Steganographic Tools for BMP Image Format

Prof.Sumedha Sirsikar Prof. Asavari Deshpande

Department Of Information Technology
MAEER'S Maharashtra Institute of Technology
Pune, Mahatashtra, 411038, India.
{sirsikarsd, asavari.deshpande}@gmail.com

***Abstract*:** The goal of steganography is to transmit a message through some innocuous carrier i.e. text, image, audio and video over a communication channel where the existence of the message is concealed. In this paper we present characteristics, performance, and robustness of various Steganographic freeware tools. Out of this few tools are used for steganography and steganalysis that evaluate and identify the shortcomings which are useful to Forensic analysts. Performance measurement is carried out on the basis of visual inspection and statistical comparison. The result for few tools is presented in this paper.

***Keywords*:** Steganography, BMP format, Tools

1. Introduction

Private and personal data communication is a need of today's world. A solution to this is a Cryptography [1] that scrambles the confidential information which can be read by only intended recipient. But the communication is easily recognized because of encrypted data and hence privacy and confidentiality is lost. Alternate technique of hiding information is Steganography that provides privacy and security by making confidential communication invisible. Cryptography is not related to the invisible communication, where the goal is to secure communication from an eavesdropper. But steganography hides the existence of the communication channel itself. The output of steganography operation is not apparently visible whereas in cryptography output is scrambled, hence it can draw attention.

In literature the term 'information hiding' is often used as a synonym for steganography. Steganography need to be robust against distortion like compressions or color adjustment. Also, it communicates in a completely undetectable manner unlike watermarking.

It is used in the field of secret communication ex, exchange of highly confidential data in a covert manner say on public discussion board or forum. It can also be used for secure and invisible storage of confidential information like patents that can be stored on hard disk partitions.

The objective of this paper is to analyze and carry out statistical study of various Steganography tools (freeware). To support this experimental results are carried out which identifies their characteristics.

The rest of the paper is organized as follows. Section 2 introduces history technical aspect of steganography. Section 3 gives perspective of Steganography. Section 4 details of various tools for data hiding. Section 5 describes comparative results of tools. Section 6 conclusion and future work.

2. History of Steganography

Steganography is derived by Johannes Trithemus (1462-1516) from "Steganographia" and comes from the Greek word, defined as "covered writing". Hidden message will not arouse an eavesdropper's suspicion.

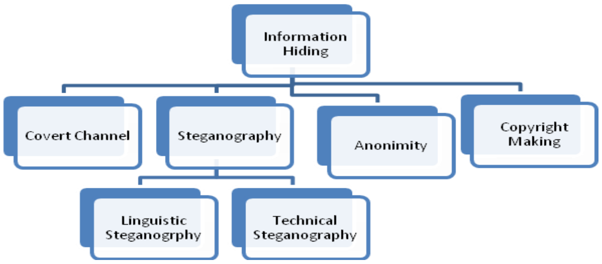


Figure 1: Classification of Information Hiding Techniques

As shown in Figure 1 information hiding has many subparts, one of the most important is steganography. The Linguistic steganography is defined by Chapman et al. [25] as "the art of using written natural language to conceal secret messages". Here the cover medium is composed of natural language text and the text itself which can be generated to have a cohesive linguistic structure. In the Technical steganography, carrier is physical medium such as microdots and invisible inks rather than a text.

2.1 Technical aspect of information hiding

There are three aspects in information hiding systems which contend with each other: capacity, security and robustness [17]. Capacity refers to the amount of information that is hidden in the medium. However, security is important when a secret communication is kept to be secret and undetectable by eavesdroppers. Robustness can be explained as the amount of modification the stego-medium can withstand before an adversary can destroy the hidden information.

Information hiding techniques are used, to fuse the digital content within the image regardless of the different file formats and the status of the image (digital or analog). For example, extra data about an image is added in special tags such as file headers. This information will be lost when the image is printed. As headers are tied to the image as long as image exists in digital form. Hence secret data is not communicated using file headers.

Various techniques are used to implement Steganography, which are used in different tools such as Least Significant Bit (LSB), manipulation of image and compression algorithms, and modification of image properties such as luminance [2].

3. Perspective of Steganography

Internet publishes images to convey ideas for mass communications that acts as a good carrier for hiding information using various tools. These tools are divided into two groups: Image domain ex LSB and Transform domain.

In LSB technique, change in 1 or 2 bit is unnoticeable to the human eye . LSB has a limitation on amount of secret message to be added into cover image. If it exceeds stego-image would appear to be suspicious .Tools used in this group are StegoDos, S-Tools, Mandelsteg, EzStego, Hide and Seek, Hide4PGP, Jpeg-Jsteg, White Noise Storm, and Steganose[1][3][4][5]. Here lossless image formats are used where data is directly manipulated and recovered for ex. Windows Bitmap (BMP). Due to the use of reliable compression algorithm hidden message is not lost.

The transform domain group that involves manipulation of algorithm and image transform for ex. Discrete Cosine Transformation (DCT) and Wavelet transformation. For hiding data it uses more significant area of cover images and luminance of image. Examples of tools are PictureMarc, JK-PGS, SysCop, SureSign. These techniques are more robust than bit-wise techniques. JPEG uses DCT to get image compression for ex. Jpeg-Jsteg tool.

Both image and transform domain characteristics are present in few techniques for example pattern block encoding, spread spectrum methods and masking [2].The addition of redundancy to the hidden information protects data from image processing methods such as cropping and rotating. In this paper we are giving details of various tools belongs to image domain.

4. Evaluation of Steganalysis tools

4.1 S-Tool 4.0

S-Tool [6] reduces the total number of 256 colors to 32 colors. Then basic colors are expanded over several palette entries sorted by their luminance. Though the block of colors appears to be same but it differs by 1-bit value. Same approach is used for color and gray scale images. The stego-image produced from gray scale image no longer remains a gray scale image as the RGB value within pixel may vary by 1-bit. It works with 24-bit images. It can hide 115,184 bytes of data. Encryption algorithm like IDEA, DES, Tripledes, MDC are used for encryption of secret data. Steganography algorithm implemented here uses concept of color reduction (average color, average pixels) as large RGB and luminosity distance. It also enables floyed Steinberg dithering concept.

4.2 Steghide 0.5.1

StegHide [7] hides data into JPEG and BMP. It has features like compression of embedded data, encryption of embedded data and automatic integrity checking using a checksum. The default encryption algorithm used is Rijndael with a key size of 128 bits (AES) in the cipher block chaining mode. The checksum is calculated using the CRC32 algorithm.

Color and sample frequencies are not changed. Graph theoretic approach is used to implement steganography algorithm. Secret data is first compressed and then encrypted. By using pseudo random number generator positions of the pixels from cover image is determined to embed secret data.

Those pixels that need to be changed are sorted out. Then graph theoretic matching algorithm is used to find pair of positions where embedding is carried out. The pixels at the remaining positions (not part of pairs) are also modified by overwriting pixels to contain embedded data. Exchanging pixel values imply that the first order statistics (number of times color occurs in the picture) is not changed.

4.3 Hide In Picture (HIP):

HIP [8] hides any kind of file inside standard bitmap pictures by modifying its color in a way that is almost unnoticeable by the human eye. For too large hidden files noise is inserted in the stego image. One color of the picture may be set as a transparent color; nothing is stored in that area. It also supports for overwriting hidden data. Blowfish (default) and Rijndael encryption algorithm and checksum is also supported. For 24-bit images the size of hidden file should not more than 40% of the picture size.

4.4. wbStego4.3

wbStego4 [9] is used for Windows95/98/ME, and Windows NT 4.0/2000/XP. In it information about the carrier file (e.g. copyright - information) is added without using a separate file. Any data, texts, graphics or even executable programs can be hidden in the carrier files by slight changed, so that the manipulation is not detected. This version of wbStego4 uses bitmaps (*.BMP), text files (*.TXT), HTML files (*.HTM) and Adobe™ Portable Document Format (*.PDF) as carrier files. It also offers cryptographic methods.

Steganographic algorithm uses the concept of color depth (how many bit per pixel define the color value). For higher security it requires more color. Very large areas in one color Bitmap should be avoided. The color depths and amount of data hidden are shown in Table 1.

Table 1: Number of color and amount of hidden data

Bitmap Size	**Number of colors or gray scales**	**Amount of hidden data (size of bitmap in byte : size of hidden data)**
4 bit	16	4 : 1
8 bit	256	8 : 1
24 bit	16,777,216	8 : 1

It also uses lossless compression (e.g. PCX) technique, but the color depth may not be changed. Lossy JPEG may not be used. To reduce the size of the carrier file, which is very important for online transmission, to reduce the size of carrier file any compression utility (e.g. ARZ, LZH, PKZIP, WinZip) can be used, as they are lossless.

4.5 CryptaPix 3.05

CryptaPix ™ [10] is an image file management and encryption program for Windows. In CryptaPix steganographic functions are built around a pixel shuffling routine. AES random number generator is used. The plaintext data is divided into 3-bit segments. Those are overwritten into the lowest red, green, and blue bits in the selected pixels. A maximum of 3 bits (out of the 8 available) for each color channel may be used.

4.6 StegoStick 1.0

StegoStick [11] hides any kind of file like BMP, GIF, and JPEG and the result is in the BMP format. Perceptible distortion is not observed in the stego-image. It uses encryption techniques like DES, TripleDES, and RSA.

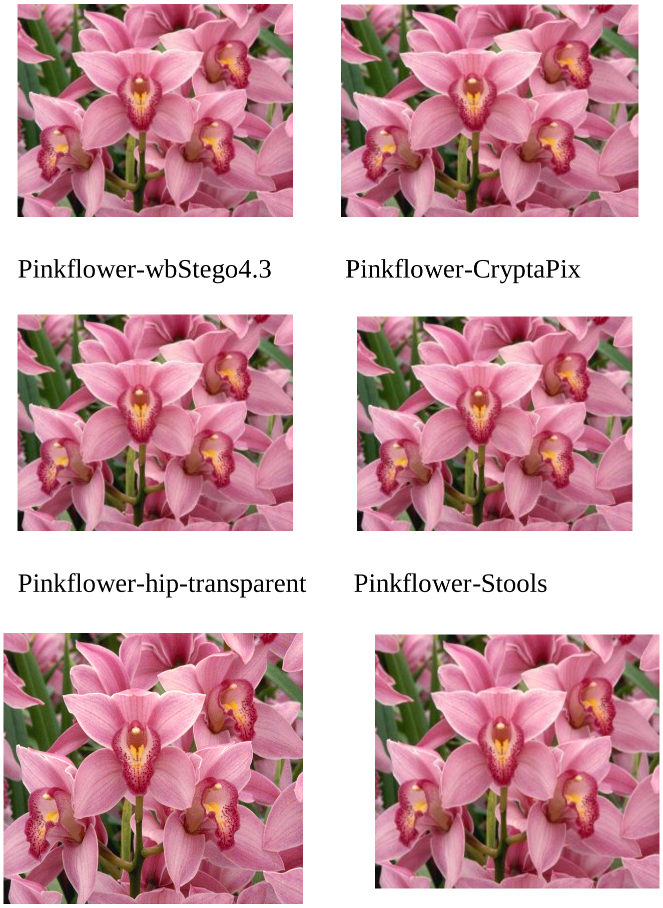
Table 2: Features of Steganographic tools

Name of Tool	**Cover image**	**Utility type**	**Encryption Techniques**	**Steganlysis Algorithm**
S-Tool 4.0	GIF BMP	GUI	IDEA,DES, Triple DES, MDC	1-bit LSB & color reduction
Steghide 0.5.1	JPEG BMP	Commandline	DES,TDES, Blowfish, Rijandael,RC2 , All block ciphers, CRC32	Graph theoretic approach using pixel pair exchange
Hide in picture (HIP) 2.1	BMP	GUI and Commandline	Blowfish, Rijandael, CRC	one colour : transparent (Index 88 RED 0) that does not hide secret data
wbSteg o4.3	BMP	GUI	DES,TDES, RSA	Color depth
CryptaPix 3.05	BMP	GUI	AES	Secure data division is into 3-bit segment. Bit/pixel/color
StegoStick 1.0	JPEG , BMP, GIF	GUI	DES , Triple DES , RSA	---

All the Steganographic tools studied in this paper are summarized in the Table 2. Stego-images for all tools are generated in BMP formats except for Steghide (BMP, JPEG) tool. All tools support Windows but StegoStick, StegHide, and HideinPix supports linux.

4. Comparative results of Tools

Test and experiments are carried out using all above tools, with the help of cover image of size 301 kb, and secret data (file hidden.txt) of size 9 bytes. That results into all stego-images which is shown in the Table 3. Here we have observed the size of the cover image and stego-image is slightly varied. All stego-images are shown in the Figure 2.



Pinkflower-wbStego4.3 Pinkflower-CryptaPix

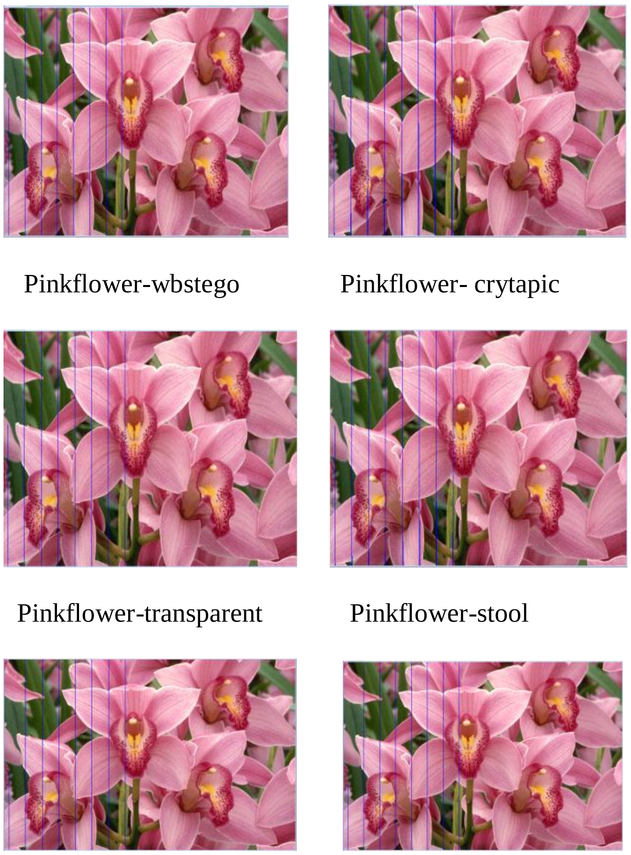
Pinkflower-hip-transparent Pinkflower-Stools

Pinkflower-StegoHide Pink flower StegoStick

Figure 2. Stego-images resulted from various tools

Peak-Signal-to-Noise-Ratio (PSNR) is used as a major of performance for image distortion. PSNR is expressed o a logarithmic scale in decibels (dB). PSNR values below 30dB indicates that the distortion caused by embedding secret data is very low.

Data distribution of quantitative variables is displaced graphically using technique called as Histogram as shown in Figure 3. In case of images variables are nothing but intensity values of image. Histogram is used to test the presence of any abnormalities observed in the stego-image as compared to the cover image.



Pinkflower-wbstego

Pinkflower- crytapic

Pinkflower-transparent

Pinkflower-stool

pinkflower_stegoHide

pinkflower_stegostick

Figure 3. Histogram of Stego Images

Table 3. Comparative study of Steganographic tools

Steganographic Tools	**Image Size in (Kb)**	**Name of stego-file**	**Size of Stego-file**	**PSNR**
StegoStick 1.0	301KB	pinkflower_Tdes_stego	1.17MB	17.05961257
S-Tool 4.0	301KB	pinkflower_stool_stego	900KB	17.03729143
StegHide0.5.1	301KB	pinkflower-stego-StegHide	900KB	17.07062074
Hide In Picture (HIP) 2.1	301KB	pinkflower-stego-HIP	301KB	17.03717922
WbStego4.3	301KB	pinkflower-stego-wbstego	301KB	17.03719218
CryptaPix3.05	301KB	pinkflower-stego-cryptapix	900KB	17.03736634

6. Conclusion and Future work

Information hiding techniques has become important in security research. Invention of applications and technologies brings new threats that require new protection mechanisms. Hence for ex applications such as e-banking, e-trading, mobile telephony, medical data interchanging etc., requires study of Steganograpic tools. Thus this paper throws light on the various features of these tools.

This study can be further extended for JPEG, GIF, PNG file formats. The result of this paper can guide the steganalyst to develop a tool which can automatically extract hidden messages in images.

References

[1] S. Das, Subhendu Das, B Bandyopadhyay, and S Sanyal, "Steganography and Steganalysis: Different Approaches". Internatioanl Journals of Computer Applications,Volue No7, Number 9,year 2010.

[2] Neil F. Johnson, and Sushil Jajodia, "Steganalysis of Images Created Using Current Steganography" Software, Springer Verlag (1998), proceedings for Second Information Hiding Workshop in Portland, Oregon, USA, April 15-17, 1998.

[3] Ahmed Ibrahim, "Steganalysis in Cmputer Forensics", Security Research Centre Conferences "Australian Digital Forensics Conference",available at http://ro.ecu.au/adf/10, Dec Year 2007.

[4] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul McKevitt, "A Comparative Analysis of Steganographic

Tools", Information technology and Telecommunication Conference 2007 ,pp 29-36

[5] Pedram Hayati, Vidyasagar Potdar, and Elizabeth Chang, "A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator", Workshop of Information Hiding and Watermarking with IFIPTN New Brunswick, Canada, July 2007.

[6] S-Tool4.0: ftp://ftp.funet.fi/pub/crypt/mirrors/idea.sec.dsi.unimi.it/code/s-tool4.zip

[7] Steghide0.5.1.: http://steghide.sourceforge.net/

[8] Hide in Picture http://sourceforge.net/projects/hide-in-picture/

[9] wbStego4.3: http://members.xoom.com/wbailer/wbstego/index.htm

[10] CryptaPix 3.05 http://www.briggsoft.com

[11] StegoStick1.0 http://www.infosectechnologies.com/StegToolandWatermarkingTable.pdf

Author Biographies

Sumedha D Sirsikar sumedha.sirsikar@mitpune.edu.in has pursued M.E. Computer Engineering from College of Engineering, Pune, Maharashtra, India in year 200. She is presently working as a Professor and Head of Information Technology department in MIT Pune. Her area of interest is computer network and information security.

Asavari A. Deshpande (asavari.deshpande@gmail.com) has pursued B.E in Computer Science and Engineering from M.G.M. college of engineering , Nanded, Maharashtra, India in year 2004.She is presently perusing Masters in Computer engineering from 2008.and working as lecturer in MAEER's M.I.T Pune Her area of interest is database normalization.