**DATA SECURITY USING STEGANOGRAPHY TECHNIQUE**

**AYUBA philemon**

**(ST/CS/ND/21/046)**

**A SEMINAR PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**AUGUST, 2023**

**DATA SECURITY USING STEGANOGRAPHY TECHNIQUE**

**AYUBA philemon**

**(ST/CS/ND/21/046)**

**A SEMINAR PRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF NATIONAL DIPLOMA (ND) IN COMPUTER SCIENCE**

**AUGUST, 2023**

**Abstract**

*Steganography is the art of covered, or hidden, writing. The purpose of steganography is covert communication to hide the existence of a message from a third party. This proposed system deals with implementing security-using Steganography. In this technology, the end user identifies an image which is going to act as the carrier of data. The data file is encrypted and authenticated. This message is hidden in the image. The image if hacked or interpreted by a third-party user will open up in any image previewer but not displaying the data. This protects the data from being invisible and hence be secure during transmission. The user in the receiving end uses another piece of code to retrieve the data from the image.*

**Keywords:** Stenography, Encryption, Data Security, Technique.

**Introduction**

The art of writing in cipher, or in characters which are not intelligible except to persons who have the key is cryptography. *Steganography* is the art of *covered*, or *hidden*, *writing.* The purpose of steganography is *covert communication* to hide a message from a third party. This differs from *cryptography*, the art of Steganography *secret writing*, which is intended to make a message unreadable by a third party but does not hide the very existence of the secret communication. While steganography is separate and distinct from cryptography. Both have been used throughout recorded history as means to protect information, there are many analogies between the two and, in fact, some authors categorize steganography as a form of cryptography since *hidden* communication certainly is a form of *secret* writing (Altaay *et al.,* 2012).

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be combined with encryption as an extra step for hiding or protecting data. The word *steganography* is derived from the Greek words *steganos* (meaning *hidden* or c*overed*) and the Greek root *graph* (meaning *to write*). Steganography can be used to conceal almost any type of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. The content to be concealed through steganography -- called *hidden text* -- is often encrypted before being incorporated into the innocuous-seeming *cover text* file or data stream. If not encrypted, the hidden text is commonly processed in some way in order to increase the difficulty of detecting the secret content (Shoukat, 2011).

Steganography hides the covert message but not the fact that two parties are communicating with each other. The embedded data is the message that one wishes to send secretly. The stego process generally involves placing a *hidden message* within some transport medium, called the *carrier*. The secret message is embedded within the carrier to form the *stego medium*. The use of a *stego key* may be employed for encryption of the hidden message and/or for randomization within the stego scheme (Altaay *et al.,* 2012). Classical steganography system depend on keeping the encoding system secret, but modern steganography is detectable only if secret information is known, e.g. a secret key. The actual process of embedding information in another file usually involves two classes of files –message files and cover files. The message file is the information that is hidden or embedded during the steganographic process. Depending on what a user is hiding, the message file can be any type of information source – audio, graphic, text, or even malicious files. The only restriction on a message file is that it must fit within the cover file. The cover file is the medium that contains the message file after the steganographic process is applied. Again, the intent of steganography is to maintain the initial visible quality of the cover file after the message file is hidden. Therefore, the file should not draw undue attention to itself or compromise any features and characteristics generally found in other similar files of its particular type. A cover file can also be referred to as a container file or stego-file. The latter term usually only applies to the cover file after the message file has actually been embedded.

**Literature Review**

According to Babu (2010), steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

Information transmission through internet may include sensitive personal data which may be intercepted. Also, there are many applications on the internet and many web sites require the users to fill forms that include sensitive personal information such as telephone numbers, addresses, and credit card information. So, the users may need private and secure communications for many reasons such as protect their confidential information from hackers during it passed over an open channel, so the confidentiality and data integrity are required to protect against unauthorized access and use. Cryptography and steganography are the common methods to secure communications (Altaay *et al.,* 2012).

Cryptography is the science of using mathematics to encrypt and decrypt data to keep messages secured by transforming intelligible data form (plaintext) into unintelligible form (ciphertext). The term cryptography has come from the Greek word “kryptós” standing for “hidden” and “gràphin” standing for “writing”. Thus, the proper meaning of cryptography is “hidden writing”. Any cryptosystem consists of plaintext, encryption algorithm, decryption algorithm, Cipher text, and Key. Plaintext is message or data which are in their normal, readable (not encrypted) form. Encryption is the process of converting plaintext to cipher text by using key. Cipher text results from encryption by applying the encryption key on the plaintext. Decryption is the process of retrieving the plaintext back from the cipher text. The Key is used info to control the cryptosystem (cipher system), and it is known by the sender and receiver only. While cryptography is very powerful for securing data; the cryptanalysts could success to break the ciphers by analyzing the contents of cipher text to get back the plaintext (Babu, 2010).

Cryptographic systems are generally classified into three independent dimensions (Petitcolas, 2019):

**Operation on Plaintext**

There are two types of operations that are occurred on plaintext to transform plaintext to cipher text. According to the first operation, each element in plaintext (i.e., bit, letter, group of bits or letters) is substituted for one another in the ciphertext. In this type of operation, a one-to-one mapping between the elements such as Caesar cipher. The principle of the second type of operation is that each character in plaintext is transposed with one another based on a mapping dictated by the key. In this type, the plaintext characters stay the same but they are just moved into different positions such as Rail Fence cipher. Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions (Petitcolas, 2019).

**The Number of Used Keys**

If the sender and the receiver use one key to encrypt and decrypt the plaintext, the system is referred to as symmetric, single key, secret key or conventional encryption. Symmetric encryption is fairly straightforward and very fast. If the sender and receiver use different keys, public key and private key, to encrypt and decrypt the plaintext respectively, the system is referred to as asymmetric, two – key, or public key encryption (Petitcolas, 2019).

**The Way in which The Plain Text is processed**

Block cipher operates on fixed-length groups of [bits,](https://en.wikipedia.org/wiki/Bit) called blocks, and produces an output block for each input block. A stream cipher operates on each [plaintext](https://en.wikipedia.org/wiki/Plaintext) element continuously, and produces one element at a time, as it goes along.

On the other hand, Steganography is considered the art and science of hiding information in other information. The word Steganography is derived from the Greek words “steganos” meaning “impenetrable” and, “grafia” meaning “writing” defining it as “impenetrable writing” (Raphael & Sundaram, 2011). There are two common techniques for image embedding in steganography; spatial domain and transform domain (Petitcolas, 2019).

According to spatial domain embedding, the messages are embedded directly into the Least Significant Bits (LSBs). The least significant bits (LSB) insertion method is considered the most common and simplest Steganography method. According to transform domain embedding, the messages are embedded by modifying frequency coefficients of the cover image such as the Fourier transform, discrete cosine transform, or the wavelet transform (Babu, 2010).

Image steganography system is comprised two algorithms, one for embedding and one for extraction. The embedding process hides a secret message within a cover media (cover image), and the result of embedding process is stego image. The main issue is that the secret message will not be unnoticed if a third party tries to intercept the cover media (cover image). The extraction process is simply because it is the inverse of the embedding process, where the secret message is revealed at the end (Altaay *et al.,* 2012).

**Approaches in steganography**

The steganography approaches can be divided into three types (Saleh, Aly & Omara, 2015):

1. ***Pure Steganography;***it is a technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.
2. ***Secret Key Steganography;***it uses the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message by secret key technique and then hide the encrypted data within cover carrier.
3. ***Public Key Steganography;***it is the combination of the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

**The Difference between Cryptography and Steganography** (Saleh *et al.,* 2015):

1. Cryptography prevents unauthorized party from discovering the content of communication but Steganography prevents discovery of the existence of communication (i.e., Cryptography makes data gibberish and known the message passing while Steganography tends to conceal presence of hidden data and unknown the message passing).
2. Cryptography alters the structure of secret message while Steganography does not alter the structure of secret message.
3. Cryptography is more common technology than Steganography technology.
4. The most algorithms of Cryptography are well known, but the algorithms of Steganography are still being developed by certain formats.
5. In Cryptography, the strong algorithm depends on the key size, the more key size; the more expensive computing power is required to decrypt ciphertext. In Steganography, once the hidden message is detected, the message is become known.
6. Cryptography can provide all security objectives by implementing the public and private key(s) with hash functions or authentication codes or digital signatures. Steganography cannot provide most of security objectives (Integrity, authenticity, non-repudiation) by itself without using the cryptographic techniques. However, it provides confidentiality by itself because mostly, the concerning person knows that the message is hidden in what kind of medium (Schneier, Nitin & Ashish, 2013).

**What are examples for steganography?**

Steganography is practiced by those wishing to convey a secret message or code. While there are many legitimate uses for steganography, malware developers have also been found to use steganography to obscure the transmission of malicious code. Forms of steganography have been used for centuries and include almost any technique for hiding a secret message in an otherwise harmless container. For example, using invisible ink to hide secret messages in otherwise inoffensive messages; hiding documents recorded on microdot -- which can be as small as 1 millimeter in diameter -- on or inside legitimate-seeming correspondence; and even by using multiplayer gaming environments to share information (Sharda & Budhiraja, 2013).

**How is steganography used today?**

In modern digital steganography, data is first encrypted or obfuscated in some other way and then inserted, using a special [algorithm](https://www.techtarget.com/whatis/definition/algorithm), into data that is part of a particular file format such as a [JPEG](https://www.techtarget.com/whatis/definition/JPEG-Joint-Photographic-Experts-Group) image, audio or video file. The secret message can be embedded into ordinary data files in many different ways. One technique is to hide data in bits that represent the same color [pixels](https://www.techtarget.com/whatis/definition/pixel) repeated in a row in an image file. By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data (Schneier *et al.,* 2013).

The practice of adding a watermark -- a trademark or other identifying data hidden in multimedia or other content files -- is one common use of steganography. Watermarking is a technique often used by online publishers to identify the source of media files that have been found being shared without permission.

While there are many different uses of steganography, including embedding sensitive information into file types, one of the most common techniques is to embed a text file into an image file. When this is done, anyone viewing the image file should not be able to see a difference between the original image file and the encrypted file; this is accomplished by storing the message with less significant bites in the data file. This process can be completed manually or with the use of a steganography tool.

### **Advantage of Steganography**

Steganography is distinct from cryptography, but using both together can help improve the security of the protected information and prevent detection of the secret communication. There are advantages to using steganography combined with encryption over encryption-only communication. The advantage of steganography is as follows (Zaidan, Zaidan, Al-Frajat & Jalab, 2010):

1. The advantage of steganography is that messages do not send consideration to themselves. Clearly detectable encrypted message no matter how tough will stimulate suspicion, and may in themselves be compromising in countries where encryption is illegitimate.
2. In steganography, cryptography secures the contents of a message, steganography can be said to secure both messages and connecting parties.
3. This approach featured security, capacity, and robustness, the three needed element of steganography that creates it beneficial in hidden exchange of data through text files and creating secret communication.
4. There are some important files carrying confidential data can be in the server in and encrypted form and No intruder can receive some beneficial information from the initial file during transmit.
5. With the need of Steganography Corporation government and law enforcement agencies can connect privately.
6. The major objective of steganography is to connect privately in a completely imperceptible aspect and to prevent drawing uncertainty to the transmission of a hidden information. It is not to maintain others from understanding the hidden data, but it is to maintain others from thinking that the data even exists. If a steganography approach generates someone to suspect the carrier medium, thus the method has unsuccessful.
7. The advantage of steganography is that it can be generally used to secretly send messages without the case of the transmission being found. By using encryption, it can recognize the sender and the receiver.
8. Steganography has a double component of protection such as first, the file itself is secret and second, the data in it is encoded.

### **Disadvantage of Steganography**

The disadvantage of Steganography is as follows −

1. There are large number of information, huge file size, therefore someone can suspect about it.
2. If this approach is gone in the wrong hands such as hackers, terrorist, criminals then this can be very much critical.
3. Steganography is not without its disadvantages. However, these can be rectified and once it is performed and it can strengthen the element of steganography.
4. Most data hiding approach take advantage of human perceptual deficiency, but they have deficiency of their own. However, these can be independently rectified.
5. The major disadvantage of steganography is that, unlike cryptography, it needed a lot of overhead to hide associatively few bits of information. Because the steganographic system is found, it is rendered useless. However, it fares no worse than cryptography and is still the preferred medium.

**Conclusion**

In this paper, a new secure communication model has been presented that combines cryptography and steganography techniques to provide two layers of security, so the steganalyst can’t reach to plaintext without knowing the secret key to decrypt the ciphertext. The advantages of a steganographic file system are considerable, considering that an attacker who does not possess the name of a file and the password for accessing it cannot determine whether the file is even present. Even if a skilled attacker has unlimited access to a computer and understands it completely, a steganographic file system allows the data owner to plausibly deny that any files are hidden at all.

**Recommendations**

The following are the recommendations this paper put forward they are;

1. It is recommended that more review be made on the security technique and imbibe since it offers more advantages and benefits over other techniques.
2. It is also recommended that Steganography can make use of unlimited legal means to use any web site without attracting the attention of anybody, including the owners of the target web sites themselves and therefore be used as a major data security technique.

**References**

Altaay, A., Marvel, M. & Murphy, S. (2012). An Introduction to Image Steganography Techniques,” *International Conference on Advanced Computer Science Applications and Technologies*, 3(4), 122 – 126.

Babu, E. (2010). A Survey on Cryptography and Steganography Methods for Information Security, *International Journal of Computer Applications,* 12(2), 13-17

Petitcolas, L. (2019). Information Hiding-A Survey, *Proceedings of the IEEE, special issue on protection of multimedia content,* 87(1), 1062-1078.

Raphael, J. & Sundaram, V. (2011). Cryptography and Steganography – A Survey,” *International Journal*, 2(3), 626- 630.

Saleh, A., Aly, F. & Omara, A. (2015). Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding, *International Journal of Computer Science and Security (IJCSS),* 9(2), 397-397.

Schneier, B., Nitin, K. & Ashish, V. (2013). Comparison of Various Images Steganography Techniques, *International Journal of Computer Science and Management Research,* 2(1), 1213-1217.

Sharda, S. & Budhiraja, S. (2013). Image Steganography: A Review. *International Journal of Emerging Technology and Advanced Engineering (IJETAE)*, 4(1), 707–710.

Shoukat, A. (2011). A Survey about the Latest Trends and Research Issues of Cryptographic Elements, *International Journal of Computer Science Issues,* 8(2),140-149.

Zaidan, A., Zaidan, A., Al-Frajat, A. & Jalab, H. (2010). On the Differences between Hiding Information and Cryptography Techniques: *An Overview* *Journal of Applied Sciences,* 10(15), 1650-1655.