International Journal For Technological Research In Engineering
Volume 1, Issue 10, June-2014 *ISSN (Online): 2347 - 4718*

ENHANCING STEGANOGRAPHY ALGORITHM FOR HIDING DATA USING COMPRESSED FILES

Ashish C. Dhami[1], Asst. Prof. Risha Tiwari[2]
[1]Master of Computer Engineering, Gujarat Technological University
[2]Hasmukh Goswami College of Engineering
Ahmedabad, Gujarat, India.

Abstract: The use of internet has grown rapidly form last few year. This growth has increased the demand for techniques that can ensure information security. To provide security to data, steganography and cryptography is commonly used in recent year. Here, we propose a new steganography technique which use compress file as a cover medium to hide secrete message. We introduced new algorithm for Hiding file into compress 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 compressed file. The integration of cryptography with steganography provides an extra layer of security that ensures 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: Seganographyt, cryptography.

I. INTRODUCTION

At present scenario, every people use computer networks to share resource and to exchange information. Here for exchange of information they are communicate with each other. The most important factor has been the security of information. There are mainly two type of technique is used to provide security to the information: Cryptography and Steganography. Cryptography is a technique for securing the secrecy of communication. Many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Sometimes it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. Steganography is the technique used for implementing this. Steganography is the art and science of invisible communication of messages in such a way that no one can seen the existing of message except sender and receiver and the goal of steganography is to hide the very presence of communication. This is done by hiding information in other information, i.e. hiding the existence of the communicated information. The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography. The World Wars had accelerated the development of steganography by introducing a new carrier – the electromagnetic waves. Presently, the most popular carriers include digital images, audio and video files and communication protocols. Steganography derives from the Greek word, "Steganos", meaning covered or secret, and "graphy" means writing or drawing. On the simplest level, steganography is hidden writing, today, steganography is most often associated with data hidden with other data in an electronic file. This is usually done by replacing that least important or most redundant bits of data in the original file.

The information to be hided is called the secret message and the medium in which the information is hided is called the cover document. The cover document containing hidden message is called stego-document. The algorithms employed for hiding the message in the cover medium at the sender end and extracting the hidden message from the stego-document at the receiver end is called stego system.

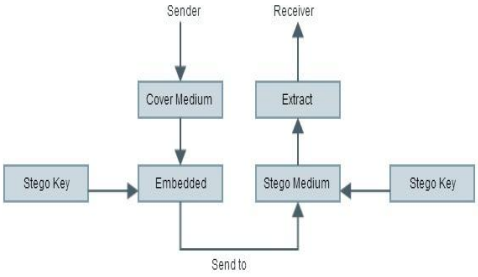


Fig. 1: Block Diagram of Stegnography Mechanism [5]

Here a secret data is being embedded inside a cover image. So it produces the stego image. A key is also needed in the embedding process. The proper stego key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

A. Various application of stegnography

Steganography is applicable to the following areas.

1) Confidential communication and secret data storing
2) Protection of data alteration
3) Access control system for digital content distribution
4) Media Database systems

B. Types of Stegnography[4]

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

C. Text steganography: A steganography technique that uses text as the cover media is called a text steganography. It is one

of the most difficult types of the steganography technique. This is because text files have a very small amount of redundant data to hide a secret message.

D. Image steganography: A steganography technique that uses images as the cover media is called an image steganography. Hiding secret messages in digital images is the most widely used method as it can take advantage of the limited power of the human visual system (HVS) and also because images have a large amount of redundant information that can be used to hide a secret message.

E. Audio-video 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. A steganography technique that uses video as the cover media is called a video steganography

F. Protocol Steganography: The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. Sometime cryptography is used with stegnography to provide extra security layer.

II. PROBLEM DEFINATION

Data security is very needed in communication because of attack on data. Cover file is used to hide data by using stegnography 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 but steganography is not used in compressed 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 taking compressed file. New algorithm use compressed file as cover file and it converts content of cover file & secret file into bytes and then hides that at the end of file. It also encrypt secret key for provide more security. Another reason for implementing stagnography is that we using block wise manner. So it require less time for hiding data than current techniques.

III. PROPOSED STEGANOGRAPHY METHODE

In our proposed method we use compressed file as a cover document.

Algorithms:

A. Hiding Process

Input: Cover File, Original File, Password
Output: Stego Document
1) Find the length (size) of the cover file
2) Implement padding of 50 to the size with '+' e.g. if size is 10 (2 digits) then add 48 '+' signs to it If size is 1000 (4 digits) add 46 '+' to it So in any case length will become 10 digits 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 50 to the size with '+'
5) Implement padding of 10 to Extension of original message with '+'
6) Implement padding of 50 to the password with '+'
7) 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
So total length of string will become: 50 + 50 +10+ 50 + 5
So embeded file is like: 50 characters of length of cover file message + 50 characters of length of the original file + 10 characters length of extension + 50 characters of encrypted password + 5 characters of special characters. So total characters are 165 (this calculation will be checked in retrieve module)
8) This combination of the string will be encrypted by converting it into ASCII value and then this ASCII value converted into HEX code. After this encrypted string and original file are embedded into cover file after the EOF

B. Retrieving Process

Input: Password
Output: Original Document
1) Retrieve padding data
2) Decrypt this Retrieve data
3) Read 165 characters of the embedded file, so we will get 50 characters length of cover file+ 50 characters length of hidden file + 10 characters of Ext.+50 characters of password + 5 special characters
4) Check 5 special characters to check whether its implemented by our algorithm or not
5) Check 50 characters to check password
6) Find extension of original file from 10 characters.
7) Find length of original file from 50 characters.
8) Find length of cover file from 50 characters.

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.

IV. PROPOSED EXPERIMENT AND RESULTS

In our experiment we take cover file which is compressed file (.rar or .zip) and we can hide any type of file. In hiding Process we can hide our original file into cover file. Here we have to select .rar or .zip file as a cover file (Source File). Next we select finalhide.rar file with size 4.37 MB as a Cover file (Source File) and The below image is an original file(File to be hidden) with size 1.75 MB for this experiment.
Figs 2 show an original file which we will hide it with the help of proposed method.

Fig. 2: Original File before Hiding Process

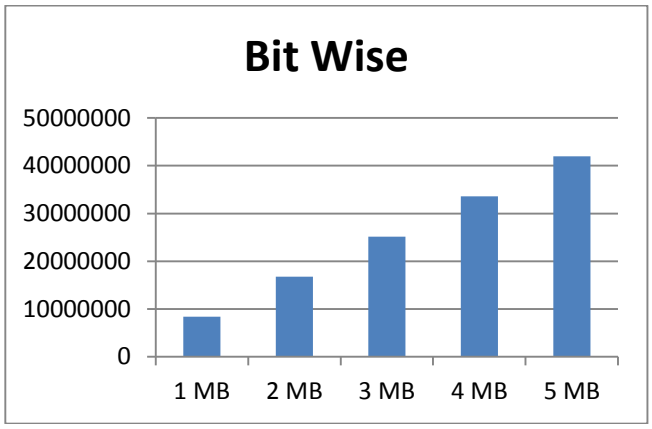
Fig. 3: Original File Extracting Process

This is our original file after extracting process. There is no any modification done through hiding and extracting process. In this experiment, we use image file as a secrete file. We can also use other types of file like video, text, doc, pdf, jpg etc. in same way.

Performance Analysis

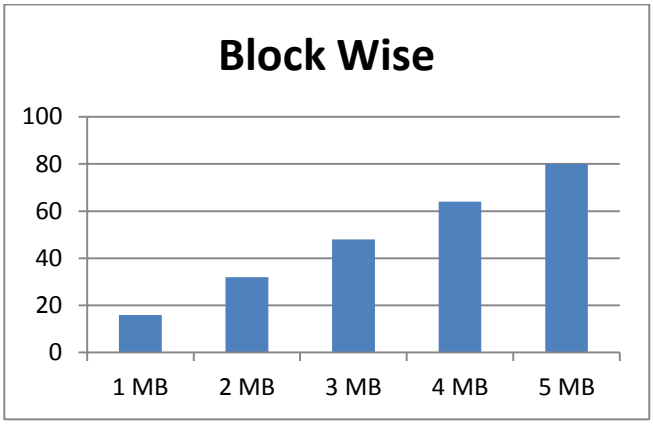
	Proposed Algorithm	**Bit-Wise Algorithm**
Process of hiding data	Block wise	Bit wise
Data Hiding Capacity	Very High	Low
Time For Hiding Process	Less For Ex: 1 MB file size 1MB=1024 KB 1024 KB=1048576 bytes 1048576/65536=16 Loop= 16 times	More For Ex: 1 MB file size 1MB=1024 KB 1024 KB=1048576 bytes 1048576*8=8388608 bits Loop= 8388608 times
Effect in Cover File	None	Depends on Hidden Data
Size of secret data	No limitation	Less than cover file size
Invisibility	High	Depends on method
Robustness against attacks	Low	Medium
Robustness against cover file manipulation	Very Low	Medium
Original file format	We can use more than one file format. Like .jpg, .txt, .doc, .pdf etc	We can use only one file format Depends on algorithm used for hiding process

Table 1: Performance Analysis



Graph: 1 Bit Wise method

This graph show total loop required to hide data using bit wise method like LSB, MSB etc.



Graph: 2 Block wise method

This graph show total loop required to hide data using block wise method that is our proposed method. From comparison of two graph we can say that block wise method is more reliable and faster than bit wise method.

V. 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 introduced about new cover object which is compress file (.rar or .zip) act as a cover document and also presented efficient algorithm for embedding data into this compress 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.

VI. FUTURE ENHANCEMENTS

The existing technique is hide data at the end of compressed file. We can also hide data in cover file as well as at the end of compressed file. We can implement this algorithm on another

file or we can optimize algorithm and improve the efficiency that require less time and more data for hiding process.

VII. ACKNOWLEDGMENT

With the cooperation of my guide, I am highly indebted to Asst. Prof. Risha Tiwari, for his valuable guidance and supervision regarding my topic as well as for providing necessary information regarding research work. I am very much thanks to Asst. Prof. Indraji Rajaput and Asst. Prof Vinit Gupta for helping me in text preparation.

REFERENCES

[1] J. Fridrich, Multimedia Security Technologies for Digital Rights Management. Academic Press, 2006, ch. Steganalysis, pp. 349–381.J. Fridrich, R. Du, and M. Long, "Steganalysis of LSB encoding in color images," *in Proceedings of the IEEE International Conference on Multimedia and Expo. New York, USA: IEEE Computer Society Press, 2000.*

[2] N. Provos and P.Honeyman "Hide and Seek" An introduction to steganography, *IEEE Security and Privacy, p.p. 32-44, May/June 2003.*

[3] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, Silman, J., "Steganography and Steganalysis: An Overview*", SANS Institute, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999*

[4] A.Joseph , Raphael,Dr.V Sundaram "Cryptography and Steganography – A Survey", *Int. J. Comp. Tech. Appl., Vol 2 626-6302*

[5] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, Silman, J., "Steganography and Steganalysis: An Overview*", SANS Institute, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999*

[6] Mr . Vikas Tyagi*1, Mr. Atul kumar2, Roshan Patel, Sachin Tyagi, Saurabh Singh , Gangwar "Image steganography using least significant bit with cryptography*" International Journal of Advanced Science and Technology-2010*

[7] Daisy Jacobs, Deshpande Neeta, Kamalapur Snehal," Implementation of LSB Steganography and Its Evaluation for Various Bits*" in IEEE-2012*

[8] Dr. R. Siva Rama Prasad, Kalavathi.All, "An Evolution of Hindi Text Steganography*", in IEEE-2009*

[9] Mohit Garg," A Novel Text Steganography Technique based on Html Documents*", in International Journal of Advanced Science and Technology-October 2011*

[10] Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm" *in International Journal of Engineering Reserch and Apllication-February 2013*

