A Survey on Information Security

Smitha.G.L\textsuperscript{1}, Dr. E.Baburaj\textsuperscript{2}
Research Scholar\textsuperscript{1}, Professor\textsuperscript{2}
Dept of CSE\textsuperscript{1,2}
Sathyabama University, Chennai, India\textsuperscript{1}
Narayanganur College of Engineering, Manjalumoodu, India\textsuperscript{2}

Abstract:
This paper presents two techniques that deals with information security: steganography and cryptography. Brief overview of terminology, history, features and limitation of both techniques are presented. Many individuals get confused between steganography and cryptography. Therefore, a comparison between both techniques is shown at the end of this paper.

Keywords: Steganography, Information Hiding, Cryptography, Encryption.

I. Introduction
Nowadays individuals exchange information straightforwardly using the existing communication technologies such as a local area network, a wide area network or simply the Internet. This information can be very sensitive and need to be protected against any intruder who can intercept them during the communication phase. Therefore, transferring sensible information cannot be solely relied on the existing communication technologies channels. We need then a robust technique to protect the information and ensure that they cannot be detected by other parties.

Cryptography is used to encrypt information based on some mathematical formulas. It is widely used to protect information exchanged over the Internet. World Wide Web (WWW) and e-mail are both public channels for transferring information. However, both technologies are vulnerable to attacks [3] and exchanged information can be detected relatively easily. In cryptography the secret information is modified using some public and private keys and become unreadable (e.g., encryption). They are then sent over the public channels to the destination where the original information would be retrieved using the corresponding keys (e.g., decryption). This technique does not prevent against hacker’s attacks that can intercept the decrypted information and apply their own techniques to retrieve the secret information. Therefore, it is necessary to find another methodology to protect the information exchanged safely over public channels without raising suspicions. This methodology is known as steganography and has become very popular in the last decade [4]. Steganography is the art of concealing sensible information into digital media (i.e., images, audio, text). It is a mechanism that completely differs from cryptography. In fact, in cryptography the information is modified but still can be seen in this unreadable format once sent over the networks, whereas in steganography the information is simply embedded into a digital support and cannot be noticed as long as the quality of the carrier is not deteriorated [5]. The steganography technique has been used many years ago to convey secret messages. For instance, a king in ancient Greece used to shave the slave’s head and tattooed some secret information on it. When the hair was grown, the slave was sent to distribute the message. The receiver then shaved the hair and get the secret message [6]. In modern life, steganography is employed for many purposes such as embedding copyright [6], embedding individual’s detail in smart IDs and inserting patient detail in medical imaging system. There has been a rapid growth of interest on steganography particularly with intelligent service institutions. For instance the US Pentagon has recently allocated significant funds to conduct research in this area, as they believe that terrorists may use this methodology to exchange information [6]. Steganography hides information into a digital media called cover object which can be a video clip, a digital image, an audio file or simply a text. This digital media is called respectively a cover image, a cover audio, a cover video, and a cover text. Once the information is embedded in that cover it is called a stego-object. If the cover is an image or an audio file, then the result of embedding the information in the cover is referred to as stego-image or stego-audio respectively. It is shown that images are excellent carriers to hide and exchange sensible information over networks [7]. Many algorithms have been proposed recently to hide information into images and preserve their quality. In this Master thesis we focus on image steganography algorithms. An image consists of light lumiance or pixels represented as an array of values at different points. A pixel consists of one byte or more. For example in 8-bit images each pixel consists of 1 byte (i.e., 8 bits). While each pixel in a 24-bit image is represented as three bytes representing the Red, Green and Blue (RGB) colors [6]. Any variation of the bits can lead to a different color. In a good steganography algorithm, there are five vital features that should be considered [8]. The first one is the capacity payload which refers to the amount of secret information that a stego-cover can carry before the distortions become noticeable. The second feature is the undetectability which means that the existence of the secret information should be undetectable whenever the stego-object is detected and analyzed. Other features that should be considered are: invisibility, security and robustness [7].

II. Information Hiding
Recently with the rapid use of information in modern technology, information hiding methods received much attention from the research community in information security. We give the main terminologies used in information hiding and we detail some applications.

a) Terminology
Information hiding refers to embedding secret message into a digital medium. The secret message can be a simple text [4],
an image [4], an audio [8] or any object that can be presented by some number of bits. In this thesis, secret data is referred to as secret message, secret information or confidential information and will be used interchangeably. It is desired to embed the secret message in an unsuspected object. This object can come in several formats such as image, audio, video, file or any other types that can carry information without destroying it. It is then referred to as cover image, cover audio, and cover video respectively. Once the secret message is embedded in the cover object it is called stego-object. After the stego-object is sent, the receiver should extract the message from the stego-object. Both the sender and receiver can agree on stego-key that is used at the extraction phase. The stego-key is used to control the hidden message from being recovered by eavesdropping. In addition, the receiver extracts the message based on the stego-key since it defines how the secret message is embedded [10].

Steganography, watermarking and covert channel are all fields related to information hiding. Figure 1 shows the categorization of information hiding techniques detailed in [11]. Each field differs from the other based on purpose and the desired character.

Figure 1 Categorization of Information Hiding Techniques

For instance, steganography is about making the sent messages between two parties in such a way the presence of embedded data of stego-object is not detectable. It is vital that the embedded message is secure against attacker. Also capacity is another factor and requirement for Steganography. Whereas, watermarking involves embedding copyright and intellectual property into cover object to protect the copyright. In this case high capacity is not a real concern while robustness is an important requirement. It should be designed in such a way that it is hard to remove the copyright mark. Watermarking systems can make the copyright marks visible (i.e., perceptible) [12] or invisible (i.e., imperceptible) [13] to human perception. Moreover, Covert communication and Anonymity are two techniques for hiding information. Covert communication purpose is to hide the presence of communication between two parties or beyond [14] so it becomes unknown to attackers. Anonymity involves hiding the identity of users who surf the web secretly from others [15].

b) Applications

Information hidings are exploited in many domains as follows:

• Copyright Protection, Single Ownership and Joint Ownership [16] are applications to advocate intellectual property based on watermark techniques.
• In E-commerce, registration information can be hidden in electronic papers that can be used to identify authentication [17] based on steganographic techniques.
• In medicine, doctors can embed some information such as name, comments or diagnoses of the patient into their medical imagery and exams. The medical images can be of different types such as embedding information into ECG images [18].
• In military, not only the content of communication but also the communication itself between agencies must be kept secret. Information hiding technique can be used when two or more agencies communicate thorough Digital Short Radio [19].
• In remote sensing, information can be hidden into some site images to provide secret only to authorized users [20].

III. Steganography

Steganography is a field in the domain of information hiding. The numbers of research works in this area have increased. With the boost of the Internet technology, steganography becomes a trend for exchanging information. Steganography is not a new discovery. It existed many years ago. This section gives a brief background about steganography.

a) Terminology

Steganography is a word of Greek origin. The word Steganos means covered and Gaptos means writing [7]. It’s conducted in a way that the existence of secret communication between two parties or more are hidden to snoopers. The secret messages can be hidden in less suspicious digital objects that are not detectable by human perceptibility. Then the person who possesses the stego-key can only extract the message from the stego-object at the target destination.

An illustration of the steganography process to embed and extract a message is presented in Figure 2.2. This example uses an image as the cover object to carry bits of the secret message. At the sender’s side, the secret message is embedded into the cover image by using some embedding function and the stego-image can be parameterized by a stego-key. Then the stego-image is sent over a communication channel to the receiver. The communication channel can be any type of transmission technologies that exist such as the Internet or E-mail. Then at the receiver’s side the secret message is extracted using the extracting function. In addition, the extracting function uses the shared stego-key if it was used in the embedding phase.

Figure 2 Steganography Process

a) History

Figure 1 displays that steganography is divided into two categories, which are linguistics and technical. Linguistics techniques refer to the use of digital object to hide data. For example linguistics technique involves changing redundant bits of pixels of an image. On the other hand, technical steganography engages physical ways such as using inks or microdots [11]. Steganography techniques are not new innovations but it goes back to antiquity. This section presents some methods used technical steganography in the history.

Steganography as stated previously is widely used by militaries and political leaders to communicate secretly. In the Histories [21], Herodotus narrates that at Susa, a city in Persia, Xerxes wanted to fight his army against Greece. The Greek Demaratus discovered the intention of Xerxes and warned the Greek king by the following technique. He removed the wax out of a tablet and wrote message about Xerxes pending invasion on it. Then he covered the message with a wax again and sent it to Sparta [4], [5]. Moreover, Harpagus wanted to initiate a revolt against the king of Persia. Persians guarded the roads; he had to send his messages secretly to his supporter Cyrus. He sent secret message by placing the message into belly of a hare. Then, the
harem was sent to Cyrus by one of his slave acting as hunter [21].

Microdot is another technique for steganography used by Germans during World War II. The Nazis took photograph of typed or written secret texts. After that, the photos were reduced to the size of dots. When the microdots were detected by Americans, Federal Bureau of Investigation (FBI) director Edgar Hoover referred to this technique as “the enemy’s masterpiece of espionage” [23].

Another procedure was used earlier by hiding each letters of the secret message as the first letter of each sequential word in the sentences of a covert text. Alternatively, each letter of the secret message is placed in the first letter of consecutive chapters of a book [23].

b) Features

The five features of steganography recognized in [8] are: undetectability, invisibility, security, capacity and robustness. The following paragraphs will explain each type of the properties that characterize steganography.

It is critical in any steganography system to provide undetectability feature [8]. The existence of the secret message in the stego-object should not be revealed by steganography systems that detect the presence of secret information. The steganography systems that use statistical analysis to detect the existence of secret messages in a stego-object are called steganalysis [9].

Besides the undectactability, invisibility is a mandatory property for the steganography’s system. The changes in the cover image should be imperceptible to human visual system (HVS) characteristic. This means that the modification conducted to the cover-object should not be visible to the human naked eyes.

Security is another characteristic of steganography. In which the confidentiality is guaranteed by embedding the sensitive information in a way that is invisible and secured. The authentication and identification are provided by steganography. To ensure identification between sender and receiver, a shared security key is used. The successful extraction of the embedded message ensures the authentication.

Payload capacity is another significant criterion wanted in steganography. It is preferred to embed as much as information possible in a stego-object without degrading the object’s quality. Many research works are conducted on the area of embedding more messages with fewer modifications [10]. There is a tradeoff between the imperceptibility and payload capacity. As the capacity rate increases the imperceptibility decreases.

On the other hand, robustness is not as crucial as other properties of steganography [22]. Robustness measures the amount of alteration that the stego-image can take against attacks before destroying the secret information. Attacks can be either intentional or unintentional [24]. The intentional attacks involve eavesdroppers trying to remove the embedded information or adding noises to the image to destroy the hidden message. However, unintentional attacks include manipulating the object by compression, conversion, etc.

c) Limitations and Problems

Steganography received lots of attention in the last few years. However, the evolution of the study of steganography technology has not been without some risks. In some cases steganography can be used in an inappropriate manner. It is suggested that steganography can be used to conduct terrorist attacks. Some intelligent agencies suspect that Mr. Osama bin Laden [6] used steganography as a method of communication with his followers to conduct the World Trade Center attacks [25]. In addition, Steganography can be used illegally to exchange baleful criminal materials.

A problem that constraints steganography is how to deliver the shared stego-key between the sender and the intended recipient. The key should be delivered securely and not be intercepted by snoops.

IV. Encryption

Nowadays information sharing and transferring is rapidly increased. This technique is associated with a main concern that is snoops accessing the information. Secret encryption and steganography are widely used to handle secret codes but each one has a different technique and with different purposes. This section presents briefly a description about encryption.

a) Terminology

Cryptography is defined in [26] as the science of writing secret code by cyphering and deciphering of the secret message. It is a mechanism of transforming the secret information from readable format to unreadable [27]. It is the art of protecting the sensitive information. Tradition scenario of encryption includes first party wanting to send a secret message through unsecure channels such as the Internet. The second party will receive the message while the snoop may interpret the communication. Many terminologies refer to cryptography such as plain text, cipher text, encryption, and decryption. Plain text is the secret information that the first party wants to send. Before the text is sent, the plain text is converted to another format that is not understandable by anyone and it is called a cipher text. Encryption is a mechanism of converting the plain text to cipher text. It involves utilizing a key and an algorithm. Decryption involves transforming the cipher text to plain text using a secure key. The right key is a vital factor to ensure high security [28].

An illustration of the cryptography process is shown in Figure 3. It is clear that at the sender side the plain text is encrypted using a certain key. Then the cipher text is transferred through a communication channel to the recipient. Finally, at the receiver side the cipher text is decrypted using a key. This key may be the same or different than the sender key.

Figure 3 Encryption Process

Different algorithms and techniques exist to encrypt a plain text. Encryption algorithms are classified based on the type of transformation and keys. The use of key in different algorithms is handled differently. In some algorithms the key should be agreed and distributed between two parties prior to the communication of encrypted the cipher text, while other do not have this restriction. Symmetric-key cryptography is a cryptography approach in which the encryption and the decryption algorithms use the same key. Public-key cryptosystems use two keys in which the sender uses a key different than the receiver. These keys are determinant by some mathematical functions.
Parties who wanted to communicate secretly used the earliest form of cryptography long ago. The earliest form of cryptography started by Julius Caesar (100-44 BC) used to substitute some alphabet with other when secret communication required. He used simple cipher shifting technique of letters by a fixed amount. Moreover when he wanted to communicate with his followers he transformed Latin letters to Greek [29].

Hebrew (500 – 600 BC) also used substitution cipher (Atbash cipher) that uses units to be replaced with the letter of plain text. The unit consists of one letter, pairs or several of letters or even mixture of letter. The receiver then uses the inverse way of deciphering the cipher text [29].

In 1466 Leon Battista Alberti was the first one to publish the information on polyalphabetic cipher. In addition, in 1585 Blaise de Vigenère wrote the book that is about authentic plaintext and cipher text autokey systems. Moreover, During the second world war cipher mechanical and electromechanical machines were widely used [29]. Germans for example used electromechanical rotor machine called Engima. Many Mathematics efforts were conducted to decipher that enigma [29].

Adequate cryptography systems must achieve some goals to ensure high security. Purposes of cryptography are summarized into five classes.

First confidentiality is to ensure that the information is encrypted and can only be correctly decrypted by the authorized party. Confidentiality depends on how a strong encryption algorithm which is difficult to be broken. It is the assurance that no one other than the intended authorized party can read the information. Second aspect authentication is the assurance that the received information is arrived from an authorized person not a false identity. Third, Integrity is the assurance that the transmitted information is not modified or altered by some unauthorized person. It ensures that the received secret message is not corrupted over communication channel. Non-repudiation is making sure that first party or the second party should not be able to deny transmission. Access control is the last aspect of cryptography this is used to prevent unauthorized parties from rejecting actions they performed [28].

Many problems are associated with cryptography. In case of a symmetric-key algorithm if the key is stolen then the cipher text can be easily decrypted. In addition, the sender and receiver should agree on the key prior to the encryption and communication. Either the sender has to pass the key to the receiver face-to-face or communicate through a secure communication channel or even through a cryptographic channel [30]. With a public-key algorithm the problem of distribution of key does not matter. Since the key depends on some mathematical functions. However, it is not yet proved that these functions are unsolvable and few known public keys are still unbroken [30].

We mention that cryptography is illegal to be used without permission in some countries. For instance, in China parties who want to use cryptography must get approval from a legal Commission. Iranians have to require license from Supreme Council for Cultural Revolution to use cryptography. They must submit the encryption algorithm, the keys and information about the parties who exchange the data. Also, In Russia licenses are obligatory to be acquired from Federal Security Service to develop, implement and/or use cryptography [31].

The biggest concern in the field of cryptography is the advance of progress research study on Cryptanalysis. Cryptanalysis is the opposite technology of cryptography. It aims at breaking a cipher text without the knowledge of the key used. According to Kerckhoff’s principle the privacy of encryption system depends on the key [27]. Attacks are performed by taking advantages of the weakness of the algorithmic design of the encryption system. Attacks are categorized into the following classes: Ciphertext-only, known plaintext, chosen plaintext, chosen ciphertext and related-key.

For more detail it can be referred to [27]. According to Göllmann [26] cryptography does not really solve the problem of secure communication. It transforms from one problem to another simpler problem that is key management problem.

V. Steganography VS. Cryptography

Steganography and Cryptography are two different approaches to ensure secure communication. Each approach has different purposes, aspects and limitations. After the main background information has been presented previously, it is simple to conduct the following comparison.

As mentioned earlier the purpose of steganography is to hide the covert communication information, while the purpose of cryptography is to protect the contents of the secret information. Steganography and cryptography are related to two parties who wish to communicate securely to exchange some confidential information. In case of security service offered by Steganography and cryptography, both achieve security through authentication and identification. Also confidentiality should be guaranteed for both approaches. Both approaches should be undetectable for the case of steganography and unbroken for the case of cryptography against steganalysis and cryptanalysis respectively. Other features that are handled in cryptography and not in steganography are data integrity and non-repudiation. Whereas payload and robustness are aspects associated with steganography.

Steganography can be attacked by steganalysis techniques, while cryptography can be attacked by cryptanalysis techniques. Moreover, key distribution is another limitation that cryptography deals with and with some case of steganography if a key is used. Steganography is sometimes used in an inappropriate manner. Cryptography sometimes used in countries where it is prohibited.

Lastly many research works proposed to use steganography and cryptography together to guarantee higher secure communication [32][33]. Cryptography science takes care of preventing unauthorized access to information; however it cannot prevent from illegally duplicating the decrypted content. A brief description of the differences between both systems is presented in Table 1.

VI. Conclusion

It can be summarized from this paper the following: Data hiding techniques and encryption are both branches of information security. Many methods exist in data hiding techniques in which the main category is steganography. Steganography and cryptography are two sciences with different techniques. The main differences between both techniques were presented.

We have surveyed the two techniques that deal with information security: steganography and cryptography. Brief
overview of terminology, history, features and limitation of both techniques are presented.

Table 1 Comparison between steganography and cryptography

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Steganography</th>
<th>Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Conceal message</td>
<td>Encryption</td>
</tr>
<tr>
<td>Carrier</td>
<td>Digital media</td>
<td>Data</td>
</tr>
<tr>
<td>Output Format</td>
<td>The object is hidden in the cover object</td>
<td>The object is hidden in the cover object</td>
</tr>
<tr>
<td>Key</td>
<td>Optional</td>
<td>Required</td>
</tr>
<tr>
<td>Features</td>
<td>Undetectability, invisibility</td>
<td>Confidentiality - Integrity, Non-repudiation - Access control</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Steganography</td>
<td>Cryptography</td>
</tr>
<tr>
<td>Problem</td>
<td>Misuse by criminals</td>
<td>Illegal in some countries</td>
</tr>
</tbody>
</table>

VII. References


