International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP90-96

INFORMATION SECURITY AND DATA HIDING

Ruchika Dahiya
M. Tech Scholar, Department of Computer Science, Gateway Institute of Engineering & Technology, India

Abstract:-Increase in the number of attack recorded during electronic exchange of information between the source and intended destination has indeed called for a more robust method for securing data transfer. Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. In this paper, information security and data hiding system that is based on steganography and cryptography is proposed to secure data transfer between the source and destination. A LSB (Least Significant Bit) method is the easiest way of hiding information in an image and yet it is effective. The proposed system was evaluated for effectiveness and the result shows that, the encryption and decryption methods used for developing the system make the security of the proposed system more efficient in securing data from unauthorized access. The system is therefore, recommended to be used by the Internet users for establishing a more secure communication.

Keywords: Information security ,

1. INTRODUCTION

Information Technology is the most essential aspect in today's world. Based on this fact computer application is still developing to handle securely the financial as well as the personal data more effectively. These data are extremely important from every aspect and we need to secure this from unauthorized access. Security is the process of preventing and detecting unauthorized use of data or computer or network. Prevention measures help us to stop unauthorized users from accessing any part of computer system. Detection helps to determine whether or not someone attempted to break into the system, if they were successful, and what they may have done. To achieve that security we may use various cryptography techniques. However, today data encryption is not everything or we cannot achieve strong security through this, we also need to secure the presence of date. Here comes the necessity of steganography.

1.1 What is Cryptography?

Cryptography is the study of hiding information and it is used when communicating over an untrusted medium such as internet, where information needs to be protected from other third parties. Modern cryptography focuses on developing cryptographic algorithms that are hard to break by an adversary due to the computational hardness therefore could not be broken by a practical means. In the modern cryptography, there are three types of cryptographic algorithms used called Symmetric key cryptography, Public-key cryptography and hash functions. Symmetric key cryptography involves encryption methods where both the sender and the receiver share the same key used to encrypt the data. In Public-key cryptography, two different but mathematically related keys are used. Hash functions does not use a key, instead they compute a fixed length hash value from the data. It is impossible to recover the length of the original plain text from this hash value.

Fig. 1 Cryptography

1.2 What is Steganography?

Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attention. Steganography was used even in ancient times and these ancient methods are called Physical Steganography. Some examples for these methods are messages hidden in messages body, messages written in secret inks, messages written on envelopes in areas covered by stamps, etc. Modern Steganography methods are called Digital Steganography. These modern methods include hiding messages within noisy images, embedding a message within random data, embedding pictures with the message within video files, etc. Furthermore, Network Steganography is used in telecommunication networks. This includes techniques like Steganophony (hiding a message in Voice-over-IP conversations) and WLAN Steganography (methods for transmitting Steganograms in Wireless Local Area Networks).

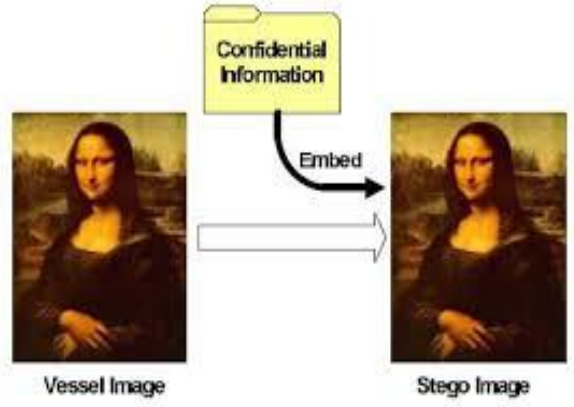

Fig. 2 Steganography

1.3 What is the difference between Cryptography and Steganography?

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. 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 the world. Due to this, Steganography removes the unwanted attention coming to the hidden message. Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better security.

II. TECHNIQUES FOR INFORMATION SECURITY

2.1 Private Key Cryptography or Symmetric Cryptography:

In private key cryptography, both the sender and receiver share the same private key. The key is used to encrypt the plaintext and also to decrypt the cipher text. The key must be kept private to ensure system security. A spy who obtains the key will likely be able to decrypt encoded messages. In the encryption schemes currently in use, keys are often either very large prime numbers or the product of large primes. A simple example, using a cipher that is not secure, should clarify the idea behind private key cryptography. Suppose Alice wants to send this message to Bob.“meet me at the roadhouse at noon urgent”For example, if Alice and Bob agree on a key of 5, the cipher text of Alice’s message will be“meehannearotutetounrttasogmhdeoe”When Bob receives the cipher text, he decrypts it using the private key, 5. First, Bob counts the number of characters in the cipher text, which in

this case is 32. Since there are 5 characters per row, based on the agreed-upon cipher and key, Bob realizes that the message is seven rows long—six full rows and onr row containing two characters. Bob writes out the message in row-formats as follows:

meetm
eatth
eroad
house
atnoo
nurge
nt

Writing the text horizontally row-by-row, Bob obtains meetm eatth eroad house atnoo nurge nt. Reading from left to right, Bob can determine the original message. If a spy knew the cipher and the private key, he or she could also decrypt the intercepted message. Few features of private key cryptography are:

- Traditional private/secret/single key cryptography uses one key Shared by both sender and receiver.
- Also is symmetric, parties are equal, Hence does not protect sender from receiver forging a message and claiming is sent by sender.

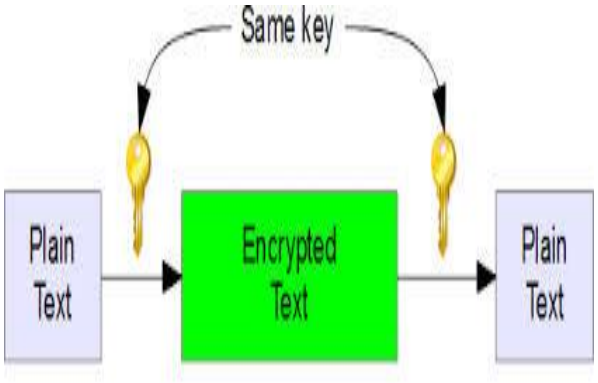

Fig.3. Private Key Cryptography

2.2 Public key Cryptography or Asymmetric Cryptography:

Another security issue is the problem of authentication. When Bob receives a message, how can he be sure that Alice sent it? That is, how can he be sure that the message is authentic? Private Key Cryptography allows two parties to exchange messages and maintain confidentiality but not authenticity. If the cipher text is intercepted, it will be difficult to decrypt without access to the private key and without knowing the encrypting cipher. Public Key Cryptography is useful for this purpose.In Public Key Cryptography one key is used to encrypt the plaintext and other key is used to decrypt the ciphertext. The important here is that it doesn't matter which key is applied first but that both keys are required for the process to work. Because a pair of keys is required, this approach is called Asymmetric Cryptography.Alice wants to sends the message to Bobs and she encrypted the message by using her private key. When Bob receives the ciphertext, he tries to decrypt it by using Alice public key which is available to everyone. If Bob can decrypt the message he know that it must come from the Alice, because Alice public key can only decrypt the message and encrypted by her private key and Alice know her private key.Notice that if Alice message had been intercepted, anyone could have decrypted it using her public key. Privacy is not provided by Public key cryptography only authentication.

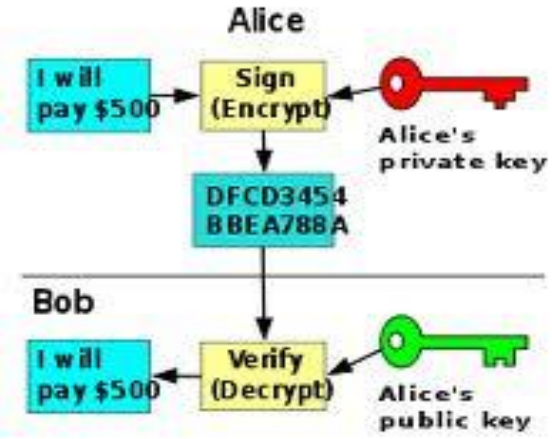

Fig. 4 Public Key Cryptography

III.METHOD FORINFORMATION HIDING

3.1 LSB (Least Significant Bit):

This method is the easiest way of hiding information in an image and yet it is effective. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. So in an image for example, the following steps would need to be taken

[1] First load up both the host image and the image you need to hide.
[2] Next choose the number of bits you wish to hide the secret image in. The more bits used in the host image, the more it deteriorates. Increasing the number of bits used though obviously has a beneficial reaction on the secret image increasing its clarity.
[3] Now you have to create a new image by combining the pixels from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM- one byte per pixel, JPEG- one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: **10110011**

[4] Get the original image back you just need to know how many bits were used to store the secret image. You then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change the bits extracted now become the most significant bit

Host Pixel: 10110011
Bits used: 4
New Image: **00110000**

Fig. 5 Least Significant Bit Method

This method works quite well when both the host and secret images are given equal numbers of bits. When one has significantly more room than another, quality is sacrificed. Notice that the same technique could be used to hide sound or text inside an image. All you need to do is change how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data; and of course, it is unlikely to survive lossy compression very well.

3.2 Encoding:

LSB method allows large amount of secret information to be encoded in an audio file. Audio file contains set of bytes which can be used for encoding. Some audio files may contain several bytes depending on their sizes. The following steps were used during the encoding stage:

- Encrypt the message using public key
- Convert the audio file into bit stream
- Convert each character in the message into bit stream
- Replace the LSB bit of the audio file with the LSB bit of character in the message to hide.

3.3 Decoding:

- In this stage, the encoded file is decoded to get the hidden message. The message is decoded first and then decrypted by the public key that is known only by the authorized receivers or users of the proposed system.

3.4 Encryption:

- During encryption, the user is allowed to enter a password/key in any combination of numbers, symbols and characters. The key contains set of characters, which are used to encrypt the message before encoding.

3.5 Decryption:

- The user's password/key is supplied to decrypt the encrypted message in order to get the original message. The processes of encryption and decryption are handled by DES (Data Encryption Standard) algorithm.

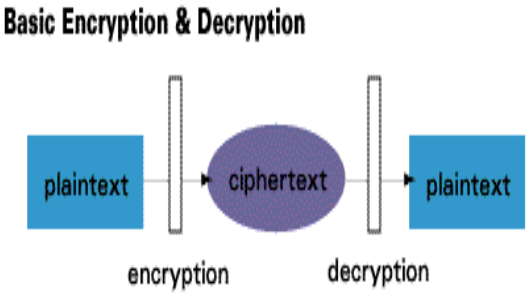

Fig. 6 Basic Encryption and Decryption

3.6 Use Case Diagram:
Use case diagram represents the functionality of the system from the user's point of view. In Unified Modeling Language, use case diagrams are used to show the functionality that the system will provide and to show which users will communicate with the system in some way to use that functionality [6].

IV. APPLICATIONS OF STEGANORAPHY

4.1 Secret Communications:
The use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

4.2 Feature Tagging:
Feature Tagging Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying thestego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

4.3 Copyright Protection:
Copy protection mechanisms that prevent data, usually digital data, from being copied. The insertion and analysis of water-marks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding.

V. CONCLUSION

In today's world, we often listen a popular term "Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem. In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down.

VI. REFERENCES

Journal Papers:
[1]Raphael, A.J., and Sundaran, Cryptography and Steganography-A Survey, *International Journal of Computer Technology Application, 2(3),* 2011, 626-630.
[2] Doshi, Ronak, Pratik Jain and Lalit Gupta, Steganography and Its Applications in Security, *International Journal of Modern Engineering Research, 2(6),* 2012, 4634-4638.

Books:

[3] Greenlaw, Raymond and Ellen Hepp, In-line/On-line: *Fundamental of the Internet and the world wide web*-2nd ed. (CA, USA, Mcgraw-Hill, 2001)

[4] Wayner, Peter, *Disappearing Cryptography: Being and Nothingness on the Net* (Boston, AP Professional, 1996)

Proceedings Papers:

[5] Johnson, Neil F., Zoran Duric and Sushil Jajodia, *Information hiding: Steganography and Watermarking- Attacks and Countermeasures* Volume 1 of Advance Information Security (Heidelberg, Germany, Springer Science and Business Media, 2001)

Theses:

[6] Jenita Kshetrimayum, *A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique,* National Institute of Technology, Rourkela, India, 2013.