A Survey on Crypto-Steganography

Sunita
Department of Computer Science and Engineering, Shri Baba Mast Nath Engineering College, Rohtak, India.

Rajiv Sharma
Department of Computer Science and Engineering, Shri Baba Mast Nath Engineering College, Rohtak, India.

Arvind
Department of Computer Science and Engineering, Shri Baba Mast Nath Engineering College, Rohtak, India.

Abstract – Cryptography is the study of Secret (crypto-) writing (-graphy) that is concealing the content of message from all except the sender and the receiver and to authenticate the correctness of message to the recipient. Data security is the challenging issue of today that touches many areas including computers and communication. Recent cyber security attacks have certainly played with the sentiments of the users. Cryptography is one such way to make sure that confidentiality, authentication, integrity, availability and identification of user data can be maintained as well as security and privacy of data can be provided to the user. We have analyzed cryptographic technique(IMAGE, AUDIO & VIDEO) using LSB algorithm and RSA is an asymmetric key cryptographic algorithm, they have been analyzed on their ability to secure data.

Index Terms – Cryptography, Cyber Security, Attacks.

1. INTRODUCTION

Popularity of digital media increase day to day its raise security related issues. Cryptography is a Greek work Steganous meaning "covered" and graphy meaning "writing". Now a days, digital media and network are getting more use and more popular. So that requirement of secure transmission of data also increased. Data Hiding is the technique of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Cryptography is a technique which is used to hide the message and prevent the detection of hidden message. Audio- video Cryptography is a modern way of hiding information in a way that the unwanted people may not access the information. In audio Cryptography consists of Carrier that is audio files and this file modified in such a way that they contain hidden information means data hide in the sound file and in video Cryptography data is hide in video frame and these modifications must be done in such a way that data is recovery correctly without destroying the original signal.

In propose work we introduce novel method for audio video cryptography. In this method we can hide secret image behind video and text behind audio. For video Cryptography LSB algorithm is used and for audio Cryptography parity algorithm is used. In proposed work sender used any audio video file and divide it separately as audio file and video file. After that image hide behind the video using passkey and video converted into "stego vidphyeo" same as secret text hide behind the audio and audio become the "stego audio". These stego audio and stego video file combine and send to the receiver side. At receiver side this image audio-video file again separated and using passkey. The secret image and data from stego video and stego audio recover respectively. Video is a set of images. It is an electronic medium. In audio Cryptography sound file is modified in a way they contain hidden information. In video per unit of time of video ranges from six to eight frames per second. Video stenography algorithm based on fact on each pixel represented by 3 bytes where each byte representing 3 primary colors that is red, green, blue (RGB).Size of image file is directly related to number of pixels and granularity of color definition. For hide a secrete image behind the video we need AVI audio video interleave) video. There are different format of video file like MPEG,MPG these all file first convert into AVI format first.

2. RELATED WORK

There is different technique available for video Cryptography. [1] Advance video Cryptography algorithm describes data embedding and extraction for high resolution AVI videos. In this method instead of changing the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. There encrypt secret message using a simple bit exchange method before the actual embedding process starts. [2] Video Cryptography for Hiding Image with Wavelet Coefficients. This method based on discrete wavelet transform and used random coefficient selection approach as well as the methods using the discrete wavelet transform.[3] In this work author has aimed to hide secret information behind image and audio of video file. By embedding text behind audio file and an authentication image is embedded behind frames of video file. As video is the application of many still frames of audio and picture (i.e. image), any frame can be selected from video and signals from the audio for hiding secret data. Authors have used 4LSB method for image Cryptography whereas Phase Coding algorithm for audio

Cryptography. [3] An approach to hide data in video using Cryptography apply double hash function technique to choose a pixel from row and column. But after Appling the hash function on pixel may not found in the frame to resolve this problem using collision function. [4] Cryptography In Mpeg Video Files Using Macro blocks Data Hiding Technique: Audio Cryptography using LSB Technique in this technique use a flexible micro blocks ordering feature of H.264/AVC [7] have proposed a method which is an audio-video crypto-steganographic system, it is the combination of audio Cryptography and video Cryptography 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 Cryptography and LSB substitution algorithm with location selection for audio Cryptography. The use of the video based Cryptography can be more eligible than other multimedia files because of its size and memory requirements. Video are set of frames and the number of still pictures per unit of time of video ranges from six to eight frames per second. There are different type of video files like MPEG, AVI, MOV etc. There are different technique and algorithm for video Cryptography like LSB substitution, Bit exchange method etc. The best technique is that hide Secret message without affecting the quality of video, structure and content of the video file. In video Cryptography after hiding a secrete data in video create “stego” video file which send to the receiver side. Proposed system introduces a novel and more secure method of video Cryptography.

Cryptography Algorithms

There are some goals of cryptography that are given below:

1) Authentication: Sender and data receiver must be authenticated before sending and receiving data.

2) Confidentiality: The user who is authenticated, can access the messages.

3) Integrity: Data is free from any kind of modification between sender and receiver.

4) Non-Repudiation: The sender the receiver cannot deny that they had sent a message.

5) Service Reliability: Attackers can attack on secure systems, which may affect the service of the user.

Encryption Algorithm:

a. take two arrays flag text and flag key of size of length of text and key and fill it with zeros.

b. Do this process till the length of key Process for encryption of data by the key:

for k=1 to m J=1 for i=1 to n (n is length of padded text)

{ if(j>m) { j=1 a[i] =a[i] + b[j] j++ }

else { a[i] =a[i] + b[j] j++ }

End for Process of hiding of key:

Do for j=1 to m-1 b[j]=b[j]+b[j+1]

end

for b[m]=b[m]+b[1]

End

for Change the array A and B in to character form:

Eg. For i=1 to n

while a[i]>256

a[i]=a[i]-256

flagtxt[i]+=1

end

while end

for for i=1 to m

while b[i]>256 b[i]=b[i]-256

flagkey[i]+=1 end if

end

for

Decryption Algorithm:- this is reverse process of encryption Change the encrypted data in ASCII format:

Eg A[20]={20,143,29,231,256}
B[20]={10,2,230,19,23}

Decryption of data and key:

for i=1 to n (n is length of padded text)

while flagtxt[i]!=0 a[i]=a[i]+256 flagtxt[i]—

end while end for

for i=1 to m

while flagkey[i]!=0

b[i]=b[i]+256

flagkey[i]—

end while

end for

for k=1 to m

b[m]=b[m]-b[1]

for j=m-1 to 1

b[j]=b[j]-b[j+1]

end for j=1 for i=1 to n if(j>m) j=1 a[i]=a[i]-b[j] end if

3. PORPOSED MODELLING

Cryptography refers to hiding information. To embed hidden information, one need :

- the Cover File and
- the Secret Message itself, that is to hide.

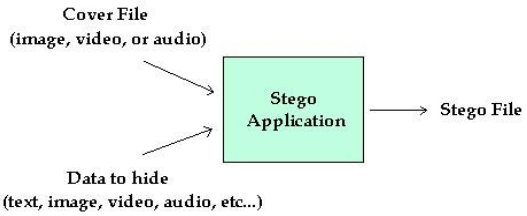


Figure 1.1 Stego Application

The secret message is hidden within a cover signal (object) in the block called embeddor using a stego key. The output of embeddor is a stego signal that is then transmitted over the network. After transmission and other signal processing which may contaminate and bend the stego signal, the embedded message is retrieved using the appropriate stego key in the block called extractor. And thus, the required secret message can be obtained at the receiver side separating it from the cover object. This can be shown as :

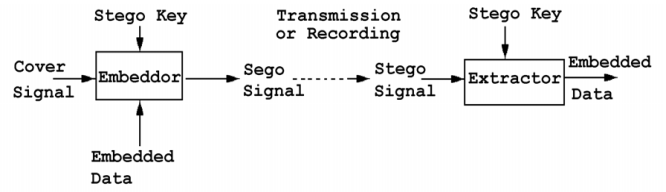


Figure 1.2 Block Diagram of Data Hiding and Data Retrieval.

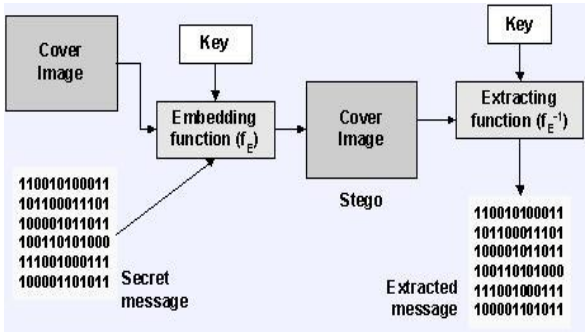


Figure 1.3. A Graphical Version of the Steganographic System.

In a computer-based Audio Cryptography system, secret messages are embedded in digital sound. And, for this also various algorithms are available. LSB Coding is one of the method but it lacks robustness. So, a genetic approach towards the same can help out.

4. RESULTS AND DISCUSSIONS

1. Object/Project Snapshot

At first, the cover audio file format that is chosen is WAVE audio file format because this format is original of all the formats.

Figure 1 Wave Audio

Now,initially the cover audio file is played.

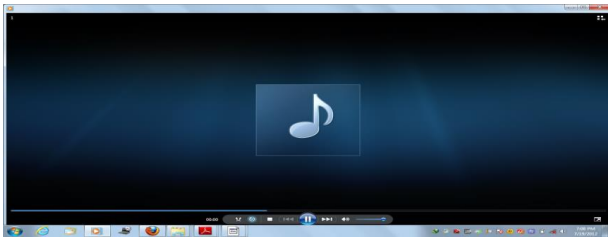


Figure 2 Input played

And the signal is analyzed in .NET using the function Waveread and the plot is obtained as:

Figure 4 Secret Message

Now, after embedding the secret message the Stego Audio is obtained in output and again the plot for the Audio, this time the Stego Audio is obtained. And, the output i.e. the Stego Audio is played.

2 Evaluation

PSNR Values for the case when the secret message, to embed is same and the size of cover audio is varying.

Wave Audio	Wave Size (Audio Size In Bytes)	Message Size (Image Size In Bytes)	PSNR
Bird Wave	315,392 bytes	12,288 bytes	86.358
Drum & Bass Wave	471,040 bytes	12,288 bytes	77.099
Express Wave	307,200 bytes	12,288 bytes	74.545
Funky Wave	208,896 bytes	12,288 bytes	85.514
Philtered Wave	212,992 bytes	12,288 bytes	85.985

Table 1 Message(Image) is same & the Wave Files size differ

And, the graph generated after observing the values given in table 1 is shown as:

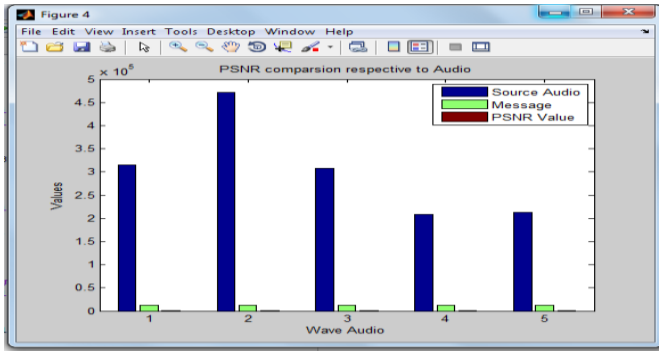
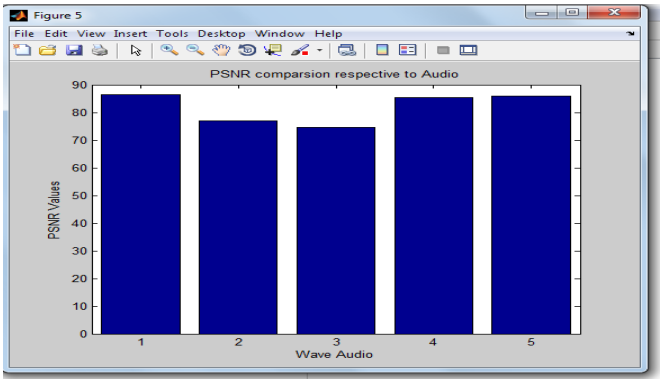


Figure 3 Comparision respective to different Audio covers where Source File, Message & PSNR measure is compared.



PSNR Values for the case when the secret message, to embed is of different size and the size of cover audio is same.

3 Summary

The PSNR block computes the peak signal-to-noise ratio, in decibels. This ratio is often used as a quality measurement between the original and the Stego audio. The higher the PSNR, the better the quality of the Stego, or reconstructed audio[15].

Where f(x,y) and g(x,y) means the values at the at position (x, y) in the cover-audio and the corresponding stego-audio respectively. The PSNR is expressed in dB's. The larger PSNR indicates the higher the image quality i.e. there is only little difference between the cover-audio and the stego-audio. On the other hand, a smaller PSNR means there is huge distortion between the cover-audio and the stego audio.

From table 1, it is observed that for all images, PSNR is near about 70-80 and the hidden capacity is about 12288 bytes. The better value of PSNR indicates least distortion.

Different host and different message files have little effect on PSNR.

5. CONCLUSION

This paper is a short form of world Steganography. We have shown how the simplest methods work and how they can be explored. We have used symmetric encryption algo to provide more security. Research in this field has already begun. Next to Cryptography, one of the most active fields of research is mass detection tools for hidden contents. The problems are really big. At first, known statistical tests are fragile and for many embedding schemes we still do not know which properties to test. At second, the today traffic in public networks is so overwhelming, that is too hard to rigorously Practically, asymmetric algorithms like RSA are used for the key exchange and symmetric algorithms are used for encryption / decryption. Further, general implementation limitations of cryptographic algorithm emphasis the selection between hardware and software cryptosystem, choosing among symmetric and Asymmetric key algorithm and the essential factors to be followed to have a secure key management.

REFERENCES

[1] A Tutorial Review on Steganography-Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das1 http://www.jiit.ac.in/jiit/ic3/IC3_2008/IC3-2008/APP2_21.pdf

[2] SANS Institute InfoSec Reading Room Cryptography: A right way Steganography_1584.pdf

[3] Cryptography& Steganalysis:Different Approaches-Soumyendu Das,Subhendu Das,Bijoy Bandyopadhyay,Sugata Sanyal http://arxiv.org/ftp/arxiv/papers/1111/1111.3758.pdf

[4] A review of audio based Cryptographyand digital watermarking-M. L. Mat Kiah1, B. B. Zaidan2,3,4, A. A. Zaidan2,3,4*, A. Mohammed Ahmed1 and Sameer Hasan Al-bakri1 http://www.academicjournals.org/IJPS/abstracts/abstracts/abstract2011/18Aug/Kiah%20et%20al.htm

[5] A Detailed look of Audio Cryptography Techniques using LSB and

[6] Genetic Algorithm Approach Gunjan Nehru, Puja Dhar IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012 ISSN (Online): 1694-0814 www.IJCSI.org
[7] Algorithm For Audio Watermarking & Steganography-Nedeljko,Cvejic http://herkules.oulu.fi/isbn9514273842/isbn9514273842.pdf
[8] Data Hiding in Audio Signal: A Review-Poulami Dutta1, Debnath Bhattacharyya1, and Tai-hoon Kim2 http://www.sersc.org/journals/IJDTA/vol2_no2/1.pdf
[9] Efficient Method Of Audio Cryptographyby Modified LSB Algorithm & Strong Encryption Key With Enhanced Security-R Sridevi, DR. A Damodram, DR. SVL.Narasimham http://www.jatit.org/volumes/research-papers/Vol5No6/15Vol5No6.pdf
[10] A Genetic-Algorithm-Based Approach for Audio Steganography-Mazdak Zamani 1, Azizah A. Manaf 2, Rabiah B. Ahmad 3, Akram M. Zeki 4, and Shahidan Abdullah5 http://www.waset.org/journals/waset/v54/v54-63.pdf
[11] SANS Institute-InfoSec Reading Room Steganography: The Right Way http://www.sans.org/reading_room/whitepapers/stenganography.pdf