Academic Science

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Issue2
February 2015

Comparative Study of Steganography Tools

Vidya V
MCA Student
Department of computer Science
Christ University

Shoney Sebastian
Associate Professor
Department of Computer Science
Christ University

***Abstract*—** This paper intends to perform a detailed comparison of different tools that are used for image steganography. Image steganography, which is the art of hiding secret data within the images, can be performed using different software tools available. These software tools use different steganography algorithms to perform the operation. Steganography hides the fact that the communication is taking place by hiding the secret data within a carrier file whereas cryptography is a technique that encrypts the secret data during communication. Steganography along with cryptography is more secured data hiding technique and is thus used in many software tools. The paper aims at comparing the properties of the stego image of a carrier file produced from different tools. The steganography methods are experimented and their results are analyzed. Different measures of the stego images such as peak signal to noise ratio, mean squared error etc. are compared and are graphically represented. Thus the paper provides comparison of the different steganography tools.

KEYWORDS:-Carrier file, stego image, steganography, LSB, PSNR, MSE, steganalysis.

I. INTRODUCTION

Security of data can be defined as the major requirement in the modern era of information technology. Maintaining the secrecy of information is considered to be one of the major challenges in the process of data communication. Securing the data ensures the security of communication, but more the security will be if the process of communication itself is hidden. Cryptography and steganography are the most commonly used two techniques to keep the message secret during communication [1]. When cryptography encrypts the data to hide the information during communication, steganography is the technique which hides the fact that the communication itself is taking place. Steganography is thus the science of hiding data [2]. It can be defined as the process in which the information that is to be hidden is stored in the redundant bits of the cover medium (medium within which the data is hidden) and produces the stego medium (the medium produced after steganography). The different cover mediums used for the process of steganography are text, images, video etc. One of the commonly used medium for steganography is *image*. This paper intends to provide a detailed comparison on the different tools used for image steganography. The performance of these open source software are compared to find the best image steganography tool available.

The rest of the paper is organized as follows. Section 2 gives a review of existing Steganography algorithms and Steganography tools. Section 3 describes the features of the Steganography tools selected for comparison. The methodology used in this paper is described in section 4. The experimental results are discussed in Section 5 and the conclusion of the work is discussed in section 6.

Academic Science

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Issue2
February 2015

II. RELATED WORK

In order to analyse the basic features of steganography different papers and websites are referred and a detailed study of steganography algorithms, tools and measures are done.

STEGANOGRAPHY ALGORITHMS

The study of different steganography tools indicates that it works with different algorithms and the commonly used steganography algorithms are LSB method, DES, AES, battlesteg, blindhide, blowfish, SLSB, hideseek, filter first, dynamic filter first, dynamic battlesteg etc.

LSB method: It is a method in which data to be hidden is stored in the LSB of the cover image [3]. The paper [4] discusses a new LSB technique which uses a secret key. In this new technique, the hidden data is inserted at the least significant bit of the bytes depending on the secret key.

DES: This symmetric encryption technique uses 56 bit key and its converts 64 bit input data to 64 bit output. This encryption technique is then replaced by AES method. This method is found to be easily attacked [4].

Blowfish : It is a symmetric encryption method which uses a variable length key [32-448 bit], which helps in securing the data and it is considered to be secured encryption technique .

Advanced Encryption Standard (AES): It is symmetric cipher method in which a same key is used for both encryption and decryption. It allows different key lengths 128, 192 or 256 bits and the encryption process includes 10, 12, 14 rounds respectively for the key lengths [5].

STEGANOGRAPHY TOOLS

Different papers and websites discuss about the various steganography tools. The paper [6] does a detailed comparative study of various tools used for steganography. Detailed comparison of the tools invisible secrets, hermit stego, puffer, Stella, revelations, S-tools etc. are done in the paper. Some of the steganography tools are defined below -:

QuickStego, QuickCrypto : QuickStego is windows based program which lets you hide data within an image whereas QuickCryptro is advanced software which encrypts the secret data before hiding it in the image and thus improves the security of secret data [7].

OpenPuff , Open stego : OpenPuff is a portable steganography and marking software with different data encryption options. It can conceal a text file, image or other files of 256 MB. Open stego is a very simple software that performs data hiding and water marking [8] [9].

Hide and seek : This is one of the older methods and it is carried out by taking the lower order pit of each pixel and using it to encode one bit of the character in the secret data [4] [6].

The other tools used for steganography are Stego PNG, Steganography studio, Stella, Revelations, S-tools .

There are different approaches used for the purpose of hiding data within an image. In order to identify different measures with which the steganography output images are measured different papers are referred. In the paper [10] the evaluation measures of stego image is discussed. MSE and PSNR are the two measures commonly used to compare the image compression quality. PSNR (peak signal to noise ratio) represents the peak error and MSE (mean squared error) represents the cumulative squared error. PSNR is calculated from MSE and larger the PSNR value larger will be the quality of the image and smaller will be the possibility of attack by human eye.

The formula for calculating MSE is

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Issue2
February 2015

PSNR can thus be defined as

$$PSNR = 10.log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20.log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

III. PROPOSED WORK

There are varieties of software available to perform image steganography and this appear intends to compare the following given five tools of steganography using the various steganographic measures. The tools used are QuickStego, QuickCrypto, Open Stego, Stego png, Steganography Studio

QUICKSTEGO

QuickStego [7] is the open source software developed by Cyberscience to perform the concept of hiding a secret text message within an image. The basic operation performed by QuickStego is image steganography. The cover medium that can be used in the software is an image file of formats jpeg, jpg or bmp. User friendly interface of QuickStego provides basic options such as open image file, hide text, get text from the hidden file etc.

Working of QuickStego**:-**QuickStego accepts jpeg (.jpg) images as the cover medium (source file). The output of the steganography process produces a stego medium in the form of a BMP file. As jpeg files are in the compressed mode, the size of the source file will be small, but since bitmap pictures are uncompressed the size of the bitmap files are much larger than a jpeg file.

QUICKCRYPTO

QuickCrypto is the software which implements the concept of improving the security of communication by combining the two techniques called cryptography and steganography. When cryptography encrypts the data to ensure security, steganography hides the channel with which the communication is taking place. QuickCrypto is thus a security software product which hides the fact that communication is taking place as well as encrypts the data to be hidden and so is the name QuickCrypto. It can be considered as an improved and advanced version of QuickStego. The fact that the hidden data is as well as encrypted makes the software a perfect tool for covert communication.

OPEN STEGO

Open stego [9] can be defined as a free steganography software that performs image steganography in the most simple manner. It is the software that is developed purely in java and so is it supported by all the java platforms. The software uses DES algorithm for password based data encryption and MD5 hashing technique is used for the derivation of key. The software provides two major tabs in their interface known as hide data and extract data

As the name implies, the option hide data is used to hide data within a cover file. This process follows the following simple steps such as selecting message file, selecting cover file ,output stego file and provide the passwords.

Extract data is the option provided by the software to decrypt the data which is hidden using the software. The process involves the following steps selecting the input stego file and output folder for the message file. The software is very user friendly, simple and freeware. It also provides digital watermarking options.

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Issue2
February 2015

STEGANOGRAPHY STUDIO

Steganography studio [6] is the complete steganography software developed in java which helps in analyzing the best steganography algorithms. The software is usable in any operating system and it implements variety of steganography algorithms with a variety of filters. The major advantage of this software is that, it could be used to analyze and compare the best steganography algorithms or methods. The software provides steganography using the following algorithms:-Battlesteg, Blindhide, SLSB, Hideseek, Filter first, Dynamic filter firstand Dynamic battlesteg. Steganography studio also provides the option to encode, decode, simulate, analyse.

A feature that differentiates this software from the rest of the software discussed in the paper is the fact that it provides different tools to compare the original file and the stego file. The following analysis methods can be performed using the software.

Steganalysis : Steganalysis performs a RS analysis where in the pixels of the image is statistically analyzed to detect the hidden image. The percentage of RGB in the overlapping and non-overlapping group is analyzed statistically in the method and the average is computed.

Benchmark : Benchmarking technique used in the software analyses the average absolute difference, mean squared error, peak signal noise, correlation value etc. of the original and the cover image.

Histogram : The ratio of the RGB components, saturation, brightness etc. of the original and cover image is generated in the form of histogram.

STEGO PNG

Stego png [11] is the software that is used to encrypt and hide data in png or bmp file. It is a very simple windows program which helps to hide data within an image, and the file could be a ext file, MS word document or an excel spreadsheet. The algorithm used for developing the software is considered to be more secured than other steganography programs due to the reason that data is inserted in the image in random way. Insertion of data is basically dependant on a key (same key is used for encryption process as well). Bits of image file are modified to insert the data within the image file. In order to compensate this modification, other bits of the image files are also changed accordingly and thus the properties of the image are not altered. The randomized data insertion using key increases the security of the steganography. The software also provides option to add ‘watermark’ to the images.The encryption key must be of length 16 to 64 characters and the checksum value of the key is displayed immediately. It helps the user to check the error while typing the encryption key. If same key is used for many encryptions it generates the same checksum value and thus helps the user to ensure the key value while typing.

IV. METHODOLOGY USED

In order to compare the performance and efficiency of different steganography tools, a particular data is hidden within an image using different tools. The steganography software QuickStego, QuickCrypto, Open stego, Stego png and Steganography studio are installed and image steganography is performed in each of these software.

An input file (image file) of specified format is selected and the data (text, image) is hidden within the image. The output files obtained from each of the software are studied and analysed to compare the performance of the software.The size of the output file, means squared error, average absolute difference, peak signal to noise ratio etc. are the various measures used to perform steganalysis. The

steganography studio provides an option to compare the original image with the stego image. Using steganography studio, a detailed comparison is performed.
An input file (image file) of specified format is selected and the data (text, image) is hidden within the image. The output files obtained from each of the software are studied and analyzed to compare the performance of the software.The size of the output file, means squared error, average absolute difference, peak signal to noise ratio etc. are the various measures used to perform steganalysis. The steganography studio provides an option to compare the original image with the stego image. Using steganography studio, a detailed comparison is performed.

V. EXPERIMENTAL RESULT

Consider the image given below:

Fig 1 : m1.jpg

Image size: 8.99 KB
Format : .jpg file
Secret text: Steganography is the technique of hiding private or sensitive information within something that appears to be nothing out of the usual.
Original image + secret text = stego image
The image (Fig 1) is used as the cover image and the secret text is stored within it using different algorithms.

Software 1 : QuickStego
Output Features:-
Size : 147 KB
Format : .bmp file
Avg Absolute Difference : 0.015476001271455818
Mean Squared Error : 0.03176652892561983
Peak Signal to Noise Ratio : 72.34142960843042 dB
Correlation Quality : 150.90888948447636

Software 2 : QuickCrypto
Output Features:-
Size : 13.4 KB
Format : .jpg file
Avg Absolute Difference : 0.0
Mean Squared Error : 0.0
Peak Signal to Noise Ratio : 0.0 dB
Correlation Quality : 150.90898579324713

Software 3 : Openstego
Output Features:-
Size : 70.3 KB
Format : .bmp file
Avg Absolute Difference : 0.012396694214876033
Mean Squared Error : 0.012436427209154482

Peak Signal to Noise Ratio : 76.41417091378847 dB
Correlation Quality : 150.90841220836722

Software 4 : Steganography studio

Output Features:-

Size : 70.3 KB
Format : .bmp file

Avg Absolute Difference : 0.011224570883661793
Mean Squared Error : 0.01333041958041958
Peak Signal to Noise Ratio : 76.11268904420284 dB
Correlation Quality : 150.90821133985273

GRAPHICAL REPRESENTATION

The following are the graphical representations of the comparison results.

Fig 2 shows the difference in the size of stego file generated in different software.

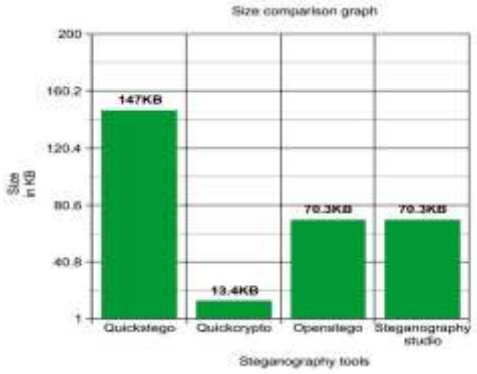

Fig 2: Size comparison grap

The size of stego image produced from Quickstego is much larger than other stego images and the least sized stego image is produced by Quickcrypto.

Fig 3 shows the difference in Mean squared error value in different output files

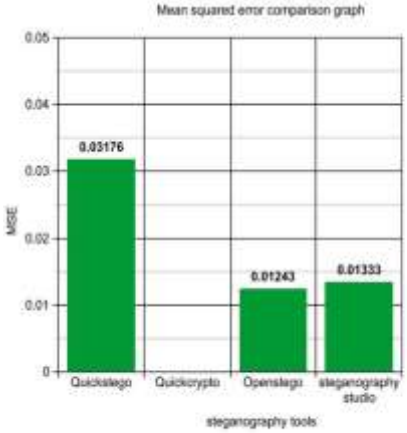

Fig 3: MSE comparison graph

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Issue2
February 2015

Fig 4 shows the difference in peak signal to noise ratio in different output files.

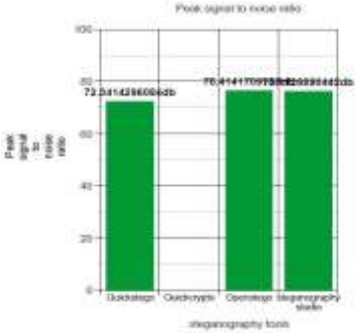

Fig 4: PSNR comparison graph

It can be analysed that the largest PSNR value is generated from the software open stego(76.41 db) and so larger is the quality of stego image produced.
Fig 5 shows the difference in average absolute difference in different output files.
Average absolute difference is the mean difference of two independent values drawn from a distribution. It can be analysed from the graph that the avg absolute difference between the original and cover image is maximum for the software Quickstego (0.0154)
Fig 6 shows the difference in correlation quality.

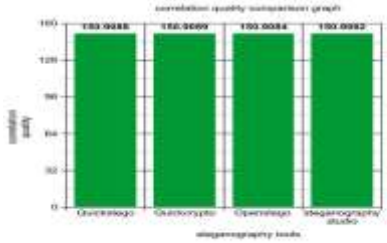

Fig 6: Correlation quality comparison graph

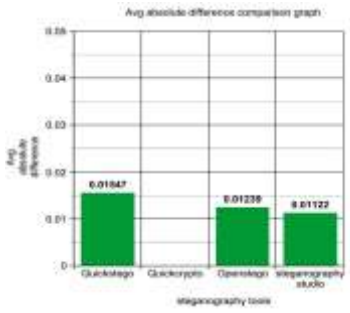

Fig 5: Avg absolute difference comparison graph

Correlation quality values of the output files falls in the same range (approximately 150.9).

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Issue2
February 2015

COMPARISON TABLE

The Table - 1 provides detailed comparison of the software based on the various features.

TABLE-1

Features	QuickStego	QuickCrypto	Openstego	Steganography studio	Steg png
Operating system	Windows XP,Vista,7,8	Windows XP,Vista,7, 8	Windows ,Linux	Windows, Linux	Windows
Source files	bmp, jpeg, gif	bmp, jpeg, gif, pdf, doc, text	bmp, gif, jpg, jpeg, png, wbmp	Bmp, png, gif	Bmp, png
Technology used	Steganography	Cryptography and steganography	Steganography and watermarking	steganography	Steganography, cryptography and watermarking
Availability	Freeware	Not free	Freeware	Freeware	Not free
Algorithms used to hide data	Alters the pixels of the image, encodes secret data by adding small color variations.	AES, Triple DES, Blowfish	DES algorithm,MD5 hashing technique	Battlesteg, Blindhide, SLSB, Hideseek, Filter first, Dynamic filter first, Dynamic battlesteg	Encryption using key
Features	Hides text within image	Encrypts text, files, folders.	Hides text within an image	Hides data within an image	Hides files(txt, image) within an image
Output file	Bitmap file	Overwrites the same file		Bitmap file	Bitmap or png file

VI. CONCLUSION

The paper presented a comparative study on the various tools used for image steganography. The experiment result shows that depending on the algorithm used for image steganography the efficiency, quality and noise rate of the stego image varies. Each of the software discussed above uses different algorithm and the efficiency of the algorithm determines the efficiency of the software. MSE and PSNR are used as a measure to determine the quality of the stego image and the value of PSNR analysed reveals that the software that are discussed above have a similar performance level. The quality of the image measured defines the level of security ensured by the steganography methods and it succeeds in the process of hiding the fact that communication is taking place.

References

[1] Jassim Mohmmed Ahmed and Zulkarnain Md Ali "Information Hiding using LSB technique" IJCSNS International 18 Journal of Computer Science and Network Security, April 2011.
[2] F. Hartung and M. Kutte "Information hiding-a survey, "Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Content, Volume: 87 Issue:7, pp. I062-I078, July. 1999.
[3] Namita Tiwari and Dr.Madhu Shandilya "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format" International Journal of Computer Applications (0975 – 8887).
[4] S. M. Masud Karim, Md. Saifur Rahman and Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key" International Conference on Computer and Information Technology (ICCIT 201 I).
[5] Jawahar Thakur and Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" International Journal of Emerging Technology and Advanced Engineering
[6] Akram M. Zeki , Adamu A. Ibrahim Azizah A. Manaf and shahidan M. Abdullah "Comparative Study of Different Steganographic Techniques"
[7]"Quickstegosoftware"http://www.QuickCrypto.com/free-steganography-software.html
[8] "Openpuff v4.00 steganography & watermarking " http:// embeddedsw.net /doc/ OpenPuff_Help_EN.pdf
[9]"Openstego features" http://www.openstego.info/features.html
[10]Naitik P Kamdar, Dipesh G. Kamdar and Dharmesh N.khandhar "Performance Evaluation of LSB based Steganography for optimization of PSNR and MSE" Journal of information, knowledge and research in electronics and communication engineering.
[11]"Stego png" http://www.hermetic.ch/stpng/stpng.h