IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-8 E-ISSN: 2347-2693

STEGO: A Tool for Implementing Text-Audio-Video Steganography

Hitendra Donga[1*], Kishor Atkotiya[2]

[1]*Dept. of CSIT, Shree M. and N. Virani Science College (Autonomous), Rajkot, INDIA*
[2]*Dept. of Statistics, Saurashtra University, Rajkot, INDIA*

Corresponding Author: hndonga@vsc.edu.in

Available online at: www.ijcseonline.org

Received: 02/Jul/2017, Revised: 14/Jul/2017, Accepted: 10/Aug/2017, Published: 30/Aug/2017

***Abstract*:** Steganography is the creative method of hiding any important information or data like passcode, data file, image; spreadsheets behind the original cover file. In this paper we proposed the text-audio-video cryptstego which is the combination audio steganography and video steganography using algorithm implemented using C#.Net tool and Libraries. The main goal of our research paper is to hide the important data file or any spreadsheet behind the audio, video, or image file and also one more method we have used is to store it as cipher text. Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. The implemented algorithm is 6LSB is used for image steganography. We made out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. A proposed cryptstego-key has been applied to the system during embedment of the message into the cover image, it also provide the technique to hide plain text file or any other data behind bitmap image any audio file. So the proposed system secures the data transmission using proposed stego tool. This paper mainly focuses the idea of computer forensic technique and its use of audio-video steganography technique for providing better security in concern.

***Keywords*:** *Steganography, Data Extraction, Cipher, RSA Algorithm, LSB*
Subject: Computer Science: Information and Data Security

I. INTRODUCTION

Steganography is the art of smacking the fact that communication is taking place between two entities or single, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most standard because of their frequency on the internet. One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and extracted. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack for the same. Solitary answer to this problem is, through the use of steganography and cryptography. Steganography is a technique of hiding information in digital cover media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists in it that is the beauty of steganography. Steganography include an array(bunch of different elements) of secret communication methods that hide the message from being seen or discovered behind cover. Due to advances in ICT technique, most of information is kept in form of electronically distributed. Therefore, the security of information has become a fundamental concern issue. In cryptography, the message or encrypted message is embedded in a digital host or in cipher text using different algorithm before passing it through the network, thus the existence of the message is unknown in network. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: text, audio, video and images. The rising prospects of modern communications need the special means of security especially on computer network & Security. The network security is becoming more significant as the number of data being exchanged or transmitted on the internet increases day by day. Therefore, the confidentiality and data integrity are requires to shield against unauthorized access and use. Steganography hide the secrete message within the host data set and presence invisibly and is to be reliably communicated to a receiver side also. The host data set is intentionally corrupted, but in a concealed way, designed to be invisible to an information analysis.

II. RELATED WORK

In paper author explained Steganography and cryptography in computer forensics: The paper focuses on Computer forensic technique is use to find the parameter like height and width, frame number of data, PSNR, histogram of secrete message data before and after hiding to audio-video using steganography. If all these parameters are verified and found to be correct then only it will send to receiver

otherwise it stop the secrete message data in computer forensic block itself[1]. In [2] Image hiding in video Sequence based on MSE: This paper suggests a method for hiding image in selected video sequence based on MSE. It has proposed algorithm in which the image-hiding scheme is based on discrete wavelet transforms (DWT) and singular value decomposition (SVD). In this, the author is not directly inserting the secret image on the wavelet coefficients but on the singular values elements of the cover images DWT sub bands the cover image file and also find the SVD of the cover image or each block of the cover image, and then the singular values get reformed to embed the watermark. First the video sequence and frame translation is to be done. Calculate MSE for each frame and the watermark is to be embedded on a frame which has low MSE. The model proposed by the author is more secured against attacks and satisfied both security and robustness [2].The paper also explained the LSB based audio steganography using lifting wave transform and as a result the proposed algorithm gives the improved quality audio and full recovery option [3].The paper discusses the optical crypto technique with adaptive steganography for audio-video sequence cryptography having more hiding capability to store and more security but it described as the data quantization increased the PSNR value also increased and it becomes bulky file[4].

III. PROPOSED APPROACH

In this paper our aim is to hide important and secret information behind the .wav and image cover file in such a way there would be no perceivable changes in the image and audio file after the message insertion. At the same time, if the message that is to be hidden were encrypted, the level of security would be higher to quite a satisfactory level. Now, even if the hidden message were to be exposed the person trying to get the message would only be able to lay his hands on the encrypted message with no way of being able to decrypt it. In Order to be able to define our system architecture, we must first dearly state how our system works. There are basically two types of encryption technique we have proposed one is to hide the information behind the wav file and other is to hide the important information behind the bitmap image file. The modules of the proposed system are as follows:

Data hiding and extracting from a bitmap file is done using two techniques.

- Novel Image Embed technique e.g. (Module 1).
- Novel Image Extract technique e.g. (Module 2).

Data hiding and extracting from a wav file is done using two techniques.

- Novel Embed technique e.g. (Module 3).
- Novel Extract technique e.g. (Module 4).

All the information , text or any file that is to be hide using the above technique will be converted into cipher text using custom-RSA Algorithm proposed here.

The overall flow of the proposed system is described in the figure 1

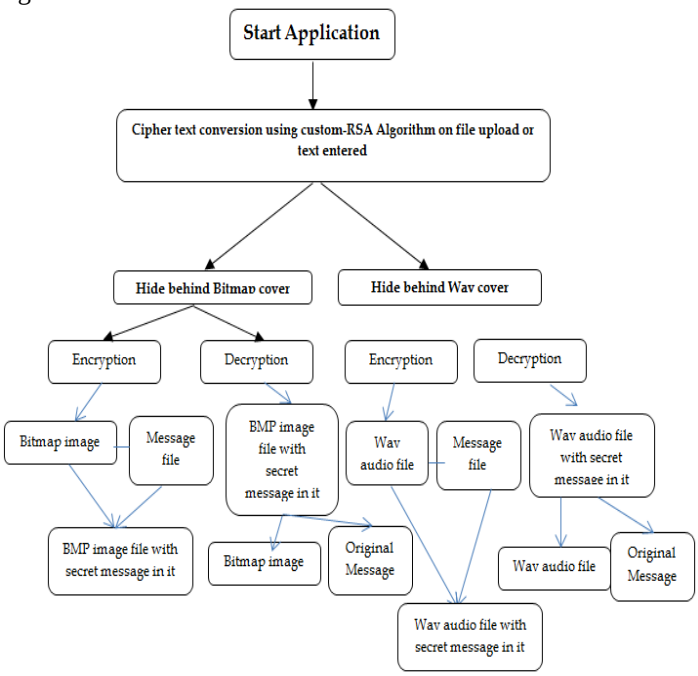

Figure 3.1 Proposed system architecture

Custom-RSA Algorithm for converting the plain text message to cipher text:

Now, even if the hidden message were to be exposed the person trying to get the message would only be able to lay his hands on the encrypted message with no way of being able to decrypt it. The implementation is as below:

Step1: Enc no=
Dec no=

Step2: P=3 (this P and Q number will be prime and it will be allocated by operating sys)
Q=11

Step3: N=P*Q
N= 3*11=33
@N=(P-1)(Q-1)
@N= 2*10=20
(so whatever @n we get between that number we have to take no for Enc no so here sassasa0-20 and that number must be PRIME(take 3 or 7 for convince)).

Step4: O < Enc no <= @N

Step5: So now it will select number between 0-20 in this case 7 so now **Enc no=7**

Step6: Message(M)=2

Step7: Cipher Text(C) = M^Enc no% N
2^7%33=29

Cipher Text= 29 (encryption is message is done !!)

Step8: After encryption we have to perform decryption so for decryption we have to find D

Dec No = Dec No * Enc no % @N=1

= Dec No * 7 % 2 = 1

= 3 * 7 = 21 % 20 = 1 Dec No= 3

Step9: we got the dec no so we can easily convert cipher text to palin text

Plain Text = C^Dec no % N

=29^3 % 33 =2

Output Message= 2

Procedures for hiding the information behind the bitmap image cover:

-

Novel Image Embed technique e.g. (Module 1).

We have implemented the overall application in C#.NET. Microsoft .Net framework prepares a huge amount of tool and options for programmers that they simples programming. One of .Net tools for pictures and images is auto-converting most types of pictures to BMP format. The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires.

The novel encrypt technique is used to hide information into the image; no one can see that information or file. This module requires any type of image and message and gives the only one image file in destination.

Procedures for extracting the information from the bitmap image cover:

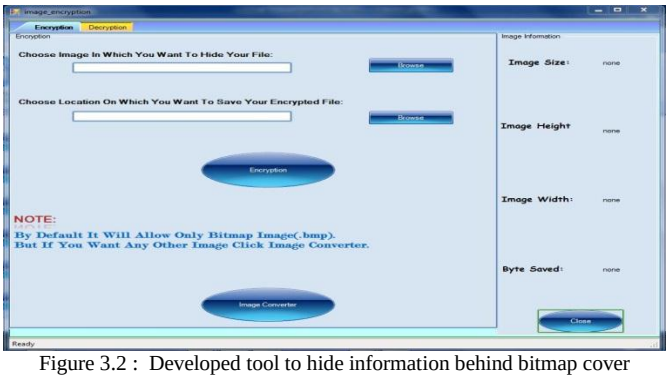

Figure 3.2 : Developed tool to hide information behind bitmap cover (Encryption)

Novel Image Extract technique e.g. (Module 2). The novel decrypt technique is used to get the hidden information in an image file. It take the image file as an output, and give two file at destination folder, one is the same image file and another is the message file that is hidden it that. Before encrypting file inside image we must save name and size of file in a definite place of image. We could save file name before file information in LSB layer and save file size and file name size in most right-down pixels of image. Writing this information is needed to retrieve file from encrypted image in decryption state.

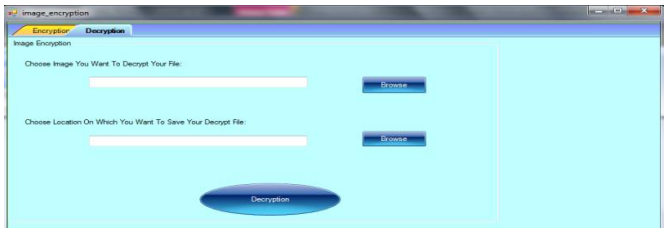

Figure 3.3: Developed tool to hide information behind bitmap cover

Procedures for hiding the information behind the wav audio cover:

Data hiding and extracting from an wav audio file is done in two main technique.

- Novel Embed technique e.g. (Module 3).
- Novel Extract technique e.g. (Module 4).

Novel Embed technique e.g. (Module 3)

(To embed the text file into the audio file)In this technique, the first step is selecting an input wav audio file. The selection is made through opening a new open file dialog box and the path selected is displayed through a textbox to enter file name.

The second step is selecting an output audio file in which text data or a text file is embedded. The third step is choosing a text file or typing any text message for embedding in the selected wav file. Fourth step is selecting a key file to select the unique key for the encryption. In the fifth step whatever the files that we have selected are viewed and verification of the path is done through the open file dialogue box provided by the C#.NET. In the sixth process data is embedded in to the audio file using custom low bit encoding technique. After embedding the content both the audio files are played and a listener cannot find any difference between the audios. Implemented tool is shown in the below figure 3.4

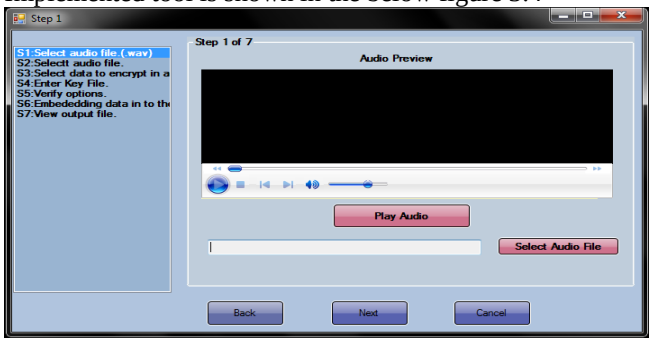

Figure 3.4: Developed tool to hide information behind wav audio cover (Encryption)

Novel Extract technique e.g.(Module 4). (To extract the text file from the wav file)

In this technique, the first step is the process of selecting the encrypted audio file. This is the file that a user has to extract information from the output audio. Second process involved in selecting a new text file to display the embedded message. Symmetric encryption method is used here, so the key selected during the embedding process is used in decrypting the message.

All the process done till now are displayed using a list box and finally the embedded message can be viewed with the help of a file or in a textbox. The C#.NET provides the built in libraries to code the above technique but we have customized the built in libraries for the implementation of this tool for better security.

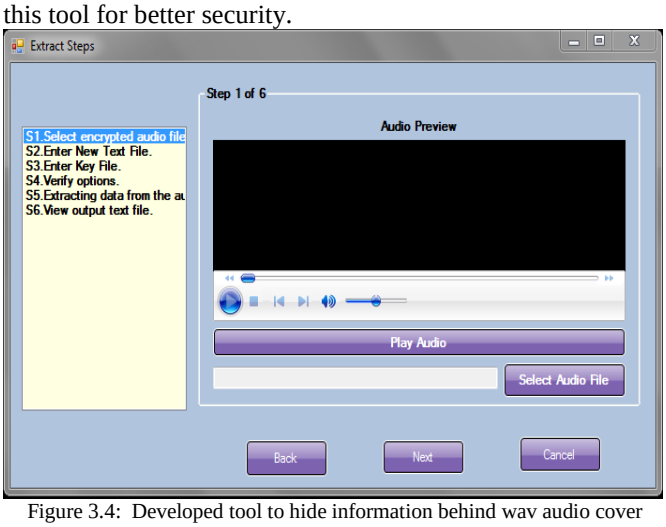

Figure 3.4: Developed tool to hide information behind wav audio cover (Encryption)

IV. CONCLUSION

Data security using two different hiding technique e.g wav audio file and bitmap image file with the help of the computer forensic technique provided by the language used c#.Net for the implementation purpose is better and provide the advance security to the file. We are also working on the hiding the important image and other large file files to hide behind the audio wav file and image file. According to our knowledge this method is very robust for hiding the secret information and provides the communication and exchange of information secretly. We are also working on to implement the secure socket gateway for the mail communication to provide the high end security during the communication also. At present we have gained the satisfactory result with wav audio and bitmap image file steganography.

REFERENCES

[1]. George Abboud, Jeffery Marean, "*Steganography and cryptography in computer forensics*", 2010 IEEE Fifth international workshop on systematic application to digital forensic application. pp. 25-30. doi: 10.1109/SADFE.2010.14

[2]. Sakshi and A. Kaur , "*Secure Data Hiding Using Neural Network and Genetic Algorithm in Image Steganography*", International Journal of Computer Sciences and Engineering, Vol.5, Issue.2, pp.95-99, 2017.

[3]. Mandeep Kaur Gill and Rupinder Kaur Randhawa , "*Comparative Study of Multibit LSB Steganography with Cryptography*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.7, pp.120-123, 2015.

[4]. Sghaier Guizani,Nidal Nasser, "*An Audio/Video Crypto Adaptive Optical Steganography Technique* "IEEE 2012,pp, 1057-1062.

