iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review on Steganography & Cryptography Techniques

Vijay Prakash[1], Aakash Gupta[2]
[1,2]Department of Computer Science Gateway Institute of Engineering & Technology (GIET)
Deenbandhu Chhotu Ram University of Science & Technology (DCRUST), Sonepat

Abstract: ***There is a need for more secure methods for transferring data between source to destination due to increase in the number of attack recorded during electronic exchange 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.***

Keywords: Cryptography, Decryption, Encryption, LSB, Steganography

I. INTRODUCTION

In today's world Information Technology (IT) is the most important aspect. The computer applications are developing to handle securely the monetary as well as the personal data more effectively. These data are very necessary from every phase and we need to protect this from unauthorized access. The process of preventing and detecting unauthorized use of software or hardware is the task of security. We can use prevention measures to prevent unauthorized users from accessing any part of computer system. On the other hand detection helps to determine whether anyone try to break into the system. To attain that security we may use various cryptography methods. But today data encryption using cryptography is not sufficient instead we require more security using Steganography methods where secure data is not visible to anyone.

A. What is Cryptography?

It is the process of changing information which are need to be transferred on insure transmission medium (e.g., Internet) so that no one except sender or receiver can understand the meaning of information. The cryptographic technique uses various types of algorithms which are generally impossible for unauthorized users to break.

Cyptography can be divided into following three categories depending upon the types of key used: secret key (symmetric) cryptography, public key (asymmetric) cryptography and hash functions. With Symmetric key cryptography where both the sender and the receiver share the same key for encryption of data. With Public-key cryptography, two different keys are used for encryption and hash function computes hash value of fixed length from the given data for encryption. It is impossible to recover the length of the original plain text from this hash value.

B. 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).

Figure 2 below shows the Steganography image (right) after hiding secret data.

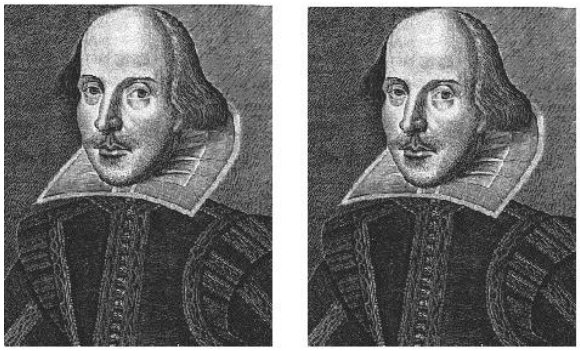


Fig. 2 Steganography

II. TECHNIQUES FOR INFORMATION SECURITY

A. *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.

Few features of private key cryptography are:

1) Traditional private/secret/single key cryptography uses one key
2) Shared by both sender and receiver
3) if this key is disclosed communications are compromised
4) Also is symmetric, parties are equal
5) Hence does not protect sender from receiver forging a message and claiming is sent by sender.

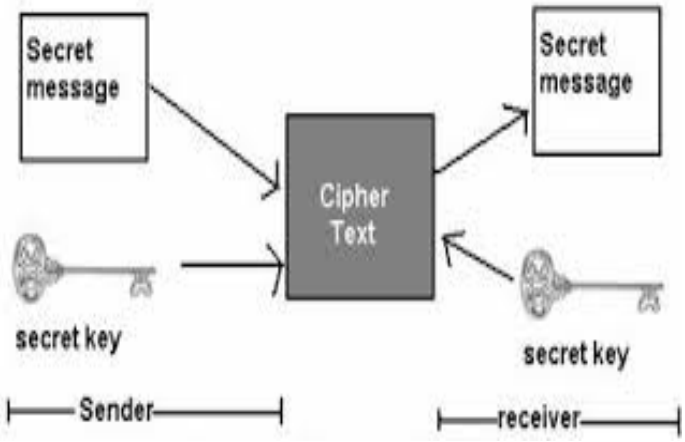


Fig.3. Private Key Cryptography

B. *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. 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.

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

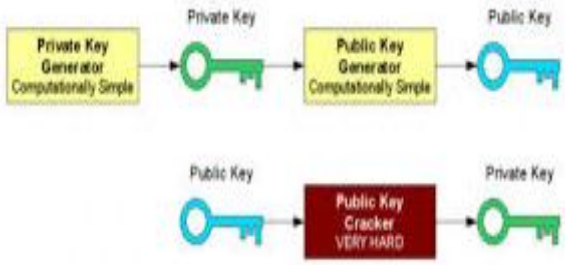


Fig.4 Public Key Cryptography

III. METHOD FOR INFORMATION HIDING

A. *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

First load up both the host image and the image you need to hide.

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.

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

Get the original image back you just need to know how many bits were used to store the secret image. 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

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.

B. *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:

1) Encrypt the message using public key
2) Convert the audio file into bit stream
3) Convert each character in the message into bit stream

C. *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.

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

D. 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.

E. 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.

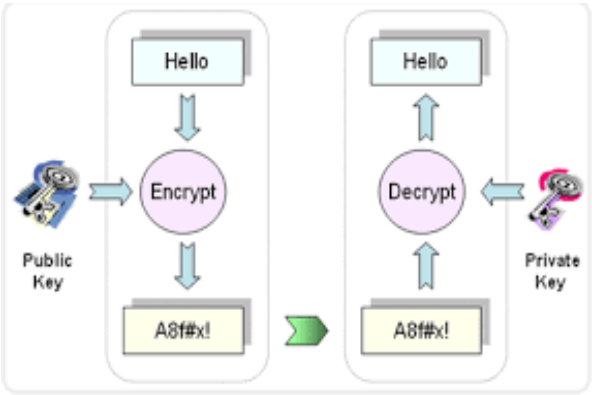


Fig. 5 Basic Encryption and Decryption

F. 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]. The use case diagrams for the encoding and decoding processes of the proposed system are shown below:

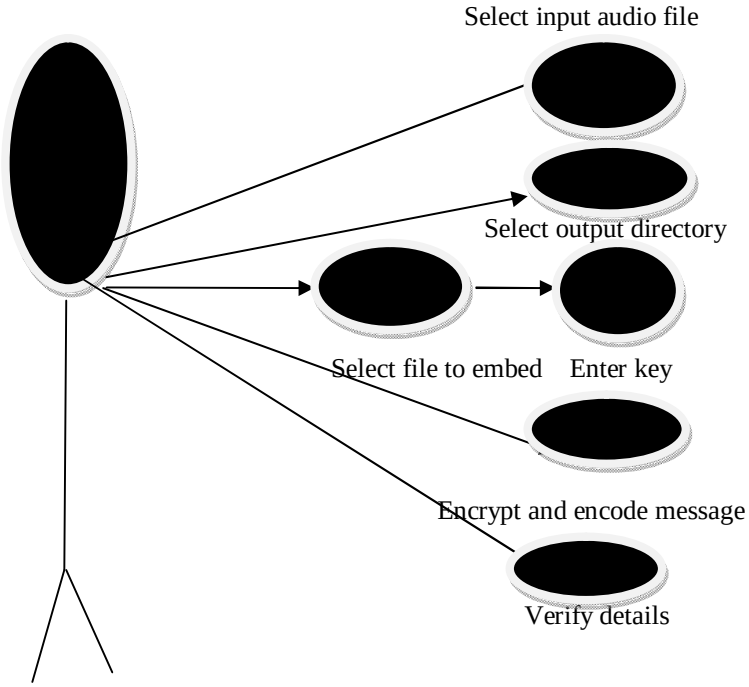


Fig. 6 Use case diagram for embedding/encoding

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

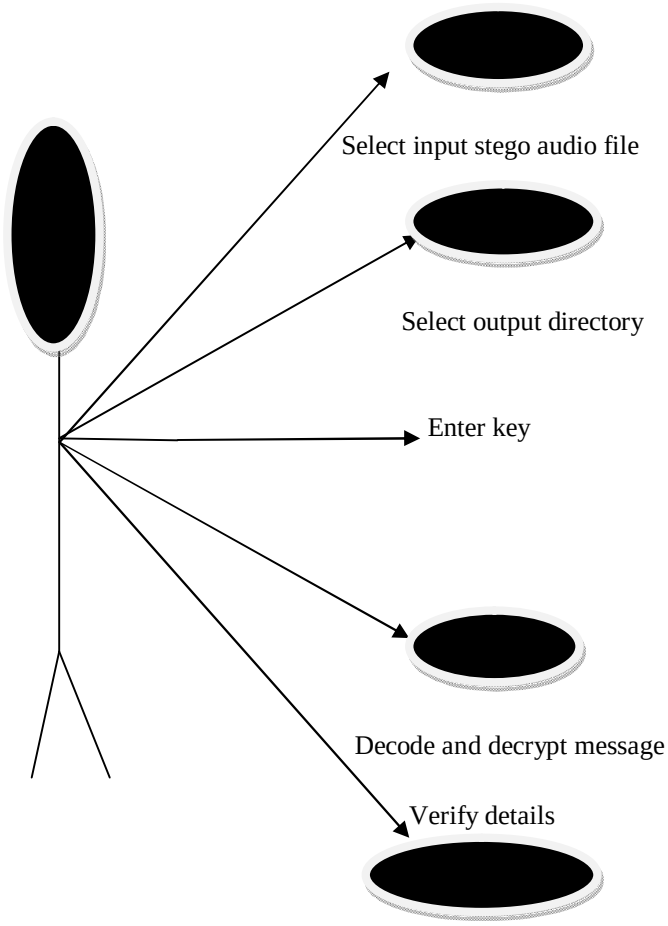


Fig. 7 Use case diagram for extraction/decoding

IV. 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.

REFERENCES

A. Journal Papers

[1] Raphael, A.J., and Sundaran, Cryptography and Steganography-A Survey, International Journal of Computer Technology Application, 2(3), 2011, 626-63

[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.

B. Books

[1] 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

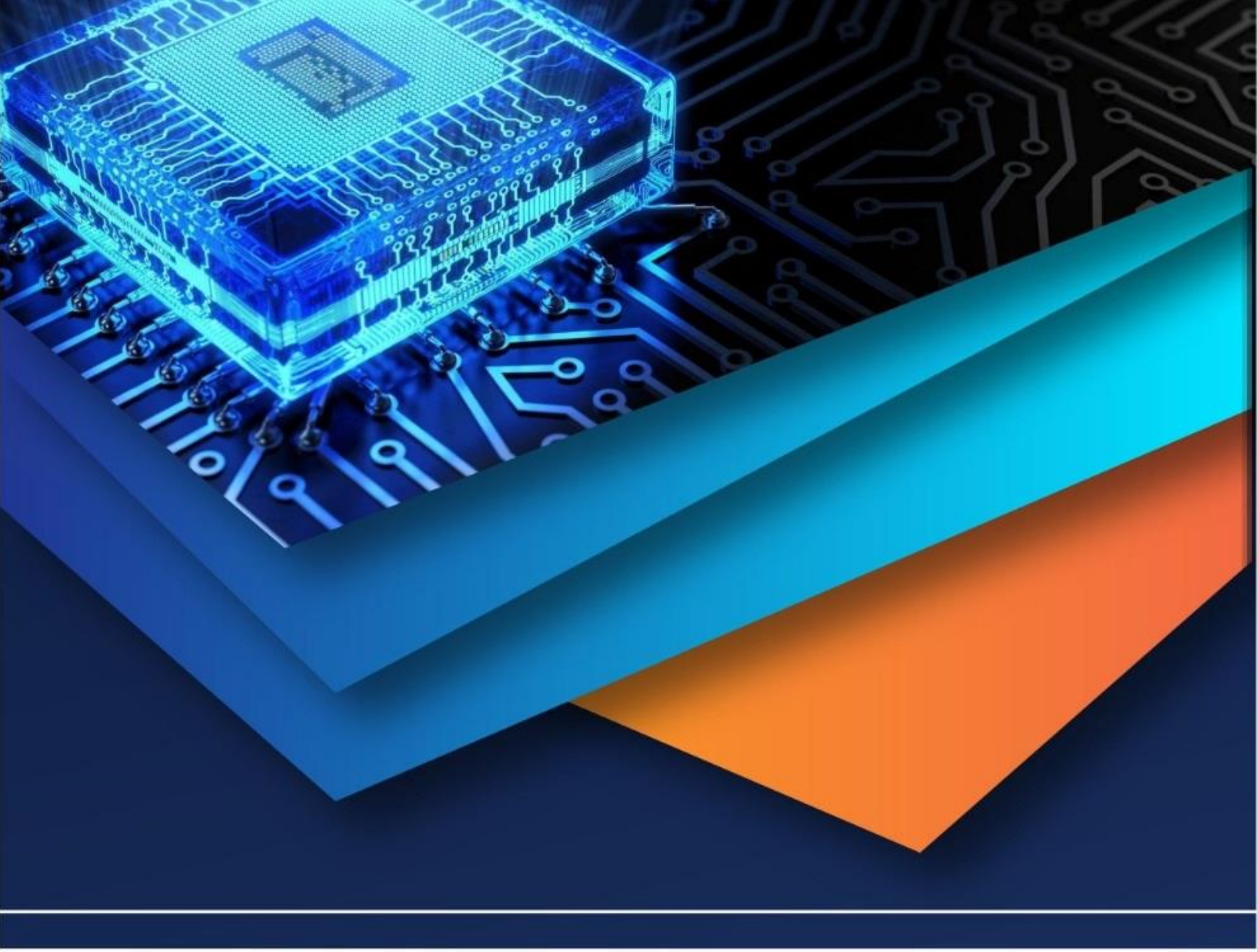
[2] Wayner, Peter, Disappearing Cryptography: Being and Nothingness on the Net (Boston, AP Professional, 1996)

C. Proceedings Papers

[1] 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)

D. Theses

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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY