ISSN: 2348 9510

International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 3, June 2015

Steganography and Encryption: A critical Review

Vaidehi verma
Computer science department
S D bansal college of engineering and technology
Indore, India
verma.vaidehi@yahoo.com

Trapti ozha
Computer science department
S D bansal college of engineering and technology
Indore, India
trapti_ozha@yahoo.com

Abstract

Steganography is a art of communicating by hiding a type of information in some other information. In the present era, more attention is given to the art of displaying and sending hidden information because of security purpose. Therefore, different methods have been proposed so far for hiding information in different cover media. In this review paper, we are highlighting the various study and research done before. Steganography's primary goal is to hide data within some other data such that the hidden data cannot be detected even if it is being sought. A lot of researchers have put a tremendous effort in this art but there is still lack of a place under one roof where all this information can be concentrated. This paper aims to fill that pit-hole. It also highlights the difference between the various techniques of steganography.

Keywords—*Steganography,cryptography,encryption,Aes,Des*

I. Introduction

Network security cab is divided into two branches- Cryptography and Steganography. Security has become one of the most important issues for distributing new information. It is necessary to protect this information while communicating through insecure channels. The word steganography has been derived from two Greek words namely "STEGANOS" meaning "Covered" and "GRAPHIE" meaning "Writing" [1]. The main goal of steganography is to hide information in the cover media so that trespassers don't notice the presence of the information. In other words, it is an art of writing hidden messages in such a way that no one except the intended recipient knows if a message for a long time, simple techniques of steganography have been used., But with the increasing use in an electronic format new techniques for information hiding have become achievable. Thus, there is a need for developing technology that will help protect the secrecy of digital content and secure the intellectual property rights of owners. Steganography is mainly of two types- FRAGILE and ROBUST Steganography[2].The former involves enclosing information into a file which is destroyed if the file is modified, while later aims to protect information into a file which cannot easily be destroyed.

Cryptography and Steganography are the two main techniques for secret communication. The contents of secret message are jumbled up in cryptography, the secret messages are jumbled up but in steganography, the messages are secured in a cover medium. In the model we are proposing, we are developing a combination of cryptographic and stegnographic security for a high level of security. Advanced Encryption is being used in cryptography. Advanced Encryption Standard (AES) algorithm to encrypt secret message and then Pixel Value Differencing (PVD) with K-bit Least-Significant-Bit (LSB) substitution is used to hide encrypted message into true color RGB image. The decoder should have secret key to decode the data.

The secret key is designed in such a manner that it can’t be found out by an unauthorized user [3].

A better difference between both the phenomenon’s is given by Jonathan et. Al. [4].According to them the main difference is that with encryption anybody can see that both parties are communicating in secret but Steganography hides the existence of any secret message and nobody can see that both parties are communicating in secret. This makes steganography suitable for some tasks for which encryption are not, like water marking. Adding encrypted copyright detail to a file could be easy to remove but embedding it within the contents of the file itself can prevent it from being easily identified and removed.

II. Basic Components of Steganography

Its basic components are:-

1) Cover object that is used to cover the original message image.
2) A next object that is the message or main image which is to be transmitted.
3) A stego-key which is used to hide the message image into cover cover image.
4) The steganography algorithm to carry out the required object.
Stegno-image is the output which is sent to the receiver where he retrieves the hidden message in the image by de-steganograohy methods. [5]

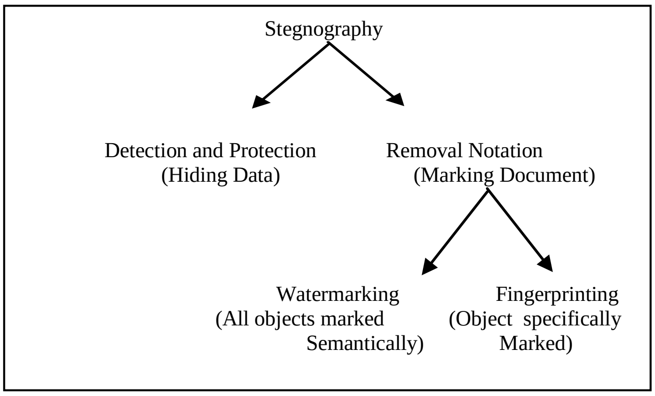
steganography is the process in which the information is concealed in any carrier like a text, an image, a voice , a video or any other medium. The most popular and commonly used one is image. Because of its frequency of use on the internet and good capacity of transmitting

data without affecting its quality adds to its popularity. This also makes it a very secure means of transmission. Some important issue that need to be considered when studying steganographyic systems: - robustness capacity and security. As we can see in Fig.2, the steganography triangle presents a relation the above issues. All of them work individually and for one to be successfully executed; one on the remaining two others have to sacrifice.
Robustness: - Message's ability to survive any attack- deliberate or random, by a third party or by noise during transmission phase. [6]

Capacity: - Maximum number of bits that can be capsulated in an image without the message being detected and everything intact.

Security: - It helps in capsuling the data in a way that it remains undiscovered.[7]

The figure given below shows the different elements of the steganography:


Stegnography
Detection and Protection (Hiding Data)
Removal Notation (Marking Document)
Watermarking (All objects marked Semantically)
Fingerprinting (Object specifically Marked)

Techniques Of Steganography:

In a wider sense, the word steganography can be divided into three major techniques. They are:

1) Injection: Injection is a simple method which involves injecting the secret information directly into the carrier file.
2) Substitution: In this, the least significant bits of information that determine the meaningful content of the original file are replaced with new data in a way that causes the least amount of distortion.
3) Generation: The generation technique requires only a hidden file, as it is used to create the hidden file.
A steganography must have the integrity of the hidden information after it has been embedded inside the stego object. Moreover, it also helps in making sure that the stego object must remain unchanged when seen by the naked eye. The techniques are implemented with an assumption that the attackers know that there is hidden information inside the stego object.

Text Steganography: This type of steganography can be achieved by changing the text formatting and/or by changing the particular characteristics of various textual elements [8]. The main aim in the design of coding methods is to develop changes that are de-codable, even in the presence of noise,yet largely closed to the reader.The file formats used are-PostScript2, TeX, @off, etc. The three main techniques used in text steganography- Line shift coding, feature coding and word shift coding. Chapman[9] describes one more technique as text steganography in which he proposed to use written natural languages to hide a secret message.

In Line shift coding,one can change the existing document by vertically shifting the locations of the text lines to encode the documents on the other hand in word shifting coding,one has to change the document by horizontally shifting the locations of words within text lines to encode the documents. In feature coding method,depending upon the codeword,the features of the image are altered.Before doing the alterations,the image is closely checked for the chosen features.This method is used to format file as well as to a bitmap image of a document. Steganography’s main advantage is that the alterations are not visible to the human eye.

Image Steganography: Images are the most common objects used for steganography. An image with a secret message inside can easily be distributed over the World Wide Web or in newsgroups. The various steps involved in this type of steganography is given in figure 3.

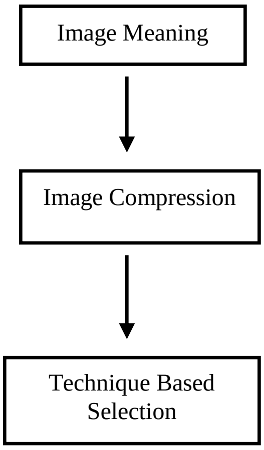


Image definition is the process in which a computer identifies the image in a numeric representation.Bit depth(number of bits used in a color scheme),refers to the bits used for each pixel.8 bits describe the color of each pixel. .Monochrome and gray scale images used 8 bits for each pixel but digital color images stored in 24 bit file.Color variations of a 24 bit image for the pixel are derived from three basic colors-red, greensand blue. The size of the file depends on the amount of colors. As the amount of colors increase. So will the size of the file .The larger amount of colors that can be displayed,the larger the file size.Image compression is defined as the techniques which make use of mathematical formulas to analyse and condense image data and reduce its file sizes.This is an important step before applying steganography methods since larger images of greater bit depth tends to become too large to transmit over a standard internet connection and displaying such image consume more time as compared to compressed image.As surveyed from past work on compression , there are mainly two types of compressions[10]:

a) **Lossy compression**: In this type of compression, minute details which cannot be differentiated by the human eye are remove and thus excess image data is discarded to create a smaller file.JPEG format of image makes use of this type of compression.

b) **Lossless compression**: This type of compression uses mathematical formulae to represent the data rather than removing any data from the image. This type of compression is used by the .gif files.The original image's integrity is maintained and the decompressed image's output is bit-by-bit identical to the original image [11].

Both type of compressions have their own limitations and advantages.Dunbar [12] elaborates in his paper that Lossy compression results in smaller file sizes but the possibility of losing embedded message due to removing to excess image data during compression.Unlike,Lossless compression retains the original digital image without the chance of losing, but does not compress the image to such a small file size. Different steganography techniques are used depending upon the method of compression.

Basic Terms Used in Cryptography

- **Plain Text**

The actual message without hiding any information is the plain text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, If aaditiya wants to send a message to ankit that "Hi Friend" then Here "Hi Friend " is a plain text message.

- **Cipher text**

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text[13]. In Cryptography the original message is transformed into non readable message before the transmission of actual message.

For example, "Aj)$%@abh&*%" is a Cipher Text produced for "Hi Friend ".

- **Encryption**

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel.

An encryption algorithm and a key are the basic needs of encryption. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side [13].

- **Decryption**

A opposite process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from cipher text. The process of decryption requires two things- a Decryption algorithm and a key. Generally the encryption and decryption algorithm are same, with the understood reverse concepts.

Various Methods of encryption

- **DES (Data Encryption Standard)**

The Data Encryption Standard is one of the first commercially developed ciphers. DES is the result of efforts done by IBM (International Business Machines) corporation, NBS (National Bureau of Standards) and NSA (National Security Agency). DES is a block cipher that encrypts 64-bit data blocks and encryption of the data is performed using a 56-bit secret key. DES consists of sixteen rounds and two permutation layers. DES uses a shared key both to encrypt and decrypt the message. The decryption process is the reverse of encryption process. DES possesses strong Avalanche effect and is flexible as it works in CBC, ECB, CFB and OFB modes. DES easily falls pray to Brute Force attack and relatively slow in software.

- **AES (Advanced Encryption Standard)**

The algorithm was invented by Joan Daemen and Vincent Rijmen. AES can process 128 bit data block and uses key lengths of 128, 192, or 256 bits. For the key length of 128,192 and 256 bits, AES may be referred to as AES-128, AES-192 and AES-256 respectively. Unlike DES, AES is not a fiestel structure. Number of rounds in AES depends on key length i.e. for a key length of 128, number of rounds is 10 and similarly for 192 and 256 bit keys, it is 12 and 14 respectively. AES provides resistance against all known attacks, simple in design and good speed of computation.

The problems of key distribution are solved by public key cryptography. Some examples of public-key cryptosystems are: Elgamal, RSA, Diffie-Hellman and DSA. [14]

- **DSA (Data Signature Algorithm)**

Data Signature Algorithm as an approved signature scheme was invented by David Kravitz. DSA is a variant of the ElGamal and Schnorr algorithms. Digital Signature Standard (DSS) used DSA proposed by National Institute of Standards and Technology (NIST) in 1991. Security of DSA is based on the difficulty to solve discrete logarithms. DSA has been accepted widely. DSA is more efficient and faster than RSA.

- **RSA (Rivest, Shamir and Adleman)**

A public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977. It widely used in electronic commerce protocols, and is believed that its security depends on the difficulty of decomposition of large numbers. RSA is secure because it is able to resist concerted attack.

- **Diffie-Hellman**

Whitfield Diffie and Martin Hellman discovered Diffie- Hellman (DH) algorithm in 1976 was the first public key algorithm ever invented. Diffie-Hellmanestablishes a shared secret key that can be used for secret communications by exchanging data over a public network. Diffie–Hellman algorithm does not need any known key before communication begins and Discrete Logarithm Problem makes it extremely difficult to crack. Diffie–Hellman algorithm easily falls prey to man-in-the-middle attack. [15]

III. Conclusion

Steganography is a broad area of research. Many present and future researchers choose their area of research as steganography due to an increase in demands of techniques of hiding data. This paper acts as a guide for all beginner researchers. This paper clearly shows an outline of all the techniques of steganography. However, this study also depends on the past study of research work done on steganography. One can find more detailed information on a particular technique as compared to the information available in this paper.At last an overview of the techniques and terms used in the encryption are given. The differentiation of the techniques has been done successfully so that according to the situation influencing the environment of steganography, the techniques are chosen.

References

- Moerland T.,“Steganography and Stegan alysis”,Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

- Shashikala Channalli,Ajay Jadhav,”Steganography:An art of hiding Data”,International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141

- Rakhi, Suresh Gawande,”A review of staganography".

- Jonathan Cummins, Patrick Diskin, Samuel Lau & Robert Parlett,”steganography-the art of hiding data ”.

- Nadeem Akhtar, Pragati Johri, Shahbaaz Khan Enhancing the Security and Quality of LSB based Image Steganography978-0-7695-5069-5/13 © 2013 IEEE

- Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena Security Improvisation in Image Steganography using DES 978-1-4673-4529-3/12/_c 2012 IEEE

- Md. Rashedul Islam1, Ayasha Siddiqa2, Md. Palash Uddin3, Ashis Kumar Mandal4 and Md. Delowar Hossain5 An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography 978-1-4799-5180-2/14/ ©2014 IEEE.

- Masoud Nosrati ,Ronak Karimi ,Mehdi Hariri,"An introduction to steganography methods",*World Applied Programming, Vol (1), No (3), August 2011. 191-195.*

- M.Chapman, G. Davida, and M. Rennhard, "A Practical and Effective Approach to Large-Scale Automated Linguisti Steganography ", proc eedings of the Information Security Conference, October 2001, pp

- Maninder Singh Rana, Bhupender Singh Sangwan, Jitendra Singh Jangir, " Art of Hiding: An Introduction to Steganography",International Journal Of Engineering And Computer Science ,Volume1 Issue 1 Oct 2012

- Moerland,T.,"Steganography and Steganalysis",*Leiden Institute of Advanced Computing Science*, www.liacs.nl/home/ tmoerl/privtech.pdf

- Dunbar B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January2002.

- E. ThambirajaG. RameshDr. R. Umarani A Survey on Various Most Common Encryption Techniques Volume 2, Issue 7, July 2012

- Veerpal Kaur, Aman Singh ,"Review of Various Algorithms Used in Hybrid Cryptography",IJCSN International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013 ISSN

- C. Cachin,"AnInformation-TheoreticModelfor Steganography", *Proceedings of 2nd Workshop on Information Hiding.*