



Improved Data Security using Steganography

Twinkal J. Patel,
Cyber Security Dept.,
Raksha-Shakti University,
Ahmadabad, Gujarat, India

Chandresh D. Parekh
Cyber Security Dept.,
Raksha-Shakti University
Ahmadabad, Gujarat, India

Abstract : The use of internet has increase from last few year. The people use internet every day for data communication. Steganography and cryptography is commonly used for providing security of data in recent year. Steganography is the art and science of the hiding data. Here , we propose steganography technique which use Image as a cover medium to hide secrete message . We introduced new algorithm for Hiding file into image file in block wise manner So it increase the speed of hiding process. Content of Original file will remain as it is. The technique proposed by us also integrates cryptography with steganography by first encrypting the secret message and then hiding the encrypted secret message in image. The integration of cryptography with steganography provides an extra layer of security that ensure the safe and secure delivery of message to the intended recipient. The experimental results show that the proposed method can hide a large amount of secret data in less time as compare to other techniques.

Keywords: Steganography, steganalysis, capacity, stego image quality

I. INTRODUCTION

The internet is a large collection of networks. It is connects places all over the world. Internet is the rapidly growing technologies in the present time. This growth has focused attention on one of the important aspect of internet viz. information security. Internet is a public network, secure the information on internet is very important. Various techniques including cryptography, steganography etc are used to secure data on the internet. Cryptography is a method of storing and transmitting data in a particular form , such that it is not understandable to anyone other than the intended sender and recipients. cryptography are both ways to secure information from unwanted parties but neither technology alone is perfect and can be compromised. Steganography is the technique that hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in regular files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information, such that the existence of information is concealed to everyone except for the intended sender and receiver. The strength of steganography can amplified by combining it with cryptography.

II. STEGANOGRAPHY TYPES

Steganography can be broadly classified into Five types on the basis of the type of the cover media used viz. text steganography, image steganography, audio, video and Protocol steganography.

Image steganography : A steganography technique that uses images as the cover media is called an image steganography. images are the mostly used among other types of steganography. Many different image file formats exist, most of them for specific applications. The conventional image steganography algorithm is LSB embedding algorithm.

Audio Steganography : A Steganography technique that uses audio as the cover media is called an audio steganography. It is the most challenging task in steganography. This is because the human auditory system has a large dynamic range that it can listen over.

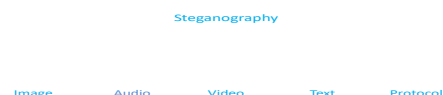


Fig 1. Types Of Steganography

Video Steganography : This technique is uses video as a cover media so it is called video steganography. The Video file should be undetectable by attacker.

Text steganography : Text Steganography is uses text as the cover media so it is called a text steganography. Text files have a very small amount of redundant data to hide a secret message. So it is difficult type of steganography.

Protocol Steganography: Protocol steganography is the technique of embedding information within messages and network control protocols used in network transmission. A network packet has packet headers, user data and packet trailers. So during some of the layers of the network model, steganography can be used. When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography.

III.LITERATURE SURVEY

1) An Evolution of Hindi Text Steganography[7]

Authors: Dr. R. Siva Rama Prasad, Kalavathi.All

Published: IEEE-2009

This paper presents a novel Steganography scheme suitable for Hindi text. Methods of Steganography are mostly applied on images, audio, video and text files. This paper presents a novel Hindi text steganography, which uses Hindi letters and its diacritics. This method is not only useful to Hindi Text but also to all other similar Indian Languages. Different Languages and their structures make differences in the preferred Steganographic system. Normally no single technique is to be used for all languages. Normally information is transferred in the form of bit streams.

They are introducing a new algorithm which encodes the bit 0 with vowel and consonant letters. In the same way letter diacritics and compound letters encode with bit 1. To implement this method, all we need is a message for example.

```

01 01 0011 011 1 010 001100 1
इसे यहाँ जबरदस्त पढ़ाना तो बहुत अरुण्यरोदन हैं ।
01 01 100 11 1
अभी उसे लाकर दादा से
011 0000 1 01 1011 1 0011 011
अखाड़ा रखकर मैं उसे पाठशाला में इलतिजा करूँगी ।

```

Now transfer this Hindi Text to its destination, so that they can decode this message by applying the algorithm in the reverse way. This is very tedious and it takes a lot of time to decode because he gets perplexed with this type of irrelevant text, which is transferred on the network. Advantages of this technique is this method is not only useful to Hindi Text but also to all other similar Indian Languages.

2) A Unique Approach for Data Hiding Using Audio Steganography[8]

Authors : Tanmai G. Verma, Zohaib Hasan, Dr. Girish Verma

Published : 2013

In this paper, Steganography and cryptography both are used together for process of hiding data. First step is to apply cryptography to secret data and after that apply steganography to this cipher data and cover medium like audio file. In this method data is entered by the user. Then the sampling rate is being entered by the user. Now the sampling rate entered by the user is being compared with the Nyquist rate.

If the sampling rate entered by the user is greater than Nyquist rate then next step is followed else previous step is repeated. Then this step is followed by ASCII conversion in which the data is converted in ASCII format. Now the input is given by the user which is in the form of voice. This step is followed by generation of cipher. In the following step stegano-object (i.e. voice generated by the user) and the cipher so generated are combined and the output wave is being generated. Advantages is that the combination of both cryptography and steganography provides better protection of the data from the intruders.

IV.PROBLEM STATEMENT

Data security is very needed in communication because of attack on data. Cover file is used to hide data by using steganography but hiding data is limited because of size of cover file. Various file system like as audio, video, image, text and protocol are use as cover file. If size of file is less then we can hide less data than cover file size. So we have implemented new algorithm to overcome this problem by using image file. New algorithm use image as cover file and it read the content of cover file & secret file into bytes and then hides that at the end of file. we using block wise manner. So it require less time for hiding data than all current techniques.

V.PROPOSED DIAGRAM

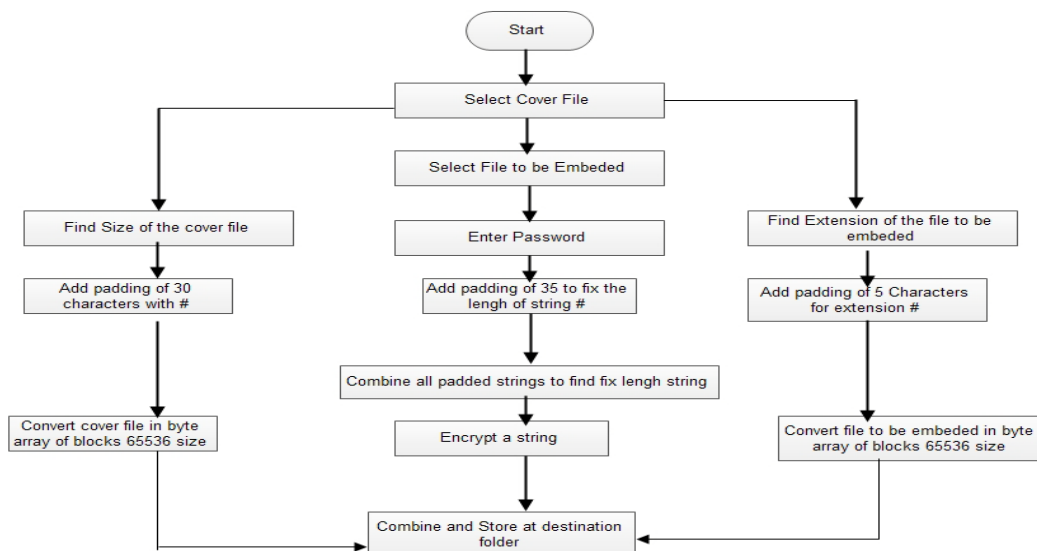


Fig 1.Proposed Diagram

Proposed Algorithm

Hiding Process

Input: Cover File, Original File, Password

Output: Stego Document

- 1) Find the size of the cover file
- 2) Implement padding of 30 to the size with '#'
This will help to get size of the file while retrieving the content
- 3) Find the length (size) of the original file
- 4) Implement padding of 30 to the size with '#'
- 5) Implement padding of 5 to Extension of original message with '#'
- 4) Implement padding of 35 to the password with '#'
- 5) Add few special characters to identify whether this file have embedded message or not, And also check that this file embedded with our algorithm or not, in our case we have added @#!\$% (5 characters) string at the end of the string.
- 6) This combination of the string will be encrypted in binary at the end of file. After this encrypted string and original file are embedded into cover file.

Retrieving Process

Input: Password

Output: Original Document

- 1) Retrieve padding data
 - 2) Decrypt this Retrieve data
 - 3) Read characters of the embedded file, so we will get
 - 4) Check 5 special characters to check whether its implemented by our algorithm or not
 - 5) Check 35 characters to check password
 - 6) Find extension of original file from 5 characters.
 - 7) Find length of original file.
 - 8) Find length of cover file.
- if password is correct read the file from starting to the length of cover file and after that EOF, Now remaining file is our original file.

VI.RESULT AND ANALYSIS

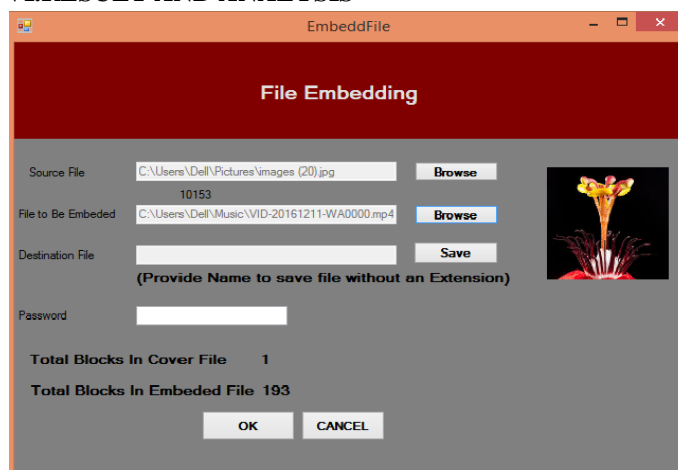


Fig 2.Embedding Process Form

Fig shows Embedding Process form which we can hide our original file into cover file. Here we have to select image file as a cover file (Source File). Next we select video file with size 12 MB as a Cover file and The below

image is an original file (File to be hidden) with size 9.9 KB for this experiment. Fig shows Hiding Process form in which you have to select Source file, original file, select destination path for storing stego document and at the last, enter password.



Fig 3.Original file Fig shows a original file which we will hide it with the help of proposed method. Hide data behind this image.

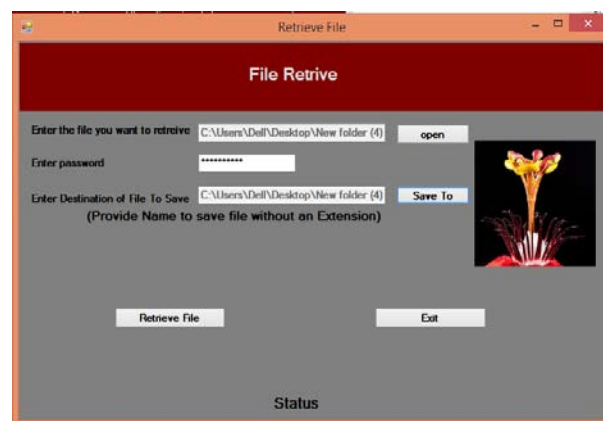


Fig 4.Retrieved Process Form

Fig 12 shows Retrieve Process form which we can retrieve our original file from Stego-Documnet. First select stego file then enter password and select destination path then click Retrieve file. File will be retrieve in destination path.



Fig 5.Original file

This is our original file after extracting process. There is no any modification done through hiding and extracting process.

In this experiment, we use video as a secrete file. We can also use other types of file like audio, text etc.

CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one can see that message except the sender and receiver. We used image file act as a cover document and also presented efficient algorithm for embedding data into this image file. It can be implemented block wise so speed will be faster compare to bitwise or character wise. It will be implemented on binary file so any file can be encrypted. Time required will be less compare to bitwise algorithms available for the plaintext. So we can say that it is the efficient method for steganography.

REFERENCES

- 1) Mohit Garg, A Novel Text Steganography Technique Based on Html Documents, International Journal of Advanced Science and Technology Vol. 35, October, 2011 129.
- 2) M. Pavani¹, S. Naganjaneyulu², C. Nagaraju³, A Survey on LSB Based Steganography Methods, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467
- 3) VIJAY KUMAR SHARMA ,VISHAL SHRIVASTAVA, A STEGANOGRAPHY ALGORITHM FOR HIDING IMAGE IN IMAGE BY IMPROVED LSB SUBSTITUTION BY MINIMIZE DETECTION Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1© 2005 - 2012 JATIT & LLS
- 4) <https://en.wikipedia.org/wiki/Steganography>
- 5) <http://www.webopedia.com/TERM/S/steganography.html>
- 6) <http://steganography-info.blogspot.in/2008/04/steganography-and-attacks.html>
- 7) Dr. R. Siva Rama Prasad, Kalavathi.All, “An Evolution of Hindi TextSteganography”, in IEEE-2009
- 8) Tanmai G. Verma, Zohaib Hasan, Dr. Girish Verma” A Unique Approach for
- 9) Data Hiding Using Audio Steganography”, International Journal of Modern Engineering Research , Jul - Aug. 2013.