International Journal of Research (IJR) Vol-1, Issue-9, October 2014 **ISSN 2348-6848**

Survey on Information Hiding in Audio and Video File

Vaishali Bhagat[1*],Prof.P.Kulurkar[2]

[1]*M.Tech Research Scholar,Department of Computer Science and engineering, VIT, Nagpur University,Maharashtra,India*

[2]*Professor,Department of Computer Science and engineering, VIT, Nagpur University,Maharashtra,India*

**E-mail: bhagat.vaishali14@yahoo.in, pkulurkar@gmail.com*

Abstract:

Demand of security is increasing day by day as internet and communication technology advances.Security is provided to data through steganography and cryptography Steganography is popular method of hiding information in cover media.In cryptography,encryption process is carried out to produce cipher text.This cipher text is easily detected by intruder because it attract them more.so steganography methods are widely used by many people to sent their confidential data over internet.Nowdays cryptography and steganography method are combined together to provide higher level of security to data.We explained various methods of steganography and make brief survey on it.

Keywords:

Cover image; Data hiding; Stego image; 4LSB; PSNR; Error correction code; encryption

Introduction

Due to rapid development of information and communication technologies,most of the people frequently transmit their valuable data over internet.Internet is very vulnerable to interception by unauthorized person over the world.Nowdays most of the scientist and researcher are trying to develop the techniques and methods to reduce the detection of information convey on internet.Hence,data hiding in digital multimedia object are gaining more popularity.Various techniques have been implemented for hiding information behind the digital media are steganography and cryptography.Digital media may be images,audio,video,text.Steganography is a technique that facilitates hiding of message that is to be kept secret inside other message.This result in the concealment of the secret message itself.Historically,the sender used methods such as invisible link,tiny pin punctures on specific charactes,minute variartions between handwritten characters,pencils marks on handwritten characters,etc.There are various types of steganography used by

many people to send their secret data over communication network.Recently most of the work has focuses on developing different methods and techniques for audio and video steganography.Audio steganography is one of the process of hiding data in audio signals in such way that unauthorized persons are not aware of the existence of secret data.Video Steganography is one of the type of steganography through which secure data transmission is possible.In this type,secret data is hided behind the one of the frame of video.With the help of video steganography,large amount of data is hidden.It automatically overcome the problem of image steganography where only limited data can be embedded.In image steganography,data is hidden inside the image.Secret data may be text,image.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.

Audio and Video Steganography Data Hiding Methods

Data hiding technique in video is very similar to data hiding technique in images.So we are giving brief overview of them.

1.LSB Modification:-

It is one of the popular and simple method of data hiding in video files.Cover image is used to hide the secret message.This method mainly uses bit of each pixel in image.Main disadvantage of this method is secret data gets lost after the few transformation so lossless compression formats need to used to overcome such type of problems.

2.Masking and filtering:-

This technique is specially used for 24 bit and gray scale images to hide secret message.Masking technique make changes in visible properties of images.This changes can not be noticeable by human eyes.Secret data is hidden in visible part of image rather than noise level.This method is more robust than LSB modification method.

3.Transformation:-

Transformation methods are widely used in watermarking technology and has become more and more popular in audio communication.The basic idea is that secret information can be hidden in most important part of carrier.Thus,as long as attacker do not excessively destroy the carrier,Hence hidden information can be preserved.Commonly used methods are Discrete Fourier Transform (DFT),Discrete Cosine Transform(DCT),Hadmard transform,Wavelet Transform,Modular complex lapped transform(MCLT) methods.This methods embed secret information into coefficient of frequency domain.With the help of this methods,transperancy and robustness are improved and they also used filtering technology to eliminate high frequency noise included by hiding process.For hiding data in video,DCT method is widely used.In this method,some part of the image is altered in such way that human eyes can not detect it.It alter the part of image values,it usually round them up.

Audio steganography Methods

1.Low Bit Encoding Method:It is one of the simplest way to embed secret information by replacing the minimum weight value sampled speech signal into binary bits of secret information data,secret information can be hidden in speech.To increase the detection difficult of secret data,psedorandom sequence can be used to control the location into which secret binary information is going to be hidden.Noise addition and lossy compression of stego audio will very likely destroy the data.so attacker can easily uncover the message by just emoving entire LSB plane.To improve the robustness of LSB method against distortion and noise addition,depth of embedding layer need to be increases from 4^{th} to 6^{th} layer without affecting the perceptual transperancy of stego audio.

2.Echo hiding:-It embed data into audio signal just by introducing short echo into host signal.It has good transparency,usually it is still able to restore hidden information after being attacked.

3.Phase hiding method:-In this method ,absolute phases of speech information should be replaced by reference phases which represent secret information.To ensure fixed relative phase between signals,all subsequent signal changes the absolute phase at the same time.In the receiving end,phase detection is done according to synchronization mechanism.To improve the accuracy of information extraction,phase offset can be set at $\pi/2$.When we compared with LSB method,phase hiding method hide smaller amount of data,but it has ability to fight against noise attack.

4.Spread Spectrum method:- The basic spread spectrum technique is designed to encode a stream of information by spreading the encoded data across as much of the frequency spectrum as possible. This allows the signal reception, even if there is interference on some frequencies

Brief Literature Survey

A lot of research work has been carried out on audio and video steganography which concentrate on secret data hiding in audio and video file without image distortion.

Xiaoxiao Dong, et al[7] have presented two new phase coding methods for hiding data in audio Files. In this methods,upto 20kbits of data are to be embedded in uncompressed or compressed audio files per minutes. In this technique the phase of chosen components of the host audio signal is manipulated in a way that may be detected by a receiver with the proper “key”. Without the key, the hidden data is undetectable, both aurally and via blind digital signal processing attacks. It can be applied to both analog an digital audio signals.This method provide good audio quality and robustness.

Sutanoe,et[5] have developed an interesting application of steganography and cryptography where a secret file embedded into an image file using random LSB insertion method. Before embedding data into image file,data is first encoded.In their method, the secret data are randomly

spread over the cover file.Pseudorandom numbers are generated using key and this key is used to find out order of hidden message and location of secret data.This method withstand different attacks and very strong and secure.

A.Mane,et al[22] developed the new method of audio steganography in which speech signal is embedded inside music file by replacing LSB of each sample of carrier signal with message bit.LSB replacement method is used to do it.They have used secret key concept to provide security to message.Before embedding speech signal into music file,password(secret key)is used by sender.This key is shared between sender and receiver.At reception end,receiver have to enter the same password to extract the speech signal from music file.LSB replacement method is found to be more secure.

Padmashree G,Venugopala P[8] proposed a novel method where secret message is embedded at 4^{th} bit and 5^{th} bit LSB of original audio file.In this paper RSA algorithm is used for encrypting text file and for secret data insertion in cover media,LSB algorithm is used.Experimental result shows that the SNR and PSNR values reduces as the file size increases.

Budda Lavanya,et al[6]have propsed a novel image steganography method to hide data in audio signals.In this method,text data is first hided behind the image and this stego image is then embedded in audio signals.Audio file is read bit by bit and kept in another file.First 50^{th} byte are left untouched and embedding procedure is started from 51th byte and every alternate sample has been modified to hide textual information.As a result,LSB of audio file has been successfully modified without degrading the sound quality.

Kamalpreet Kaur and Deepankar Verma[4] have proposed a new method for audio steganography where three secret messages are hidden behind the audio file.In this scheme,multilevel security is provided to data with layering approach in which first secret message is embedded at first layer using LSB technique and produce the stego file which is served as input to next level.At second level parity coding technique is used to hide secret message.Output of this step is given to third step where third message is hided under decoy object using phase coding technique.Hence stego object is very difficult to decode.

DP Gaikwad,et[11]discussed the new scheme where variable size secret data is embedded into video file.Camparison is made between size of secret file and cover media.Message is compressed using LZW compression algorithms if it is bigger than length of cover file.Compressed secret message is embedded inside the cover file using LSB method and produce the Stego image.Authentication is also provided by supplying user credential to system.This method is only for AVI video formats.

Chantana C,Karnkanak C,Jitdamrang P proposed a method in which image is hidden behind the video file.This method is based on wavelet transform.Main goal is to

hide image pixels in the coefficient of frames.So video frames are transformed and then proper positions of the coefficient are selected to hide the secret image.Then comparision is made between the coefficient of each frame and coefficient of secret image.Similar coefficient are selected to hide image pixels.But coefficient values are not exactly same.This paper is mainly focuses on the frequency domain,for that two common techniques are used:Wavelet transform and DCT transform.

Linu Babu,et al[12] discussed a scheme where secret data is hidden in preprocessed sound wave using LSB technique.In this scheme,some sort of preprocessing method such as scaling is applied on sound wave cover media,so it take the shape of an colored RGB cover image in which secret data is hidden. LSB and DCT method is used to hide secret data in audio signal and improve the PSNR ratio at some extent.Authors had successfully retrieved the hidden secret data with minimum distortion.

Mashallah,A.Dezfouli,et[16]proposed a new image steganography method which make secret message detection nearly impossible for intruder.In this scheme,image is read from top to bottom and left to right pixel by pixel.Six MSB(Most Significant Bit) are selected from each channel in pixels and then compare with neighbouring pixel.if difference is higher than those color pixel is used to embed the data in two least significant bits.But changes made in second least significant bit causes grater changes in the color pixel values.Hence quality of image is distorted.

M Abhilash Reddy,et al[9]presented a method in which image is hidden inside the video frames.Author have discussed the new compressed domain steganography.Embedding secret data and hidden data detection is completely done in compressed domain.DWT(Discrete Wavelet Transform) and LSB technique is used to hide data in specific location of selected frame and last bit of original pixel value of selected region is replaced with secret data.Data is embedded in secret frame and this stego frame is inserted in the place of cover frame and finally video is reconstructed.

A. Hamsathvani[21]has developed hybrid image hiding scheme to hide image in selected video sequence.He discussed the DWT and singular value decomposition technique.In this scheme image is divided into several subbands and secret image is embedded in singular values of cover media.SVD(Singular Value Decomposition) algorithm is applied on the cover image and then modify singular values to embed the watermark.Video is taken as input and perform some preprocessing to select video frame and then calculate MSE of each frame.Frame having low MSE is mainly selected for embedding watermark.

Yadav P,et al[10] discussed a new video steganography method in which secret video stream is hidden in cover video stream.Secret video is divided into number of frame and each frame is broken into individual component.This component is converted into 8 bit binary values and encrypt it.This encrypted value is XORed with secret key and produce encrypted

frame.Encrypted frame is hidden in least significant bit of cover video using sequential encoding method.Experimental result shows that it has better performance than traditional steganography method

H. Gupta,Dr. S.Chaturvedi[15]poposed a video data embedding scheme in which secret information is hidden in gray scale image.This scheme is specially used for AVI video.One or two or three LSB of each pixel is replaced in video frame.After hiding data inside the video,video are converted into 20 equal gray scale image and transmitted over the network.Hence intruder is not able to detect image in video frame.

V.Thakur ,M.Saikia [13] developed a new data hiding and extraction procedure for AVI(Audio Video Interleave).The gray scale pixels values are converted to binary values and this values are then embedded in higher order coefficient value of DCT of AVI video frames.Hence intruder can not able to unhide the image.High level of security is maintained during data transmission.

Zhexing Qian,et al[14] proposed a new framework of reversible data hiding in an encrypted JPEG bitstream.The original JPEG bitstream is properly encrypted to hide the image content with the bitstream structure.The secret message bits are encoded with error correcting code and embedded into encrypted bitstream .With the help of encryption and embedding keys,original image can be approximately recovered with good quality at receiver side.In the absence of embedding key,receiver can recovered the image without extracting the hidden data.Experimental result show that it has perfect image reconstruction and data extraction ability.

Conclusion

In this paper,we discussed about various data hiding methods and techniques in audio and video files used in previous research work.We also discussed the merits and finding of methods. Based on our study,we will suggest more secure framework with combined features of cryptography and steganography for hiding data in audio and video files.

Acknowledgement

The authors would like to thank the guide and parents for their valuable support and suggestion,feedback who always support for writing this paper.We also like to thank all the authors of reference papers.

References

[1]F.A.P. Petitcolas, R. J. Anderson, and M. G. Kuhn —Information hiding A survey,|| Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul.1999.

[2]Hide & Seek: An Introduction to Steganography:Niels Provos and Peter Honeyman, IEEE Security & Privacy Magazine,May/June 2003.

[3]Exploring Steganography: Seeing the Unseen Neil F. Johnson, Sushil Jajodia,

George Mason University IEEE Computer, February 1998:26-3

[4]Kamalpreet Kaur,Deepankar Verma" Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014

[5]Sutaone,M.S.,Khandare,M.V."Image based steganography using LSB insertion technique",IEEE WMMN,pp.146-151,January 2008.

[6] Budda Lavanya, Yangala Smruthi,Srinivasa Rao Elisala." Data hiding in audio by using image steganography technique"IJETTCS Volume 2, Issue 6, November – December 2013.

[7] Xiaoxiao Dong, Mark F. Bocko, Zeljko Ignjatovic" DATA HIDING VIA PHASE MANIPULATION OF AUDIO SIGNALS" IEEE ICASSP 2004.

[8] Padmashree G,Venugopala P S,"Audio steganography and cryptography:Using LSB algorithm at 4th and 5th LSB layers",International Journal of Engineering and Innovative Technology(IJEIT),volume 2,Issue 4,Octomber 2012,pg no 177-181.

[9] M Abhilash Reddy,P.Sanjeeva Reddy" DWT AND LSB ALGORITHM BASED IMAGE HIDING IN A VIDEO" [IJESAT] [International Journal of Engineering Science & Advanced Technology] Volume-3, Issue-4, 170-175

[10] Yadav P,Mishra N, Sharma S. "A secure video steganography with encryption based on LSB technique" Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on DOI: 10.1109/ICCIC.2013.6724212,Publication Year: 2013 , pp: 1 - 5

[11]Prof.D P Gaikwad,Trupti Jagdale,Swati Dhanorkar,Abhijit Moghe,Akash Pathak,"Hiding the text an image message odf variable size using encryption and compression algorithm in video steganography"IJERA,vol.1Issue 2,pp.102-108.

[12]Linu Babu,Jais John s,Parameshachari B D,Muruganantham C,H S DivakaraMurthy "Steganographic method for data hidng in audio signas with LSB and DCT"IJCSMS,volume 2 Issue 8,August-2013,pg no 54-62.

[13]Thakur V.Saikia M."Hiding secret image in video"Inteligent Systems and Signal Processing(ISSP),2013 International Conference on 1-2 march 2013 IEEE,pp150-153

[14] Zhenxing Qian,Xinpeng Zhang and Shouzhong Wang"Reversible data hiding in encrypted JPEG bitstream" IEEE transcation on multimedia ,Vol.16 no 5,August 2014,pp1486-1491.

[15] H. Gupta,Dr. Setu Chaturvedi" Video Data Hiding Through LSB Substitution Technique" Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 32-39

[16] Mashallah Abbasi Dezfouli, Sajad Nikseresht and Seyed.Enayatallah Alavi "A New Image Steganography Method Based on Pixel Neighbors and 6 Most Significant Bit(MSB) Compare" ACSIJ Advances in

Computer Science: an International Journal, Vol. 2, Issue 5, No.6 , November 2013

[17]D.-Y. Fang and L.-W. Chang, —Data hiding for digital video with phase of motion vector,|| in Proc. Int. Symp. Circuits and Systems (ISCAS), 2006, pp. 1422–1425.

[18]He and Z. Luo, —A novel steganographic algorithm based on the motion vector phase,|| in Proc. Int. Conf. Comp. Sc. and Software Eng., 2008, pp. 822–825.

[19]Budhia, U.; Kundur, D.; Zourntos, T.; , "Digital VideoSteganalysis Exploiting Statistical Visibility in the Temporal Domain," Information Forensics and Security,IEEE Transactions on , vol.1, no.4, pp.502-516, Dec.2006

[20] Manikopoulos, C.; Yun-Qing Shi; Sui Song; ZhengZhang; Zhicheng Ni; Dekun Zou; , "Detection of block DCT-based steganography in gray-scale images,"Multimedia Signal Processing, 2002 IEEE Workshop on, vol., no., pp. 355- 358, 9-11 Dec. 2002

[21] A. Hamsathvani" Image Hiding in Video Sequence Based On MSE" IJECSE,Volume1,Number 3,ISSN 2277-1956/V1N3-1489-1493.

[22] Ashwini Mane., Gajanan Galshetwar., Amutha Jeyakumar" DATA HIDING TECHNIQUE: AUDIO STEGANOGRAPHYUSING LSB TECHNIQUE" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012,pp.1123-1125

About Authors

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.

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.