International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 4, Issue 2 (August 2014) PP: 01-07

Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm

Praveen. P[1], Arun. R[2]
[1, 2] *M.Tech, Asst. Prof, Dept of Computer Science and Engineering, Sree Narayana Gurukulam College of Engineering, Kadayiruppu, Ernakulam, Kerala*

Abstract: *Steganography is the technique of hiding any secret information like password, data andimage behind any cover file. This paper proposes a method which is an audio-video crypto steganography system which is the combination of audio steganography and video steganography using advanced chaotic algorithm as the secure encryption method. The aim is to hide secret information behind image and audio of video file. Since video is the application of many audio and video frames. We can select a particular frame for image hiding and audio for hiding our secret data.4LSB substitution can be used 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 which are found to be identical at both ends. Reversible data hiding methods for both video and audio are also being mentioned. Hence the security of the data and image can be enhanced. This method can be used in fields such as medical and defence which requires real time processing.*

I. Introduction

In this digital world the data security and data communication is changing and advancing day by day. The most excited thing isto know that the advancement in these fields had led to the improvement in secure data transmission. Broad band internet connections almost an errorless transmission of data helps people to distribute large multimedia files and makes identical data copies of them. Sending sensitive messages and files over the internet are transmitted in an unsecured form but everyone has got something to keep in secret. The aim of steganography is to hide the secret data inside the cover medium without changing theoverall quality of cover medium. In steganography actual information is not maintained in its original format but is converted in such a way that it can be hidden inside multimedia file e.g. image, video, audio. The current industries mainly demands for digital watermarking and finger printing of audio and video steganography. The music and movie industries are continually searching for new methods for steganography. In "broadcast monitoring" [01] broadcast detectors are used to extract the watermark of a given file or medium and report to the broadcasting events to notify the owner or distributor of broadcast status (medium played, time and date).since internet is now the major medium for the communication and data transfer purpose it become necessary for each nation to make some counter measures to prevent the foul use of internet. The steganography remains intact under transmission and transformation allowing us to protect our secret data. For this the image is converted into bit stream and this bit stream is then embedded in the changing frame. The cybercrimes are also reporting rapidly nowadays hence the steganographic methods should be that much effective and secure so that crimes can be minimised for that cryptography should be combined with steganography for the security of the data come information.

II. Related Work

The paper discusses the combination of cryptography with adaptive steganography for audio video sequence with chaotic algorithm as the encryption algorithm.as the encryption increases the PSNR value also gets increased.[05]The author discusses different methods for audio steganography and LSB method is found to be more secure.[02]The paper discusses LSB audio steganography with location identification and it provides good audio quality and robustness.[04]The paper explains the advanced chaotic algorithm for the encryption and decryption purpose and it consumes minimum time and less complex.[06]The paper discusses the different audio steganography methods such as echo hiding, parity hiding, phase coding and their comparison.[07]The author explains how an image can be hidden in AVI video using 4LSB method. Security techniques are used to find the parameters such as frame number, height and width of the image, PSNR and histogram of the image before and after hiding. If all the verification of these parameters are found to be correct the data is send to receiver. Fig 1 shows the block diagram of the proposed method.

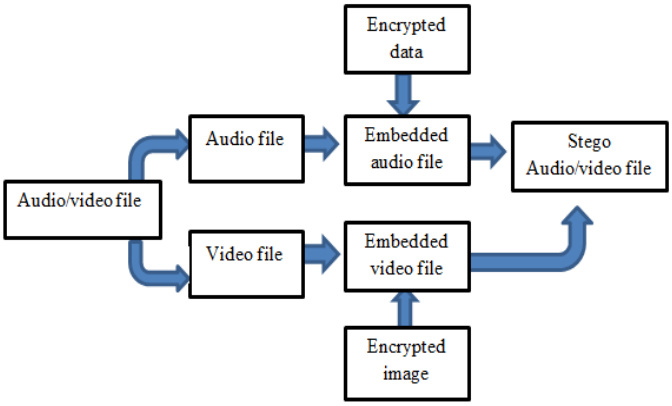

Fig 1: Block diagram for embedding

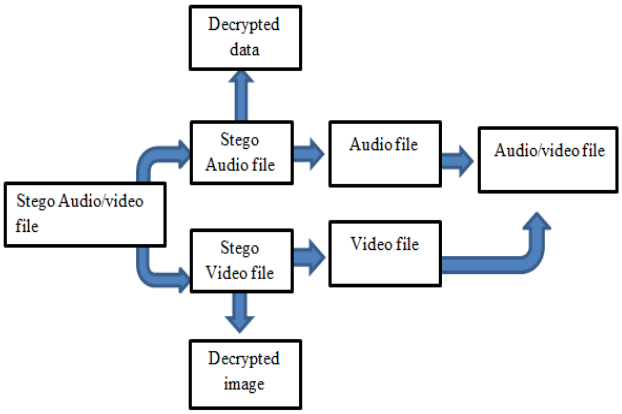

Fig 2: Block diagram for retrieval

III. Selecting Audio-Video file

Here the steps for selecting a specific audio-video file and the separation of audio and video part are explained.

1. Select any available audio video file inwhichuser wants to hide data.
2. Separate the audio and video from the fileusing software.
3. Save the audio and video files separately.

IV. Hiding image in Video (transmitter)

Here the steps for embedding a secret image in one of the selected video frame are explained.

1. Select the video file and read the videofile.
2. Play the video.
3. Select the particular frame in which the Image is to be hidden.
4. Select the encrypted image which has tobe hidden.
5. Extract the msb of the frame by bitand frame with 240 using “bitand” function.
6. Extract the msb of the encrypted image byBitand image with 240 using “bitand” function.
7. Reverse the place of msb to lsb by dividing by 16.
8. The image data is embedded into theframe matrix by adding each databits to the last 4 bits of frame bits.
9. Stego frame is created.
10. Stego video is played.
11. Close file.

V. Hiding data in Audio (transmitter)

Here the steps for embedding a secret message into the audio file are explained.

1. Encrypted message is taken.
2. It is converted to ASCII.
3. Provide the data hiding key.
4. Convert each audio sample into 8 bitsequence.
5. From each sample read first two MSBbits and convert it to decimal. This is the insertion position of the secret messagein that sample.
6. Insert a secret bit into a selected position determined using the previous method.
7. Repeat the steps until all the secret bits are replaced.

VI. Creating stego Audio-Video file

1. Combine stego audio and video fileusing software.
2. This forms the stego audio-video file which contains both text and imageat the transmitter side.

VII. Chaos and Cryptography

Chaos functions [04] have been mainly used to develop mathematical models for nonlinear systems. Due to their extremely sensitive nature to initial conditions and many more interesting characteristics, they have attracted the attention of many mathematicians. Chaotic functions were first studied in the 1960s and have shown several remarkable properties. Sequences produced by these functions are very random and complex. The sensitivity to initial conditions is a characteristic of any chaotic system. This characteristic in addition to some other interesting properties, such as pseudo randomness, ergodicity, wide spectrum, and good correlation, may be related to the confusion and diffusion properties in cryptography Detailed theoretical analyses have shown that chaotic functions have excellent cryptographic properties. So, chaotic systems can provide a secure and fast method for data encryption and security.

The main advantage using chaos lies in the shape of the chaotic signal that looks like noise for the unauthorized users. Moreover, chaotic values are often generated with simple iterations, which make chaos suitable for designing strong and high-speed stream ciphers. Chaotic stream ciphers use chaotic generators to produce pseudorandom stream of bits to encrypt the plaintext using XOR operation. Many different chaotic generators have been proposed, such as 2-D Henon attractor, logistic map and its generalized version, PWLCM, and piecewise nonlinear chaotic map, Frey map, etc.PWLCM is the one we are using here.example for PWLCM is below

$x(k+1)=C[x(k); n] = x(k)$, if $x(k) \in [0, n]$
$[x(k) - n]/(0.5-n)$, if $x(k) \in [n, 0.5]$
$C[1 - x(k); n]$, if $x(k) \in [0.5, 1]$

VIII. Encryption

Chaotic algorithm described above is used for the encryption of both data and image which are to be embedded in both audio and video. Triple key encryption algorithm used. The initial and control parameter keys provided decide the extent of the encryption. The same concept is used at the receiver side for decryption. These keys provide the tool for authentication. Fig 3 gives the block diagram for encryption.

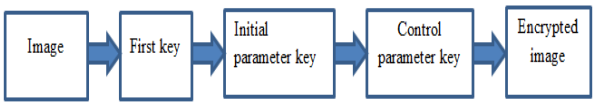

Fig 3: Block diagram for encryption.

IX. Retrieval of image (Receiver)

1. The stego audio-video file is received atthe receiver side.
2. Select the frame number; the frame noshould be same at both transmitter and receiver then only image can beretrieved.
3. The embedded image is present at the LSBof the selected frame.
4. Get the hidden bits by using the "bitget"function.
5. Recover the encrypted image at the receiver.

6. Reshape the image matrix using"Reshape" function.
7. Decrypt the original image using triplekey chaotic algorithm.
8. Compare the original image and decrypted one.

X. Recovering data from Audio

1. Retrieve the stego audio file fromstego audio-video obtained at receiver.
2. Provide the data hiding key provided at the transmitter side.
3. Select the random bits from the audioin which the hidden bits are present.
4. Get the length of the bits by using the"bitget" function.
5. Convert it into decimal.
6. The encrypted message is retrieved.
7. Decrypt the message using the triplekey chaotic algorithm and display themessage to the end user.

XI. Authentication

Authentication is mainly done to confirm the real identity of the data or image or whatever emtities.it is mainly done to ensure that it came from the real user. Here authentication is mainly done for the security purpose at both the transmitter as well as the receiver for secure communication. The data hiding key provided at the transmitter side act as the authentication key in audio steganography.in case of video hiding the frame number and the triple key provided as the encryption key acts as the tool for authentication. The strength of the key used decides the strength of authentication.

XII. Experimental analysis and results

Here the implementation results and analysis of the proposed mechanism is mentioned to check whether it meets the standards.

1 ***Time analysis***

The speed of the encryption algorithm has to be high then only the encrypted data or image can be embedded inside the video and can be transmitted to the receiver end.at the receiver side also the decryption time should be less then only the retrieved data/image can be viewed instantly.in our method the chaotic algorithm provides efficient encryption and the encryption time is also very less so it can be used in real time applications.in real time application such as military purpose the encryption time should be less then only speedy data transfer can be done. The secret image/data can be easily encrypted and embedded and transmitted to the receiver side securely. Speedy and secure transmission medium also has to be ensured for efficient transmission. Fig 4 shows the encrypted image.

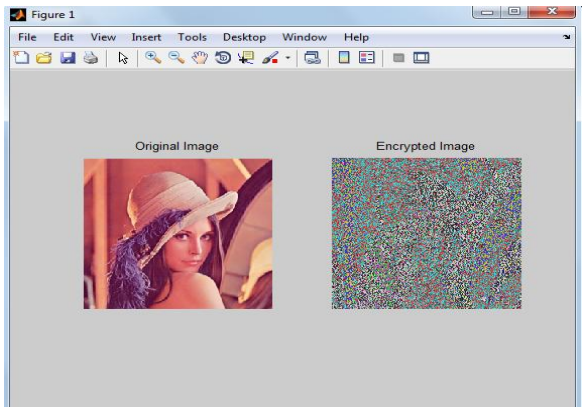

Fig 4: Encrypted image

2. ***Key Space analysis.***

Large key space is very much important for an encryption algorithm to prevent the Brute Force attack. For this purpose we use the triple key chaotic algorithm for both data and image encryption and decryption. The triple key provided can be used not only as a tool for encryption but can be used as a tool for embedding both image and data in video and audio components. The data hiding key provided in audio embedding can be used as a tool of authentication. Only when all these keys are provided at receiver side the exact image as well as data can be retrieved. All these keys are subjected to sensitivity analysis because any change in any of these keys will result in decryption failure fig 5 and 6 shows the keys used.

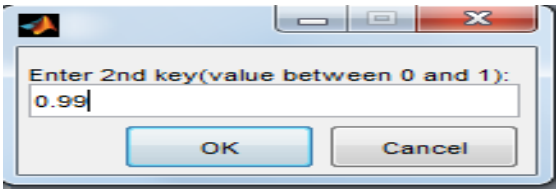

Fig 5: Initial parameter key

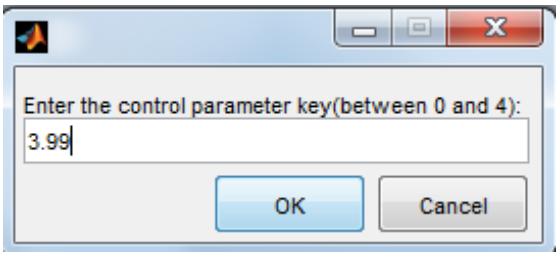

Fig 6: Control parameter key

Fig 7 gives the stego video.

Fig 7: Stego video

3. *Audio-video analysis.*

The main advantage of the proposed method is that the quality of the audio video files may not be compromised even after embedding. Since location based LSB substitution is done in audio, the quality and robustness is not at all disturbed.in the case of video frames also after embedding and mixing the secret image the quality of the video is not disturbed.one drawback is that the exact secret image cannot be retrieved since only 4MSB bits are embedded into the frame, but the overall complexion of the image can be obtained which is the advantage of 4LSB substitution. Fig8 and 9 gives the retrieved image and the histogram of original and retrieved image.

Fig 8: Retrieved image

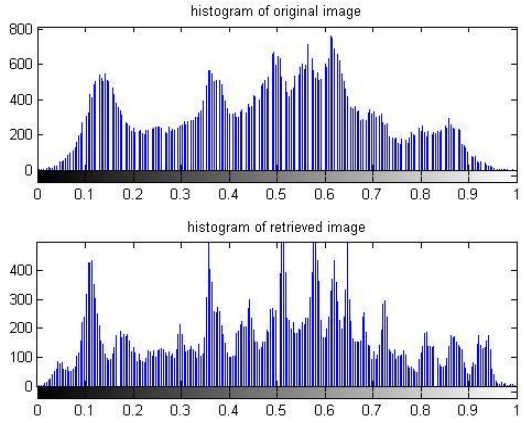

Fig9: Histogram of original and retrieved image

From the histogram we can see that there is not much variation in retrieved image with original. Exact image cannot be retrieved because we are embedding only 4MSB bits of the secret image and these bits can be retrieved.

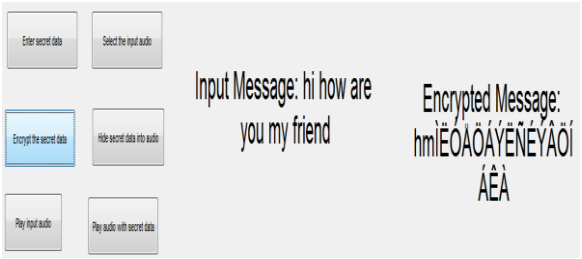

Fig 10: Encrypted message

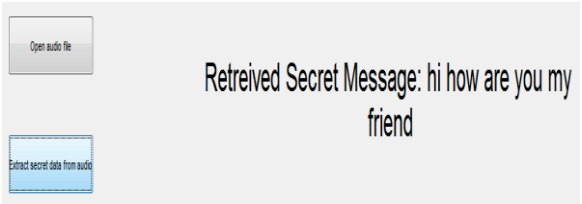

Fig 11: Recovered message

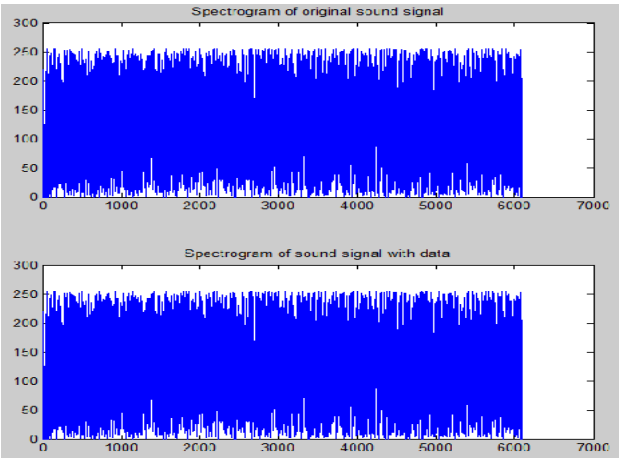

Fig 12: spectrogram of original and stego audio

XIII. Conclusion

Securing the secret data by embedding it in audio-video file with chaotic algorithm as encryption algorithm is providing high security and hiding. We are hiding an encrypted secret image and data behind a video frame using 4LSB method and in audio file using LSB method with location identification. We obtained satisfactory result in both audio and video steganography. We embedded encrypted image successfully into a selected frame and the PSNR value between original and encrypted image also found out which is found to be in the range of 10 to 40 dB according to the size of image and size of video. 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.

XIV. Future works

The future work mainly focuses on audio-video steganography with chaotic algorithm and reversible data hiding mechanism. Through reversible data hiding method the exact image and data can be retrieved along with the cover video and audio. The audio and video quality can also be preserved. The reversible data hiding method is mainly based on interpolation and error prediction mechanism.

Acknowledgement

The authors would like to thank all the staffs of the CSE department of SNGCE and friends for their valuable suggestions and feedback. We also like to thank all the authors of the papers which we have referred to get a clear idea regarding our work.

REFERENCES

[1] Sunil.k.Moon, Rajesree.D.Raut, "Application of data hiding in Audio-Video using anti forensics techniques for authentication and data security", Advanced Computing Conference (IACC) 2014IEEE International.

[2] Pathak.P, A.K.; Nag.A"A New Audio Steganography Scheme based on Location Selection with Enhanced Security", ACES First International Conference 2014.

[3] Sunil.k.Moon, Rajesree.D.Raut, "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security", IEEE Second International Conference on Image Information Processing (ICIIP-2013).

[4] BassemBakhache, Joseph M. Ghazal, and Safwan El Assad,"Improvement of the Security of ZigBee by a New Chaotic Algorithm", IEEE Systems Journal 2013.

[5] V.Sathyal, K.Balasuhramaniyam, N.Murali, M.Rajakumaran, Vigneswari,"data hiding in audio signal, video signaltext and jpeg images",IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012)

[6] FatihaDjebbar, BeghdadAyad, HabibHamamandKarim Abed-Meraim,"A view on latest audio steganography techniques", International Conference on innovations in Information Technology 2011.

[7] K.A Navas, Vidya.V, Sonia.V.Dass,"High security data embedding in video",Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE.