International Journal of Scientific Engineering and Science
Volume 5, Issue 2, pp. 41-44, 2021. ISSN (Online): 2456-7361

An Overview of Steganography through History

Nujud Alabdali[1], Sabah Alzahrani[2]
[1, 2]College of Computers and Information Technology, Taif University
Email address: nujud.alabdali.2 @ gmail.com[1], Sa.sabah @ tu.edu.sa[2]

Abstract*— *Steganography is the science of hiding information. The information can take any form and type including images, audio files, and texts. The practice of hiding information is not new and has taken uncommon ways to hide secret messages. People used to convey secret information on rabbits' stomachs and the scalp of slaves. In this paper, we briefly examine the history of steganography from a technical perspective. We focus specifically on the classification adapted to categorize the techniques used in steganography. We concisely touch on null ciphers and digital carriers.

I. INTRODUCTION

Steganography is the art of hiding information. It is an ancient practice that has evolved with time. The main objective of the practice is to communicate a hidden message. The communication is usually achieved via a public/known medium. However, it carries within a secret message meant to be revealed by a specific party.

Steganography is more geared towards hiding the information rather than securing it. Cryptography is more concerned with securing the information. One can argue that hiding the information is part of securing it; hence, the two disciplines may be overlapped. In this paper, however, I focus on steganography through techniques rather than delving into their security implementations.

The use of steganography dates back to the 15th century when physical secret messages were hidden through different means. One example was the use of wax tablets. Messages were hidden on the back of the wax tablet. Another technique was writing with an invisible ink. It has been used either for fun or espionage purposes [1]. One has to use chemical materials to reveal the hidden text including flame and light [2]. Searching for places to hide the secret message stretches the imagination to include writing on rabbits' stomachs and tattooing on the scalp of slaves [1].

The process of hiding a message involves at least two parties. The communication of the two parties is not hidden. The covered message is hidden though. The process takes a covered message and embeds it in a carrier, a medium to transfer the message to the intended receiver. A steganography may be used to encrypt the message, adding more security to the process.

The process can be summarized as follows: *steganography_medium = hidden_message + carrier + steganography_key* [1].

Steganography can be classified and better explained based on the technique used. The following figure is adapted from [2].following figure is adapted from [2].

Figure 1 shows a general classification of steganography.

- Technical steganography depends on scientific methods to conceal the secret message. Methods include and not limited to: invisible ink, microdots, and resizing-related methods.
- Linguistic steganography is concerned with hiding information through written natural language such as alphabets substitution and rearrangement. It also includes unexpected ways as well. This branch can further be classified to semagrams and open codes.

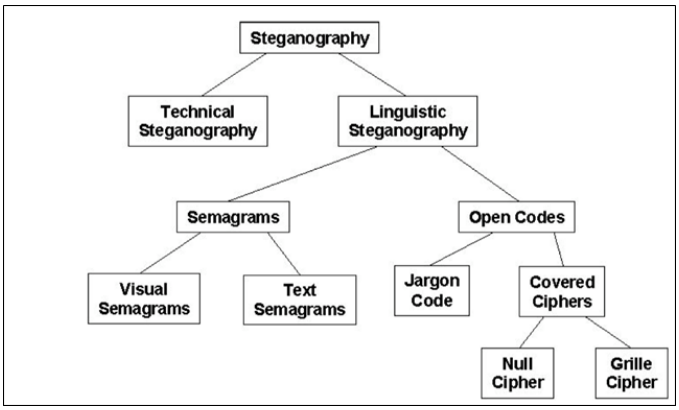

Figure 1. Steganography Based on the Technique Used.

- Open codes hides information in a text such that if read, it is not obvious what it means. Only those concerned with it are able to reveal its hidden meaning, or the hidden information. This category is further classified into jargon codes and covered ciphers.
- Jargon code uses language that is only meaningful to a certain party. It may include symbols and shortcuts.
- Covered ciphers embed information openly such that it can be recovered by someone who knows the "secret key" for how it was concealed. Null ciphers can be recovered through rearrangement of certain words/letters such as "read the second letter of each word in a new line". A grille cipher conveys the hidden information through a template. The words appeared on the openings of the template are the "key" to recover the information.

There are many applications of steganography that can be used for good and bad purposes. Criminals use steganography to communicate their secret messages publicly. They be the ones who understand that a public image may reveal more information than what it presents. In addition, good purposes are achieved with steganography as well. Authorship is protected via digital watermarks. They are embedded to preserve the author's rights such that, if done carefully, the quality of the original content does not get compromised, leading to maintaining the integrity of the content and protecting its authorship.

International Journal of Scientific Engineering and Science
Volume 5, Issue 2, pp. 41-44, 2021. ISSN (Online): 2456-7361

II. ARE NULL CIPHERS STILL USED?

This category of Steganography does not rely on complicated means to hide the secret message. It depends on texts and sets predefined rules to recover the message. One of the classic demonstration is shown below. The example (1) in Figure 2 below is adapted from [5].

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Figure 2 example (1)

During World War 1, the German Embassy in Washington D.C. sent the two messages above to the headquarters in Berlin via telegrams [5]. The message if read instantly does not convey any meaningful insight to what the Germans were up to. Reading the first letter of each word in the first message or the second letter of each word in the second message yields the following hidden information:

Pershing Sails From N.Y. June 1

This practice is still used today. Spam emails convey hidden messages with the help of null ciphers. Consider the example (2) shown on the Figure below adapted from [6][7].

Spams are usually ignored and deleted if read. The email above may resemble a spam, but it hides a secret message. It was encoded using a spam tool that takes a short text and turns it into a longer one. The new version of the text contains unnecessary words and numbers and means nothing to the reader. Only those who are expecting the hidden message to be embedded in the email will be able to decode it. [1, 6, 7]. The hidden message is as follows:

Meet at Main and Willard at 8:30

Dear Friend , This letter was specially selected to be sent to you ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1621 ; Title 5 ; Section 303 ! Do NOT confuse us with Internet artists . Why work for somebody else when you can become rich within 38 scam days ! Have you ever noticed the baby boomers are more demanding than their parents & more people than ever are surfing the web ! Well, chance to capitalize on this ! WE will help YOU sell more & SELL now is your You can begin at absolutely no cost to you ! But don't MORE . Anderson who resides in Missouri tried us believe us ! Ms where to park all my cars" . This offer is and says "My only problem now is forever if you don't order now ! Sign up a 100% legal . You will blame yourself too . Cheers ! Dear Salaryman , Especially friend and your friend will be rich are not interested in our publications and for you this amazing news . If you simply do NOT respond and ignore this wish to be removed from our lists, compliance with Senate bill 2116 , mail ! This mail is being sent in business proposal ! Why Title 3 ; Section 306 ! This is a ligitimate within 68 months ! Have work for somebody else when you can become rich the web and nobody is you ever noticed more people than ever are surfing capitalize on this . getting any younger ! Well, now is your chance to and SELL MORE . We will help you decrease perceived waiting time by 180% free for you ! But don't The best thing about our system is that it is absolutely risk "My only problem now is where to believe us ! Mrs Ames of Alabama tried us and says operate in all states ! You will park all my cars" . We are licensed to Sign up a friend and you'll blame yourself forever if you don't order now ! Your email address has been get a discount of 20% ! Thanks ! Dear Salaryman , briefing ! If you no submitted to us indicating your interest in our Subject: of longer wish to receive our publications simply reply with a "REMOVE" and you will immediately be removed from our mailing list . This mail is being sent in compliance with Senate bill 1618 , Title 6 , Section 307 . THIS IS NOT A GET RICH SCHEME . Why work for somebody else when you can become rich within 17 DAYS ! Have noticed more people than ever are surfing the web and you ever are surfing the web ! Well, now is your chance to capitalize more people than ever help YOU turn your business into an EBUSINESS and on this ! WE will the customer's doorstep ! You are guaranteed to succeed deliver goods right to the risk ! But don't believe us . Ms Simpson of Wyoming because we take all "Now I'm rich, Rich, RICH" ! We assure you that tried us and says applicable laws . We implore you act now ! Sign we operate within all discount of 50% . Thank-you for your serious up a friend and you'll get a consideration of our offer.

Figure 3 example (2)

III. How is an Image Encoded?

Common methods employing digital carrier include the use of audio and image files. To achieve this, knowledge about the hiding process is necessary. In this section, we examine the general structure of the encoding process.

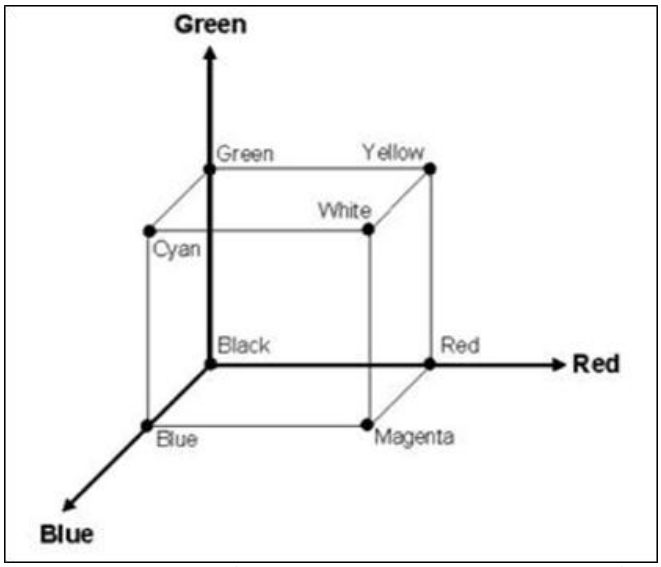

Figure 4. Representation of the Color Cube Concerning RGB. Adapted from [1].

The cube is used to represent a color. The given color is evaluated based on its relative intensity to the three main colors: red, green, and blue. Each one of these main colors is represented with an axis. Any chosen/given color is the result of the intersection of these three axes. For instance, black is rexprensetd with (0, 0, 0), indicting the absence of the three main colors. White, on the other hand, is the presence of all colors, (100, 100, 100) [8].

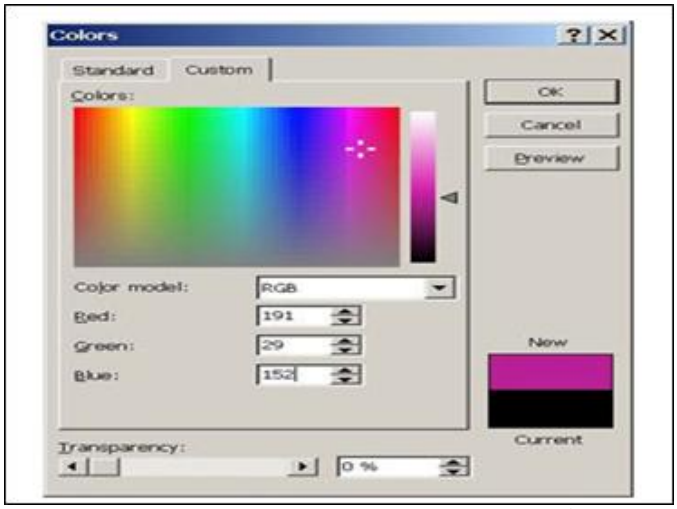

Figure 5. RGBLevels Regarding the Selected Color. Adapted from [1].

In the figure above, a random color was selected and its intensity levels to each one of the three main colors are shown. To elaborate, each color in the RGB component is represented with a single byte. Each value shown by the RGB component ranges from 0-255. In the example above, the color selected has intensity values as follows: 191 (BF in hexadecimal) for red, 29 (1D in hexadecimal) for green, and 152 (98 in hexadecimal)

for blue. Each value is then converted to hexadecimal to encode the color. Finally, the color is encoded using 24 bits filled from the values of the RGB components [1].

Images can be embedded based on the encoding process explained above. A map of a city could be hidden inside an image on a public website, showing no suspicion whatsoever. In addition, audio files are embedded as well. This depends on decoding the signals and inputting the values as binary numbers: 0 and 1.

IV. Can We Detect Steganography?

Steganography can be detected via various tools. The process of hiding information takes into account three main components: a sender, receiver, and medium. Each one of these components presents a threat in some sense. There are attacks that target the sender and others that focus on the receiver. The medium is also targeted and can be attacked either passively or actively. A passive attack relies on observing the communication, the two parties, and the medium they are using. Once an attacker gets these details, he is more capable of recovering the hidden message, especially with the use of advanced technologies.

Moreover, the medium varies greatly across communications. One may embed the secret message, image or text, inside a packet header. Another may embed information in a website component such as an html image tag. Each way/method has its own weaknesses and strengths. Therefore, being able to maintain secrecy may be challenging, especially with the advancement seen in technology.

V. Conclusion

Steganography is an ancient practice that has taken many forms and shapes. It has seen various means to hide intended secret messages. Writing on the wax tablets and stomachs of rabbits are some examples. Recently, digital technology has been utilized to serve purposes via steganography. Good practices include protecting author's rights via watermarks that maintain integrity. Bad practices are conducted via criminals to hide records of illegal activities such as fraud in financial institutions.

The filed is evolving and adapting to latest methods. Deep learning technologies are now used to embed information. Some of the methods used hide a large image in an image carrier. Others embed audio files or use audio files as carriers. The field is also creating a room for creativity and can be further utilized to advance technology and serve good purposes.

References

[1] Arnold, M., Schmucker, M., and Wolthusen, S. D. Techniques and Applications of Digital Watermarking and Content Protection. Artech House, Norwood, Massachusetts, 2003.
[2] Baluja, Shumeet. "Hiding images in plain sight: Deep steganography." Advances in Neural Information Processing Systems. 2017.

[3] Barni, M., Podilchuk, C. I., Bartolini, F., and Delp, E. J. Watermark embedding: Hiding a signal within a cover image, IEEE Communications (2001) 39(8):102108.
[4] Bauer, F. L. Decrypted Secrets: Methods and Maxims of Cryptology, 3rd ed. Springer Verlag, New York, 2002.
[5] Johnson, Neil F., and Sushil Jajodia. "Exploring steganography: Seeing the unseen." Computer 31.2 (1998): 26-34.
[6] Kahn, D. Codebreakers: The Story of Secret Writing. Revised ed., Scribner, New York, 1996.
[7] Kessler, Gary C. "An Overview of Steganography for the Computer Forensics Examiner (Updated Version, February 2015)." (2015).
[8] MoreCrayons. Color cube [Online]. (December 12, 2003). Available: http://www.morecrayons.com/palettes/webSmart/colorcube.php.