force attack, and others.

Steganography is one of the methods for security of data. Steganography is the art and science of writing hidden messages is such a manner that no one apart from sender and intended recipient can discern the presence of hidden message. Various data formats like image, text, audio, video, and many others can be used as a cover media in steganography. In this paper we are going to discuss about the hiding of text message in video. The advantage of using video file as a cover media because of the large memory of video then image and video is more secure against attacks by unauthorized person due to the complexity of video as compare to image files.

Video steganography is the art of hiding any kind of information like text, image, audio, video and etc in any extension into a carrying video file in ways that avoid the showing of hiding information in videos. The addition of this information to the video is not identifiable by the human as the change of a pixel color is negligible. It is focused on

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

spatial and transform domain. Spatial domain algorithm hides information directly in the cover image with no visual changes and provides good quality. The result of algorithms has the improvement in steganography capacity. Transform domain algorithm embeds the secret message in the transform space. This kind of algorithms has the benefit of excellent stability, but the drawback of small capacity. Video steganography can use for about all digital file formats, but the formats that are more appropriate are those which has a high degree of redundancy. Redundancy can be defined as those bits of an object that provide accurateness far more than necessary for the object's use and display.

The objective of this paper is to develop a Video steganography scheme that can provide more security with high imperceptibility, that embed encrypted secret text messages into video frames in random manners without producing noticeable changes. Additions of data randomly in frames add another layer of security.

II. RELATED WORK

Information hiding is very important in today digitized world. Everyone wants the secrecy and safely delivery of their communicating data. Steganography plays an important role in field of Information Security and it is mainly used to convey messages secretly by hiding the presence of communication. Depending on file formats as cover medium i.e. audio, video, image, and text various steganographic algorithms have been introduced in recent years as possible solutions for the hiding of secret message.

In [1] authors have proposed a method of embedding data into video stream. They have investigated a typical signal path for data embedding. In this security is established by indeterminism within the signal path. In [2] authors have used a spread spectrum image steganography(SSIS). The system hides and recovers a message of substantial length with digital imagery while maintaining the original image size and dynamic range. In [3] new steganography scheme for hiding a piece of critical information in a host binary image (such as facsimiles). A secret key and weight matrix are used to protect the hidden data. In [4] authors have used a pixel value differencing (PVD)method for data embedding in image. This method provides both high embedding capacity and outstanding imperceptibility for the stego-image. In [5] authors have introduced GLM (Gray level modification) technique which is used to map data . It provide one-to-one mapping between the binary data and the selected pixels in an image by modifying the gray level of the image pixels. In [6] authors have proposed a new data-hiding method based on pixel pair matching (PPM). The necessary idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit. This method provides better performance than those of OPAP(optimal pixel adjustment process)and DE(diamond encoding).In [7] authors have used a scheme of data hiding in compressed MPEG video using macroblock ordering multivariate regression and macroblock ordering. The proposed solutions are superior in terms of message payload and cause less distortion and compression overhead. In [8] authors have proposed a schemes which embed the data during the process of MPEG-4compression of video by considering the HVS characteristics. The proposed scheme provides better visual quality and large embedding capacity. In [9] authors have used a DeRand method (data embedding in random domain) based on histogram mapping and high entropy random signal can be utilized for data embedding. In [10] authors have used a enhanced hidden markov model(EHMM) to enhance the speed of embedding and extracting secret data, the proposed method reduce the data hiding time, improve the data retrieval rate and security.

III. PROPOSED METHOD

The proposed method consist of these steps

- Consider a cover video.
- first convert Video into frames.
- encrypt a message using RC4 Cryptographic algorithm.
- Frames are randomly selected.
- embed the encrypted message inside a video frames.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

The aim of the proposed approach to embed the secret message in video frames of the cover video. In this approach we first convert Video into frames and then encrypt a message using RC4 Cryptographic algorithm to enhance the secrecy of the message and then embed the encrypted message inside a video frames. For insertion of message in frames, frames are selected in random manner. In this way secret message is embedded in random manners in frames and frame is selected randomly until all message is hidden. Our research focuses on providing a solution for transferring and sharing important data without any compromise in security.

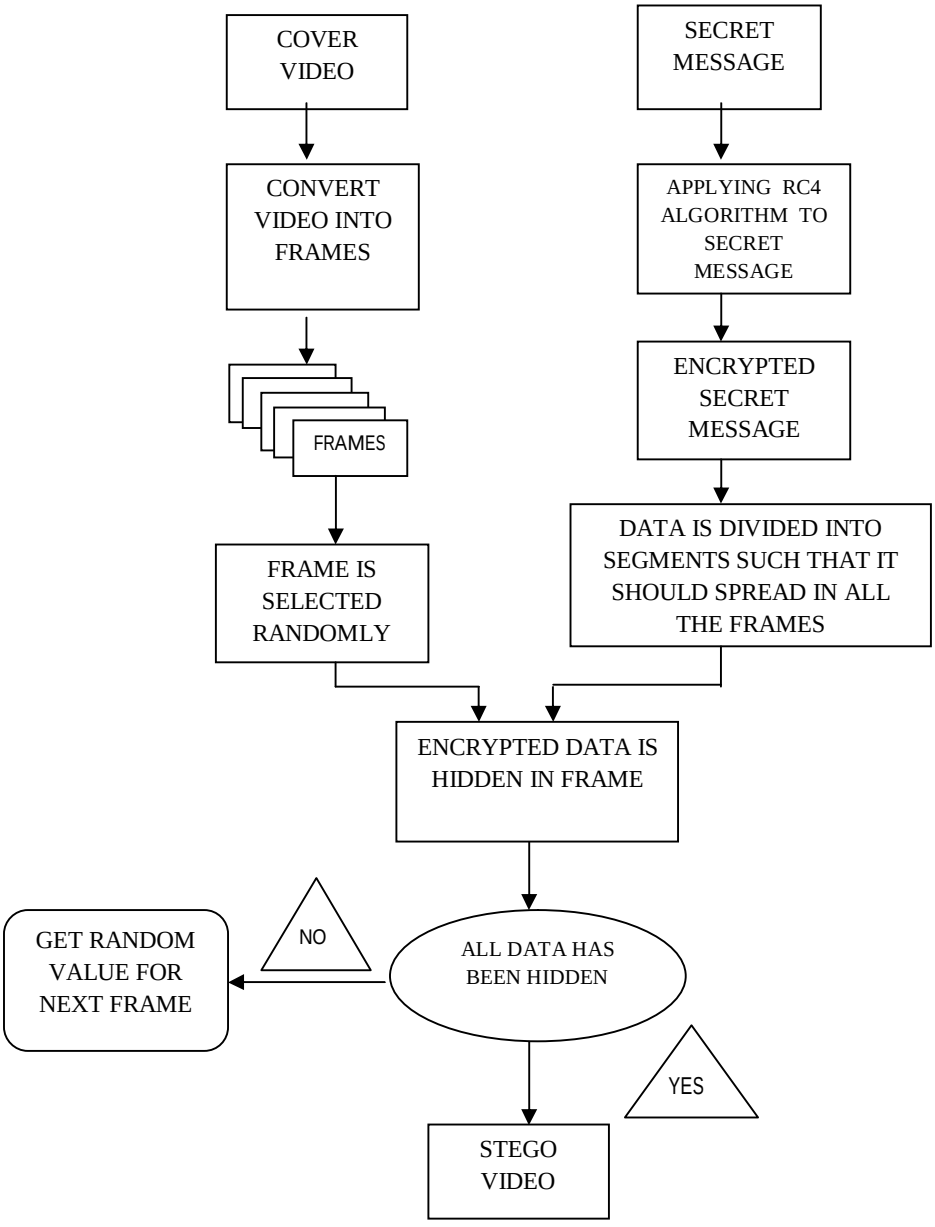

Fig. 4.1 Block diagram of the work

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

IV. EXPERIMENTAL RESULTS

The proposed method is implemented in MATLAB with an objective of better security and lesser detect ability.It is capable of hiding an encrypted text message (by RC4 Algorithm) within video Frames. Frames are selected in random manner for insertion of encrypted message. Then the stego video so formed contains secret information. Thus more security, confidentiality and lesser detect ability is obtained from this work.

The proposed method is compared the PSNR, IF and MSE value between the stego video with random addition of unencrypted data and the stego video with random addition of encrypted data.

To Show this we have computed the PSNR, IF and MSE values of this technique.

- Mean square error (MSE)
  MSE is another important evaluation parameter for measuring the deformation between pixels of stego frame and original frame. It compares the original data and reconstructed data and results the level of distortion. The MSE between the cover frames and stego frame is given by

$$MSE = \frac{1}{H \times W} \sum\sum (P_{(i,j)} - S_{(i,j)})^2$$

Where $P_{(i,j)}$ represents original frame and $S_{(i,j)}$ represents stego frame . H and W are the height and width. MSE value should be low. Lower the MSE means minimum error and stego frame is similar to the original frame. In our result we get the MSE value which is low it means quality of stego frame is high.

- Peak signal to noise ratio
  Peak Signal to Noise Ratio (*PSNR*) has been the most popular tool for measure the quality of the video .The term peak signal-to-noise ratio (PSNR) means the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality. PSNR expressed in decibel it calculation is

$$PSNR = 20 \times \log_{10}\left(\frac{(255 \times 255)}{\sqrt{MSE}}\right)$$

  255 is the maximum possible value of the luminance. The larger the PSNR value higher will be the quality means the stego frame is similar to original frame) and low means the stego frame and original frame have less similarity.

- Image fidelity(IF)
  Image fidelity is used to measure the fidelity. Fidelity means the perceptual similarity between signals before and after processing. IF is expressed as

$$IF = 1 - \frac{\sum\sum (I(i,j) - J(i,j))^2}{\sum (I(i,j))^2}$$

Where i and j are coordinates of the pixel, $I_{(i,j)}$is pixel value of carrier frame and $J_{(i,j)}$ is pixel value of stego frame.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

(a) (b) (c)

Figure 5.1 (a) show the cover video (Akiyo.yuv Video), (b) show the stego video with random addition of unencrypted data, (c) show the stego video with random addition of encrypted data.

(a) (b) (c)

Figure 5.2 (a) show the cover video (Container.yuv Video), (b) show the stego video with random addition of unencrypted data, (c) show the stego video with random addition of encrypted data.

Table 5.1 and 5.2 compare the PSNR, IF and MSE value between the stego video with random addition of unencrypted data and the stego video with random addition of encrypted data.

Table 5.1 Parameters of unencrypted data hidden in cover video in random sequence

Name of the video	PSNR(dB)	IF	MSE
Akiyo.yuv	38.2946	0.99762	9.68897
Container.yuv	36.2644	0.99796	15.1708

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Table 5.2 Parameters of encrypted data hidden in cover video frames in random sequence

Name of the video	PSNR(dB)	IF	MSE
Akiyo.yuv	43.796	0.99912	3.57391
Container.yuv	42.6795	0.99893	7.95696

V. CONCLUSION AND FUTURE WORK

In today digitized world, protection of information in field like military, diplomacy, corporation, medicine and even the individual is of great importance. There is a need of security of information from unauthorized user. Concealing a message with steganography methods decrease the chance of a message not visible for intruders and provide a secure transmission of information from sender to intended receiver. This paper explores a method of hiding text message in video frames. In this paper we have achieved two layer of security, first due to encrypted data and second due to addition of encrypted data in random sequence in frames. With the proposed approach we found that stego video is similar to the cover video. PSNR, MSE, IF value of stego video with random addition of encrypted data is better than the stego video with random addition of unencrypted data and also the parameters of stego video is better than the cover video. In future we can enhance this work by using other more suitable encryption algorithm to encrypt the information and we can embed any kind of information other than text like video, image, audio in cover video. We can hide this kind of information in encrypted video also. These enhancements in work further increase the security level.

REFERENCES

1. Andreas Westfeld and Gritta Wolf,' Steganography in a Video Conferencing System', Springer-Verlag Berlin Heidelberg , LNCS 1525, pp. 32-47, 1998.
2. L. M. Marvel, C. G. Boncelet and C. T. Retter.'Spread spectrum image steganography'. IEEE Transactions on Image Processing, Issue 8, pp.1075–1083, 1999.
3. Y. Tseng, Y. Chen and H. Pan,'A secure data hiding scheme for binary images', IEEE Transactions on Communications, Vol. 50 Issue 8, pp. 1227 -1231, Aug. 2002.
4. Wu. and W.H. Tsai,'A steganographic method for images by pixel value differencing', Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003.
5. Wien Hong and Tung-Shou Chen,'A Novel Data Embedding Method Using Adaptive Pixel Pair Matching', IEEE Transactions on Information Forensics And Security, Vol.7, No.1, pp. 176-184, 2012.
6. Tamer Shanableh,'Data hiding in MPEG video files using Multivariate Regression and Flexible Macrobloc Ordering',IEEE Transaction information forensics and security ,Vol.7, No.2, april 2012.
7. Sagar Gujjunoori, B.B. Amberker,'DCT based reversible data embedding for MPEG-4 video using HVS characteristics', Journal of information security and application Vol. 18, pp. 157-166, 2013.
8. Mustafa s.abdul karim,kokshiek wong,'Data embedding in random domain', computer science and information technology,university of Malaya,Malaysia, 2014.
9. Mritha Ramalingam,nor ashidi mat isa,'Fast retrival of hidden data using enhanced hidden markov model in video steganography',Imaging and intelligent system research team,school of electrical and electronics engineering university sains Malaysia 2015.