STEGANALYSIS TECHNIQUES AND COMPARISON OF AVAILABLE SOFTWARES

[1]Muhammad D. Hassan, [2]Murad A. Mohammed AMIN and [3]Suzan T. Mahdi
mdhmm@ntu.edu.iq; murad@ntu.edu.iq; mdhmm75@yahoo.com
[1,2] Northern technical university of Iraq, [3]Northern Oil Company, Iraq

Abstract. The technological advancements of the present time bring along the necessity to maintain the security of the data which are available on the digital platform. Encryption and steganography techniques include the solution techniques used to ensure this security. The robustness of these techniques are also tested by analysis techniques. In this study, the steganalysis methods which are being used are explained. The results obtained are indicated in the charts.

Keywords: Image Security, Steganography, Data Security

1 Introduction

Steganography can be defined as hiding data inside an object [1]. The word Steganography was derived from the words "στεγαυος" and "γραΦειν" which are in the Greek alphabet. The exact meaning for these words is "hidden text" or "covered writing" [2].

Another branch of science advancing in parallel with the development of steganography is steganalysis. The aim of steganalysis is to reveal the existence of hidden data in an image, sound or a file. Steganalysis is the complete set of methodology to differentiat between carrier, original and stego object.

There has been a lot of researches in the 2000's regarding steganalysis, especially in the steganalysis of image and sound files [3].

Various steganographic methods have been developed to hide information on image files. The methods can be classified under three headings [4]:
- Adding to the least significant bit
- Masking and filtering
- Solutions methods and file data alterations.

2 Steganalysis Applications In The Literature

There have been many studies on the topic of steganalysis [8,9,10,11,12,13,14].

- Westfeld and etal. (2000) developed a method of steganalysis dealt with on a statistical analysis of value pairs that change as a result of storing the message on images. This method has given more reliable results in instances such as sequential storage [13].

IMDC-SDSP 2020, June 28-30, Cyberspace

DOI 10.4108/eai.28-6-2020.2297970

- Fridrich et al. (2000) have presented a method in a study based on a statistical analysis of pairs of color values close to each other to determine the data storage performed by the LSB method in 24-bit color images, that can give reliable results in pictures where the single color ratio is less than %30 of the total pixel number. They reported that this method could not be successful in images taken by today's digitals cameras with uncompressed high resolution and also that this method cannot be applied to gray-level images [9].

- Provos and Honeyman (2001) conducted a comprehensive study on the steganalysis of JPEG images and with the software they developed, they were able to detect thousands of suspicious images on the Internet.

- Farid (2001) presented the universal detection study which carries on steganalysis predictions without the need to know the steganography algorithm after his analysis and feature inferences on a database consisting of carrier and stego images [12].

- Fridrich et al. (2001), had established a method on the steganalysis of colored and gray-level images which they named RS. In this method, as well as the changing pairs of values during data storage, statistical analysis of the pixel positions where this change took place was performed. The success of this method is lower where embedding is random than sequential storage [10, 11].

- Fridrich (2006) has detected in his study which analyzes the inverse ratio between the change occurring as a result of data storage and the number of changes, has found that it is not optimal in any detectability profile (detectability profile refers to the distribution of the embedding effect) to use the pixels with the smallest embedding effects [14].

2.1. Techniques Used In Steganalysis

Some of the steganalysis approaches are as below :
1. Visual Detection
2. Detection of steganographic Artifacts
3. Steganalysis Based on Image Quality Metrics
4. First-order statistical Analysis
5 Steganalysis Based on JPEG Compatibility
6. RS Analysis
7. Pairs Analysis
8. Palette Quick Pairs Analysis
9. Raw Quick Pairs Analysis
10. Chi square Attack
11. Other Methods

Visual detection occurs when the image resulting from the data embedding is visible to the eye and the difference from the original image is recognized or if the original image is not present, it occurs by detecting defects and features on the image which are unexpected. However, in this case, it will not be possible to distinguish between self-noisy images and stego images. It is clear that the reliability of visual detection is debatable.

Steganalysis Based on Image Quality Metrics is dependent of statistical prediction of pixel value pairs which are the results of embedding data in an image.

RS Analysis, in addition to the Stegoanalysis Based on Image Quality Metrics, contains the statistical analysis of the location of the pixels in which the change occurs.

Identifying Based on Algorithm or Type contains the steganalysis studies of images such as JPEG and the methods of revealing the message in a stego image created by steganography applications where the algorithm is known.

Artifact Detection Systems includes the methods of distinguishing the original image and the stego image by extracting some features of the image.

RQP Analysis was developed by Fridrich and his friends [9]. This method was developed in order to analyze similar color pairs created by LSB concealing. First of all, the ratio of similar color pairs to all color pairs is calculated fort he selected image. Then, the ratio is recalculated after hiding a test message in this image. If the difference between the measured ratios is large, it is assumed that there is no information hidden within the image. If the ratios are close to each other, it indicates an information hidden in the image.

3. Existing Steganalysis Softwares

There are several softwares which are called steganalysis software which can detect the presence of steganography. While some of these softwares are open-sourced, some other may be very expensive. This study is limited with the testing of available free tools, therefore, it only discusses the licencing options based on public descriptions.

Once the confidential information is detected, the embedded message will try to be extracted. A key is needed to pull out the message. On these systems, Brute force/dictionary attack may be used on these systems that uses software in supporting the dictionary attack against Steganography. Table 3.1 illustrates the steganalysis tested software tested applied in this section.

Table 4.1. Steganalysis software

Name	Title	State of Licence
StegSpy	3.1	Open Source (OS)
Stegdetect	3.2	OS
Stegbreak	3.3	OS
Stego Suite	3.4	Licenced
StegAnalyzer	3.5	Licenced

3.1. Stegspy

StegSpy software can determine if any kind of data is stored in the file and in which file it is stored. It cannot make universal detection, but only stego files created with several steganographic softwares such as JPHideandSeek and Invisible Secrets. The software is available for free download.
StegSpy V2.1 is a free software established by Michael T. Raggo. They claim that it can detect steganography patterns from Hiderman, JPHideandSeek, Masker, JPegX and Invisible Secrets.

The Project owner presented StegSpy at InfoSec 2004, BlackHat 2004 and DefCon 2004.

The current version of StegSpy is written in VisualBasic v2.1. There is a graphical interface that allows the user to manually select a file to review.

3.2. Stegdetect

Stegdetect is a free steganalysis software that can detect the data stored in a JPEG image with softwares such as Outguess 0.1 and Invisible Secrets.

Stegdetect is an OS software created by Niels Provos. It is able to detect parts of the message with jsteg, jphide (Unix and Windows), Invisible Secrets, Outguess 0.1, 3b, F5 (page header analysis), AppendX and camouflage.

3.3. Stegbreak

Just as Stegdetect, Stegbreak was also established by the similar developer. However, Stegbreak is not for detecting the presence of Steganography, nonetheless a software for message abstraction. It attempts a dictionary attack against Jsteg-Shell, JPHide and Outgues. Stegbreaks success is no doubt dependent on the password and the dictionary. The rules of changing the order of the words in the dictionary is also closely related to escure success.

From a legal point of view, the permutations may be the password being used, research can provide clues to the passwords. These tips such as name, birthday, name of a pet, etc. can be added to the lexicon used by Stegbreak.

Stegbreak requires a technquie to prove that the removed bit string is not just a sound but and embedded message.

3.4. Stego Suite

Over the last decade, Technologies for digitally processing image, video and audio data have greatly improved, leading to the rapid retention of information within binary files. Numerous websites offer “stego” programs open to download. The latent for industrial espionage, theft of trade secrets, cyber arms exchange and criminal coordinations are endless.

Many governments and commercial institutions are looking for tools to detect the use of digital steganography in all its forms. Stego Suite is a tool that detects the steganography presence without known past information that can be used against the target file. This ability, recognised as “blind” detection of steganography, that is unique to Suite of Stego software.

Active web browsing is increasingly a necessity to ensure that unauthorized persons on a website do not use the site to exchange harmless video messages or steal property-related data. Stego Suite tool continually scans a domain fort he presence of confidential data in digital images based on a web domain.

The subsequent data analysis collected at a digital crime scene can take long process. This is also increased the complecity when we consider many images, or audio records or videos that may have confirmed evidence. Stego Suite tools support the assessment evaluation of such long computational process applied for confidential information or communication.

Stego Suite 3.1 is a monitoring/scanning service made available to someone else and as a standalone software consisting of three type of applications. The selection authority is suitable for customers who wish to leave the management of the program with expert from Wetstone personnel. The software is used by customers who is able to perform the steganography detection purpose within their own systems. Both selections provide technical support and the team expertise from Stego team.

Stego Suite is one of the most advanced commercial steganalysis software which can detect the existence of data stored in picture and sound universally without the need of knowing the storage algorithm. BMP, GIF, PNG, JPG and WAV files can be steganized. Whetstone Technologies offers Stego Suite, which includes Stego Watch and Analyst detection tools and a PW cracker, Stego Break. They also propose training to use these tools together with others at the USA conference 2005.

It is not clear how these tools do steganalysis, and it is not known which steganography tools they detect.

WetStone Stego Suite consists of four products:

- Stego Hunter™ – Steganography program detection
- Stego Watch™ – Steganography detection tool which is the admiral of WetSyone
- Stego Analyst™ – Latest technology image and audio file analyst
- Stego Break™ – Steganograph password breaker

3.3.1. Stego Hunter

The latest feature added to the Stego Hunter Suite is that it allows researchers to quickly and punctually determine whether steganography programs are available in the suspected system. Once Steganography applications are detected, Stego Hunter will automatically redirect you to the carrier files associated with the detected programs.

From the rsearch process the design and model could be done so quickly to detect the steganography program. Even somebody asked, "How do you know that steganography exists?" The results of applications installed with Stego Hunter or even pre-installed are easily reported to the researcher. We take this step a little further and mark some suspicious carrier types that you should look for later in the research process. There is ability to diifereniate between forensic

images from common resources for wexample, EnCase, FTK, dd, raw, ISO and safeback images.

3.3.2. Stego Watch

Steganography detection tool based on the latest technology represents the state of the art of the present work. Once suspicious files could be found; Stego Watch that scans the whole file and to bring the results to an easy interface with suspicious files marked. The marked files are detected by a blind detection technique that searches for artificial phenomena. It should be noted that no prior knowledge required for steganography programs.
Stego Watch allows users to detect digital steganography or the presence of communication stored in digital images or audio files. The technology under the Stego Watch software is the result of WetStone Technologies' long-term and intensive research effort and is now commercially available, forming the basis of the Stego Suite offer.

There were many new algorithms applied to improve results and detection methods including the use of wav data files in supporting the process. Stego Watch along with the help of applying the disctinary attack through Steganography software tools can extract embedded information in the data files.

It is not possible to examine the tools without accessing them. And as stated above no alternative resources available to discuss the Stego Watch, as the only tools presented at the Black Hat USA 2005 conference.

3.3.3. Stego Analyst

Stego Analyst is a multi-level imaging tool that allows researchers to hunt for visual traces that shows that steganography is actually used in both image and audio files. Stego Analyst is fully integrated with Stego Watch, allowing visual inspection of suspicious individual images. It is frequently these visual traces that help the investigator to confirm Stego Watch's suspicion of embedded steganography. The color properties, can also tested through the use of stero Analyst to identify the RGB values and their densities..

A file viewing screen displaying individual file image or sound wave, and display details, DCT coefficients, color pairs, and so on. file attributes are provided. To allow researchers to search for more traces of the use of steganography, in which filter selection is introduced to convert images into one of three different presentations, Density, Saturation, or Tone. Other filter selectors display only the selected custom coloured Least Significant Bits (LSB).

3.4. Stego Break

Stego Break is a program developed and embedded in order to acquire the password phrase in a file that it has been used. With the purchase of the tool, popular password dictionaries are also provided to carry out a dictionary attack.

Researchers are also capable of bringing in other dictionaries if they find the password via a suspicion query. If you find and remove an encrypted file, we may encourage you to contact an

encryption specialist.

3.5. Steganalyzer

Security offers three versions of StegAnalyzer. StegAnalyzer AS searches for file systems for traces of known software for steganography. StegAnalyzer SS includes the functionality to detect known stego file signatures. StegAnalyzer RTS is a network application that can be used in real-time for fingerprints and signatures.

A copy of this software is not available, but there are still some ideas. StegAnalyzer is quite expensive; sold for about $2000. However, its functionality can be obtained from other tools. Detection of file corrupt signatures, as well as known stego file signatures, are supported by free tools (eg Sleuthkit / Autopsy). Thus, the actual value of StegAnalyzer is in the database for which its quality is unknown.

3.5.1. Steganography Analysis Artificial Case Scanner (StegAlyzerAS)

StegAlyzerAS (Steganography Analyzer Artifact Scanner) is a digital forensic analysis tool designed to extend the scope of traditional digital forensic analysis by allowing the examiner to scan suspected media or suspected media images for known artificial phenomena in steganography applications.

Artificial phenomena can now be detected by scanning the file system and Microsoft Windows® system records in the same way. CRC-32, MD5, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 which are stored in the Steganography Application Fingerprint Database (SAFDB) which is included in the package of StegAlyzerAS, allows the search of files using hash values and record entries stored in the Artificial Case Record Master Database (RAKDB)

3.5.2. Steganography Analysis Signature Scanner (StegAlyzerSS)

When certain steganography applications are used to embed confidential information in StegAlyzerSS (Steganography Analyzer Signatures Scanner), StegAlyzerSS is a digital forensic analysis tool which allows the reviewer to scan for files on suspicious media or forensic images of suspicious media, allowing for unique hexadecimal byte models or known signatures within the files to scan for a broader scope.

StegAlyzerSS can also extend the signature scanning capability by allowing the examiner to use other techniques to determine if the information is attached to or hidden in potential carrier files.

Defense Cyber Crime Institute (DCCI) and CyberScience Laboratory (CSL) have demonstrated that StegAlyzerSS is effective in detecting files containing hidden steganographic data.

3.5.3. Steganography Analysis Real-Time Scanner (StegAlyzerRTS)

StegAlyzerRTS is a network security application that able to provide real time detection of fingerprints and signatures of digital steganography.

Steganography applications are widely available in the free or shared format on the Internet. They represent an important insider threat since it is easy to download and use in many applications.

StegAlyzerRTS detects insider downloading as it compares the fingerprints with fingerprints of files associated with steganography applications. Detecting a download is a warning and an indication that the insider will likely use the application to steal the information and used as a carrier file to a website or sending the carrier file to an external recipient.

StegAlyzerRTS also detects the internal use of steganography applications downloaded and installed on the network before StegAlyzerRTS is deployed. Using a proprietary signature scanning approach developed at the Steganography Analysis and Research Center (SARC), StegAlyzerRTS attempts to upload insider user carrier files containing confidential information to external websites, send carrier files containing confidential information as an e-mail attachment, and even form a spam-like form and even detects the use of a technique known as spam counterfeiting to convert and hide.

6. CONCLUSION AND DISCUSSION

We are summarized our conclusions remarks in the following:

Steganalysis Method	Description	Targeted Steganographic Techniques
RS Steganalysis	Contains the statistical analysis of the location of the pixels in which the change occurs	Various LSB Modification Techniques
Chi square Attack	The chi-square test compares each other to embed constant value pairs and message bits	Steganography method based on the Exchange of pixel, grey-level color or DCT coefficient value pairs
Palette Checking	The feature of Pallete rankings is a clear sign of systematic changes	Steganography in Palette Shapes
RQP Method	A method based on the increasing number of similar color pairs resulting from embedding applications	LSB when embedding in true-color shapes
Steganalysis Based on JPEG Compatibility	The steganalysis studies of images such as JPEG and the methods of revealing the message in a stego image created by steganography applications where the algorithm is known.	The ways of using steganography were first stored in JPEG format
Steganalysis Based on Image Quality Metrics	Based on statistical analysis of pixel value pairs which are the results of embedding data in an image.	QIM or other quantitive index embedding methods
Detection of steganographic Artifacts	Methods of distinguishing the original image and the stego image by extracting some features of the image.	Various Steganographic Techniques

Product Name	StegSpy	Stego Suite	Stegbreak	StegAnlyzer	stegdetect

Code	Open Source	Licanced	Open Source	Lisanced	Open Source
Software Language	Visual Basic	Unknown	Visual Studio.NET	Unknown	Visual Studio.NET
Developer	InfoSec 2004, BlackHat 2004 and DefCon 2004	Wetstone Technologies	Niels Provos	Backbone Security	Niels Provos
Current Formats	Detects stego files created by steganographic softwaressuch as JPHideandSeek, Hiderman , JPegX,Invisible Secrets (only images)	Image, Bmp,gif,png,jpg Sound, wav	JSteg-Shell, JPHide and OutGuess 0.13b (Only jpg. images)	Unknown	jsteg, jphide, invisible secrets, Outguess 0.13b, F5, appendX and camouflage. (Only jpg. images)
Techniques	Detects if there is an information in a file and if there is, detects which file	Artifact Detection	Detection Based on Algorithm	Artifact Detection	Detection Based on Algorithm
Websites	spyhunter.com/ stegspydownload.htm	www.wetstonetech. com/	www.outguess.org/ detection.php	www.sarc-wv.com /products.aspx	www.outguess.org/ detection.php
Supported Services	Unknown	Wetstone Technologies	Wetstone Technologies	Backbone Security	Unknown
Update Status	No Updates	Stego Hunter Stego Watch Stego Analyst Stego Break	No Updates	StegAnlyzerAS StegAnlyzerSS StegAnlyzerRTS	OutGuess 0.2 - 2001-02-12 Stegdetect 0.2 x-2001–07–23 Stegdetect 0.3 - 2001-10-02 Stegdetect 0.4 - 2001-12-21 Stegdetect 0.5 - 2002-01-26 Stegdetect 0.6 - 2004-09-06

References

[1] Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G., "Information Hiding–A Survey", Steganalysis ApplicationsProceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7):1062-1078 (1999).

[2] Murray, A.H., Burchfiled, R.W (eds.), "The Oxford English Dictionary: Being a Corrected Re-issue", Oxford, England: Clarendon Press, (1933).

[3] Phan, R.C.W., Ling, H.C., "Steganalysis of Random LSB Insertion Using Discrete Logarithms Proposed At Cita03", MMU International Symposium on Information and Communication Tecnologies/M2USIC 2003, Petaling Jaya, Malaysia,, 2-3 (2003).

[4] Muhammad D. H., Murad A. M. A. and Suzan M. , "Sound based Steganalysis for Waveform Audio File Format (WAV) and Audio File Format (AU), Journal of Electronic Systems,8(3) (2018).

[5] Fridrich, J., Du R., Meng, L., “Steganalysis of LSB Encoding in Color Images”, Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conferece, New York City, USA, 3: 1279-1282 (2000).
[6] Fridrich, J., Goljan, M., Du, R., "Detecting LSB steganography in color, and gray-scale images", Multimedia, IEEE , 8 (4): 22-28, (2001).
[7] Fridrich, J., Goljan, M., Du, R., "Reliable Detection of LSB Steganography in Color and Grayscale images", Proc. of the ACM Workshop on Multimedia and Security, 27-30 (2001).
[8] Farid, H. "Detecting Steganographic Messages in Digital images." Technical Report TR2001-412, Dartmouth College, 1-9 (2001).
[9] Westfeld, A., Pfitzmann, A., “Attacks on Steganographic Systems”, Proceedings of the Third International Workshop Information Hiding, Dresden, Germany, 61-76 (2000).
[10] Fridrich, J., "Minimizing the embedding impact in steganography", Proceeding of the 8th Workshop on Multimedia and Security, Geneva-Switzerland, 2-10, (2006).
[11] Avcıbaş, İ., Kharrazi, M., Memon, N., Sankur,B., "Image Steganalysis With Binary Similarity Measures," EURASIP Journal on Applied Signal Processing, (17): 2749- 2757 (2005).
[12] Sankur B., Memon, N., Avcıbaş, İ., "Automatic Detection of the Presence of Stegosignals and Watermarks in Images," European Conference on Visual Perception, 38-38 (2001).
[13] Proves, N., Honeyman, P., “Detecting Steganographic content on the internet”, Tech. Rep. CITI 01-1a, University of Michigan, 1-14 (2001).
14. Böhme, R., Westfeld, A., "Statistical Characterisation of MP3 Encoders for Steganalysis", the Multimedia and Security Workshop, Magdeburg, Germany, 25-34 (2004).