Compressing Confidential Data by using Hide-n-Send

Ms. Shruti
Assistant Professor
School of Computer Science and Engineering,
Lovely Professional University, Jalandhar.

Abstract
Steganograpgy is a technique in which data will be hidden but it is visible to the actual sender and decorder. Steganograpgy is the another pillor of Information security likewise in case of encryption we needs to scramble the text but in case to this technique we need not to scramble we just needs to hide confidential data in some cover image,videos and audios. In this paper, Hide-n-Secret tool is used for implementing Steganography for hiding data from intruder. This tool is highly potent, because as with this secret data will be hidden in any cover image and then further it will be encrypted by using different algorithm such as SHA, DES and Triple DES . We can use hashing algorithm for encrypting secrete data.

Keywords
SHA Algorithm; Xaio Steganography; PSNR; DES; Hashing Algorithm; Triple DES; S-tools; Invissible Secrets

Introduction

Without internet nothing is possible and if we want to send something over the wireless network then internet is the good source. So steganography is the term which is given by Johannes Trithmius that started in 1499 , in this he explained that how data is being transfered without opening secret information among intruders.[1]. In this paper I have studied about six steganogragy tools and they all will work upon the basis of Least significant bit insertion, Masking and filtering, Transformations. [6] Stegnography is the technique which is used to hide data in any medium and that cover image may be of any image format type like BMP,JPEG,GIFF,PNG or any other type. To hide image or any secret data we have many tools with us and in the second part of this paper I have discussed about them also. Using steganography, we can hide secret data by using multiple cover mediums like images ,videos and audio but this paper is concerned about only image type of cover medium. When the data will be hidden it will not be identified by the intruder.[7] When the confidential material is kept concealed in between any medium , then the cover image still remain same. It will give identical look ,it will not change and will provide robustness also and also easily send over the network also; after hiding secret data the image will not become heavy rather it will not detected by man in the middle and intruder is not aware about the secrecy of that image. In this research paper as the first section id dedicatedly for the introduction part ,second section which is literature review in this complete literature is given that I will study different tools and discuss the advantages and disadvantages of each and every tool. In the third section I discuss about one tool which is hide-n-send, in which I actually performed implementation part that how the image will be hide. In fourth section of this paper it will cover the result part. In Fifth section of this paper it will cover the conclusion part.

2. Literature Review

Almost every steganography tool[2] have its own pros and corns,and theyhave there own advantages and disadvantages. But they almost all the softwares work upon Least Singificant bit techniques(LSB). And they will be created in any programming language.

Various software[4] which is selected for the comparisions are InvisibleSecret, Hermetric, Puffer, S-tools, Hide-n-send,Xiao-Steganography.

Invisible Secret is a tool which is again used to hide data but in this cover image is BMP only and this tool will work upon Least Significant Bit(LSB) strategy only and it is used to hide data by using multiple algorithm such as AES, DES and various hashing techniques also. Detection rate is not higly preferable as according to the puffer tool which is also discussed below.

Puffer is the tool which is againg used to hide most sensitive and highly authenticated data inside the cover image which is only of jpeg type. This tool will generally used various algorithm like AES, DES, Triple DES, Diamond 5, MD5 and many more. This tool will provide low detection rated means to say that whenever the image will be hides then the confidential data will bot be checked by the intruders.

Hermetic Steganography is a tool which is developed in 2009. In this type of software we can hide our data in BMP cover image only. That's the drawback of using this tool that we are restrict towards BMP type of images only.Concealing is done by encryption then after that image will be hidden and then it will be send over the network as a stego image.

S-tool is created by andy brown in 1996. This tool will be able to hide files or cover images can be of BMP, GIF and WAV files. This tool will be able to hide sound as well as images also.

This tool will be able to hide image or secret data but first it will encrypt that file the after image or data will be kept hiden inside some type of cover images. This tool is good in capacity means to say that user can store maximum no. of secret data. Encryption os done by various algorithm like DES, AES, triple DES and many more.

Table:-1 Shows Steganography Software's along with there description.

Steganograp-hic Software	Software Size	Software Description	Software Creator	Software Sources
Invisible Secrets 4	2.7 MB	Security suite software that can hide files, encrypt files, destroy Internet traces, shred files, make secure IP to IP password transfer and even lock any application on the computer	NeoByte Solutions	1. http://www.invisiblesecrets.com/download.html
Hermetic Stego 8.04	2.30MB	Uses encryption and hiding technique to hide files of any type and of any size in BMP images, with or without the use of a user-specified Stego key	Hermetic system	1. http://www.hermetic.ch/hst/hst.htm
Puffer 4.04	1.90MB	It a security is general purpose encryption and Steganographic software; with Extensive wiping options are also available to permanently erase sensitive data.	Briggs Softwors	1. http://www.soft32.com/download_7842.htm
Xiao Steganography2.6.1	2.14MB	It is security software that implements cryptography/Steganography. It offers unique art of encrypting and hidden files. It can Includes attach any file, doesn't matter the type of file (limited by the size of host image)	Nakasoft	1. http://download.cnet.com/XiaoSteganography/3000002092_410541494.html
S-Tools	561 KB	It is a Steganography that hide files in BMP, GIF, and WAV files. And also uses some encryption technique as an added layer of security.	Andy brown	1. http://www.jjtc.com/Security/Stegtools.htm

In Table 2, I have clearly stated the features of Steganography tools which covers name of software, host image format, software capacity, memory usage, encryption support and steganographic algorithm. Each and every software is easy to use[4] and friendly to hide every data inside any medium.

Table:-2 Capabilities of steganographic software

Steganographic Software	Host Image Format	Software Capacity	Memory Usage	Encryption Support	Steganographic Algorithm
Invisible Secrets 4	BMP,JPEG, PNG	12.8	10.104KB	AES,Twofish,RC4,Diamond2	Least Significant Bit(LSB)
Puffer 4.04	BMP,JPEG, PNG,GIF	38.40	4.512 KB	Deffe-Helman	Least Significant Bit(LSB)

Hermetic Stego	BMP	12.20	7.22KB	DES encryption algorithm, ME6 encryption	Least Significant Bit(LSB)
Xio-Steganography 2.6.1	BMP	12.50	6.256KB	Rajindal algorithm and substitution method	Least Significant Bit
S-tools	BMP	12.80	1.224KB	Idea,DES,Triple DES	Least Significant Bit
Hide-n-Secret	JPEG	13.5	7.22KB	RC2,RC4,DES, Triple DES, Hashing,MD5,MD 4,SHA.	Least Significant Bit

There will be trade off between all the software's such that particular software[5] is good in some specific parameter and some is perfect in some other parameter. So, I can not justify that only specific software is proved o be best.

In all the software the capacity[5] means to say that how much data is being stored inside your images. In general as per the capacity of holding secret data then we can say that puffer is the tool which will be able to store bulk amount of confidential data.

3. Proposed Method for Covering Data:-

In Section 2 of this paper, shows different tools of steganograpgy but in this section I implement Concept of suppressing data by using Hide-n-Secret-Steganography.

Most of the vital thing is in steganography[6] is to hide the confidential data inside any cover image. Not even any single person will be able to detect about the confidential data, apart from sender and receiver, no one will be able to know about the confidential data.

Over the internet there are multiple software[3] which is used to hide secret data by using steganogragy and over the internet there are multiple software who work on encryption also.

Hide-n-Secret provides multiple features for the security to confidential data by various concealment algorithm are like M-f5,M-lsb,Fs, LSB. There are multiple options in hashing algorithm also such as SHAS12,RIPEMD,MD5 under encryption algorithms data can be protected by AES,RC2,RC4.Hence with the help of concealment algorithm ,hashing algorithm and encryption techniques we can encode our secret data and further more provide prevention from intruder attack.

3.1 Hide-n-Secret Steganography

Hide-n-Secret Steganograpgy is a tool which is used to hide Secret Data from un-athorized users just to prevent confidentiality,integrity and availability of data. Hide-n-send is the tool, which is simpler to use,and it is going to use cover medium like JPEG or JPG. This tool is based upon Pixel value differncing technique and this tool is developed in language C. This tool will be able to conceal data by using multiple algorithm like encryption techniques, concealing techniques and various hashing stratigies.

Hide-n Send is the tool which implements image stenography. It includes encryption, concealment and hashing methods to hide secret data inside the cover image and that should be JPEG image format only. Hide-n-send is a tool which is exactly based upon LSB techniques and that software is created in C++.

Following are the various steps that shows encodding and decodding is achived by Hide-n-Secret:-

Step:1 Open Hide-n-Secret tool to implement Steganograpgy as shown in Fig:-1 and add file which will be act as you Cover Image.

Step:2 For selecting cover image Fig:-2 shows you wizard from where you can select your target file.

Step:3 After Loading cover image in Fig:-2, now from this wizard we need to select target file which is to be kept secret.

Step:4 In Fig:-3, under settings you can select any option from concealment algorithm, which means that how you can concela your file.

Step:5 In Fig:-4 shows that several option undwer hashing algorithm again for the prevention purpose.

Step:6 In Fig:-5 at last you can select encryption algorithm option.

Step:7 From Fig. 3,4 and 5 , it is mandatory that user must select the option to hide confidential data.

Step:8 It is mandatory that for both the sender and reciver must work on same tool, because it is useful for the extraction purpose as well.

Step:9 In Fig 6. Wizard shows the extraction module that how we will be abole to extract the secret file from cover medium.

Step:10 From fig 6, decoder will first select the image by clicking on first browse button.

Step:11 in Fig 6, then decoder must select extraction directory as well.

Fig:-1

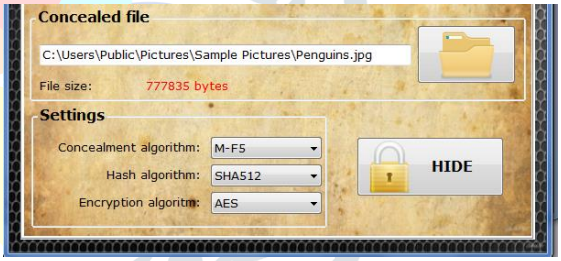

Fig:- 2

Fig :- 3

Fig:- 4

Fig:- 5

Fig:- 6

4. Results

In the third section of this paper I have worked upon Hide-n Send tool, So, in the previous section I have clearly stated the steps that how Hide-n Send will be able to hide secret data and how decoder will extract the files or the secret data from the cover image. To work with this , it is mandatory that both encorder and decoder must use same platform only the encryption and decryption will take place otherwise not possible. On the certain few parameters I have compare all the six tools and each and every tool is better in its own way . If we spot a light on PSNR value then Fig:-7 shows the difference in this value by using different software.

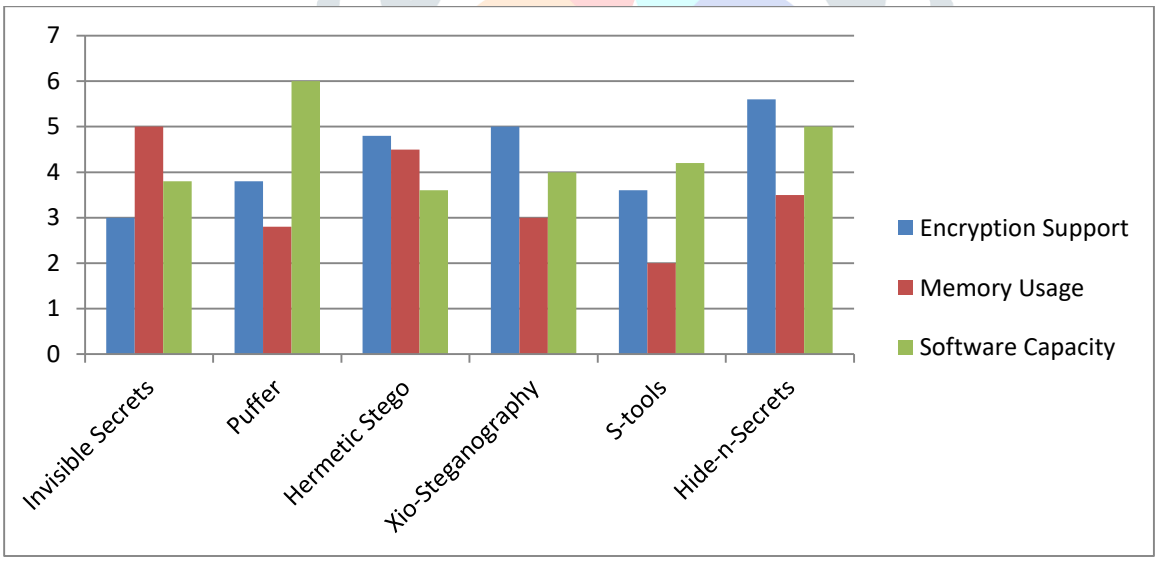

Fig:-7:- Compairing PSNR Values of stego-image by using all the different tools

5. Conclusion

In this research paper, I have studied about six steganography tools, and each and every tool is best in its own way but there are few parameters which makes a particular tool proved to be best.

As per according to encryption support, Hide-n-Send is working properly because it provides several options to hide secret data inside the cover image. For encryption, options are like hashing algorithm, concealment algorithm and encryption techniques. At last of this section I would like to conclude that if we consider encryption support, Hide-n-Send is prove to be the best among all , as per according to memory usage then the software which will take less memory i.e S-tools is prove to be best. If we consider about Software capacity, then puffer is the tool which will contain maximum data inside cover image.

6. References

[1] M.K. Arnold, M. Schmucker, and S.D.Wolthusen, ―Techniques and Applications of Digital Watermarking and Content Protection‖, Artech House, Norwood, Massachusetts.

[2] L.Y. Por1, W.K. Lai2, Z. Alireza3, B. Delina4 StegCure: An Amalgamation of Different Steganographic Methods in GIF Image 12th WSEAS International Conference on COMPUTERS, Heraklion, Greece, July 23-25, 2008 ISSN: 1790-5109

[3]http://resources.infosecinstitute.com/steganography-and-tools-to-perform-steganography/

[4] AKRAM M. ZEKI , ADAMU A. IBRAHIM AND AZIZAH A. MANAF Steganographic Software: Analysis and Implementation International Journal Of Computers And Communications Issue 1, Volume 6, 2012

[5] A. Piva, M. Barni, F. Bartolini, and V. Cappellini,‖ Capacity of the channel: How many bits can be hidden within a digital image‖. Security and Watermarking of Multimedia Contents, Proceedings of SPIE, Wong, Delp. San Jose, CA, 3657: 437-448. 1999.

[6] K.S, Ntalianis, ―A Short-Message Robust Steganographic Method for Effective Information Recovery Under Transmission Losses of Cellular Networks‖, Proceedings of the 9th WSEAS International Conference on Systems, Greece, 2005, pp. 955-957.

[7] J. J. Liaw, L. H. Chang, Y. S. Liao, ―An Improvement of Robust and Blind Data Hiding Based on Self Reference in Spatial Domain‖, Proceedings of the 2007 WSEAS International Conference on Computer Engineering and Applications, Gold Coast, Australia, 2007, pp. 259-263.