Data Hiding with the Help of Cryptography and Steganography

Juhil P. Zalavadiya
Department of Information and Technology Engineering
A. D. Patel Institute of Technology New Vidhya Nagar, Anand, Gujarat, India

Abstract— Nowadays, security over the transmission of information is the major concern due to the likelihood of attacks and other unethical changes during active communication over the network. However, the confidentiality of the secret message can be secured using either cryptography or steganography. Cryptography is the science of using mathematics to encrypt and decrypt data; the message is converted into some meaningless form, and then the encrypted message or data are transmitted through transmission-channel. While steganography is the method of hiding communication. In steganography, the message is embedded in a harmless-looking cover such as image, audio, text file, etc. But alone cryptography or steganography cannot provide a better security approach. So, a new method based on the combination of both cryptography and steganography can overcome each other's weaknesses and make difficult for intruders to attack or breach the security. In this paper, a new encryption technique is used in order to enhance security.

Keywords: Cryptography, Steganography, Stego-Text, Encryption, Decryption

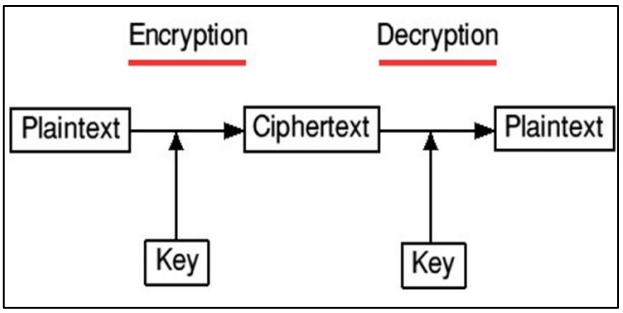
I. INTRODUCTION

Network security has become a crucial part of the modern era. The need for network security was arisen to obtain the integrity and confidentiality of the data and protect it against unauthorized access. The steganography and cryptography are the two sides of a coin where the steganography hides the traces of communication while cryptography uses encryption to make the message incomprehensible. The steganography does not change the structure of the message. On the other side, cryptography alters the standard secret message structure when transferred along with the network.

A. Cryptography

Cryptography is a method of protecting information and communications through the use of codes.so, only those people for whom the information is intended to deliver can read and process it. The pre-fix "crypt" means "hidden" and the suffix "graphy" stands for "writing". Earlier cryptography was effectively synonymous with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.

Data that can be read and understood without any difficulty is called plain text. The method of encoding plain text in such a way as to hide its content is called encryption. For that key is used. Encrypting plain text results in a vague text called ciphertext. One can use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plain text is called decryption[7].



Modern cryptography concerns itself with the following four objectives:

1) Confidentiality: The data cannot be understood by anyone for whom it was unintended
2) Integrity: The data cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3) Non-repudiation: The sender of the information cannot deny at a later stage for service
4) Authentication: The sender and receiver can confirm each other's identity and the origin/destination of the information

There are two types of cryptography:

1) Symmetric-key Cryptography:

In this methodology both the sender and receiver share a single key. The sender uses this key to encrypt the plaintext and send the ciphertext to the receiver. On the receiver's side he/she applies the same key to decrypt the message and recover the plain text.

List of Symmetric Algorithms

- Advanced Encryption Standard (AES)
- Data Encryption Standard(DES)
- Triple Data Encryption Standard
- Blowfish Encryption Algorithm
- International Data Encryption Algorithm etc.

2) Public-Key Cryptography:

This is the most revolutionary concept in the last 300-400 years. In Public-Key Cryptography two related keys (public and private key) are used. The public key may be freely distributed, while its paired private key, remains a secret. The public key is used for encryption and for decryption private key is used.

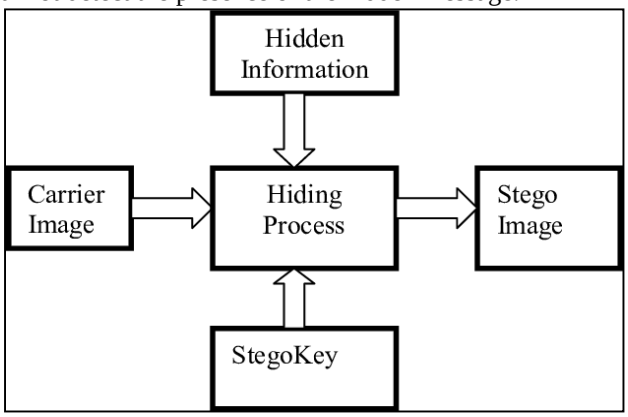
List of Asymmetric Algorithms

- RSA
- DSA
- Diffie-Hellman etc.

B. Steganography

Steganography is the art of writing a hidden message so that only the intended user will be able to know the existence of the original message. It comes from the Greek words Steganos and Graphy. Steganos means "covered" and Graphy means "writing". So steganography means covered writing. The main purpose of steganography is to hide a secret message within a cover-media (Image, audio, and video) in

such a way that others can not detect the presence of the hidden message. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot detect the presence of the hidden message.



The carrier files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the hidden information it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict the detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages, steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been hidden inside a digital Picture, Video or Audio file.

There are 4 ways to implement steganography:

1) Using Text:

In this steganography, the text can be used as a cover media. To hide the message a word or line can be shifted; whitespaces can be used, even the number and position of the vowels are utilized to conceal the secret message.

2) Using Images:

It is the most ubiquitous form of steganography, the reason behind this is that it causes the least suspicion. The main disadvantage of using steganography is a significant amount of overhead it produces for hiding a small amount of information. Moreover, the system must not be discovered otherwise it is useless.

3) Using Audio:

Audio stenography can conceal the secret message in the audio file with the help of its digital representation. It can be achieved easily as a typical 16-bit file has 216 sound levels, and a few levels difference could not be detectable by the human ear.

4) Using Video:

Video steganography brings more possibilities of disguising a large amount of data because it is a combination of image and sound. Therefore, image and audio steganography techniques can also be employed in the video.

C. Comparison

The combination of cryptography and steganography will enhance the security of the data embedded. This combined will satisfy the requirements such as capacity, security, and robustness for secure data transmission over an open channel[5].

The difference between cryptography and steganography is a significant issue and outlined by Table1.

Steganography	Cryptography
Little known technology	Common technology
It is known as cover writing.	It means secret writing.
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message
Its goal is to communicate with secrecy.	Its goal is to protect the data.
Technology still being developed for certain formats	Most of the algorithm known by all
Steganography relies on a parameter such as Key.	While cryptography does not relies on any parameter.

Table 1: Comparison between steganography and cryptography

Although both methods provide security, this study proposes to combine both cryptography and steganography methods into one system in order to provide robustness and security, by using two levels of data encryption.

II. Related Work

In [1], Md. Khalid Imam Rahmani, Kamiya Arora, and Naina Pal introduced a new method based on the combination of both cryptography and steganography known as Crypto-Steganography which overcome each other's weaknesses and make difficult for the intruders to attack or steal sensitive information is being proposed.

In [2], Shristi Mishra and Prateeksha Pandey proposed various methods where cryptography and steganography are combined to encrypt the data as well as to hide the data in the image.

In [3], Hardikkumar V. Desai, Pacheri Beri, and Distt. Jahunjhunu Raj published a paper on a comparison of three ways to hide the information: Steganography, Cryptography, Watermarking.

In [4], Herman Kabetta, B. Yudi Dwiandiyanta, and Suyoto proposed a new scheme using web tools like CSS for hiding information. It is a secret communication mechanism using text steganography techniques that are embedded messages on CSS files and is further encrypted using RSA as a public key cryptographic algorithm.

In [5], Hayfaa Abdulzahra, Robiah Ahmad, And Norliza Mohd Noor introduced a new method of hiding secret messages in the image, possibly by combining steganography and cryptography. A new encryption technique is used in order to lower the space of representing the characters.

In [6], Sultan Almuhammadi and Ahmed Al-Shaaby conducted a comparative study of steganography and cryptography. They investigated a number of methods combining cryptography and steganography techniques in one system. Additionally, they presented a classification of these methods, and compare them in terms of the algorithm used for encryption, the steganography technique and the file type used for covering the information.

In [7], Ajit Singh and Swati Malik published a paper in which data hiding's importance is described. They used a combination of steganography and cryptography for improving security.

III. PROPOSED WORK

Either it is cryptography or steganography, both alone cannot make the data secure efficiently and effectively. So a better technique is developed by combining these two techniques. A combination of steganography and cryptography is used which will take advantage of both the techniques. We are using the AES Algorithm for encrypting the message. After encryption, we will apply the Line Spacing method of Text-Steganography for further enhancing security. Below we will first explain the AES Algorithm and then the Line spacing method.

A. The AES Algorithm:

Advanced Encryption Standard (AES) is the most popular and widely adopted symmetric encryption algorithm. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable to exhaustive key search attacks. Triple DES was designed to overcome this drawback but it was found slow.
The features of AES are as follows:

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

B. Line Spacing Method of Text-Steganography:-

In this method, white space to encode data is to insert spaces at the end of lines. It allows a predetermined number of spaces at the end of each line. Two spaces encode 1 bit per line, 4 encode 2, 8 encode 3, etc., dramatically increasing the amount of information Additional advantages of this method are that it can be done with any text, and it will go unnoticed by readers since this additional white space is peripheral to the text.

C. System Flow of the Proposed Scheme:

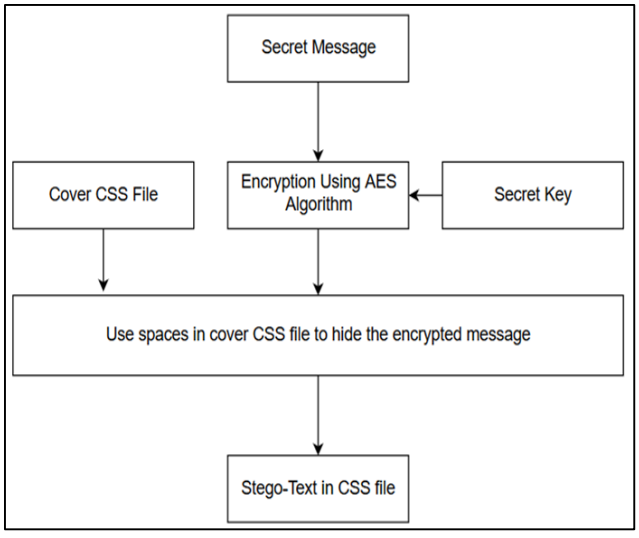


Fig. 1.1: At Sender's site

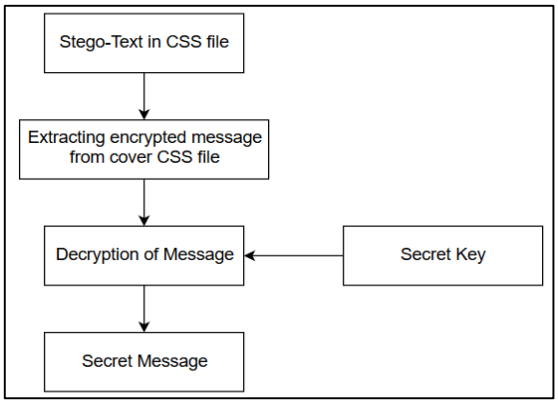


Fig. 1.2: At Receiver's Site

The procedure of the proposed method:-

1) Step 1: Firstly, the sender uses the AES encryption algorithm to generate a ciphertext with the help of a secret-key.
2) Step 2: From the use of the Line spacing method of Text-Steganography, we can hide encrypted messages in the CSS file(with spaces).
3) Step 3: After that, the Stego-Text file is created.
4) Step 4: Sender sends this CSS file to the receiver, which looks like a normal file.
5) Step 5: At the receiver's site, the receiver gets the stego-text in CSS and extract it for getting the ciphertext.
6) Step 6: For decrypting the ciphertext, secret-key is necessary. The sender sends the secret-key for the receiver to extract the secret message.

IV. CONCLUSION

This novel technique shows that the stego-text looks exactly the same as the original text. By using the "Line Spacing" technique for the embedding process makes no obvious changes as shown in figure 2.

```
<!DOCTYPE html>
<html>
<head>
<style>
body {
  background-color: lightblue;
}

h1 {
  color: white;
  text-align: center;
}

p {
  font-family: verdana;
  font-size: 20px;
}
</style>
</head>
<body>

<h1>My First CSS Example</h1>
<p>This is a paragraph.</p>

</body>
</html>
```

```
<!DOCTYPE html>
<html>
<head>
<style>
body {
  background-color: lightblue;
}

h1 {
  color: white;
  text-align: center;
}

p {
  font-family: verdana;
  font-size: 20px;
}
</style>
</head>
<body>

<h1>My First CSS Example</h1>
<p>This is a paragraph.</p>

</body>
</html>
```

Fig. 2: Original CSS File (Left), Stego CSS File with Hidden Information (Right)

In this paper, we proposed a method that combines Text-Steganography and Cryptography. It is achieved by the AES algorithm and Line Spacing method of steganography. A combination of cryptography and steganography enhances the security and reliability of the message as the first message encrypts the data and using steganography we can hide the information into another career such as CSS file. It gives better security compared to individually applying cryptography and steganography methods.

REFERENCES

[1] Md. Khalid Imam Rahmani, Kamiya Arora, and Naina Pal proposed a paper on "A Crypto-Steganography: A Survey"
[2] Shristi Mishra and Prateeksha Pandey proposed a paper on, "A Review on Steganography Techniques using Cryptography"
[3] Hardikkumar V. Desai, Pacheri Beri, and Distt. Jahunjhunu Raj proposed a paper "Steganography, Cryptography, Watermarking: A Comparative Study"
[4] Herman Kabetta, B. Yudi Dwiandiyanta, and Suyoto proposed a paper, "Information Hiding In CSS: A Secure Scheme Text-Steganography using public-key Cryptosystem"
[5] Hayfaa Abdulzahra, Robiah Ahmad, And Norliza Mohd Noor, "Combining Cryptography and Steganography for Data Hiding in Images"
[6] Sultan Almuhammadi and Ahmed Al-Shaaby, "A SURVEY ON RECENT APPROACHES COMBINING CRYPTOGRAPHY AND STEGANOGRAPHY"
[7] Ajit Singh and Swati Malik proposed a paper, "Securing Data by Using Cryptography with Steganography"

