INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

AUDIO AND VIDEO STEGANOGRAPHY: USING LSB AND PHASE ENCODING ALGORITHM

VAISHALI B. BHAGAT[1], PROF. P. N. KULURKAR[2]

1. M. Tech Student, CSE, Vidarbha Institute of Technology, Nagpur, India
2. Professor, Computer Science And Engineering Department, Vidarbha Institute of Technology, Nagpur, India

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Electronic communication is increasingly susceptible to eavesdropping and malicious interventions. The issues of security and privacy have traditionally been approached using tools from cryptography and steganography. Steganography can be feasible alternative to cryptography in various countries where usage of encryption is illegal. In this paper, a novel scheme of data hiding is introduced which provide high level of security to digital media.4LSB and phase encoding algorithm are used for data embedding in video and audio files respectively. Quality of video file is strictly preserved even after secret data embedding. Experimental results have demonstrated the feasibility and efficiency of the proposed work.

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

Corresponding Author: MS. VAISHALI B. BHAGAT

Access Online On:

www.ijpret.com

How to Cite This Article:

Vaishali B. Bhagat, IJPRET, 2015; Volume 3 (9): 1640-1648

PAPER-QR CODE

INTRODUCTION

Internet had become user friendly after the invention of web browser and it quickly became clear that people wanted to download pictures, music; video. We can say that internet is an excellent distribution system for digital media because it is inexpensive, easily eliminate warehousing. Hence content owner see high risk of piracy. High capacity recording devices are used by pirates. They can easily record and distribute copyright protected material without appropriate compensation being paid to actual copyright owner. Thus, Content owner are eagerly seeking technologies that promised to protect their rights. Interest in steganography increased significantly after the terrorist attacks on september11, 2001, when it became clear that means of concealing the communication itself are likely to be used by criminal activities.

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 popular. 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.

2.0 OBJECTIVE & SCOPE OF WORK:-

The objective of this paper 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 combine audio and video steganography together to provide more secure and robust system which can be able to withstand against different types of attack.

3.0 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. K. A. Navas**,** et al[7] have developed new algorithm for data embedding in AVI videos. Two different phases are used to employ this method in cover video. In first phase, self generating keys are used to embed data in cover video. Image is encrypted and then embedded into video in spatial and transform domains in second phase. This method requires high resolution digital video as a cover media. This method has ability to hide significant quality of information but it require large payload. 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 random 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. Shakir, et al[22] discussed the new method of audio steganography in which digital media can be securely transmitted over public network using internet as a distribution medium. Author has suggested new technique for hiding ciphered message into digital color bitmap image. Experimental result demonstrates that conjunction between steganography and cryptography produce immune information.Budda Lavanya,et al[6]have proposed 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 50th bytes 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. Nabin Ghoshal and Deepankar Pal[4] have proposed a new steganography method which promises to provide maximum secrecy, high capacity and robustness against many of the attacks. This method works in time domain and utilizes the uncompressed digital audio signal as cover media and embeds multiple payload bit at pseudo random position. This technique can be withstood against white noise and collusion attack. 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.

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 cannot able to unhide the image. High level of security is maintained during data transmission. 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. 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 sub bands 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.

4.0 PROPOSED SYSTEM

In the sender side, Audio-video file is selected to hide secret data and file is then separated using separator. Thus audio and video files are obtained. Secret image is then embedded into video file using 4LSB algorithm. Authentication image is embedded into audio file using phase encoding algorithm. Audio-video combiner is then combined both stego audio and stego video file. Hence stego audio-video file is reconstructed at the sender end.The proposed work is planned to be carried out in the following manner

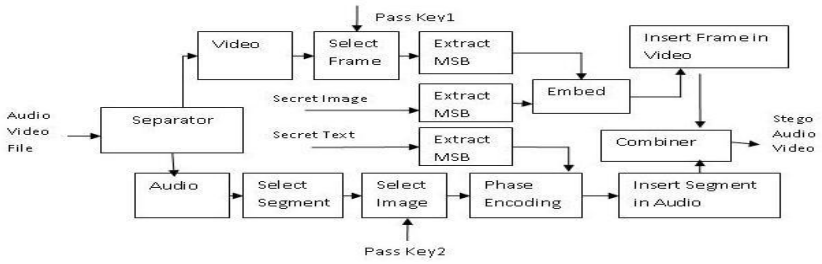


Fig1. Block Diagram for Embedding

On the receiver side, Stego audio–video file is separated using separator. Embedded audio file is selected to extract the authentication image. Similarly passkey is also provided to extract the secret image from the video file and secret images are compared before embedding and after embedding.

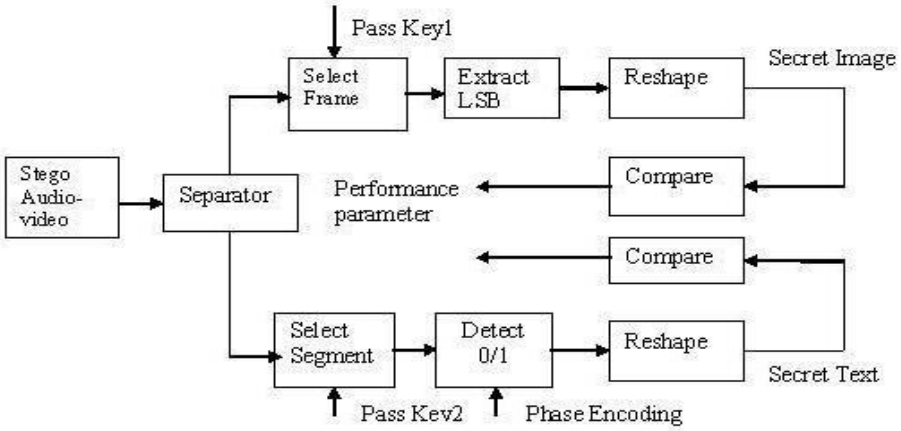


Fig2.Block diagram for Retrieval

The General Framework of Proposed system

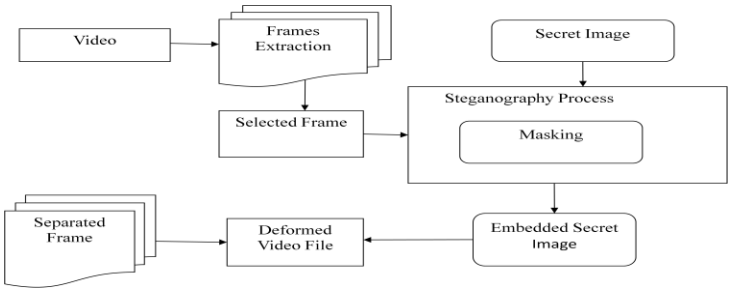
Entire flow-work of proposed system is described as follows:

I. Selection of video files: In this step, user will select the video file from the set of video files that are present on the system. User can select any length of the video file. Here we use AVI (audio video interleave) video. This video file may also contain audio data which we need to separate in second step to hide the secret image.

II. Separation of audio and video files: To provide more security to secret data, we need to separate audio and video files. As we know video is series of frames and these frames are nothing but images. We use simulink model to separate audio and video data. With the help of Simulink model, audio part is extracted from video file. Separated audio and video data are stored in separate variables.

III. Hiding Image in Video: In this step, user will select the secret image which he/she want to hide. This secret image is converted into gray scale image. To hide secret image, user have to enter the frame number which will extract the frame from the video data. User can extract any frame from video files. Secret image and extracted frame will be embedded using embedding key.4LSB algorithm is used for embedding this data. Overall complexion of image can be

obtained but somewhat distortion may be occurring in the image after mixing secret image into the frame of video file.



IV. Hiding Image in Audio file: To make the system more robust and secure, user will select data sample from the audio files. Audio file is made of number of data samples. To select the data sample, user has to provide passkey which will extract the audio data sample from the subset of data samples. Secret image will be embedded into extracted audio data sample using phase encoding algorithm. Before image embedding, secret image is first converted into gray scale image. Finally stego audio sample is constructed.

V. Creating stego audio video file: In this step, stego audio segment is inserted into audio file. Hence, stego audio is reconstructed. Similarly, stego video frame is inserted into video file to create stego video file. Now proposed method will combine both stego audio and stego video file together to produce stego audio-video file.

5.0 Methodology

5.1 Phase Encoding Algorithm

In phase encoding algorithm, Original audio file is broken into number of segment or blocks and then embed the whole secret message into first phase of audio segment. Only limited amount of data can be embedded behind the audio file. Only first block of audio file is used for secret data embedding.

Secret message is not distributed over cover media. So it becomes easier for attacker to detect and delete that data. Drawback of phase encoding algorithm is it minimizes the data transmission rate. This method is good for small amount of secret data transmission.

Phase coding algorithm is explained as follows:

1. The original audio file is taken as input to proposed system then extracts the header of file.

2. The rest of the audio data is divided into number of audio segments or blocks. The length of block should be equal to size of secret message because whole secret message is going to embed inside the first phase of audio block.

3. FFT (Fast Fourier Transform) is applied to each segment of audio file to create the matrix of phases.

4. Secret message is then inserted into first phase vector of audio segment.

5. New phase of first segment and original phase matrix are used to create new phase matrix.

6. Sound signal is reconstructed using new phase matrix. Inverse FFT is applied on sound signal and all the audio segments are combined together to produce the sound signal and then original header is added to it.

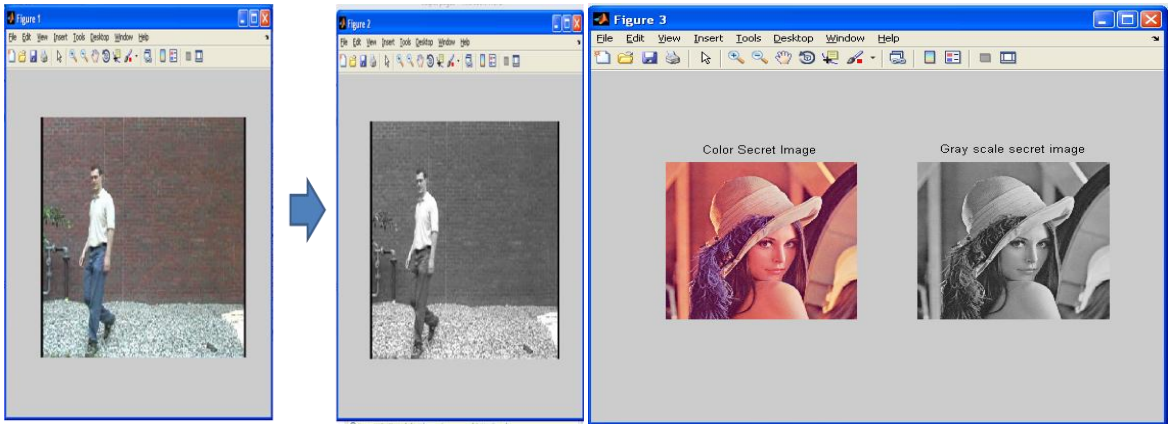
5.2 4LSB modification Algorithm

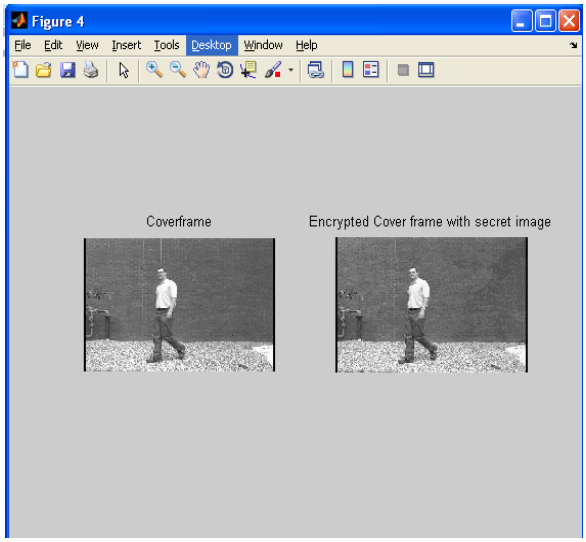
In this proposed work, masking technique is used to vacant the last four bit position of cover media (here video file) as well as secret message. Fixed mask value is used. XOR operation is performed on both cover media and mask value. Thus; last 4 LSB positions of cover media become vacant. Then extract 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. 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.

Experimental setup and result

The proposed video steganography is implemented with MATLAB 7.10.0(R2010a) using windows 7 operating system.





REFERENCE:

1. Dipankar Pal, Nabin Ghoshal "A Robust Audio Steganographic Scheme in Time Domain (RASSTD)" International Journal of Computer Applications© 2013, Volume 80.

2. 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.

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

4. Budda Lavanya, Yangala Smruthi, Srinivasa Rao Elisala." Data hiding in audio by using image steganography technique" IJETTCS Volume2, Issue 6, November – December 2013.

5. 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),volume2,Issue 4,October 2012,pg no 177-181.

6. 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.

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

8. 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.

9. 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

10. 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.

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