**Summary**

This paper talks about steganography, steganography is the art or hiding data within a medium without letting others know about that data is existing. I will go through an introduction about the topic, then proceed to explain it’s background and more information about the uses of this technique, and how organizations use it in their advantage.

**Introduction**

Steganography is the art of hiding a message. The purpose of steganography is to hide a message from a someone you don’t want to see it. It is different than cryptography, the art of secret writing, which is intended to produce a message that cannot be read but does not hide the existence of the secret communication. Although steganography differs from cryptography, there are many analogies between the two, and some authors classify steganography as a form of cryptography since hidden communication is a type of secret writing. Steganography works by changing bits of useless or bot used data in regular computer files (such as graphics, sound, text, HTML) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.

**Background**

Information hiding is related to two fields, Steganography and watermarking. There are three main aspects for information hiding: capacity, security, and robustness. Capacity means the amount of information that can be hidden, security refers to the inability of an eavesdropper to detect hidden information, and robustness to the amount of modification the

cover medium can resist before the hidden information is corrupted. In general, information hiding goes through these processes:

* Identification of redundant bits in a cover medium. Redundant bits are those bits that can be edited without taking care of the quality of the cover medium.
* A subset of the redundant bits to be replaced with data from a private message. The stage medium is created by replacing the selected redundant bits with message bits. The modification of redundant bits can change the statistical properties of the cover medium. As a result, statistical analysis may reveal the hidden content.

**Uses of Steganography**

Steganography is used to carry out hidden exchanges. For example, governments are interested in two types of communication of hidden data. One of which supports national security and one which does not. Steganography support both types. Businesses also have similar concerns, about trade secrets for new technologies or products information. Of course, using steganography to communicate greatly reduces the risk of information leakage. Businesses take advantage of another form of steganography, called watermarking. Watermarking is mainly used to identify and entails hidden unique part of information within a medium without touching the medium. Steganography enhances the privacy individually, although it is not a substitute for encryption. This is effective only if the hidden embedded information is not detected. If the communication almost never exists, this will become so private to be caught. Like many tools, steganography:

1. Steganography can be a way which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.

2. It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside.

3. Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganography techniques that are being used to store watermarks in data. The main difference is on intent. While the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, steganography methods can be used to hide this.

4. Steganography software tools allows a user to attach hidden data in a carrier file, such as an image or video, and sometimes it could be an audio, and later take off that data. It is not necessary to hide the message in the original file at all. Thus, it is not necessary to edit the original file and therefore, it is hard to detect nothing. If a given part of the message is subjected to successive bitwise manipulation to generate the cyphertext, then there is no evidence in the original file to show that it is being used by a third party to encrypt a file.

9.Deep knowledge of Steganography. Steganography comes from the Greek words for “covered writing”. It is the practice of disguising the existence of a message. Generally, innocent looking carriers, e.g., pictures, audio, video, text, etc. that hold the hidden information. The combination of hidden data-plus-cover is known as the stego-object, Stegokey.

10. Stego is merely one of many methods to defend the confidentiality of data. It is probably the best used in integration with another data-hiding method. When used in collection, these ways can all be a part of a layered security mechanism. Some good complementary methods include:

* Encryption- Encryption is the operation of crossing data or plaintext through a series of mathematical processes that generate an alternate form of the original text known as ciphertext. The encrypted text can only be read by one who have been given the proper key to decrypt the ciphertext back into its original plaintext form. Encryption doesn’t hide data, but it does make it difficult to read!
* Hidden directories (Windows)- Windows provides this feature, which allows users to hide files. Using this mechanism is as easy as changing the characteristics of a directory to “hidden” and hoping that no one can view all types of files in their explorer.
* Hiding directories (Unix)- in current directories that have a lot of files, such as in the /dev directory on a Unix implementation or making a directory that starts with three dots (…) versus the normal single or double dot.
* Covert channels- Some tools can be used to transfer important data in seemingly normal network traffic. One such tool that does that is Loki. Loki is a tool that hides data in ICMP traffic (like ping).

11. Steganography vs. Encryption: The goal of steganography is to not keep others know the hidden information, but to keep others from thinking that the information even exists. If a method of steganography causes someone to suspect the medium which carries the data, then the method has failed. Encryption and Steganography achieve separate goals, encryption is changing the meaning of the message so it cannot be read, steganography does not change the meaning or change the data to make it unusable or unintended, rather, it prevents the third party from suspecting that there is a communication or data even exists. For those people who want to reach ultimate in security or privacy can combine both approaches, encryption and steganography. Encrypted data is difficult to be differentiate from normal occurring phenomena than a normal plain text (which is a raw text) in the medium. There are several steganography tools that can encrypt data before hiding them in a chosen medium.

Steganography should not be confused with encryption. Encryption disguises the content of a message. The existence of the message is usually obvious. Steganography disguises the existence of the message. However, additional security can be obtained if steganography is combined with encryption.

12. Steganalysis and its techniques: Steganalysis is the counter measure of steganography. It is the art of detecting that a steganography exists, or a decoded data within a medium. There are two main major tools in Steganalysis, information theory and statistical analysis. Mainly, this clearly reveals the tremendous potential for hidden information in the internal data of a course as long as a set of data can be compressed to smaller sizes. There should be a space for hidden data within the medium. Steganalysis can be classified in a similar way as cryptanalysis methods, largely based on how much prior information is known:

* Steganography-only attack: The steganography medium is the only item available for analysis.
* Known-carrier attack: The carrier and steganography media are both available for analysis.
* Known-message attack: The hidden message is known.
* Chosen-steganography attack: The steganography medium and algorithm are both known.
* Chosen-message attack: A known message and steganography algorithm are used to create steganography media for future analysis and comparison.
* Known-steganography attack: The carrier and steganography medium, as well as the steganography algorithm, are known.

13. Method of Steganography: A lot of methods are available for digital Steganography. But exploiting the lenient constraints of a file formats is the most famous one. There are a lot of softwares that uses this technique.

* Image as carriers: One of the ways to hide data is using images. The difficulty to reveal the data hidden increases with the details in an image, and that makes it harder to guess or to suspect that image. JPHIDE/JPSeek is a package that uses the coefficients to hide the information. There was a new method that embeds data in visually insignificant parts of an image. Both of these methods modify the image. The user however can explore image degradation with different messages and images of different length. Another way is for GIF images to modify an image’s palette for hiding its data. Gifshuffle is a tool that doesn’t modify the image itself, in any visible way. It permutes a GIF image’s color map, that will leave the original image completely intact.
* Audio File Carriers: A lot of packages also available for embedding and hiding data in the audio files. One of the tools for audio file hiding stego is the MP3. Stego does not only hide information effectively but also claims to be partly strong method of watermarking the targeted MP3 audio files. The WAV formal, which stands for Wavaform Audio File Format, is a Microsoft audio format which mainly windows depends on. However, this format lets users hide data using StegoWave or Steghide. These sites refer to both programs in order. Steghide modifies the LSB of data to be transmit in the carrier medium. Using an audio file as a medium is less popular than using an image as a steganography medium.
* Data Ordering: The data ordering, which does not have ordering constrains, is usually a very good method of steganography. Each change of a group of objects could be pointed to a positive integer. Pointing can then be used to encode the hidden data by modifying the sequence of objects that are not considered in ordered by the carrier medium. While this technique does not change the information quality, the data which are hidden can of course easily get lost if the medium is encoded again. For example, if we have a GIF which its color map consists of hidden data, we could then open the GIF in our favorite graphics-editing tool package that will be used, and save it again. Visually, the result will be both identical, from the original file to the second file, but the ordering of the color map may have been lost.

14. Limitations: Steganography is limited just like that encryption is. If bob wants to send an image with a hidden message to allice, he must first agree secretly with allice on a way of steganography. Underneath the encryption model, allice can be sure when she has got some ciphertext. Let us have a scenario about allice. When she wants to borrow bobs camera and neglects to tell him to be careful of every 73rd byte in the images she sends him, Bob will be ignorant of Alice’s steganography efforts. The chances that bob will let allice borrow his digital camera will decrease the large number of pictures he will receive from her. The amount of data that could be effectively hidden in a medium is heading to be limited by the size of the medium itself. The less limitations that exist on the integrity of the medium, the more potential it has for hiding data.

14. Conclusion: I have briefly explained and defined steganography, which is in my opinion an effective tool to do so many things regarding security or reliability in any field of communication. By that, I believe this technique can be used in any section in real life, military, business, educational, governments and more settings. Also, I have shown various tools and how they function well.

**CITATIONS**

* Chang, C.-C., Lin, C.-C., & Yang, C.-N. (2013). Steganography and Watermarking. Nova Science Publishers, Inc.
* Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, & Ton Kalker. (2008). Digital Watermarking and Steganography: Vol. 2nd ed. Morgan Kaufmann.
* Liu, Q. Y., Bu, Z. Q., Quan, M. X., Wu, Y., Ding, X., Xia, L. Q., Lu, J. Y., & Huang, W. T. (2022). A molecular paradigm: “Plug-and-play” chemical sensing and crypto-steganography based on molecular recognition and selective response. Biosensors and Bioelectronics, 209. <https://doi-org.libproxy.eku.edu/10.1016/j.bios.2022.114260>
* Bi, X., Yang, X., Wang, C., & Liu, J. (2021). High-Capacity Image Steganography Algorithm Based on Image Style Transfer. Security & Communication Networks, 1–14. <https://doi-org.libproxy.eku.edu/10.1155/2021/4179340>
* Santosh Kiran, B. v. s., & Anitha, R. (2021). Secure Data Hiding Techniques Using Image Steganography & Cryptography. Review of International Geographical Education Online, 11(7), 747–757. <https://doi-org.libproxy.eku.edu/10.48047/rigeo.11.07.71>