**DATA SECURITY USING STENOGRAPHY TECHNIQUE**

**SANI MUSA**

**ST/CS/HND/21/042**

**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 STENOGRAPHY TECHNIQUE**

**SANI MUSA**

**ST/CS/HND/21/042**

**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 HIGHER NATIONAL DIPLOMA (HND) 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, Marvel & Murphy, 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.

**Types of Approaches in stenography**

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):

|  |  |  |
| --- | --- | --- |
| **Parameter** | **STEGANOGRAPHY** | **CRYPTOGRAPHY** |
| Definition | It is a technique to hide the existence of communication | It’s a technique to convert data into an incomprehensible form |
| Purpose | Keep communication secure | Provide data protection |
| Data Visibility | Never | Always |
| Data Structure | Doesn’t alter the overall structure of data | Alters the overall structure of data |
| Key | Optional, but offers more security if used | Necessary requirement |
| Failure | Once the presence of a secret message is discovered, anyone can use the secret data | If you possess the decryption key, then you can figure out original message from the ciphertext |

## ****Steganography Techniques****

Depending on the nature of the cover object(actual object in which secret data is embedded), steganography can be divided into five types (Sharda & Budhiraja, 2013):

1. Text Steganography
2. Image Steganography
3. Video Steganography
4. Audio Steganography
5. Network Steganography

**Text Steganography**

Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts. Various techniques used to hide the data in the text are:

1. Format Based Method
2. Random and Statistical Generation
3. Linguistic Method

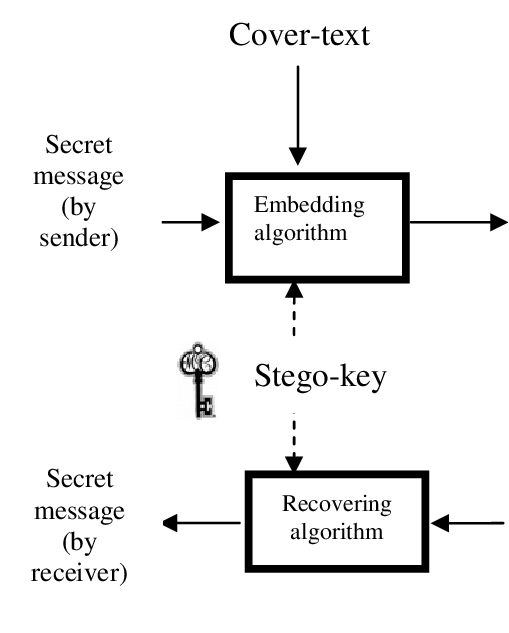


Figure 1: Text Stenography **representation**

**Image Steganography**

Hiding the data by taking the cover object as the image is known as image steganography.  In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image.

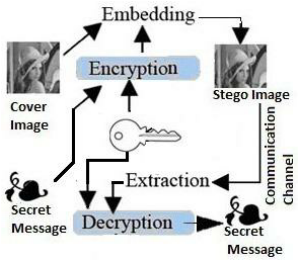


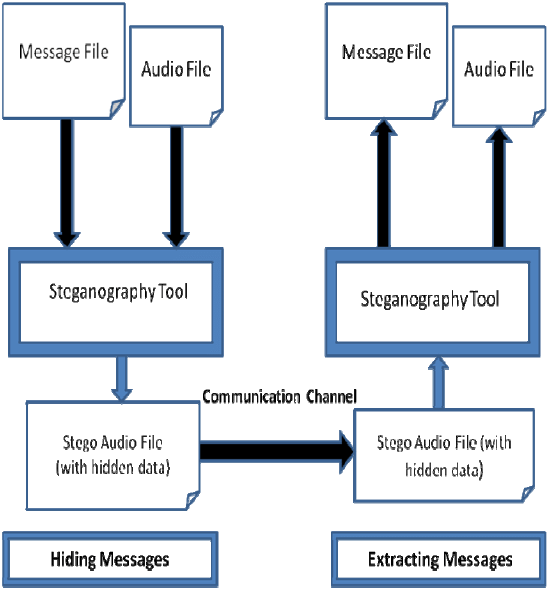
Figure 2: Image stenography **representation**

**Audio Steganography**

In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a much more difficult process when compared to others, such as Image Steganography. Different methods of audio steganography include:

1. Least Significant Bit Encoding
2. Parity Encoding
3. Phase Coding
4. Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

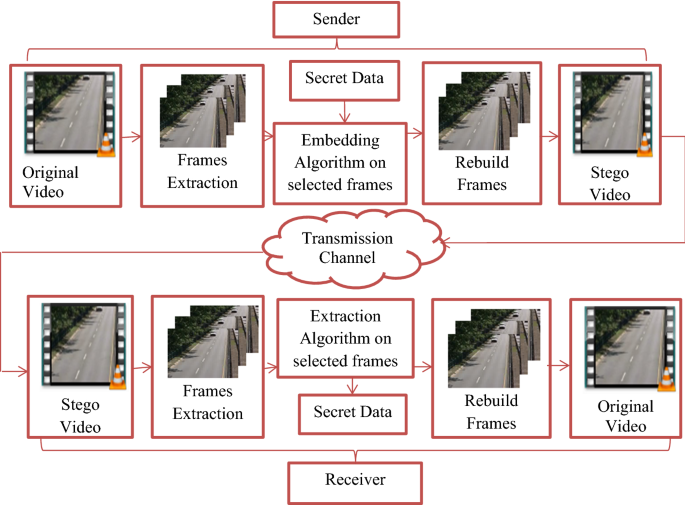


**Figure 3: Audio stenography representation**

**Video Steganography**

In Video Steganography you can hide kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. Two main classes of Video Steganography include:

1. Embedding data in uncompressed raw video and compressing it later
2. Embedding data directly into the compressed data stream

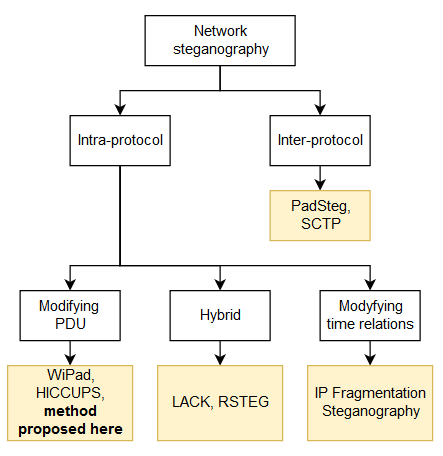


**Figure 4 Video stenography representation**

**Network Steganography (Protocol Steganography)**

It is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP etc. You can use steganography in some covert channels that you can find in the OSI model. For Example, you can hide information in the header of a TCP/IP packet in some fields that are either optional.

In today’s digitalized world, various software tools are available for Steganography. In the remainder of this Steganography Tutorial, we will explore some of the popular steganographic tools and their capabilities (Petitcolas, 2019).



**Figure 5: Network protocol stenography representation**

## FACTORS TO CONSIDER IN STEGANOGRAPHY

## Perceptual Transparency

One of the most important considerations while designing any algorithm that is used for data hiding is that it should perform its operation without raising any suspicion of the eavesdropper. Most steganographic techniques or data embedding techniques implicitly employ limitation of the Human Auditory System (HAS) or Human Visual System (HVS) to embed data. Some advanced perceptual models can also be used to determine the best way to embed data in order to conceal its identity (Petitcolas, 2019).

#### **Information Capacity**

The amount of information that can be embedded into a medium without modifying the medium also characterizes the robustness of the technique. Steganographic capacity is the size of information that can be hidden relative to the size of the cover image. The hidden information and the cover image should withstand any kind of transformations, such as rotation, blurring, denoising, adding noise, sharpening, scaling and other linear and non-linear filtering techniques.

#### **Tamper Proof**

Tamper proofing is used to indicate that the host signal has been modified from its authored state. Modification to the embedded data indicates that the host signal has been changed in some way. Even though the medium is not restricted in steganography, but mechanisms should be provided to detect the possible ‘corruption’ of the medium. This property assumes significance in watermarking and copyright protection schemes, where the copyright has to be effective even after modifying.

### **Advantages 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, 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.

**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.

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

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.

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, *IJCSI 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.