Journal of Engineering, Science and Mathematics

Volume 01, Number 01, Pages 12-17, Year 2020
https://jesm.in/archives/

Review Paper

An inclusive survey of Steganography and Steganalysis: A Review

Mohammed Wasim Bhatt[1]

Department of Computer Science Engineering, Punjab, India

Correspondence should be addressed to Mohammed Wasim Bhatt; wasimmohammad71@gmail.com

Received 5-12-2020; Accept 24-12-2020; Published 28-12-2020

Handling Editor: Rashed Qayoom Shawl

Steganography is an art of covering the secret data by using different cover files such as text, images, audio, video files etc. Steganography can be combined with cryptography to provide extra security to the data. Steganography is derived from two Greek words: (i) steganos (ii) graphia. Steganos means "covered" and Graphia means "writing". Cryptography is an art of securing the data from unauthorised access. It is derived from two Greek words: (i) kryptos (ii) graphein. Kryptos means "secret" and Graphein means "study". Steganalysis is a technique to detect hidden information using Steganography. This is similar to cryptanalysis technique which is used in Cryptography.

Keywords: *Steganography, Data Security, Cryptography, Steganalysis, Least Significant Bit, Security Breach*

1. Introduction

Internet is an innovative technology that has become very popular in the modern era [1]. It contains bulk information of different fields. It becomes convenient for people to access information from the Internet in any field [2]. With the rapid growth in Internet, risk on our confidential information is also increasing rapidly. Security has become an important issue in today's era of the Internet. Data Security is a process of securing the digital information stored in databases from unauthorised access. It protects data from data corruption throughout its lifecycle. It focuses on

protecting the data from unwanted actions of third parties. An unauthorised user is an individual who can access any organization's data, networks, devices and applications without getting any prior permission. Data Security helps in the safekeeping of data from destructive forces. A security breach is an attempt by a third party to get unauthorised access to an organization. Steganography and Cryptography both helps in securing the data from data breaches or security breaches. This review paper provides an insight into the technique of Steganography and Steganalysis. For example, a user can perform login and log out the operation from a hardware device. Using logging in and logging out operations, a user can set different privilege levels. This device uses biometric technology to prevent malicious users or unauthorised access from logging in, logging out and changing those privilege levels. Controllers such as hard disks in input/output devices keep track of the current state of a user of the device. Illegal access by a malicious user or a malicious program is interrupted based on the current state of the user. Hardware-based access control provides more security as compared to the security provided by the operating system. An operating system is more vulnerable to malicious attacks of viruses and third-party hackers. The data on the hard disk becomes corrupted when malicious access is obtained. If hardware-based protection is provided, the software cannot manipulate the user privilege level [3]. The hardware secures the operating system image and file system privileges from being altered. Hence, using a combination of hardware-based security and secure system administration policies a completely secure system can be constructed.

2. Steganography

Steganography is the art of hiding the secret information within a cover file such as text, message, video or audio file so that the secret information is converted in such a form that it cannot be easily readable or comprehend by unauthorised access. Later, the secret information is extracted at the destination. In cryptography, the encryption is a process of encoding some information. The process of encryption converts the plaintext into the ciphertext. Only authorised parties can decipher the ciphertext back to the plaintext to access the original information. Steganography is very popular in various fields where confidential communication and secret data storing is required such as cybercriminals, media database systems, cyber-physical systems and Internet of Things etc. The first recorded uses of steganography are originated in Greece 440 BC when Herodotus mentions two examples in his Histories[4]. Histiaeus sent a message to Aristagoras. He shaved the head of his most trusted servant and marked the message on to his scalp. Once his hair had regrown, he sends him on his way with the instruction. When his servant reaches the destination, Aristagoras shave the head and look thereon. Furthermore, Demaratus sent a warning about an approaching attack to Greece by writing it using the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were used as reusable writing surfaces. In a cryptographic work, Polygraphia which is written by Johannes Trithemius introduced a message encryption method "Ave-Maria-Cipher". The cipher is a table of 384 parallel columns of Latin words [5].

Steganography can be divided into five types:

1. Text Steganography
2. Image Steganography

3. Video Steganography
4. Audio Steganography
5. Network Steganography

2.1 Text Steganography

Text Steganography is the technique of hiding the data inside text files. It includes things like changing the format of existing text, changing words within a text, generate readable texts using context-free grammars, generating random character sequences. Here are a few techniques which are used to hide the data within the text: (i) Format Based Method (ii) Linguistic Method (iii) Random and Statistical Generation.

2.2 Image Steganography

In Image Steganography, the data is hidden inside the image. A huge number of bits are present in the digital representation of an image. Therefore, most images are widely preferred as a cover source. Data can be hidden inside an image using different approaches such as Least Significant Bit Insertion, Masking and Filtering, Redundant Pattern Encoding, Coding and Cosine Transformation and Encrypt and Scatter.

2.3 Video Steganography

In Video Steganography, the data is embedded inside a video. Video steganography is divided into three categories: (i) Pre-embedding (ii) Post-embedding (iii) Intra-embedding

The pre-embedding method can be applied to the raw video. Post-embedding methods are mainly focused on the bitstreams, which means the procedure of embedding and extraction of video steganography are all manipulated on the compressed bitstream. Intra-embedding methods are categorized according to the video compression stages such as intra-prediction, motion vectors, pixels interpolation, transform coefficients.

2.4 Audio Steganography

In Audio Steganography**,** information is hidden inside an audio signal in such a manner that it cannot be easily detected. While embedding the information in the cover file, one has to keep an eye on its quality. Its quality should not be degraded. Therefore, the protection of information is essential. The methods which are used for embedding the information should be able to resist the noises. [6,7]

2.5 Network Steganography

Network Steganography is a technique in which information is hidden inside active network protocols in such a way that no one can detect the information except its intended recipient.

2.6 Techniques used in Steganography

Various techniques used in Steganography are as follows:

(i) Least Significant Bit (LSB)

(ii) Palette Based Technique

(iii) Secure Cover Selection

1) Least Significant Bit

In the computer science field, the least significant bit (LSB) is considered as bit position in a binary integer which gives the value of the unit by deciding whether the number is even or odd. Least Significant Bit is also known as the low-order bit or right-most bit. It is similar to the least significant digit of a decimal integer [8]. The LSB method has a high imperceptibility and a small change of the image makes it widely used in the field of information hiding [9].

2) Palette Based Technique

On the Internet, a large number of images are present in palette-based formats such as gif, png. In Palette based images, one can hide information using two ways.

(i) By embedding the message in the palette
(ii) By embedding into the image data

The benefit of the first method is that it helps in creating a secure method by considering some assumptions related to the noise properties of image source like as a camera or scanner etc. It has a drawback that the capacity is independent of the image. And the capacity is limited by its palette size. However, in the second method, it offers higher capacity as compared to the first method but in this case, the designing of a secure scheme becomes a hard task [10].

3) Secure Cover Selection

This technique helps in minimizing the risk of detection of the message by selecting a cover image in such a way that its steganography capacity is adequate to hide the message securely [11]. Best cover can be chosen for carrying a secret message depending on the size of the message to be embedded. Secure Cover Selection assures security. Also, it offers a minimized risk of detectability [12]. By selecting an appropriate cover image using a proper selection measure help the steganographer to lower the detectability of stego images [13].

3. Steganalysis

Steganalysis is a method of extracting the information which is hidden using steganography. Steganalysis method is similar to the cryptanalysis method in cryptography. In the steganalysis process, the prime focal point is on the extraction of the hidden information [14]. Steganalysis can be classified into two classes: (i) Signature Steganalysis (ii) Statistical Steganalysis [15]

3.1 Signature Steganalysis

Steganography methods hide secret information and manipulate the images and other digital media in ways as to remain imperceptible to the human eye [16]. Steganography alters the media properties due to the insertion of message bits in the form of degradation or repeated patterns, which act as signatures that convey the existence of embedded message [17]. For detecting the existence of hidden message in a suspicious image is to look for these repetitive pattern's signatures of a steganography tool. These particular signatures automatically exploit the tool used in embedding the messages. Such methods look at palette tables in GIF images and any anomalies caused thereby common stego tools. When the message is embedded sequentially such attacks give promising results but, are hard to automatize and their reliability is highly doubtful.

3.2 Statistical Steganalysis

The statistics of an image undergo alterations due to information hiding. Statistical steganalysis analyses the underlying statistics of an image to detect the secret embedded information. Statistical steganalysis is more commanding than signature steganalysis because mathematical techniques are more responsive than visual perception [17]. Statistical Steganalysis can be further classified into two types:

(i) Specific statistical steganalysis (ii) Universal statistical steganalysis

3.3 Specific statistical steganalysis

These types of techniques are demonstrated by examining the operation used for hiding the information and by discovering image stats. This technique needs precise information about how data is embedded. This technique gives accurate results. Various statistical steganalysis tools are used for finding the hidden information which is embedded using Least Significant

Bit method, spread spectrum method, compression methods etc. [17].

3.4 Universal statistical steganalysis

Universal Steganography requires no prior information or need very less information about under attack steganographic methods for extracting the hidden information. Universal statistical steganalysis consists of the statistical steganalysis method which is not custom made for a specific steganography embedding method. This type of steganalysis uses a learning-based strategy which includes training based on stego and cover-images. Various soft computing tools, clustering algorithms and neural networks are used to build the detection model from the hypothetical data. These methods are independent of the conduct of embedding algorithms. Various steganalysis tools are handy in the market which is used for steganalysis. For example, Benchmark, StirMark, PhotoTitle and 2Mosaic etc. [18]. With the help of these available tools, one can extract the hidden information from any image. Extraction can be performed by demolishing the secret information. This demolishing of secret information can be performed using two techniques: Break apart technique and Resample technique. One of the optimal steganalysis software is Steganography Analyzer Real-Time Scanner. It can analyze all network traffic to mark out the traces of steganographic communication.

4. Conclusion

This paper presents a comprehensive study on steganography and steganalysis. Different types of Steganography are discussed in detail in this paper. This paper also emphasizes on various techniques which are used in steganography such as Least Significant Bit (LSB), Palette Based Technique and Secure Cover Selection so that researchers will have an insight of how to use such techniques. This paper also covers brief knowledge about Steganalysis. Furthermore, it also shed light on Signature Steganalysis and Statistical Steganalysis. It also gives an insight to Specific Statistical Steganalysis and Universal Statistical Steganalysis.

References

[1] Afrakhteh, Masoud, and Subariah Ibrahim. "Adaptive steganography scheme using more surrounding pixels." *International Conference on Computer Design and Applications*, IEEE, vol. 1, pp. V1-225, 2010.

[2] Babu, K. Suresh, K. B. Raja, Kumar K. Kiran, TH Manjula Devi, K. R. Venugopal, and L. M. Patnaik. "Authentication of secret information in image steganography.", *TENCON*, IEEE, pp. 1-6, 2008.

[3] Waksman, Adam, and Simha Sethumadhavan. "Silencing hardware backdoors.", *Symposium on Security and Privacy IEEE*, pp. 49-63, 2011.

[4] Petitcolas, F.A.P., Anderson R.J. and Kuhn M.G., "Information Hiding: A survey", *Proceedings of the IEEE, vol.* **87** No. 7, pp. 1062–78, 1999

[5] Bagaskara, Jordy Ardian, Tito Waluyo Purboyo, and Ratna Astuti Nugrahaeni, "Analysis of JPEG Image Steganography Using Spread Spectrum Method.",*International Journal of Applied Engineering Research,,Vol.* 12, no. 23, pp. 13944-13950, 2017.

[6] Martin, Alvaro, Guillermo Sapiro, and Gadiel Seroussi. "Is image steganography natural?.", *Transactions on Image processing,IEEE, Vol.* 14, no. 12, pp. 2040-2050, 2005.

[7] Mstafa, Ramadhan J. "Information Hiding in Images Using Steganography Techniques." ASEE, 2013.

[8] Singh, Prabhishek, Raj Shree, Ravi Prakash Pandey, Vivek Shukla, and Ramneet Singh Chadha,"A New Box Segmentation Based Digital Image Watermark Positioning Method in Spatial Domain.", *Advanced Science, Engineering and Medicine, Vol.* 10, no. 7-8, pp. 700-704, 2018.

[9] Dong, Wen. "Research on Least Significant Bits (LSB) Image Information Hiding Based on Random Bit Selection Embedding Algorithm.", *4th International Conference on Intelligent Information Processing*, pp. 41-43, 2019.

[10] Fridrich, Jiri. "A new steganographic method for palette-based images.", *PICS*, pp. 285-289. 1999.

[11] Wang, Zichi, and Xinpeng Zhang. "Secure cover selection for steganography." *IEEE, vol.* 7, pp. 57857-57867, 2019.

[12] Subhedar, Mansi S., and Vijay H. Mankar. "Curvelet transform and cover selection for secure steganography.", *Multimedia Tools and Applications*, Vol. 77, no. 7, pp. 8115-8138, 2018

[13] Sajedi, Hedieh, and Mansour Jamzad, "Using contourlet transform and cover selection for secure steganography.", *International Journal of Information Security, Vol.* 9, no. 5, pp. 337-352, 2010

[14] Avcibas, Ismail, Nasir Memon, and Bülent Sankur. "Steganalysis using image quality metrics.", *Transactions on Image Processing, IEEE, Vol.* 12, no. 2,pp. 221-229, 2003.

[15] Kaur, Manveer, and Gagandeep Kaur, "Review of various steganalysis techniques.", *International journal of computer science and information technologies, Vol.* 5, no. 2,pp. 1744-1747, 2014.

[16] Zhang, Tao, and Xijian Ping, "Reliable detection of LSB steganography based on the difference image histogram.", *International Conference on Acoustics, Speech, and Signal Processing, IEEE*, vol. 3, pp. III-545, 2003.

[17] Westfeld, Andreas, and Andreas Pfitzmann, "Attacks on steganographic systems.", *International workshop on information hiding*, Springer, pp. 61-76, 1999.

[18] Liu, Qingzhong, Andrew H. Sung, Jianyun Xu, and Bernardete M. Ribeiro. "Image complexity and feature extraction for steganalysis of LSB matching steganography.", *International Conference on Pattern Recognition (ICPR'06)*, IEEE, vol. 2, pp. 267-270, 2006.