ISSN:2229-6093

Cryptography and Steganography – A Survey

A. Joseph Raphael
Research Scholar
Karpagam University
Coimbatore, India.

Dr. V. Sundaram, Head & Director
Department of Computer Applications
Karpagam College of Engineering
Coimbatore, India.

Abstract— *Digital communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and it is important that communication be made secret. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. This has resulted in an unstable growth in the field of information hiding. Cryptography and steganography are the two popular methods available to provide security. One hides the existence of the message and the other distorts the message itself. Using cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted. In steganography, the data is embedded in an image file and the image file is transmitted. This paper focuses on the strength of combining cryptography and stegnography methods to enhance the security of communication over an open channel.*

Index Terms—Stegano object, cryptanalysis, cipher text

I INTRODUCTION

Cryptography and Steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed, steganography can circumvent such policies to pass message covertly. However, steganography and cryptography differ in the way they are evaluated: steganography fails when the ”enemy” is able to access the content of the cipher message, while cryptography fails when the ”enemy” detects that there is a secret message present in the steganographic medium.

The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called *cryptanalysis* and *steganalysis*. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages. The aim of this paper is to describe a method for integrating together cryptography and steganography through some media such as image, audio, video, etc.

II HISTORY

Cryptography has followed man through many stages of evolution [3]. Cryptography can be found as far back as 1900 B.C. in ancient Egyptian scribe using non-standard hieroglyphics in an inscription. From 500 – 600 B.C. Hebrew scribes used ATBASH, a reversed alphabet simple solution cipher. From 50 - 60 B.C. Julius Caesar used a simple substitution with the normal alphabet in government communications. Cryptography continued through history with may variations. Today cryptography has reached a new level, quantum cryptography. Quantum cryptography combines physics and cryptography to produce a new cryptosystem that cannot be defeated without the sender and receiver having the knowledge of the attempted and failed intrusion. Through the long history of cryptography, steganography was developed and flourished on its own.

Steganography comes from the Greek steganos (covered or secret) and -graphy (writing or drawing). Steganography can be defined as the hiding of information by embedding messages within other, seemingly harmless messages, graphics or sounds. The first steganographic technique was developed in ancient Greece around 440 B.C. The Greek ruler Histaeus employed an early version of steganography which involved: shaving the head of a slave, tattooing the message on the slaves scalp, waiting for the growth of hair to disclose the secret message, and sending the slave on his way to deliver the message. The recipient would have the slave's head to uncover the message. The recipient would reply in the same form of steganography. In the same time period, another early form of steganography was employed. This method involved Demerstus, who wrote a message to the Spartans warning of eminent invasions from Xerxes. The message was carved on the wood of wax tablet, and then covered with a fresh layer of wax. This seemingly blank tablet was delivered with its hidden message successfully. Steganography continued development in the early 1600s as Sir Francis Bacon used a variation in type face to carry each bit of the encoding.

The microdots were complete documents, pictures, and plans reduced in size to the size of a period and attached to common paperwork. Null ciphers were also used to pass secret messages. Null ciphers are unencrypted messages with real messages embedded in the current text. Hidden messages were hard to interpret within the innocent messages. An example of an innocent message containing a null cipher is:

Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming any day.

By taking the third letter in each word the following message emerges:

Send Lawyers, Guns, and Money.

III DEFINITION & TERMINOLOGY

Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker.

Cryptanalysis [2] is the reverse engineering of cryptography—attempts to identify weaknesses of various cryptographic algorithms and their implementations to exploit them. Any attempt at cryptanalysis is defined as an attack.

Cryptology encompasses both cryptography and cryptanalysis and looks at mathematical problems that underlie them.

Cryptosystems are computer systems used to encrypt data for secure transmission and storage.

Plaintext is message or data which are in their normal, readable (not crypted) form.

Encryption: Encoding the contents of the message in such a way that hides its contents from outsiders.

Cipher text results from plaintext by applying the encryption key.

Decryption: The process of retrieving the plaintext back from the cipher text.

Key: Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key.

Steganography is the method of hiding secret messages in an ordinary document.

Steganalysis could be simply defined as the detection of steganography by a third party.

Hash functions generate a digest of the message.

Substitution cipher involves replacing an alphabet with another character of the same alphabet set.

Mono-alphabetic system uses a single alphabetic set for substitutions.

Poly-alphabetic system uses multiple alphabetic sets for substitutions.

Caesar cipher is a mono-alphabetic system in which each character is replaced by the third character in succession. Julius Caesar used this method of encryption.

A digital signature is a block of data that is generated by the sender of a message using his/her secret key.

IV CRYPTOGRAPHY

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 [1].

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[4] which is used with cryptography such as secret key, public key, digital signature and hash function.

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 described 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.

V STEGANOGRAPHY

The word steganography comes from the Greek Steganos, which mean covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. The main goal or steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [4]. During the process, characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Digital images, videos, sound files, and other computer files that contain perceptually irrelevant or redundant information can be used as “covers” or carriers to hide secret messages. After embedding a secret message into the cover-image, a so-called stegoimage is obtained. The basic model of steganography consists of Carrier, Message, Embedding algorithm and Stego key. The model for steganography is shown in Figure 1. Carrier is also known as a cover-object, which embeds the message and serves to hide its presence.

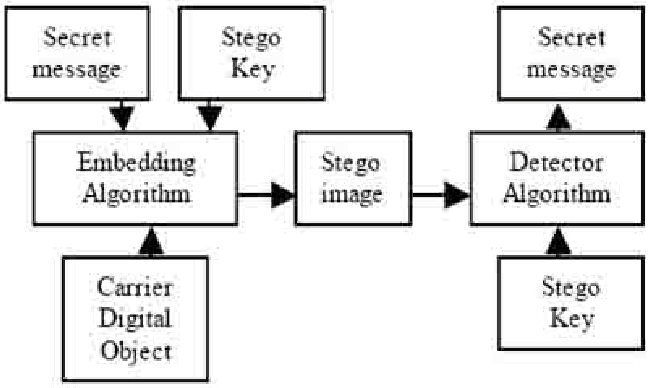
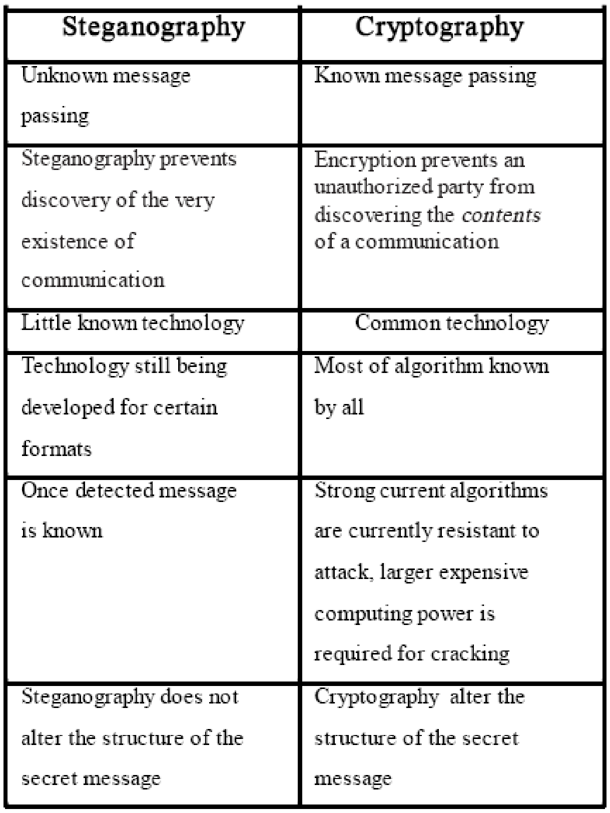


Fig. 1. A model of Steganography

Capacity, security and robustness are three different aspects affecting steganography and its usefulness. Capacity refers to the amount of information that can be hidden in the cover medium. Security relates to an eavesdropper's inability to detect hidden information and robustness is the amount of modification the stego medium can withstand before an adversary can destroy the hidden information.

VI STEGANOGRAPHY VS CRYPTOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. According to dictionary.com: Steganography is:” Hiding a secret message within a larger one in such a way that others can not discern the presence or contents of the hidden message” and Cryptography is “The process or skill of communicating in, or deciphering secret writing or ciphers.” Steganography can be used to cloak hidden messages in image, audio and even text files. It has until recently been the poor cousin of cryptography. Now, it is gaining new popularity with the current industry demands for digital watermarking and fingerprinting of audio and video. Steganography must not be confused with cryptography, where we transform the message so as to make its meaning obscure to malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated. The distinction between cryptography and steganography is an important one, and is summarized by the following table.



Steganography	Cryptography
Unknown message passing	Known message passing
Steganography prevents discovery of the very existence of communication	Encryption prevents an unauthorized party from discovering the *contents* of a communication
Little known technology	Common technology
Technology still being developed for certain formats	Most of algorithm known by all
Once detected message is known	Strong current algorithms are currently resistant to attack, larger expensive computing power is required for cracking
Steganography does not alter the structure of the secret message	Cryptography alter the structure of the secret message

Table 1: Comparison

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.

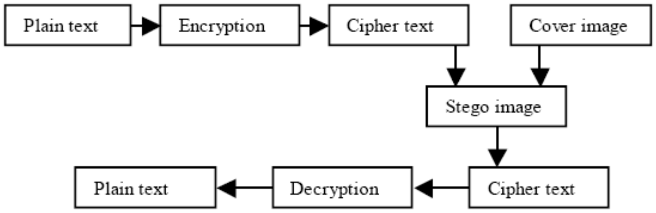


Fig. 2: Combination of steganograophy and cryptography

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 [4]:

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

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.

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.

References

[1] Neha Sharma, J.S. Bhatia and Dr. Neena Gupta, “ An Encrypto-Stego Technique Based secure data Transmission System”, PEC, Chandigarh.

[2] I. Venkata Sai Manoj, “Cryptography and Steganography”, International Journal of Computer Applications (0975 – 8887), Volume 1 – No.12

[3] Alan Siper, Roger Farley and Craig Lombardo, “The Rise of Steganography”, Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 6th, 2005.

[4] 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

[5] Domenico Bloisi and Luca Iocchi, “Image Based Steganography and Cryptography”, Sapienza University of Rome, Italy.

[6] 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.

[7] Dipti Kapoor Sarmah, Neha bajpai, “ Proposed System for Data Hhiding Using Cryptography and Steganography”, International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.

[8] Eiji Kawaguchi and Richard O. Eason, “Principle and applications of BPCS-Steganography”, Kyushu Institute of Technology, Kitakyushu, Japan, University of Maine, Orono, Maine 04469-5708.

[9]Sashikala Channalli and Ajay Jadhav, “Steganography An Art of Hiding Data”, International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.