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 8, August 2015

Design and Implementation of Robust Audio-Video Cryptosteganographic System

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, V.I.T, Maharashtra, India[2]

ABSTRACT: Due to rapid development of internet technologies, digital communication has become important part of human life. But information collected by numerous organizations and nature of digital media allows for exact duplication of material with no notification that the material has been copied. Such materials or information needs to protect themselves from unwanted surveillance, theft, false representation and reproduction. Two important aspects such as cryptography and steganography are used for secret communication over internet. Combination of these both technologies provides great security to data and increases high level protection. In this paper, text is encrypted by using Blowfish algorithm and then hides behind audio file and image is also embedded inside the video file. Combination of both stego audio and stego video is transmitted over unsecure channel. For Audio steganography, parity bit encoding algorithm is used and video steganography, modified 4LSB algorithm is used. The modified 4LSB algorithm has more hiding capacity than traditional algorithm. The MSE and PSNR are calculated and resulting PSNR is found to be good as compared to traditional system.

KEYWORDS: Blowfish, Modified 4 Least Significant bit, Peak signal to Noise Ratio (PSNR), Mean Square Error (MSE), Encryption, Steganography, cryptography.

I.INTRODUCTION

Secure code has been prevalent in modern life because of fast development of communication technologies. Our email messages or important data are transmitted through many computers before reaching their final destination, thereby making our private communication more vulnerable to interception. So there is need of secure code for private communication. But wide spread use of secure code worries law enforcement agencies and hence criminal and attacker, terrorist also make use of secure code if and when they become widely available.Crptography and steganography are most important aspect of information sharing. The process of securing data by encryption is called cryptography whereas method of hiding data behind cover media using various different techniques and algorithms is called steganography. Neither of them alone is secure enough for sharing and transmitting secret information over an unsecure communication channel but at the same time there is great chances of interception by intruder. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion. Data embedding is the process of embedding messages in multimedia signals so that the presence of the messages is oblivious. It has wide applications in secret communication, authenticity verification, cryptanalysis, steganalysis etc. Generally, in data embedding, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being embedded within another object. The abundant use of steganography tools has arouse the interest of law enforcement official investing the trafficking of illegal material via web page,audio and video ,other transmission medium over the internet. The innocus stego medium is actually broadcast over the network to the recipient where the actual message is separated from it. The importance of reducing a chance of the information being detected during the transmission is being an issue now days. Some solution to overcome these issues is cryptography, but once it is decrypted the information secrecy will not exits any more.Hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media. The traditional LSB modification technique by randomly dispersing the bits of the message in the image and thus making it harder for unauthorized people to extract the original message, is vulnerable to lose of valuable hidden secrete information.The main purpose of proposed scheme is to maximize the security of data that transmitted

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 8, August 2015

through network. Three different algorithms are used to enhance the security of transmitted data over network. These algorithms are not just related to maximize the security of secret data but also to prevent unauthorized access of user. Parity bit encoding algorithm is used for audio steganography and modified 4LSB (Least Significant Bit) algorithm is used for video steganography and Blowfish algorithm is used for encrypting secret data.

II. RELATED WORK

Lovey rana, saikat banerjee, [2] implemented an audio steganographic system that provides improved security. To achieve this, dual layer randomization approach is used. First layer of randomization is achieved by randomly selecting the byte number or samples. An additional layer of security is provided by randomly selecting the bit position at which embedding is done in the selected samples. Using this proposed algorithm the transparency and robustness of the steganographic technique is increased.Praveen P, Arun R, [1] have proposed a method which is an audio-video crypto-steganographic system, it is the combination of audio steganography and video steganography using advanced chaotic algorithm as the secure encryption method. Their aim is to hide secret information behind image and audio of video file. Since video is an application of many audio and video frames. A particular frame can be selected for image hiding and audio for hiding a secret data. They have used 4lsb substitution for image steganography and lsb substitution algorithm with location selection for audio steganography. Advanced chaotic algorithm can be used for encryption and decryption of data and images. Suitable parameter of security and authentication such as psnr value, histograms are obtained at both the receiver side and transmitter sides that may be identical at both ends. Hence they have tried to enhance the security of the data and image. This method can be used in fields such as medical and defence which requires real time processing.Muhammad Asad, Junaid Gilani *et.al*, [3] proposed a three layered model for audio steganography based on least significant bit replacement. The secret message to be transmitted is passed through two layers before it is embedded within the cover message in the third layer. The stego message is transmitted over the network to the receiver side and the secret message is recovered by performing reverse operations in reverse order. The objective of the paper is to make sure the confidentiality of the secret message. They also discussed the implementation issues of the three layered model with respect to different parameters like capacity, transparency and robustness. Experimental results have shown that three layer model achieved a signal to noise ratio of 54.78db in comparison to 51.12 db of conventional LSB method.Kamalpreet Kaur, Deepankar Verma, [4] here the user information is hide under other kind of information such as audio so that no one suspects that a sensitive data is being transferred. Its purpose is to hide the presence of communication. Here three different steganographic methods have been used instead of using one steganographic method. This has been done with a layering approach. The review of three layered approach for audio multi-level steganography has been presented. Here three secret messages rather than one can be transmitted with a single cover file. In this paper, three permutations of audio steganography methods are compared. The result of the stego audios is compared by psnr graph. Each permutation has three levels. Three levels of audio steganography can be identified as layer 1, layer 2 and layer 3. This method has provided an effective way to achieve higher security, increased un-delectability and the maintained consistency in the clarity of digital audio signal.

III. PROPOSED SYSTEM

The proposed scheme combines the basic approach of cryptography and steganography for hiding color image in audio-video file. The audio file is embedded with an encrypted text and secret image is embedded in the frame of its video part. Here, lsb (least significant bit) replacement technique is used for steganography and blowfish algorithm is used for cryptography. Encryption performed on text is by blowfish algorithm. Embedding is performed to hide encrypted image in an audio signals and image in video frame. This is done by converting the cover file and embedding file into binary bits. The last bit of cover file is being replaced by the binary bits of the embedding media. The main goal of this project is provide high security to the secret image and text. An audio-video file comprises of multiple video frames and audio signals. The secret text is hidden behind the signals of the audio and image is hidden behind video frames. So, a great extent of security is provided here. Multilayered security is provided to the secret data. The text is enveloped with the audio signals and secret image in video frames thus it is covered with layers and is more protected. The secret communication is carried through many sources like image, audio & video files. Proposed work is mainly proposing data hiding by embedding the message of interest of cryptographic algorithm, thus providing high security. In proposed scheme, video that contains audio is used as cover media to hide the secret data. Internally these cover audio-video file are separated and store in proper folder with proper extension. After successful embedding of

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 8, August 2015

secret message into audio signal, the stego audio also look like an ordinary audio because only single bit is destroyed or modified during data embedding process. Proposed scheme also allow user to select frame to hide data behind one of the frame of video file. Secret image is divided into two new frames and to hide these frames two new cover frames are needed. In this way, two cover frames are selected by new scheme and embedding procedure is done with cover video. Proposed system internally done this work without the knowledge of user.

Stego audio and video part is combined together to produced the stego video that contains secret data and send to receiver. Strong Authentication is provided at receiver side, if the correct passcode is not provided by user then system does not allow user to extract the secret data from the stego file. If hacker or cracker hack the data, it requires huge amount of computation. Receiver will extract the secret data from these cover media. For these, receiver separates the audio and video part that contains secret data. Receiver uses reverse operation to extract the hidden information from stego video part and stego audio part. In this way secret text is obtained at receiver end.

The proposed algorithm supersedes various steganographic techniques through combining both cryptography and steganography. According to the experiments, the messages can be successfully camouflaged in the cover image, and the stego images have satisfactory quality. Moreover, our scheme allows for a large capacity of embedded secret data and can be extracted from stego-image without the assistance of original image.Thus, the proposed method deals with data security in which secret data is embedded in cover video. A methodology for creation of a stego video is defined using the Least Significant Bit (LSB) Replacement algorithm.

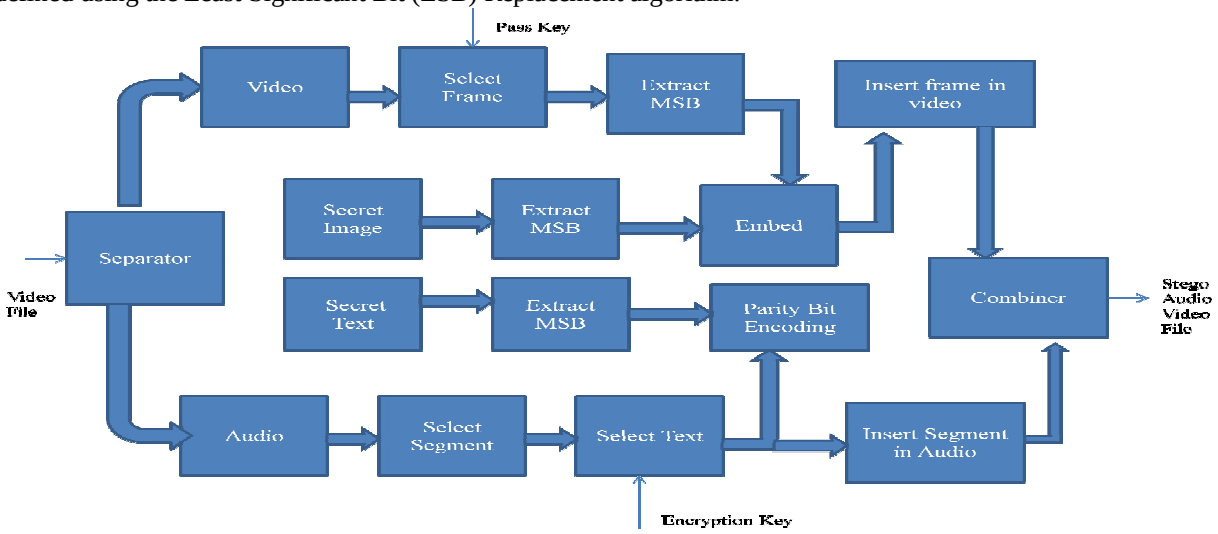

FIGURE1: BLOCK **DIAGRAM AT SENDER SIDE**

IV. PHASE IMPLEMENTATION

Phase I: Selection of AUDIO-VIDEO file and separation of it

The proposed system is designed with the SIMULINK model using MATLAB. It has inbuilt toolbox of audio-video processing. In the first phase, user will select the audio video file from the set of video files available on the system. Audio-video separator is used to separate audio and video files. This audio video separator is built in MATLAB using SIMULINK model. Any length of video file can be selected for secret data transmission.

Phase II: AUDIO Steganography

In this phase, Audio file is extracted in _.wav format and save this audio file in specific folder. Now this Audio file is read by MATLAB using _waveread function.This function returns the sampled audio data, number of bits per second and sampling frequency. File is then opened in read mode. First 40 bytes of Audio file contain header data and 41st byte to 43rd byte represent length of wav data samples. Hence only wav data samples are sufficient to hide the text. Audio file is divided into number of segments and length of the segment should be equal the size of message to be encoded.

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 8, August 2015

These one of the audio segments is selected for hiding encrypted text. Blowfish algorithm is used for encrypting secret text. Here text is taken from user which is in interleaved form and converts it into its ASCII value.ASCII value is then converted into its binary pattern.For hiding secret text, fixed audio segment is used. Header part is excluded from audio and secret message which is in binary form is inserted in fixed audio signal. Sound segments is reconstructed and then concatenating with original header. Parity bit encoding algorithm is used for embedding secret text in audio segment. Sound segment is also converted from decimal to binary value.8 bit binary sequence is needed to embed secret text data which is in also 8 bit sequence.
Now Parity bit encoding algorithm is applied on these two binary sequences and reshape the message in column vector and then concatenate original header to audio segment and finally reconstruct sound signal.

Phase III: VIDEO Steganography

Here Original video file is selected in read mode .If the original video is color video, then color video is first converted into gray scale video and collect all frame structure in one variable. Collected frame structure is then read by using MATLAB function. Same passcode which is used initially, is used for selecting frame number, behind which secret image is to be hidden. In the proposed scheme, only one passcode is used for extracting the frame and internally second frame number is selected to select second cover frame to hide MSB and LSB bits of secret image. User selected image is then converted into gray scale image and store it in variable after reading it. This image is then converted into 8 bit binary sequence. MSB bit and LSB bits of secret image are extracted. Two cover frames that are used for steganography purpose also converted into 8 bit binary sequences.Masking operation is performed on this binary sequence and finally image bits are reshaped into one row. This reshaped row vector of secret image data is embedded on frame matrix, by adding each row vector bits into last 4 bits of frame bits. This forms a stego frame, overwriting this stego frame with original video file to create stego video file. In this way, new stego video file is created, in which secret image is hidden.

Phase IV: Creating Stego AUDIO-VIDEO file

Stego audio and stego video file is combined using MATLAB function and forms the Stego AUDIO-VIDEO file.

Phase VI: AUDIO Recovery

In this phase, Audio file is opened in read mode and first 40 bytes of header is extracted from it and store it in some variable. Then all data bits after 40^{th} byte are stored in another variable. These sampled bits are only sufficient for extracting the secret text. Binary text is extracted from these sampled bits using parity bit decoding algorithm and also convert it into decimal. Audio samples are reconstructed after adding original header to it.

Phase VII: VIDEO Recovery

Here Stego video is received and split into number of frames.Passcode is taken from user and these passcode selects the stego frames along with adjacent frames.MSB and LSB bits are extracted from stego frames by use of reverse 4LSB algorithm and store it in some variable.MSB and LSB bits are converted into decimal and new secret image is reconstructed by rearranging MSB and LSB bit.

V.ALGORITHMS USED FOR IMPLEMENTING PROPOSED METHOD

Algorithm for Audio-Video Separation

Start
Step1-Read video File
Step2-Simulate Video files using Simulink software
Step3-Separate Audio and video part from selected Audio-Video file.
Stop

Algorithm for Video Steganography

Start
Step1-Calculate frame size of video part
Step2-Read secret image (Lena)
Step3-Convert Secret image into Gray scale image
Step4-Resize the secret image to frame size

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 8, August 2015

Step5-Get Passkey
Step6-Loop for Secret Image (SI)

a. Get a pixel from SI (Secret Image)
b. Convert it into Binary which is of 8 bit
c. Extract 4 MSB's and 4LSB's from Binary pattern
d. Make both of them to be of 32 bits by padding zeros and store the 4MSB which is now 32 bit in variable xl and 4LSB which is of 32 bit in variable xr.
e. Convert xl and xr into decimal number and store in variable XL and XR respectively.
f. Read encrypted image which has to be hidden.
g. Get the pixel form frame1 and frame2(Cover image)
h. Extract the MSB's of cover frame by bit and frame
i. Extract the MSB's of encrypted image by bit and image
j. Reverse the place of MSB to LSB
End.

Step7-Embed secret image data into the frame matrix by adding each databit into last 4 bits of frame bits.
Step8-Create Stego frame
Step9-Play Stego video
Step10-Close file.
Stop

Algorithm for Audio Steganography

Start
Step1-Read secret text.
Step2-Interleaved the secret text
Step3-Convert each letter of secret text into ASCII.
Step4-Divide Audio into segment.
Step6-Divide Audio segment into L parts
Step7-Drop the header part
Step8-Arrange Audio part
Step9- Enter Passkey (Data hiding Key)
Step10-Select audio segment according to passkey for encoding.
Step11-Convert each audio segment into 8 bit of sequence
Step12- Hide each bit of text into segments base of parity
Step13-Loop

a. Hide bit depending on even or odd parity
End

Step14-Create Stego Audio Segment.
Step15-Play Stego Audio File
Step16-Close File.
Stop
Algorithm for creating stego Audio-Video file
Start
Step1-Combine Stego audio and Stego video file.
Stop

Algorithm for Audio Recovery

Start
Step1-Read Stego audio file
Step2- Enter the passcode same as sender side
Step 3: Extract Secret text using Parity bit decoding algorithm
Step 4: Recovered the secret text
Stop

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 8, August 2015

Algorithm for Video Recovery
Start
Step1-Read Stego Video file
Step2- Enter the passcode same as sender side
Step 3: Extract Secret Image using 4LSB algorithm
Step 4: Recovered the secret text
Stop

VI. RESULTS

The proposed system is implemented in MATLAB 7.10.0(R2010a) using windows 7 operating system. The experimental result is carried out on hidden image in audio and video files. Figure 2 shows how to select secret image from set of image using image picker window. On the click of choose image button, this window will be displayed and user can select colour image from there.Figure3 shows how the application will ask the user to provide passkey to extract the audio and video file. Here same key is used to encrypt the text using blowfish algorithm and also encrypt image if user presses encrypt button.

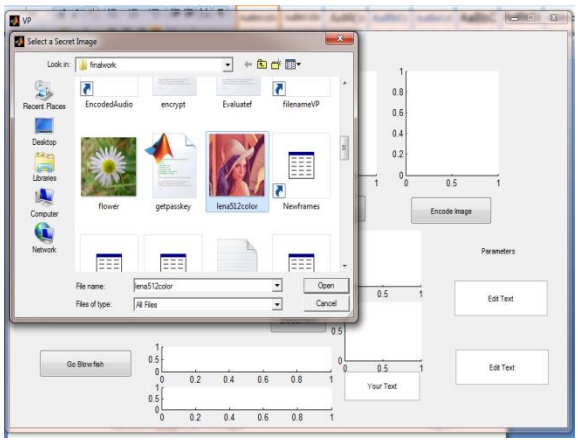

Figure 2.Image pickers Window for selecting secret image

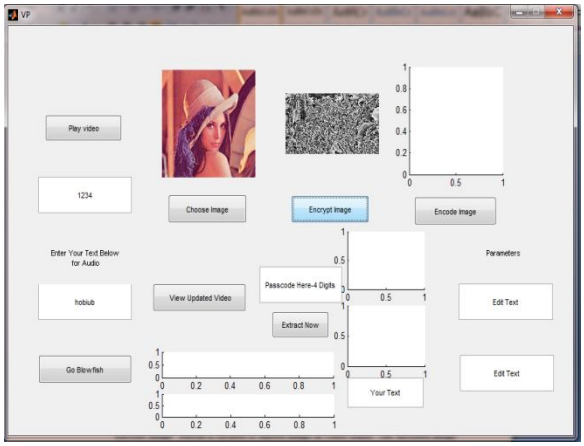

Figure 3.Encrypted Image

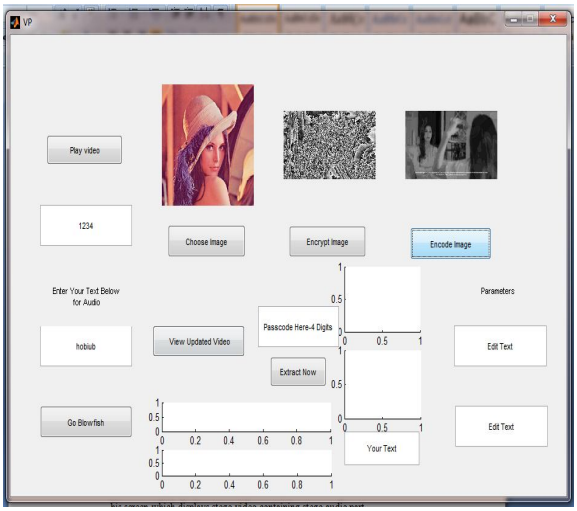

Figure 4. Encoded Image

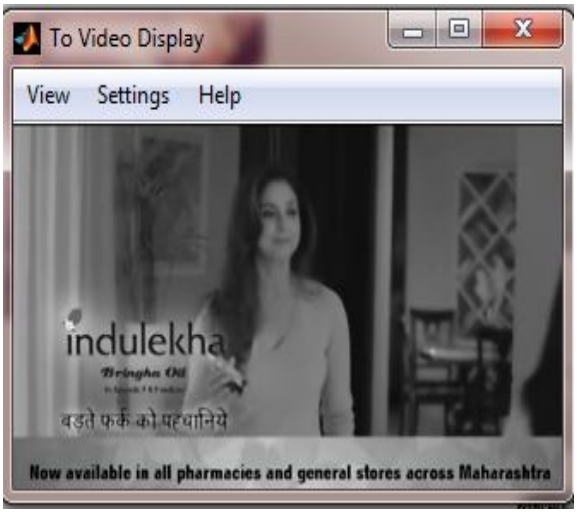

Figure 5.Playing Stego Video

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 8, August 2015

Figure 4 shows encoded image which contain encrypted secret image. Figure 5shows stego video which contains secret image and secret text.From the figure 5, we can see that quality of stego video is not compromise even after embedding.

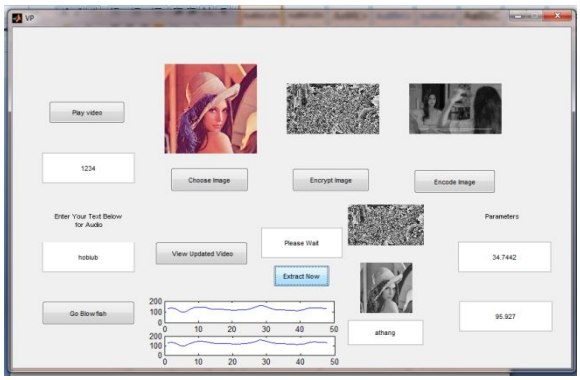

Figure 5. Recovered message and image

Figure 6 shows original message which is extracted from audio signals and secret image which is extracted from encoded cover frame of video file.

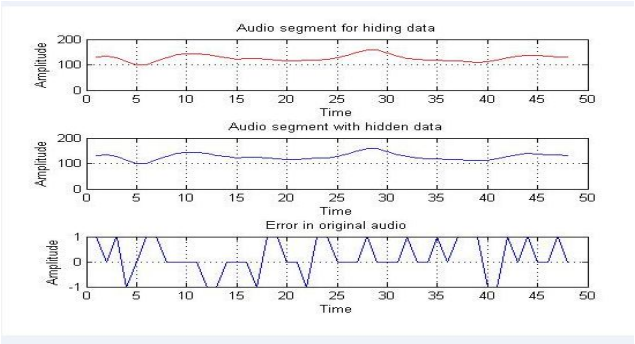

Figure 6 Original and Stego spectrograph for Audio file

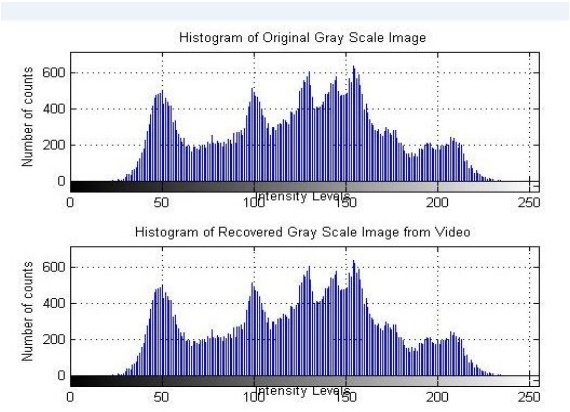

Figure 7 Original and Stego Histogram for Video file

Figure 6 and 7 gives the steptograph of original and stego audio signal and histogram of original and retrieved image. From the histogram, we can see that there is not much variation in retrieved image with original one.

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 8, August 2015

VII. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed scheme performs better than traditional method in term of performance and speed. The proposed algorithm provides robust steganographic scheme for data transmission and maximizes the overall security of data transmitted over network. This proposed method can also withstand different attacks and thus a very strong and secure method of data hiding can be obtained. The histogram and spectrograph of both image steganography and audio steganography are also obtained which looks identical before and after hiding. As the PSNR value increases the data security also increases. The future work mainly focuses on audio-video steganography with reversible data hiding mechanism. System mainly concentrates only on ".wav" format of audio files and can extended to a level such that it can be used for different types of audio file formats. At present we are hiding a single text behind the audio signal, using advanced algorithm multiple text or images can be embedded behind the signals.

REFERENCES

[1] Praveen. P, Arun. R, **"Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm",** International Journal of Engineering Inventions e-ISSN: 2278-7461, p-ISSN: 2319-6491 Volume 4, Issue 2 (August 2014) PP: 01-07
[2] Lovey Rana, Saikat Banerjee, **"Dual Layer Randomization in Audio Steganography Using Random Byte Position Encoding" ,** International Journal of Engineering and Innovative Technology, Volume 2, Issue 8, February 2013
[3] Muhammad Asad, Junaid Gilani, Adnan Khalid, **"Three Layered Model for Audio Steganography",** 2012 International Conference on Emerging Technologies (ICET)
[4] Kamalpreet Kaur, DeepankarVerma, **"Multi-Level Steganographic Algorithm for Audio Steganography using LSB, Parity Coding and Phase Coding Technique",** IJARCSSE, Volume 4, Issue 1, January 2014.
[5] S.S. Divya, M. Ram Mohan Reddy, **"Hiding Text In Audio Using Multiple LSB Steganography And Provide Security Using Cryptography",** International Journal of Scientific &Technology Research, Vol. 1, pp. 68-70, July 2012.
[6] Kirti Gandhi, Gaurav Garg, **"Modified LSB Audio Steganography Approach",** International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 6, June 2012, pp 158-161
[7] Ahmed Ch. Shakir, **"Stegno Encrypted Message in Any Language for Network Communication Using Quadratic Method",** Journal of Computer Science 6 (3): 320-322, 2010 ISSN 1549-3636 © 2010 Science Publications.
[8] Andreas Westfeld and Gritta Wolf, **"Steganography in a Video Conferencing System",** Information Hiding 1998, LNCS 1525, pp. 32-47, 1998. Springer-Verlag Berlin Heidelberg 1998.
[9] 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
[10] Saurabh Singh and Gaurav Agarwal, **"Hiding image to video: A new approach of LSB replacement",** International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6999-7003

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, and Academic.edu.

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.