

# Conceal Classified Data by using Xiao Steganography

Ms. Shruti

Assistant Professor, Lovely Professional University/ School of Computer Science and Enggining, Jalandhar, India  
shruti.jairath@gmail.com, shruti.23677@lpu.co.in

**Abstract**—Steganography is a science of hiding message in such a way that existing message should be invisible to anyone apart from sender and receiver. As we deal with several algorithm that accord with text encryption. There has been research carried out on encryption digital images video and audio files. In this paper, Xiao 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. For encoding purposes password will be assigned for double security. So that genuine person will be able to access particular Data. Now at decoding end when user want to extract hidden data then this will be possible only by assigning password which is given by encoder while hiding. Other than this I m comparing different Steganography tools on the basis of some parameters which are discussed in coming section of this paper. So from all the tools S-tools is proved to be best.

**Index Terms**— SHA Algorithm; Xaio Steganography; PSNR; DES; Hashing Algorithm; Triple DES; S-tools; Inivisible Secrets.

## I. INTRODUCTION

The internet has become the most important source of information, which offers ubiquitous channels to deliver and exchange information. The term Steganography which was earlier described as Steganographia first appears in a manuscript by Johannes Trithmius that started in 1499 [1]. The goal here is to hide data inside other harmless data in way that does not allow any suspicious present of the hidden data so that it can be used as a medium for transmission of secret information. Embedding secret data, into harmless data requires the presents of the two files. The first is the innocent-looking file that will hold the hidden information called the host file. The second file is the secret message. A message may be plaintext, cipher text, or any bit stream. When combined, the host file and the embedded message make a Stegofile. Over the years, many algorithms were proposed for steganographic technique, the common approaches include: Least significant bit insertion, Masking and filtering, Transformations. [6] Each of these techniques can be applied, with varying degrees of success. The strength of each technique relies on robustness, image quality (imperceptibility) and capacity, by definition it means the ability of information to be hidden in a carrier medium without any suspicious clue of the present of any embedded information. These have been found that when the robustness of the watermarking method improves, the imperceptibility decreases, and the capacity increases. In addition, there is also a tradeoff between these requirements and this should be taken into account whenever the steganographic method is proposed. One of the important considerations of digital steganography is that the presence of the hidden message be undetectable. [7] This means that files with and

without secret message should appear identical to all possible statistical tests which can be carried out. Another important consideration is robustness. A robust technique means the ability of the secret message embedded in a carrier file to retain its states, without been degraded by any means and maintains its quality. The final important consideration is the capacity of the communication channel. In this aspect, the challenge is to embed as much information as possible in the carrier file, while still maintaining the state of the carrier file without any distortion. This paper is divided into several sections such as Literature review, Implementation, Results, Conclusion and references.

## II. LITERATURE REVIEW

Almost all Steganographic software [2] comes with their strengths and weaknesses, and they are mostly based on different techniques and algorithms. It's a fact that each Steganographic software has been designed by different company, and developed by different programming language. Some are open source while some are not, and other comes as part of security suite software [4]. This study aimed at comparing the features and capabilities of most popular and current Steganographic software available. The software selected [4] for the comparisons are: Invisible Secrets 4, Hermetic Stego 8.04, Puffer 4.04, Xiao Steganography 2.6.1, and S-Tools.

Invisible Secrets 4 is a powerful security suite that can hide and encrypt files, also can destroy internet traces, shred files, make secure IP-to-IP password transfer and even lock any application on the computer. It is an easy to use with a powerful wizard interface. It was first released in 1999; the latest version is —Invisible Secrets 4 that was released in 2009 by NeoByte Solutions. It accepts five hosts file formats Steganography applications, which are: JPG, PNG, BMP, HTML and WAV.

Puffer version 4.04 was released as a revised version of Puffer 4.03 in 2009. It is a general purpose encryption and Steganographic software that is used to protect most sensitive data from unauthorized viewing to securely exchange message or email with other Puffer users. It hides data among the pixels of image, and distributes self-decrypting archives to non-Puffer users. Extensive wiping options are also available to permanently erase sensitive data. Puffer runs on all 32-bit versions of Windows from 98 through Vista. Puffer 4.04 has displayed the ability to hide encrypted archives among the pixels of 24-bit color image, specifically PNG and BMP files.

Xiao Steganography 2.6.1 is developed by nakasoft ([www.nakasoft.net](http://www.nakasoft.net)) in Venezuela. It is easy to use and powerful wizard interfaced. It was released in 2005; it offers an impressive and unique art of hidden writing. It accepts many different types of file. The security level use RC2, RC4, DES, Triple DES, Triple Des 112 and Hashing MD2, MD4, MD5, SHA Algorithms through using password protected.

Hermetic Stego 8.04, is part of Hermetic applications under Hermetic system which was released on 2009. Hermetic Stego is able to hide any type of file within BMP images, with an encryption key, so that the presence of the hidden file is undetectable, if a Stego key has been used when hiding the data then that data can be extracted only by someone who knows that Stego key. The Stego key is used not only to facilitate random selection of bytes for hiding data file bits but also is used to encrypt the data file.

S-tools, was developed by Andy brown in 1996. S-Tools is a Steganography tool that hides files in BMP, GIF, and WAV files. It can hide multiple files in one sound/picture and the data is compressed before being encrypted and then hidden. Multi-threaded operation means that the user can have many hide/reveal operations going simultaneously without fear of them interfering with other work. The user can even close the original picture/sound with no ill effects to ongoing threads. S-Tools use the spatial domain technique and works by spreading the bit-pattern of the file that will be hidden across the least significant bit. S-Tools use four encryption options (IDEA, DES, Triple DES and MDC) that give an additional security level to its operation. After embedding the message, normally distortion occurred which in turns affect the Stego.

The features of the software under this study were represented in table 2; they all come with Graphical User Interface (GUI), some come in collection of security applications [4] while others are specifically for Steganographic use only.

The capabilities of the software (The Image format, Capacity [5], Cryptographic algorithm and Steganographic techniques). Notice that the capacity refers to the amount of information being able to be inserted into a particular image. In general, increasing the capacity will make the hidden image more obtrusive in viewing. Measuring the embedding capacity can be done directly by dividing the size of the embedded information on the size the host image. Notice that the capacity [5] refers to the amount of information being able to be inserted into a particular image. In general, increasing the capacity will make the

TABLE I. SHOWS STEGANOGRAPHY SOFTWARE'S ALONG WITH THERE DESCRIPTION

| Steganographic 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. <a href="http://www.invisiblesecrets.com/download.html">http://www.invisiblesecrets.com/download.html</a>                                           |
| 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. <a href="http://www.hermetic.ch/hst/hst.htm">http://www.hermetic.ch/hst/hst.htm</a>                                                                 |
| 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. <a href="http://www.soft32.com/download_7842.htm">http://www.soft32.com/download_7842.htm</a>                                                       |
| 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. <a href="http://download.cnet.com/XiaoSteganography/30002092_410541494.html">http://download.cnet.com/XiaoSteganography/30002092_410541494.html</a> |
| 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. <a href="http://www.jjtc.com/Security/Stegtools.htm">http://www.jjtc.com/Security/Stegtools.htm</a>                                                 |

TABLE II. CAPABILITIES OF STEGANOGRAPHIC SOFTWARE

| Steganographic Software | Host Image Formats | Software Capacity | Memory Usage | Encryption Support                                                              | Steganographic Algorithm                     |
|-------------------------|--------------------|-------------------|--------------|---------------------------------------------------------------------------------|----------------------------------------------|
| Invisible Secrets 4     | BMP, JPG, PNG      | 12.80%            | 10.104 KB    | AES-Rijndael, Twofish, RC4, Cast128, GOST, Diamond 2, Sapphire II, and Blowfish | least significant bits (LSB) algorithm       |
| Puffer 4.04             | BMP, JPG, PNG, GIF | 38.40%            | 4.512 KB     | AES encryption algorithm                                                        | least significant 3 bits (Intermediate bit ) |
| Hermetic stego 8.04     | BMP                | 12.20%            | 8.22 KB      | DES encryption algorithm ME6 encryption                                         | LSB technique,                               |
| Xiao Steganography2.6.1 | BMP                | 12.50%            | 6.256 KB     | RC2, RC4, DES, Triple DES, Triple Des 112 and Hashing MD2, MD4, MD5, SHA        | least significant bit (LSB) substitution     |
| S-Tools                 | BMP, GIF, WAV      | 12.80%            | 1.224 KB     | IDEA, DES, Triple DES and MDC                                                   | least significant bit (LSB)                  |

hidden image more obtrusive in viewing. Measuring the embedding capacity can be done directly by dividing the size of the embedded information on the size the host image.

### III. PROPOSED METHOD FOR COVERING DATA

In Section 2 of this paper, shows different tools of steganography but in this section I implement Concept of suppressing data by using Xiao-Steganography. The main reason for using steganography is that you are hiding your secret message[3] behind an ordinary file. No-one will suspect the file. People will generally think it as an ordinary file and your secret message will go without any suspicion. The file used to hide a message will function normally and you will not suspect just by looking the file. There are various conditions when there is the need of secure transmission of files. Hackers are everywhere and always try to intercept communication to get confidential data. By using Steganography, we can reduce the chance of data leakage. Even if the attacker gets access to your account or email, he will have no clue where is the confidential file in your account. There are various ways of achieving the steganography in digital communication. However, you do not need to perform coding to achieve this. There are various software tools are available for Steganography. This software can hide your secret message behind the image file, HTML, DOC file e or any other kind of file. There are many software[3] available that offer steganography. Some offer normal steganography, but a few offer encryption before hiding the data. Few can only hide data behind image, but few can hide data behind any file.

#### A. Xiao Steganography

Xiao Steganography is a tool which is used to hide Secret Data from un-authorized users just to prevent confidentiality, integrity and availability of data. Xiao Steganography is free software that can be used to hide secret files in BMP images or in WAV files. Use of the tool is easy. You can just open the software, load any BMP image or WAV file to its interface. Then add a file, which you want to hide. It also supports encryption. So, you can select from various algorithms like RC4, Triple DES, DES, Triple DES 112, RC2 and hashing SHA, MD4, MD2, MD5. Select any one from the list and then save the target file. To read the hidden message from this file, you will have to use this software again. This software will read the file and will decode the hidden file from it. You cannot extract the hidden file from any other software. Following are the various steps that shows encoding and decoding is achieved by Xiao:-

Step:1 Open Xiao tool to implement Steganography 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:-3, now from this wizard we need to select target file which is to be ket secret.

Step:4 By selecting on Add File button in Fig:-4, we will be able to select Secret file.

Step:5 Fig:-5 shows that Secret file is embedded in Cover image.

Step:6 In Fig:-6 we need to select encryption option and pasword as well for double security of Confidential message.

Step:7 After applying encryption and pasword on secret message then in Fig:-7 shows merging of both the files i.e Cover image and Secret image.

Step:8 All the above seven steps accord with embedding process and fig:-8 finish all the embedding process successfully.

Step:9 Now at decoding end if authenticated user want to extract secret message from cover image then reciver must need to click on Extract file button as shown in Fig:-9.

Step:10 In Fig 10, we need to select Source file.

Step:11 In Fig:-11, shows Source file and by clicking on Extracting Load file we can extract our file.

Step:12 Extracted file is shown in Fig:-12.

Step:13 Now, we need to select that which particular file is to be selected as it is shown in Fig:-13.

Step:14 In Fig:-14 shows that files are extracted by reciver successfully.



Fig:-1

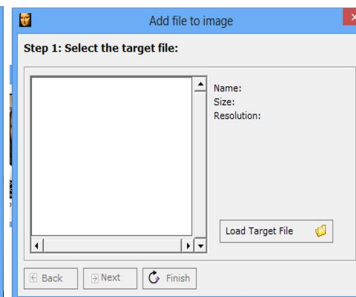


Fig:-2

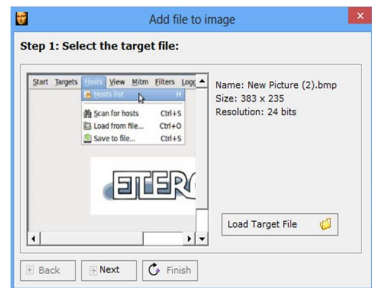


Fig:-3

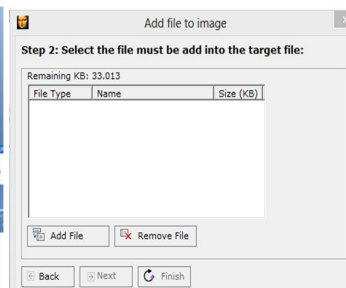


Fig:-4

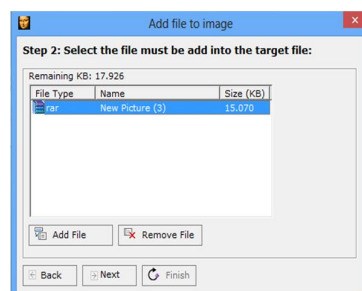


Fig:-5



Fig:-6

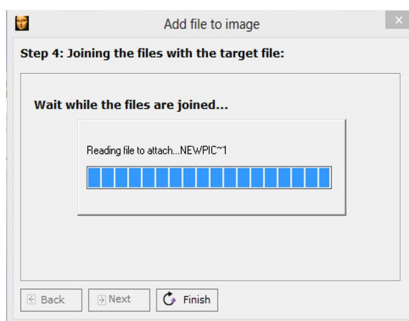


Fig:-7

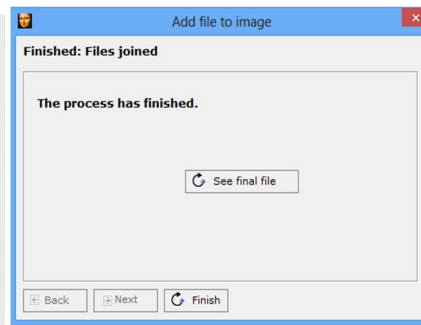


Fig:-8



Fig:-9

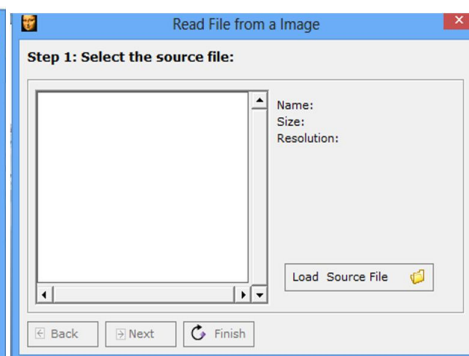


Fig:-10

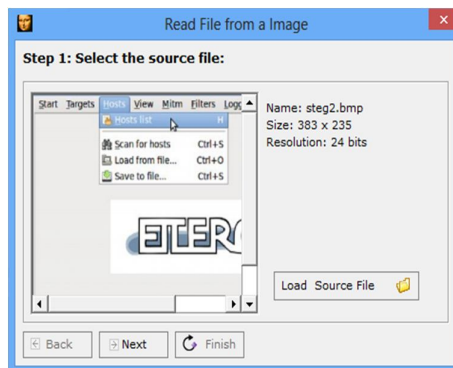


Fig:-11

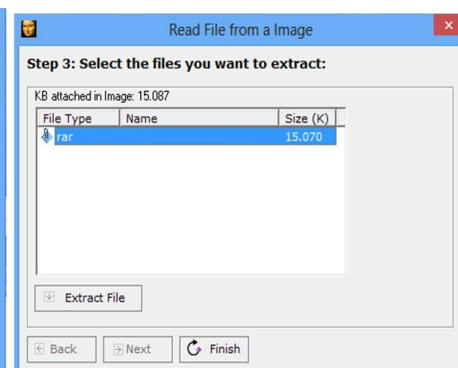


Fig:-12

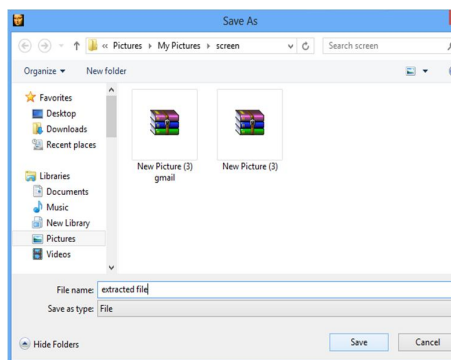


Fig:-13

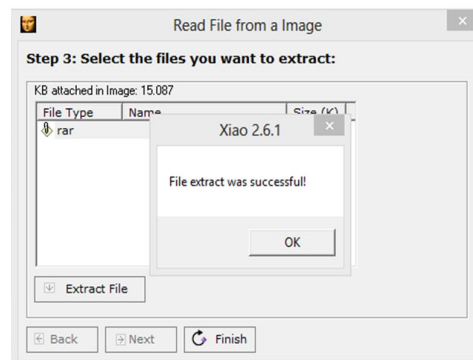


Fig:-14

#### IV. RESULTS

After embedding, the qualities of images were determined. In most applications, hiding algorithm must embed the secret file/files so that it does not affect the quality of the underlying host file. The secret file/files[4] should be truly undetectable, so that the host file cannot be distinguished from the stego image. It's a fact that an ordinary person that sees the stego image may not have previous knowledge of the image; as a result he cannot perform comparison. Therefore, it is sufficient that the modifications in the stego image go unnoticed, as long as the stego image is not compared with the host image. The image quality measure after embedding process, high image quality reflects the success of Steganographic system. If we spot a light on PSNR value then Fig:-15 shows the difference in this value by using different softwares.

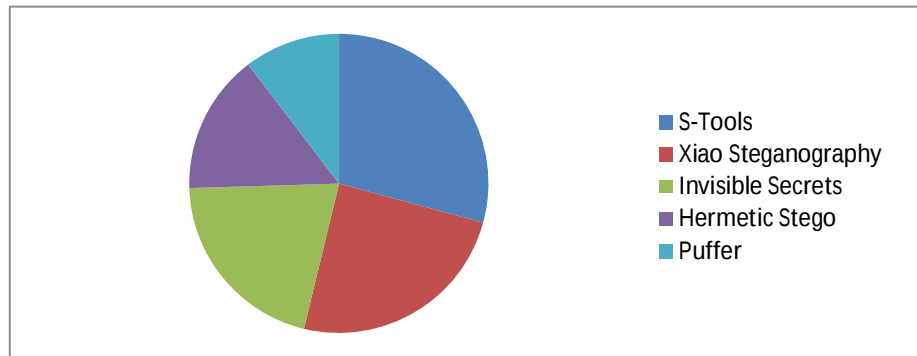


Fig:-15:- Comparing PSNR Values of stego-image by using all the different tools

#### V. CONCLUSION

This research presented a background of Steganography and a comparative study of some Steganographic software. Steganography as information security system can have some useful applications, like other seemingly related system (cryptography). The success of this study is to identify the reliable and best software available in the market for Steganography. Some of the software available in the market were selected based on the recent deployment that is five recently deployed software, these software were tested using the same input on all of them. The tools used in our experiment are images. Specific image was embedded within all host images for each of the five software selected. The results of the experiment reveal that all the five software were relatively performing at the same level, though some software performs better than others. The image quality measure after embedding usually reflects the success of Steganographic system. The tool for measuring the quality of image after embedding is the PSNR. The values of PSNR are obtained using the software under this study were all above the bench mark for the high quality image.

#### 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. Por<sup>1</sup>, W.K. Lai<sup>2</sup>, Z. Alireza<sup>3</sup>, B. Delina<sup>4</sup> 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.