Proceedings of the 34th Accra Bespoke Multidisciplinary Innovations Conference & the Africa AI Stakeholders Summit
Academic City University College, Accra Ghana
19th – 21st December, 2022
www.isteams.net/accrabespoke2022

Security During Transmission of Data Using Web Steganography

Gyimah, Seth Adjei
MSc. Digital Forensics and Cybersecurity Programme
School Of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: seth-adjei.gyimah@st.gimpa.edu.gh; sethadjeigyimah@gmail.com
Phone: +233244475540

ABSTRACT

The enormous improvements in communications and related technologies, such as the Internet of Things (IoT) and its web-based and mobile applications, have changed our way of life. We are also noticing a trend in which internet-connected electronic devices are using technology more frequently and providing customers with services of a higher standard. However, there are several complications and issues that arise when sending and receiving information via the internet. The security, privacy, and preservation of sent information are the most critical of them all. The security of information has grown to be a significant problem with the expansion of data transfer across computer networks. There are numerous ways to safeguard data and prevent unwanted users from accessing it. Steganography and cryptography are two different data hiding and protection techniques. Steganography conceals communications within some other digital media. On the other side, cryptography obscures the message's content and makes it challenging for readers to decipher. To safeguard data, steganography can be combined with cryptographic methods. Combining steganography and cryptography for hidden data transmission is the best suggested method for protecting data transferred over the internet. A data carrier that is an image can be used for the transmission. With regard to capacity, security, and robustness for secure data transmission over an open channel, this combinational methodology will be sufficient. The purpose of this paper is to explain the steganographic security measures used to protect data while it is being transmitted across a network.

Key words: Security, Transmission, Data, Web Steganography

Proceedings Reference Format
Gyimah, S.A. (2022): Security during Transmission of Data Using Web Steganography. Proceedings of the 34th Accra Bespoke Multidisciplinary Innovations Conference & the Africa AI Stakeholders Summit. Academic City University College, Accra Ghana, 2022. Pp 37-42. www.isteams.net/accrabespoke2022
https://doi.org/10.22624/AIMS/ACCRABESPOKE2022/V34P3

1. INTRODUCTION

Data transmission over the web has long been facilitated by the use of data-concealing techniques. They are divided into two categories: steganography and watermarking. The terms "steganos" and "graptos," which in Greek indicate covering and writing, respectively, are the origin of steganography.

It is the skill of concealing a message in a medium, typically a photograph, an audio file, or a video clip, so that only the sender and the intended recipient are aware of its presence. The optimum use of digital media for covert communication is to conceal information utilizing text, images, audio, and videos. The security of information is the main issue raised by the expansion in data transfer across computer networks. (Ahmed Laskar, 2012). Thus, to prevent unwanted access to the data, data confidentiality and integrity are employed. The biggest threat to enterprises around the world is data security. While transferring data over the internet, there needs to be a system in place to guarantee data confidentiality and integrity. Transferring a file over the internet is fraught with danger.

Open ports, the use of insecure software like FTP or the DMZ, and sending unencrypted plain text emails are some risks that can be encountered. Therefore, it's crucial to disguise the data in some way, like within an image, to ensure that the security or privacy of the sensitive data is protected. The most secure way to do that is to encrypt the file, but one cannot completely rely on encryption because there is a small chance that a file could be compromised even when it uses encryption. This is because encryption uses a key to encrypt the file and when the attacker is aware of that key and the encryption method being used, he can easily access and read the files. Another method, steganography, is available to safeguard files from such a significant risk. The least important bit of layers of color in natural images is where steganographic methods hide messages. Statistical steganalysis can make it challenging to find the presence of these messages.

2. RELATED LITERATURE

The problem statement of this paper is how to guarantee the security of a file while it is being transmitted over the internet. There are numerous different approaches to providing this security. However, the finest solution with the highest level of security is created when steganography and encryption are combined. This solution combines two distinct strategies for data security into a single one. For instance, text files are currently not covered by many security measures, making them vulnerable to attack. However, when combined with steganography and encryption, text files are safe when transmitted over the internet. Data or a file that a user sends over the internet when it is in the transit phase is susceptible to attack. There is a considerable danger of security being breached when using the internet as a medium because it can be accessed by the attacker. In order to prevent the attacker from compromising the file being delivered over the internet, steganography offers security.

Steganography obscures the medium rather than altering the structure of the hidden message, making it impossible to read. (Johnson & Jajodia, 1998). Conway (2003) added that the confidentiality of the data encoding method is a prerequisite for the steganography system. (Conway, 2003). When the encoding system is known, the steganography system is defeated and not useful anymore. Walia et al, 2010 also said that steganography is the invisible communication between the sender and the receiver. (Walia & Jain, 2010). According to Friedman,1967 steganography eliminates the unwanted attention coming towards the media in which the message is hidden. In Steganography, only the sender and the receiver know the existence of the message, whereas in cryptography the existence of the encrypted message is visible to everyone. (Ramesh et al., 1993).

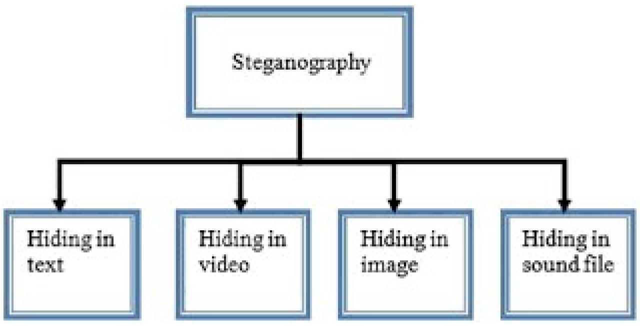

Fig 1: Steganography Component

4. FINDINGS

Reliability, integrity, and effectiveness are the three concerns related to the security of a file being transmitted over the internet: Reliability assures that no one who is not vetted or allowed will be aware of the transmission of critical data. The effectiveness component makes it difficult to find hidden information in a file even if we believe it exists, and the integrity component guarantees that concealed information will not be modified along the transmission path. This paper will discuss three types of steganography used to secure files sent over the internet. The first kind involves putting information in a text file and hiding it. This can be achieved by modifying the amount of whitespace, applying the first-letter method, and utilizing a publicly accessible cover. The other type of steganography is concealing data within an image. This is accomplished via algorithms, transformations, masking, and LSB (least significant bit) alterations. The paper will finally talk about steganography that involves concealing data within an audio or video clip. Because human hearing stops at 20000 Hz, it is better to conceal information in audio or video. This method is distinguished by the vast amount of data that may be concealed and is challenging to identify because the transmission process is sequential. It should be emphasized that employing steganography techniques for illicit purposes carries a risk. If this were to happen, victims would receive some spyware files. The receiver file contains information that one must be aware of.

5. RESEARCH GAPS

Cryptography has been used for centuries to safeguard the confidentiality and privacy of data. This science has been applied in the execution of military strategies by the Arabs, Greeks, Persians, and Romans. The second world war saw the further development and application of this science in the transmission of the so-called open encoded messages. The safeguarding of sensitive information once again became a challenge as time went on because hackers created methods to decrypt steganography messages.

This problem has emerged as one of the most significant ones, one that both researchers and users are concerned about. Researchers cannot afford to ignore the urgent need to ensure the privacy and security of transmitted data.

6. Recommendations for practices, policies, and design

The most dependable and safe method of hiding a message inside of an image without distorting or otherwise altering it is called steganography. The stego picture also keeps the original image's attributes. Pixel values stay the same as well. Steganography and cryptography work together to produce a very secure mechanism for transferring information over web applications. It is possible to create a system that can guarantee the data's confidentiality and integrity by fusing cryptography and steganography. The actual message can be concealed using steganography without having it altered, and the message can have a security layer added using cryptography. Digital steganography is the term for contemporary steganography techniques. Among these contemporary techniques are the concealment of messages within noisy images, the embedding of messages within random data, the embedding of photos containing messages within video files, etc. In addition, networks for communication use network steganography. Included in this are methods like WLAN Steganography and Steganophony, which involve hiding a message in Voice-over-IP interactions (methods for transmitting steganogram in Wireless Local Area Networks). Steganalysis innovations now come after steganography innovations.

The steganographic methods that make changes to the image that are not visible to the human eye review say that this feature is not enough because statistical methods can detect the changes in the image even if it is not visible. (Baskurt, 1990). According to the summary of image compression using the discrete cosine transform, compression is essential to picture-based steganography because the effectiveness of the steganographic technique depends on the chosen compression scheme. The stenographers are conducting additional study as they look for a more effective way to conceal the message in a digital environment in order to avoid falling victim to the methods developed by steganalysis.

7. CONCLUSION

Steganography is a very effective method for concealing data before it is transmitted over the internet in an image, text, audio, or video. Steganography and cryptography used in tandem will satisfy the needs for data transmission security, reliability, and robustness across web applications. The astonishing increase in security and power, the rise in security consciousness among people, groups, organizations, and the government allow for the implementation of these integrated techniques and the replacement of the current security techniques. Thus, the suggested way of fusing cryptography and steganography enables users to communicate data via a network in a secure manner and it may be used for applications that demand high-volume embedding with resilience against attacks. The steganography approach may be more secure if it compresses the data or information first, encrypts it later, and then embeds it inside the cover image.

8. DIRECTION FOR FUTURE WORKS

Existing cryptographic systems can provide confidentiality and privacy, but they lack a mechanism to conceal cryptographic communication. Steganography, which makes communication invisible, can be employed in specific situations to protect data, but it can also be detected, just like cryptography. (Li et al., 2011). Thus, rather than employing steganography exclusively in this case, some of its features are being transferred to cryptography. Raphael and Sundaram (2011) analyzed the effectiveness of steganography and cryptography separately and found that combining the two might result in a very effective data security approach. The steganographically concealed secret message is first encrypted with the IDEA method and then inserted into the image. The level of data security has been doubled and raised. Steganography and cryptography both use a different method to conceal data. Although they conceal data in different ways, steganography and cryptography are actually complimentary techniques.

REFERENCES

1. Ahmed Laskar, S. (2012). High Capacity data hiding using LSB Steganography and Encryption. *International Journal of Database Management Systems*, *4*(6), 57–68. https://doi.org/10.5121/ijdms.2012.4605
2. Baskurt, A. (1990). Numerical image compression using the discrete cosine transform. *Signal Processing*, *19*(4), 346. https://doi.org/10.1016/0165-1684(90)90166-v
3. Conway, M. (2003). Knowledge, Technology and Policy (Special issue entitled. *Technology and Terrorism')*, *16*(2), 171–191.
4. Johnson, N. F., & Jajodia, S. (1998). Steganalysis of images created using current steganography software. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1525*, 273–289. https://doi.org/10.1007/3-540-49380-8_19
5. Li, B., He, J., Huang, J., & Shi, Y. Q. (2011). A survey on image steganography and steganalysis. *Journal of Information Hiding and Multimedia Signal Processing*, *2*(2), 142–172. https://doi.org/10.1201/b12697-11
6. Ramesh, R. S., Athithan, G., & Thiruvengadam, K. (1993). An automated approach to solve simple substitution ciphers. *Cryptologia*, *17*(2), 202–218. https://doi.org/10.1080/0161-119391867872
7. Walia, E., & Jain, P. (2010). An Analysis of LSB & DCT based Steganography. *Global Journal of Computer Science and Technology GJCST Computing Classification F*, *10*(1), 1.