Authenticity and integrity to the data using Video steganograpy

Ms. Kalyani Rodge; Ms.Charming Pandit; Ms. Nageshwari Sakhare & Ms.Rupali Bhaisare

Abstract—*In this paper, we are using the video embedding technique to provide security to the data while it's transmission from sender side to receiver side. In previous project AES algorithm was implemented for encryption which required more time for encryption. Therefore to overcome this problem we will use blowfish algorithm which requires less time for encryption. This project focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the video. Our project is concerned with the application developed to embed information in a video signal so that data is protected from intruders. This system makes the Files more secure by using the concepts Steganography and Cryptography.*

Keywords: Steganography; Encryption; LSB; Decryption; Cryptography.

1. INTRODUCTION

The working of our project starts with selecting a text file which we want to secure then we encrypt the text data by using blow fish algorithm. The desired video is selected in which the encrypted data file is embedded so that text data is provided the two layer security for better security of data while it's transmission from sender side to receiver side. Steganography is the process in which the data is hided inside some cover media such as audio, video or images. Cryptography is the process in which the original text data is converted into encrypted form by using symmetric keys or asymmetric key. Encryption is the process in which the plain text is converted into cipher text by using the concept of symmetric or asymmetric keys as required. Decryption is the process in which the cipher text is converted into plain text by performing the reverse process of encryption.LSB stands for least significant bit it is the process in which the least significant bits are removed from the original message since the least significant bits are removed hence the meaning of the original message does not change.

2. EXISTING SYSTEM

Steganography is now becoming considerable area to study. As the demand of safe and secure intercommunication boost up .The need of concealment in secret information is growing. If a user wants to send the discreet information to other persons with security and privacy he can send it by usingimage steganography. Present day transactions are considered to be "un-trusted" in terms of security, i.e. they are relatively easy to be hacked. And also we have to consider the transfer of large amount of data through the network will give errors while transferring. Only single level of security is present in the existing systems. During the last few years lot of different methods of concealing information has been done in this field. Some of the existing methods for hiding information give good results only in case of information get hidden successfully.

In previous technique AES algorithm was used to encrypt the data this is very time consuming method it requires large memory space. In video steganography we used to hide the encrypted data directly inside video. If we use this method it becomes very easy for hackers to hack the data because the video get blur. Hence the hacker can easily detect that the secret data is transmitted through the video and hack the data from video.

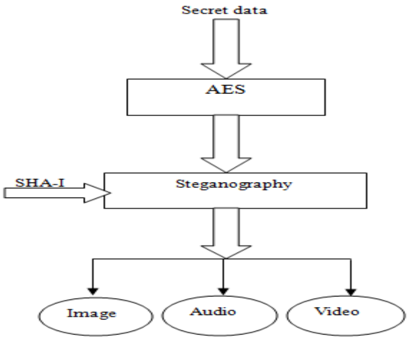


Fig. 1: The Existing Steganography

In the above Fig.1 text data is encrypted using AES algorithm. The message digest is calculated using SHA-1 algorithm which is calculated for message integrity. The encrypted data is embedded in video which consists of audio and images which is called as video steganography. Steganography is the process of hiding the text data in any cover media such as audio, video, images.

3. PROBLEM DEFINITION

1. In previous technique the data was hided in image due to which only less amount of data was made secure if the large amount of data is hided in the image then the image gets blur.
2. In previous project the AES algorithm was used for encrypting the data which required more time for encryption.
3. Only single level security was provided to the data while transmission of data.

4. PROJECT OBJECTIVE

1. In our project we are using video due to which large amount of data can be transmitted securely.
2. In our project we are using Blow fish algorithm to encrypt the data more quickly as compared to AES algorithm.
3. In our project we are providing triple layer security to the data while transmission.

5. LITERATURE SURVEY

In [1] the existing system focuses on the data securityapproach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files. The high results are achieved by providing the security to data before transmitting it over the internet. The files such as images, audio, video contains collection of bits that can be further translated into images, audio and video. The files composed of least significant bits or unused areas which can be used for overwriting of other data. The existing system uses AES algorithm for encryption of text data and video steganography enhances data security.

In [2] the data or information which is transmitted through internet need to be confidential and secure. Secrecy is an essential aspect. So, that no intruder is able to disturb the information. From the security perspective, the information should not be readable by intruder. The cryptography technique can convert the plain text into encrypted text. The target of steganography is to hide a confidential message within a cover-media in such a way that the hacker is not able detect the secret data, In the existing system the data is hidden using Three layers in Audio. Goal of this work is to increase level of security so that data can be secure.

In [3] The Steganography and Cryptography technique can be utilized to provide security and protection to information. In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. Security has turned into a discriminating highlight for flourishing systems and in military alike the steganography is the craft of concealing information inside information, for example, audio medium is used to hide the encrypted data. While cryptography brings about making the information in a format which is not readable by the humans. Though the steganography provides the data to embed in cover media such as video, image brings so that the data stays in secret and undetected by the attacker. Cryptography and Steganography are remarkable and generally utilized methods that control data (messages) security.

6. PROPOSED SYSTEM

In previous paper the AES algorithm was used to encrypt the text data which required more time for encryption and the image steganography was used which allowed fewer amounts of data to embed in it. So to overcome these problems we have used blow fish to encrypt the data because it requires less amount of memory and its execution time is less. We have used video to embed the data so that large amount of data will be provided security.

In existing system we are embedding the data in image that can be easily hacked by hacker therefore we are using video steganography to overcome this problem. In image steganography we can embed only limited amount of data where as in video steganography which we are using in our project we can provide security to large amount of data.

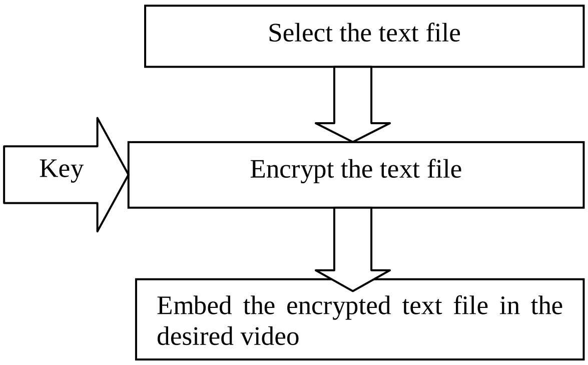


Fig 2: working of proposed system

Explanation of the above fig 2
Step 1: Select the text file which is to be transmitted securely**.**
Step 2: Encrypt the text file by using blow fish algorithm.
Step 3: Embed the encrypted text file in the selected video.

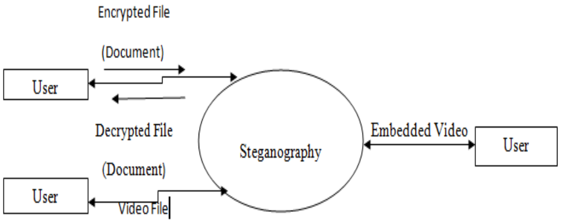
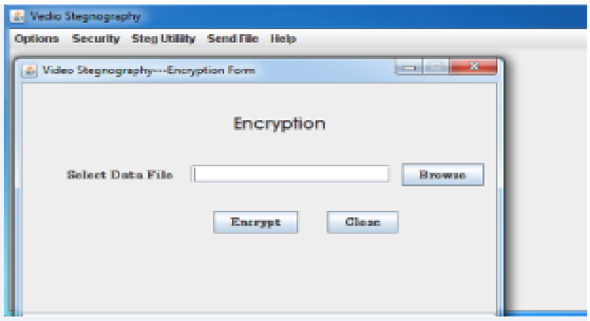


Fig. 3. Block Diagram of Proposed System

In the above Fig.3, user will select the text data filewhich the user want's to encrypt then the encryption algorithm will be applied to the selected text file for encryption Then the user will select the video in which the user wants to hide or embed the text data.Then the encrypted text data file is embedded in the selected video which process is called as video steganography.The receiver will receive the stego video which contain the encrypted data which the sender want's to send to the receiver side.

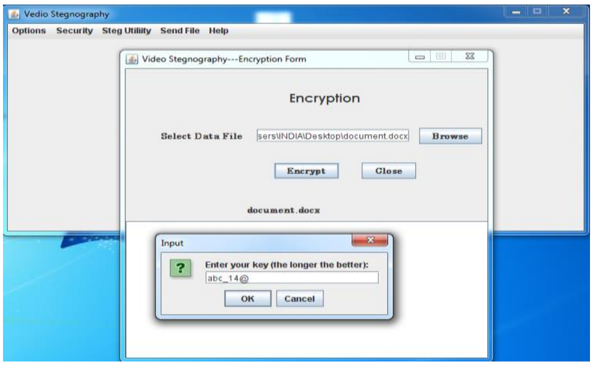
4.1 Modules

1 Encryption Form:



In this form the text file is selected by browsing the text file using the browse button which is to be encrypted. As soon as the encrypt button is clicked the text file will be ecrypted. The close button is used to exit from form.

2. Entering the key form:



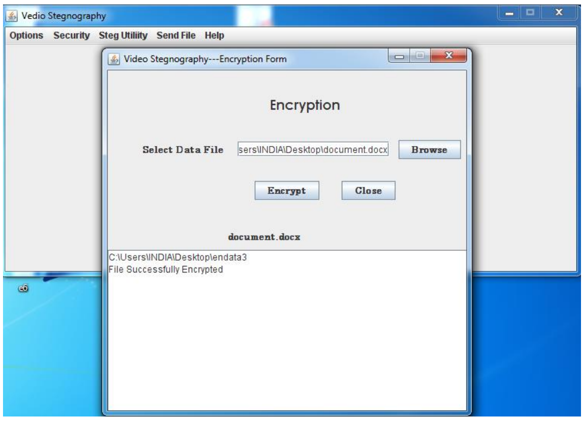
Select Data File: sers\INDIA\Desktop\document.docx

document.docx

Enter your key (the longer the better): abc_14@

In this form the key is selected to encrypt the text file. The ok button is clicked to encrypt the text file and cancel button is clicked to exit.

3. Successful encryption form:



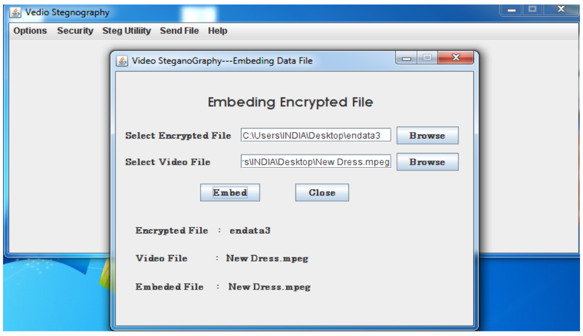
Select Data File: sers\INDIA\Desktop\document.docx

document.docx

C:\Users\INDIA\Desktop\endata3
File Successfully Encrypted

It provides the intimation to the user that the text data is successfully encrypted.

4. Embedding Form:



Select Encrypted File: C:\Users\INDIA\Desktop\endata3

Select Video File: s\INDIA\Desktop\New Dress.mpeg

Encrypted File : endata3

Video File : New Dress.mpeg

Embeded File : New Dress.mpeg

In this form the encrypted file is embedded in the selected video. The embed button is used to embed file in video. Close button is used to exit from the form.

6. RESULT

In our project we have four modules encryption, embedding of data in video, decryption, de- embedding of data from video and till now we have worked on two modules those are encryption and embedding of data in video which are explained in Fig 2 and the rest of the two modules will be performed latter.

The task that is performed in our project uptil now is described as follows:

The text file is selected then the text file is encrypted by using blow fish algorithm. The encrypted text file is embedded in the video to provide security to desired text data by using video stegnography technique.

REFERENCES

[1] Video Data Hiding Through LSB Substitution Technique Hemant Gupta Research Inventy: International Journal Of Engineering And Science Vol.2, Issue 10 (April 2013), Pp 32-39 Sin (e):2278-4721,Issn(p):2319-6483,Www.Researchinventy.Com 32.

[2] Three Layer Protection for Secure Data Transmission using Digital Audio as Carrier Parul, Mr. Vikas Kamra Student, CSE, JCDM College of Engineering, Sirsa, India Assistant Professor, CSE, JCDM College of Engineering, Sirsa, India Vol. 4, Issue 3, March 2015.

[3] Information Security of Video Steganography Utilizing RSA Algorithm Sk. Sameerunnisa K. Supriya Suhasini Asst. Prof, C.S.E, Indur College of Engineering Siddipet, Hyderabad, India, Volume 5, Issue 4, 2015.

[4] Saurabh Singh, "Hiding Image to Video" in International Journal of engineering science & technology Vol. 2(12), 6999-7003, 2010.

[5] Marghny Mohamed, "Data hiding by LSB substitution uses genetic optimal key permutation" in International Arab journal of e-technology, vol.2, no 1 January 2011.

[6] A.K. Al Frajat"Hiding data in video files an overview" Journal of applied sciences 10(15):1644-1649, 2010.

[7] Ali K Hmood," An overview on hiding information technique in images" Journal of applied sciences 10(18)2094-2100, 2010.

[8] Mohammed A.F. Al husainy" Image this form pop ups the information about the successful encryption of the text file. Steganography by mapping pixel to letters" in Journal of computer science 5(1), 33 -38, 2009.

[9] M. Abomhara,"International journal of computer theory and engineering", volume 2, 1793-8201, 2010

[10] Liu bin "an Image method based on correlation analysis and image fusion" in IEEE applied International conference on parallel and distributed computing, application and technology0-7695-2405-2/05, 2005.

[11] Alain, C. Brainos,"A study of Steganography and Art of Hiding Information,"East Carolina University.Chiungy, .W.and W. Quincy."Information Hiding in Real Time VoIP Streams". In Multimedia, 2007.ISM 2007.Ninth IEEE International Symposium on.2007.