RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ)
Research Paper
Available online at: www.rhimrj.com

A Survey Paper on Steganography and Cryptography

Z. V. Patel[1st]
Student, M.Tech.
C. U. Shah College of Engineering and Technology,
Surendranagar, Gujarat (India)

S. A. Gadhiya[2nd]
Head, B.E.(IT)
C. U. Shah College of Engineering and Technology,
Surendranagar, Gujarat (India)

Abstract: ***Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. The digital images are the most popular because of their frequency on the Web among all different carrier file formats. Image steganography, achieves the secrecy by embedding data into cover image and generating a stego-image. There are many types of steganography techniques each have their advantages and disadvantages. This paper intends to give an overview of image steganography, cryptography, its uses and techniques. It also attempts to identify and briefly reflects on which steganographic techniques are more suitable for which applications.***

Keywords: Steganography, Communication, Information, Secrecy, Techniques.

I. INTRODUCTION

Steganography is a Greek word which means concealed writing. The word “steganos” means “covered “ and “graphical “ means “writing” . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today’s most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data [3].

II. STEGANOGRAPHY CONCEPTS

Although steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner’s problem proposed by Simmons [5], where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication [6].

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A passive warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An active warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information [4].

III. CRYPTOGRAPHY CONCEPTS

Cryptography is an important element of any strategy to address message transmission security requirements. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'. The message may be converted using a 'code' (in which case each character or group of characters is substituted by an alternative one), or a 'cypher' or 'cipher' (in which case the message as a whole is converted, rather than individual characters).Cryptology is the science underlying cryptography. Cryptanalysis is the science of 'breaking' or 'cracking' encryption schemes, i.e. discovering the decryption key. Cryptographic systems are generically classified along three independent dimensions [7].

1. Methodology for transforming plain text to cipher text.

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.

2. Methodology for number of keys used.

There are some standards methods [8] which are used with cryptography such as secret key, public key, digital signature and hash function.

  ISSN: 2349-7637 (Online)

Secret Key (Symmetric): With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called as symmetric encryption.

Public Key: Public key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern Public Key Cryptography was first described publicly by Standford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their study describe a two-key crypto system in which two parties could engage in a secure communication over a insecure communications channel without having to share a secret key.

Digital Signature: The use of digital signature came from the need of ensuring the authentication. The digital signature is more like stamp or signature of the sender which is embedded together with the data and encrypts it with the private key in order to send it to the other party. In addition, the signature assures that any change made to the data that has been signed is easy to detect by the receiver.

Hash Function: The hash function is a one way encryption, the hash function is a well defined procedure or mathematical formula that represents a small size of bits which is generated from a large sized file, the result of this function can be called hash code or hashes. The generating of hash code is faster than other methods which make it more desired for authentication and integrity. Cryptographic hash functions are much used for digital signature and cheap constructions are highly desirable. The use of cryptographic hash functions for message authentication has become a standard approach in many applications, particularly internet security protocols. The authentication and the integrity considered as main issues in information security, the hash code can be attached to the original file then at any time the users are able to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code, if it's similar that is mean the message came from the original sender without altering because if there is any changed has been made to the data will changed the hash code at the receiver side.

3. Methodology for processing plain text.

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher.

IV. TYPES OF STEGANOGRAPHY

1. Text Steganography:

There are numerous methods by which to accomplish text based Steganography. I will introduce a few of the more popular encoding methods below.

Line-shift encoding involves actually shifting each line of text vertically up or down by as little as 3 centimeters. Depending on whether the line was up or down from the stationary line would equate to a value that would or could be encoded into a secret message.

Word-shift encoding works in much the same way that line-shift encoding works; only we use the horizontal spaces between words to equat e a value for the hidden message. This method of encoding is less visible than line-shift encoding but requires that the text format support variable spacing.

Feature specific encoding involves encoding secret messages into formatted text by changing certain text attributes such as vertical/horizontal length of letters such as b, d, T, etc. This is by far the hardest text encoding method to intercept as each type of formatted text has a large amount of features that can be used for encoding the secret message.

2. Image Steganography:

Hiding the data by taking the cover object as image is referred as image steganography. In image steganography pixel intensities are used to hide the data. In digital steganography, images are widely used cover source because there are number of bits presents in digital representation of an image.

Coding secret messages in digital images is by far the most widely used of all methods in the digital world of today? This is because it can take advantage of the limited power of the human visual system (HVS). Almost any plaintext, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image. With the continued growth of strong graphics power in computers and the research being put into image based Steganography, this field will continue to grow at a very rapid pace.

3. Audio Steganography:

It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files. There are different methods of audio steganography. These methods are i) Low Bit Encoding ii) Phase Coding iii) Spread Spectrum.

ISSN: 2349-7637 (Online)

Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. To put this in perspective, the (HAS) perceives over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected.

4. Video Steganography:

It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video, which is unnoticeable by the human eye. H.264, Mp4, MPEG, AVI are the formats used by video steganography.

5. Network or Protocol Steganography:

It involves hiding the information by taking the network protocol such as TCP, UDP, ICMP, IP etc, as cover object. . In the OSI layer network model there exist covert channels where steganography can be used.

V. STEGANOGRAPHY TECHNIQUES

1. Spatial Domain Methods:

In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly during hiding data. Spatial domain techniques are classified into following categories: i)Least significant bit (LSB) ii) Pixel value differencing (PVD) iii) Edges based data embedding method (EBE) iv) Random pixel embedding method (RPE) v)Mapping pixel to hidden data method vi) Labelling or connectivity method vii) Pixel intensity based.

i. **LSB:** this method is most commonly used for hiding data. In this method the embedding is done by replacing the least significant bits of image pixels with the bits of secret data. The image obtained after embedding is almost similar to original image because the change in the LSB of image pixel does not bring too much differences in the image.

ii. **BPCP:** In this segmentation of image are used by measuring its complexity. Complexity is used to determine the noisy block. In this method noisy blocks of bit plan are replaced by the binary patterns mapped from a secret data

iii. **PVD:** In this method, two consecutive pixels are selected for embedding the data. Payload is determined by checking the difference between two consecutive pixels and it serves as basis for identifying whether the two pixels belongs to an edge area or smooth area.

2. Spread Spectrum Technique:

The concept of spread spectrum is used in this technique. In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it become difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data. Thus it is difficult to remove the data completely without entirely destroying the cover .It is a very robust technique mostly used in military communication.

3. Statistical Technique:

In the technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.

4. Transform Domain Technique:

In this technique; the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT) iv) Lossless or reversible method (DCT) iv)Embedding in coefficient bits

5. Distortion Techniques:

In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.

6. Masking and Filtering:

These techniques hide information by marking an image. Steganography only hides the information where as watermarks becomes a potion of the image. These techniques embed the information in the more significant areas rather than hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image. This method is basically used for 24-bit and grey scale images.

ISSN: 2349-7637 (Online)

VI. APPLICATION OF STEGANOGRAPHY

1. Confidential Communication and Secret Data Storing
2. Protection of Data Alteration
3. Access Control System for Digital Content Distribution
4. E-Commerce
5. Media
6. Database Systems
7. Digital watermarking.

VII. COMBINED CRYPTO-STEGANOGRAPHY

Steganography is not the same as cryptography Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 2.

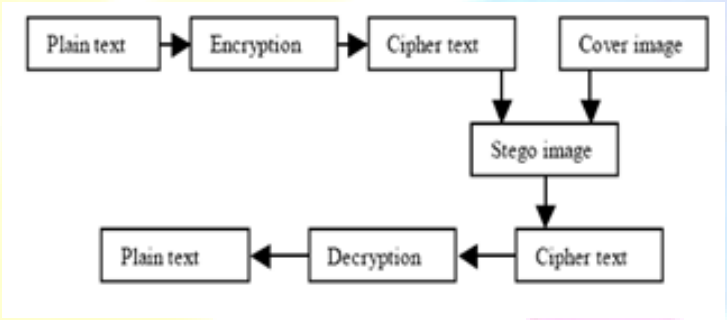

Figure-2

In figure 2, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Since then, the steganography approaches can be divided into three types [8]:

1. **Pure Steganography:** This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

2. **Secret Key steganography:** The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

3. **Public Key Steganography:** The last type of steganography is to combine 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.

ISSN: 2349-7637 (Online)

REFERENCES

1. A.Joseph Raphael,Dr.V Sundaram, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630
2. I. Venkata Sai Manoj, "Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12
3. Jasleen Kour , Deepankar Verma , International Journal of Emerging Research in Management & Technology ISSN: 2278-9359 (Volume-3, Issue- 5)
4. Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998
5. Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983
6. Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003
7. Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, " An Encrypto-Stego Technique Based secure data Transmission System", PEC, Chandigarh.
8. B B Zaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010
9. Kallam Ravindra Babu, Dr. S.Udaya Kumar, Dr. A.Vinaya Babu, "A Survey on Cryptography and Steganography Methods for Information Security", Internaltional Journal of Computer Applications(0975-8887), Volume 12 – No. 2, November 2010.
10. DiptiKapoorSarmah,Nehabajpai,"ProposedSystem for Data hiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.
11. 11] Nitin Kanzariya,Ashish Nimavat,Hardik Patel, "Security of digital images using steganography techniques based on LSB, DCT and Huffman encoding" ELSEVIER 2013
12. 12] Kanzariya Nitin K,Rathod Kirit R, Ranpura Avalik K, Jadeja Vijaysinh K,Nimavat Ashish V.
13. "A Novel Technique for Image Steganography]Techniques Based on LSB and DCT Coefficients" IJSRD - International Journal for Scientific Research & Development| Vol. 1, Issue 11, 2014 | ISSN (online): 2321-0613

ISSN: 2349-7637 (Online)