International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Comparative Study of Steganography & Cryptography

Pranali R. Ekatpure[1], Rutuja N Benkar[2]

[1, 2]Sahakar Maharshi Shankarrao Mohite Patil Institute of Technology & Research-Akluj

Abstract: ***Today, the secure communication between two parties is not an easy task as considering the possible attacks & unintentional changes during communication over untrusted medium like Internet. Steganography and Cryptography are two popular ways of sending vital information in a secret way. Steganography is the art of hiding of a message within some format so that presence of hidden message is indistinguishable. Cryptography involves converting a message text into an unreadable ciphertext. One hides the existence of the message and the other distorts the message itself. Many powerful & robust technologies of steganography & cryptography are developed. This paper is an attempt to analyze the steganographic & cryptographic techniques.***

Keywords: Steganography, Cryptography , steganalysis, cryptanalysis, stego-key

1. Introduction

The expansion of the Internet has frequently increased as the availability of digital data such as audio, images and videos to the public. We are surrounded by a world of secret communication, where people of all types are transmitting information as innocent as an encrypted credit card number to an online-store but the hackers finds it easy to steal the content.

Various communications such as electronic mail or the use of web browsers are not secure over the Internet for sending and receiving information. Information sent by those means may include sensitive personal data such as credit card information which may be intercepted. Online users may need private and secure communications. They may simply not want third parties to browse and read their e-mails or alter their content.

Steganography and Cryptography are well known and widely used to hide the original message. Steganography is used to embed message within another object known as a cover work. In Cryptography, sender convert plaintext to cipher text by using Encryption key and other side receiver decrypt cipher text which again converted into original plain text.

2. Steganography

Steganography is the art and science of communicating in a way which hides the existence of the communication. The term steganography is arrived from Greek word means, "Covered Writing". The carrier files can be referred to as cover text, cover image, or cover audio as appropriate. The steganography is not to keep others from knowing the hidden information, but it is to keep others from drawing suspicion that the information even exists. If a steganography method causes someone to suspect that there is secret information in a carrier medium, then the method has failed. The first written evidence about steganography being used to send messages is the Here dotous story about slaves and their shaved heads. The modern representation of Steganography can be given in terms of the prisoner's problem [5].

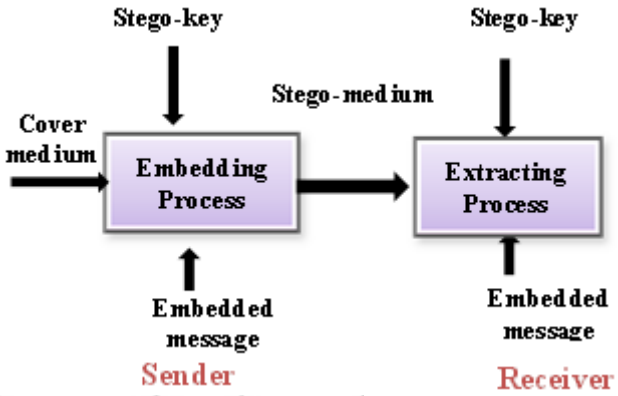


Figure 1: A Steganography Framework

In steganography, the possible cover carriers (images, audio, video, text) which will hold the hidden information. A message is the information hidden and may be plaintext, cipher text ,images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. Hiding information may require a stego-key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image. A possible formula of the process may be represented as:

Cover_medium + embedded_message + stego_ key = stego_medium

3. Categorization of Steganography

3.1 According to Steganography Technologies

The steganography can be categorized :

1) Substitution methods- substitute redundant parts of a cover with a secret message (spatial domain).
2) Transform domain techniques -embed secret information in a transform space of the signal (frequency domain)
3) Spread spectrum techniques -adopt ideas from spread spectrum communication.

Licensed Under Creative Commons Attribution CC BY

4) Statistical methods -encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.
5) Distortion techniques- store information by signal distortion and measure the deviation from the original cover in the decoding step.
6) Cover generation -methods encode information in the way a cover for secret communication is created[2].

3.2 According To Carrier Type

3.2.1 Text Steganography
Text steganography uses text as a cover media for hiding message. Message can be hidden by shifting word and line, in the open spaces , in word sequence. Properties of a sentence such as number of words, number of characters, number of vowels, position of a vowel in a word are also used to hide secret message.[7]

- Line Shift Coding Protocol
- Word Shift Coding Protocol
- Feature Coding Protocol
- White Space Manipulation
- Text Content

3.2.2 Image Steganography
Steganography on images are most popular form of steganography as images frequently occur at website, as email attachments, etc. There is minimum cause for suspicion when digital image is used. [6]

- Simple Watermarking
- LSB - Least Significant Bit Hiding (Image Hiding)
- Direct Cosine Transformation
- Wavelet Transformation

3.2.3 Audio Steganography
It is done by hiding information in audio file without difference being audible. The digital representation of audio includes representing the sound intensity at a certain point in time. Since a 16 bit audio file typically has 216 sound levels for this sound intensity, the difference of 1 level will be unnoticeable by human ear. Four main steps for audio Steganography are:
1. Alteration
2. Modification
3. Verification
4. Reconstruction

3.2.4 Video Steganography
Advantage of video steganography is that a video can conceal a large amount of data. Video file can be seen as a collection of images & sounds thus most image & audio steganographic techniques can be used on video.

4. Cryptograpy

Cryptography is the practice for secure communication in the presence of third parties. Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable cipher text. Cryptography is the process by which the data to be transmitted is hidden in a manner such that only the intended recipient can understand it[4].The process of reverting cipher text to its original plain text is called decryption.
There are two types of cryptographic techniques:
(i) Symmetric key cryptography
(ii) Asymmetric key cryptography

Symmetric Key Cryptography is actually the technique by which identical cryptographic keys are used for the purpose of both encryption and decryption. The receiver can get back original data by using the key. The symmetric key cryptography provides high data rates, usage as primitives to construct various cryptographic mechanisms and can be combined to produce stronger ciphers. The main fact here is that the security of data depends on the security of the key. So, care should be taken while exchanging keys between the sender and the receiver.

Asymmetric Key Cryptography is the technique where two keys are used. One key is used to lock or encrypt the plaintext, and another to unlock or decrypt the ciphertext. Neither key can do both the functions. One of these keys is published or made public and the other is kept private. This technique has comparatively slower data rate throughputs than the symmetric key technique.

5. Steganography & Cryptography: Comparison

5.1 Cryptography Problems

Cryptography suffers from following problems :
1) Key distribution problem
2) Legal limitation by Government
3) Cryptanalysis

5.2 Steganography Attacks

Steganographic attacks consist of detecting, extracting and destroying hidden object of the stego media. Steganography attack is followed by steganalysis. There are several types of attacks based on the information available for analysis. Some of them are as follows: -

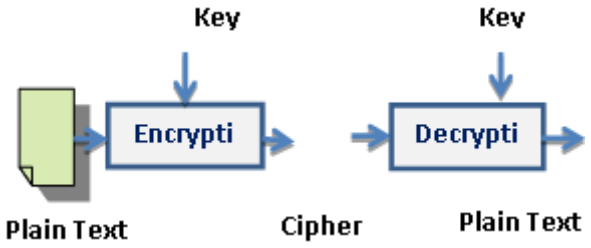
1. Known carrier attack: The original cover media and stego media both are available for analysis.
2. Steganography only attack: In this type of attacks, only stego media is available for analysis.
3. Known message attack: The hidden message is known in this case.
4. Known steganography attack: The cover media, stego media as well as the steganography tool or algorithm, are known

5.3 Steganalysis & Cryptanalysis

Steganalysis is the process of identifying steganography by inspecting various parameter of a stego media. The primary step of this process is to identify a suspected stego media. After that steganalys is process determines whether that

Licensed Under Creative Commons Attribution CC BY

media contains hidden message or not and then try to recover the message from it.



In the cryptanalysis it is clear that the intercepted message is encrypted and it certainly contains the hidden message because the message is scrambled. But in the case of steganalysis this may not be true. The suspected media may or may not be with hidden message. The steganalysis process starts with a set of suspected information streams. Then the set is reduced with the help of advance statistical methods.

Table 1: Comparison of Steganography & Cryptography

Criteria/ Method	Steganography	Cryptography
Carrier	Any digital media	Usually text
Secret data	payload	Plain text
Key	Optional	Necessary
Input file	At least two	one
Output file	Stego file	Cipher text
Objective	Secret communication	Data protection
Services	Confidentiality Authentication	Confidentiality Data Integrity Authentication Non-repudiation
Techniques	LSB Spatial Domain Jsteg	Transposition, Substitution, RSA
Naked eye identification	No, as message is Hide within other carrier (cover image)	Yes, as message is convert in Other way, which sough something is hidden
Type Of Attack	steganalysis	cryptanalysis
Fails	when it is detected	de-ciphered

5.4 Combination of Steganography and Cryptography

The 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 steganography medium. Those who seek the ultimate goal in private communication can combine encryption and steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so.

Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptographic techniques

6. Conclusion

After an inconclusive comparison, it is difficult to certainly say that Steganography can be used as an alternate to Cryptography. Cryptography offers more secure services but it also comes with some problems. However, this does not form conclusive proof that Steganography cannot be used instead of Cryptography. Thus combination of cryptography and Steganography is used so all security purpose are solved.

References

[1] Anandaprova Majumder, Suvamoy Changder, “A Novel Approach for Text Steganography: Generating Text Summary using Reflection Symmetry ” International Conference on Computational Intelligence: Modeling Techniques and Applications(CIMTA), pp. 112 – 120, 2013.

[2] C.P.Sumathi, T.Santanam and G.Umamaheswari, “A Study of Various Steganographic Techniques Used for Information Hiding” International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, pp.9-25, December 2013

[3] Mihir H Rajyaguru, “CRYSTOGRAPHY-Combination of Cryptography and Steganography With Rapidly Changing Keys ” International Journal of Emerging Technology and Advanced Engineering (ISSN) Volume 2, Issue 10, pp.329-332,October 2012)

[4] S Ushll, G A Sathish Kumal, K Boopathybagan, “A Secure Triple Level Encryption Method Using Cryptography and Steganography” IEEE Computer Science and Network Technology 2011, pp. 1017-1020

[5] Anandaprova Majumder, Suvamoy Changder, “A Novel Approach for Text Steganography: Generating Text Summary using Reflection Symmetry” International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA), pp. 112 – 120 2013.

[6] T. Morkel , J.H.P. Eloff , M.S. Olivier, “AN OVERVIEW OF IMAGE STEGANOGRAPHY”, Information and Computer Security Architecture (ICSA) Research Group

[7] Souvik Roya, P.Venkateswaran, “A Text based Steganography Technique with Indian Root” International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) ,pp. 167-171, 2013.

.

Licensed Under Creative Commons Attribution CC BY