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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

A Robust Audio and Video Steganographic Scheme

Vaishali B.Bhagat[1], Prof.Pravin Kulurkar[2]

M.Tech Research Scholar, Department of Computer Science and Engineering, V.I.T, Maharashtra, India[1]

Professor, Department of Computer Science and Engineering, Vidarbha Institute of Technology, Maharashtra, India[2]

ABSTRACT: The recent growth of multimedia systems has increased the need for the protection of digital media. With readily available equipment and software, attacks on digital media are very easy. The issues of security and privacy have traditionally been approached using tools from cryptography and steganography.In this paper, robust audio and video steganographic scheme is introduced which provide high level of security to digital media. 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 audio and video steganography make the system more robust and secure. Quality of cover media is strictly preserved even after secret data embedding.

KEYWORDS: 4LSB,PSNR ,Data embedding, cryptography,Steganography etc

I. INTRODUCTION

In recent years, there has been migration of entertainment and other content from analog format toward digital format like transition from books to pdf and ebook formats, transition from analog tape to CD, MP3 files. In general digital media enhances the increased level of interaction between end users. Digital media also causes extensive vulnerabilities to piracy of copyrighted material.Therefore it is very important to provide high level security to digital media. Data hiding and cryptography are very traditional approaches used by most of the people and organisation to safe the digital content.

Steganography can be informally defined as the practice of undetectably communicating a message in a cover media. Some notable and substantial work has been directed to data hiding method in digital media and other are still being experimented. The first steganalytic method focused on the most common type of hiding called least significant bit embedding in bitmap and GIF images and then directed to most common image format, JPEG and audio files and video files. Varieties of data hiding methods and algorithms have been developed to make steganography more robust and feasible. Recently audio and video steganography are widely used and accepted by many users and being very popul.

In this paper, audio and video steganography are used to make proposed system more robust and secure. Audio steganography is art of hiding information in audio signals in such way that existence of secret data may not be revealed easily. Video Steganography is increasingly popular because unlimited information can be hidden inside the video frames.Video steganography help to overcome the drawback of image steganography where only limited amount data can be embedded behind cover image. Secret data may be text, image, video, audio, multimedia files. All this techniques or methods are renowned and widely used in military applications and scientific research where most of the data kept confidential and secretly transfer to other party.

II. RELATED WORK

The paper address a number of fundamental issues of data hiding in image and video and propose general solutions to them and begin with a review of two major types of embedding and study the issues of hiding multiple bits through a comparison of various modulation and multiplexing techniques. This paper propose an adaptive solution switching between using constant embedding rate with shuffling and using variable embedding rate with embedded control bits[1]. The paper proposed least significant bit (4LSB) substitution method for color bitmap images (24 bit and 8 bit i.e. 256 color palette images) and wave files as the carrier media [2]. The paper explored a new 4th bit rate LSB audio

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Steganography method that reduces embedding distortion of the host audio [3] Author have proposed new Real time Compressed video secure Steganography (CVSS) algorithm using video bit stream. In this, embedding and detection operations are both executed entirely in the compressed. The proposed algorithm increases the security because the statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity [4].Author have proposed a data hiding and extraction procedure for AVI (Audio Video Interleave) videos embedding the secret message bits in DCT higher order coefficients. The secret information taken here is an grayscale image pixel values. The greyscale pixel values are converted to binary values and embedded those values in higher order coefficient value of DCT of AVI video frames [5]. Authors have proposed an efficient method of audio steganography by modified LSB algorithm and strong encryption key with enhanced security is proposed. Enhanced Audio Steganography (EAS) is a combination of audio Steganography and cryptography. EAS proceeds in two steps: it uses most powerful encryption algorithm in the first level and in the second level it uses a modified LSB (Least Significant Bit) algorithm to embed the message into audio [6].

III. PROPOSED METHOD

The main goal of proposed work is to provide multilayer security to information that convey on the internet. This paper introduces the new modified 4LSB algorithm for hiding secret information behind audio of video file. This will be helpful for hiding large amount of information behind the cover media which will enhances the hiding capacity of cover media. This system also combines audio and video steganography together to provide more secure and robust system which can be able to withstand against different types of attack. The proposed work is planned to be carried out in the following manner. In the sender side(Fig.1.a), Audio-video file is selected from available multimedia file to hide secret data that user want. Selected multimedia file is then separated using Simulink software. This software is used to extract the audio part from video file and save both part in different folder with proper extension. System asks the user to enter the passkey which will help to extract frame from the video file. As we know, video is nothing but collection of frames. Frame is nothing but image. Now user will select the secret image which he wants to hide. Secret image is then embedded into extracted frame of video file using modified 4LSB algorithm. Then stego frame is then inserted into video file. System again asks the user to enter passkey to extract the audio segment from audio file. User will select Authentication image for identity purpose. This image will be verified at receiver end to reveal the identity of sender. This image is embedded into extracted audio segment of audio part using parity bit encoding algorithm.Hence; stego audio segment is obtained which will be inserted into audio signal to get audio part. Audio-video combiner is then combined both stego audio and stego video file. Hence stego audio-video file is reconstructed at the sender end.

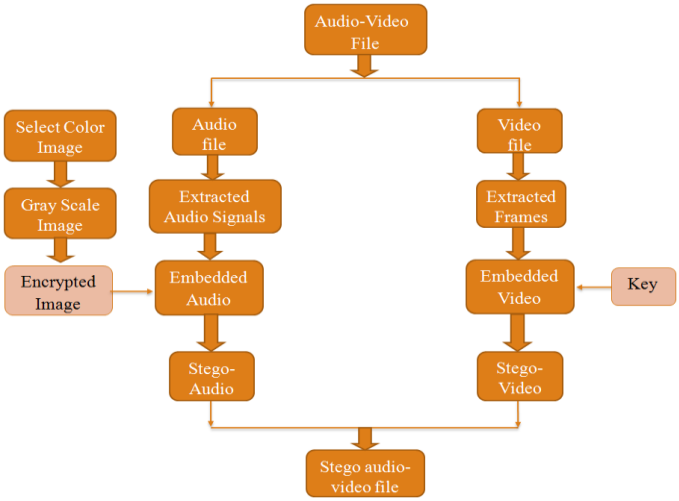

Fig.1.a At transmitter Side

On the receiver side (Fig.1.b),Stego audio–video file is separated using separator. Embedded audio file is selected to extract the authentication image. Receiver also choose the authentication image and system try to match it. If

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

match found, then only receiver will able to extract the secret image from video file. Secret images are compared before embedding and after embedding.

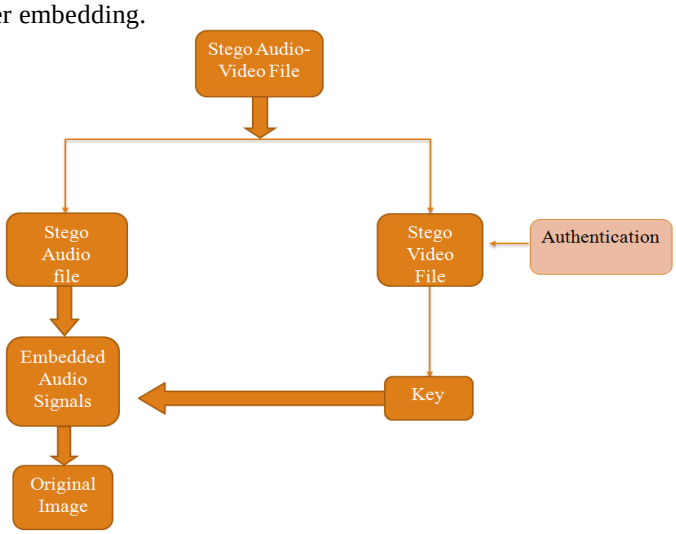

Fig.1.b At Receiver Side

IV. RESEARCH METHODOLOGY

a. 4LSB modification Algorithm:

In this proposed work, masking technique is used to vacant the last four bit position of cover media (here video file) as well as secret message. Fixed mask value is used for this purpose. XOR operation is performed on both last 4 LSB of cover media and mask value. This process will vacant the space for further data embedding. Same operation is also performed with secret image and mask value. But before doing this, last 4LSB of secret image is embedded inside the other cover frame. Then extract the MSB of cover media as well as MSB of secret Image respectively.MSB of Secret message or image is embedded into LSB of cover media.

Stego video file is obtained at the end. In this way, none of the bit of secret image is lost. The advantage of 4LSB algorithm is large amount of data can be kept inside the cover media and secretly transmitted .It means that it enhances the hiding capacity of cover media.

B.Parity Bit encoding Algorithm:

Parity coding is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit.

V. EXPERIMENTAL RESULTS

The main advantage of this system is that quality of stego audio video file may not be compromised even after embedding and mixing the secret information.The proposed algorithm is implemented with MATLAB. Fig.6 (a) was used as cover image and Fig.7 (a) shows stego image.Fig.8 (a) shows original audio and watermarked audio after embedding secret image.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Fig. 6(a): Cover image (grayscale)

Fig.7(a): Stego image (for n =4)

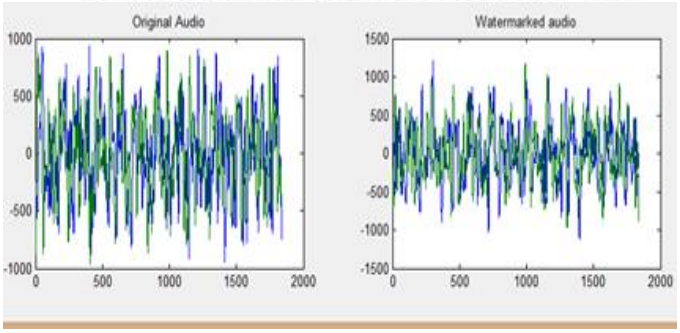

Fig.8 (a) Original audio and Watermarked audio

VI. CONCLUSION

To overcome the drawback of limited amount of secret data hiding and weak security in the widely used steganographic system, this paper presents a new method and algorithm. Experimental analysis demonstrates that the 4LSB algorithm enhances the hiding capacity of cover media, while maintaining acceptable image quality.

ACKNOWLEDGEMENT

The author would like to thank the guide for his valuable suggestions, feedback who always support for writing this paper.

REFERENCES

[1] Min Wu, Liu B. "**Data hiding in image and video .I. Fundamental issues and solutions";** presented at IEEE Transactions on Image Processing, 2003, pp.685-695.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

[2]" Data Security Using Data Hiding" Moon, S.K. ; Kawitkar, R.S. Conference on Computational Intelligence and Multimedia Applications, 2007. International Conference on Volume:4,DOI: 10.1109/ICCIMA.2007.163 Publication Year: 2007, Page(s): 247 -251
[3]Ajay.B.Gadicha, **"Audio wave Steganography",** International Journal of Soft Computing and Engineering (IJSCE), Vol. 1, pp. 174-177, Nov. 2011.
[4]S. Suma Christal Mary, "Improved Protection in Video Steganopgraphy Used Compressed Video Bitstream", International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766, ISSN: 0975-3397
[5] Thakur V. Saikia M.." **Hiding secret image in video** "Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on 1-2 March 2013 IEEE,pp150 – 153.Reference3
[6]R Sridevi, Dr. A Damodaram and Dr.Svl. Narasimham, "Efficient Method of Audio Steganography by Modified LSB Algorithm and Strong Encryption Key with Enhanced Security", Journal of Theoretical and Applied Information Technology, pp. 771-778, 2009.
[7] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb **"A Secure Covert Communication Model Based on Video Steganography,"** in Military Communications Conference, 2008. MILCOM. IEEE on 16-19 Nov. 2008.
[8] Cheng-Hung Chuang and Guo-Shiang Lin, **"An Optical Video Cryptosystem with Adaptive Steganography",** Proceedings of International Association for Pattern Recognition (IAPR) Conference on Machine Vision Applications (MVA'09), pp. 439-442, Keio University, Yokohama, Japan, May 20-22, 2009. (NSC97-2221-E-468-006)

BIOGRAPHY

Ms.V.Bhagat received the B.E degree in Information Technology from Nagpur University, Maharashtra, India in 2008 and pursuing M.Tech(CSE).Her current interest is Cryptography and Network Security ,Visual Cryptography and Digital Image processing.She is member of IAENG,ISTE.

Prof.P.Kulurkar received the M.Tech degree in Computer Science and Engineering from RGPV University,India.He is working as a Professor and HOD in the Department of computer science and engineering at Vidarbha Institute of Technology, Nagpur University, India. His current interest is Network security and data mining.