Volume 4, Issue 10, October 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Information Security Based on Steganography & Cryptography Techniques: A Review

Pramendra Kumar
M.Tech Scholar,
Department of Computer Science,
RIET, Bhankrota, Jaipur, Rajasthan, India

Vijay Kumar Sharma
Asst. Prof.,
Department of Computer Science,
RIET, Bhankrota, Jaipur, Rajasthan, India

Abstract*— Over past few decades, with the advancement of communication technology the use of internet has grown extremely to exchange information without any distance barrier. However, such network is most popular for fast and easy process to exchange information over the long distance but still the message transmissions over the Internet have face all kinds of security problems. Therefore the applications of cyber world needing high level of safeguard for expensive data and produce explosive growth to the field of information hiding. However, in recent years, a lot of research has taken place in direction to trim down the security issues by contributing various approaches but different terrains pose separate challenges. In this context, this paper presents the investigation of two popular security mechanisms, namely cryptography and steganography.

***Keywords*— Steganography, Cryptography, Information Hiding, Security**

I. INTRODUCTION

In any communication, security is the most important task. With the advancement of technology and the wide use of World Wide Web for communication increase the challenges of security. However, the challenges can be manageable with the advanced technologies of secure networks but every time these technologies may not be reliable for communication of secrete information over a long distance that produce a need of additional security mechanisms to secure secrete information. In this context, to provide the security two techniques has been used widely, Cryptography and Steganography. Cryptography is used to scramble the information, deals with changing the meaning and appearance of message. It changes the plain text into cipher text by the process of encryption, uses the mathematical techniques and various algorithms such as public key cryptography, private key or symmetric and asymmetric algorithm for securing the information. However, cryptography provide secure solutions to a set of parties, by encrypting plain text into cipher text but the cyber attacker easily arouse these text and intercepts the communication between two separate users to modify, inject, or drop any communication packet. To improve these limitations and to reduce the issues of cryptographic methods an alternative mechanism, the steganography has use widely. Generally the concepts of this techniques differ from the cryptography, where the cryptography method converted the information in a encrypted form that an eavesdropper and cannot be understand, the Steganography technique embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion in some cases, sending encrypted information may draw attention, while invisible information will not. However, both cryptography and steganography provide the security but no one standalone techniques are enough of secure information efficiently and different security categories have different requirements and problems.

II. CRYPTOGRAPHY

One of the classic techniques used for ensuring privacy of files and communication is Cryptography. It is the science of secret writing, converting messages or data into a different form to exchange messages between two parties who want the communication over an insecure channel. Without the right knowledge of the key no-one can access the correct information [1, 2]. It addresses all of the elements necessary for secure communication over an in secure channel, namely privacy, confidentiality, key exchange, authentication and non-repudiation. Figure 1 present the overview of general cryptography technique

Sender
Key(Public/Private)
Plaintext
Encryption
Ciphertext
Receiver
Receiver
Keys(Public/Private)
Sender
Ciphertext
Decryption
Plaintext

(a) Process of Encryption (At Sender Side) (b) Process of Decryption (At Receiver Side)

Figure 1 Overview of Cryptology

For securing the data three types of cryptographic schemes are mostly used to achieve the goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions (or Protocols). The type and length of the keys utilized depend upon the encryption algorithm. Cryptanalysis is a study of how to compromise (defeat) cryptographic mechanism.

A. Symmetric / Secret Key Cryptography

Secrete key encryption technique also known as the symmetric-key, single-key, shared-key, one-key and eventually private-key encryption, where a unique single key is used at both side for encrypt or decrypt the secret information. The original message also known as plain text encrypt with the key by the sender and at the receiver side same key is use by receiver to convert that encrypt message to get plain text. Only people who are authorized for the encryption/decryption would know the key. Figure 2 present the overview the process of secrete key cryptography.

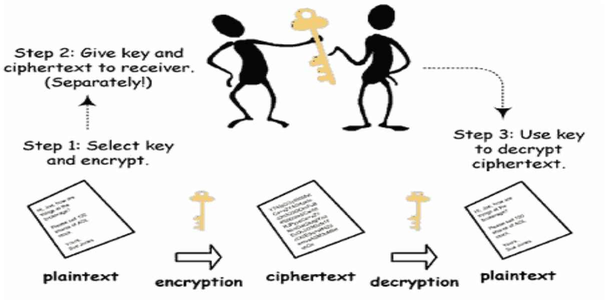
Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Figure 2 Symmetric Key Cryptography Processes [3]

However technique provides the security for communication but has problem with the distribution of the key. Once the key stole by an unauthorized person, he/she can easily get whole information without any difficulty.

B. Asymmetric / Public Key Cryptography

The asymmetric cryptosystem (or public key cryptosystem), employs two keys that are mathematically related, use separate for the encryption and decryption of data. Figure 3 shows the working steps of this algorithm.

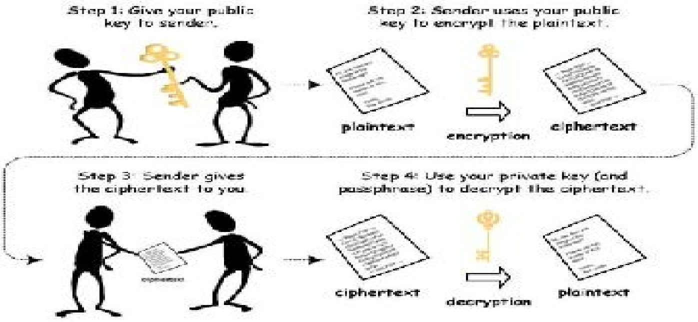
Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
decryption
plaintext

Figure 3 Symmetric Key Cryptography Processes [4]

In this technique with the single key, it is not possible to access the information or easily determine the other key. The both of keys are required for the process to work. The key used for encryption is kept public and so as called public key, and the decryption key is kept secret and called private key. The keys are generated in such a way that it is impossible to derive the private key from the public key. Few examples of Asymmetric-Key Algorithms are RSA, Diffie-Hellman,Digital Signature Algorithm (DSA), Public-Key Cryptography Standards (PKCS), Key Exchange Algorithm (KEA)etc.

C. Hash Functions

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Figure 4 shows the process of Hash function.

Figure 4 Hash Function

III. Steganography

Steganography is the art of hiding and transmitting data through apparently innocuous carriers in an effort to conceal the existence of the data. In general the Steganography and cryptography are closely related. Where cryptography scrambles messages so they cannot be easily understood by an unauthorized person, steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the first place. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Figure 5 present the steganography system overview.

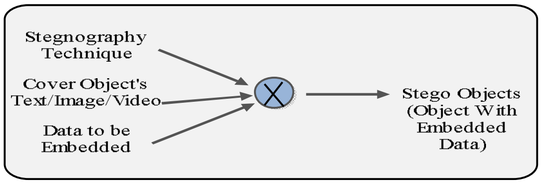
Stegnography Technique
Cover Object's Text/Image/Video
Data to be Embedded
Stego Objects (Object With Embedded Data)

Figure 5 General Steganography Model

The secret information can be embedded into the cover media by the stegosystem encoder with using the password key. A secret message can be plaintext, ciphertext, an image, or anything that can be represented as a bit stream. Once the cover object has information embedded in it, it is called a stego object. After the embedding process the stegoobject send to receiver by choosing the appropriate channel, where decoder system is use with the same stego key to find original information as sender would like to transfer. Information hiding techniques do pursue two major objectives, present in figure 6.

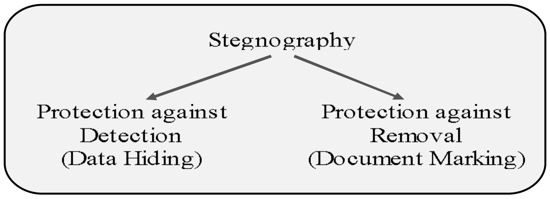
Stegnography
Protection against Detection (Data Hiding)
Protection against Removal (Document Marking)

Figure 6 Steganography Layered Security

Protection against detection can be needed if someone wants to ensure that the embedded message is not detected by a third unauthorized party. For example, a user wants to prevent others from finding out that an image contains a secret message hidden by the "Least-bit insertion method". This aim of data hiding is achieved by using schemes that do not modify the original object in a visible way; all changes should be indiscernible to the human eye or the computer. Protection against removal, on the other hand, tries to prevent the removal of hidden data without making it useless or degrading its quality. There are many types of steganography methods that support almost all the digital file formats. The high degrees of redundancy formats are most suitable for this type of techniques. Redundancy can be defined as the bits of an object that provide accuracy fargreater than necessary for the object’s use and display [5]. The redundant bits of an object are those bits thatcan be altered without the alteration being detected easily [6].Figure 7 shows the different categories of file formats that can be used for steganography techniques.

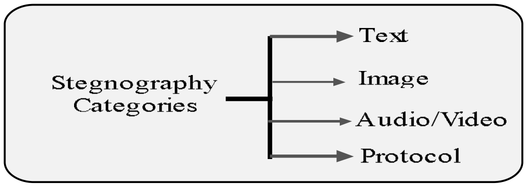

Figure 7 Categories of Steganography

IV. Related Work

The several characteristics of information hiding discuss in [7], to identify hidden information. For hiding the information images are reviewed manually and another popular method steganography technique is used toautomate the process. The developed tool is to test robustness of information hiding techniquesin images such as warping, cropping rotating and blurring.Another approach embeds the information in digital images [8] with the projected name SpreadSpectrum Image Steganography (SSIS). The proposed technique hides the desire secret information of substantial length with indigital images while maintaining the original image size and dynamic range. The hide information can be retrieve by using the key only. Based on the creation of an “adhoc” palette for BMP and GIF images, two dissimilar approaches for lossless andlossy image have been proposed [9].

A Quantization-based Steganography scheme [10] has been proposed to improve the hiding capacity component of a color image, where the secret message is hidden. Since the Quantization-based hiding method is free from the interference and simulation results the hidden message can be extracted at low BER. Another embedded method PairsAnalysis [11] proposed for detection of secret messages embedded in digital images. Although the approach isin principle applicable to many different Steganographic methods as well as image formats, it isideally suited to 8-bit images, such as GIF images, where message bits are embedded in LSBs ofindices to an ordered palette. The proposed work use Ezstego algorithm with random message and optimized paletteorder as an embedding archetype to demonstrate Pairs Analysis and compareits performance with the chi-square attacks.

The embedding of matrix [12] proposed for high payloads. One of approach constructed from simplex codes and the second onebased on random linear codes for small dimension .The embedding efficiency of the proposedmethods is evaluated with respect to theoretically achievable bounds. Several researchers have addressed the problem of video steganography. In [13] a comparative analysisbetween Joint Picture Expert Group (JPEG) image stego and Audio Video Interleaved (AVI) video stego by quality and size was performed. The authorspropose to increase the strength of the key by usingUTF-32 encoding in the swapping algorithm and lossless stego technique in the AVI file. However, payloadcapacity is low.In [14] an adaptive invertible information hidingmethod for Moving Picture Expert Group (MPEG) videois proposed. Hidden data can be recovered withoutrequiring the destination to have a prior copy of thecovert video and the original MPEG video data can berecovered if needed. This technique works in frequencydomain only. It has the advantages of low complexityand low visual distortion for covert communicationapplications. However, it suffers from low payloadcapacity.

V. STEGANOGRAPHY VERSUS CRYPTOGRAPHY

Both of the data hiding technique widely used for the purpose of hide the secret information at the time of communication over unsecure channel. These techniques have many applications in computer science and other related fields. However, Steganography technique are closely related to cryptography to protect information fromunwanted parties but the cryptography can offer two additional security services that are not offered by steganography at the moment, namely data integrity and non-repudiation. Where the cryptography technique focuses on keeping the contents of a message secret, the steganography focuses on keeping the existence of the message as secret. For this reason these two technologies cannot be directly compared in order to establish which one is better. However, the comparison can be extended by comparing what services are offered by each in terms of security.

The table 1 clearly shows that no encryption method is completely secure. Givenknowledge of the algorithm and enough time, attackerscan reconstruct most encrypted data. All the security services offered by cryptography are vulnerable to cryptanalysis - the study of mathematical functions that attempts to defeat the security of cryptographic mechanisms. Certain encryption algorithms, as well as certain hash functions, have already been broken by cryptanalysis. However, the another security technique can be provide security by the stego object but from past few decades with the advancement the steganalysis technique the steganography is also vulnerable. The process to detecting the steganography by lookingvariances in between bit patterns and unusually large filesizes known steganalysis. It involves two major techniques: visual analysis and statistical analysis. Visual analysis tries to reveal the presence of hidden data through inspection, either with the naked eye (or ear in the case of sound) or with the assistance of a computer. Statistical analysis, on the other hand, attempts to reveal tiny alterations in carrier objects of statistical characteristics caused by steganographic embedding [15, 16].

Table 1Comparison between Steganography and Cryptography

S.no.	Context	Steganography	Cryptography
1.	Host Files	Image, Audio,Text, etc.	Mostly Text Files
2.	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3.	Result	Stego File	Cipher Text
4.	Type of Attack	Steganalysis: Analysis of a file with a objective of finding whether it is stego file or not.	Cryptanalysis
5.	Objectives	Keeping the existence of a message secret	Keeping the contents of a message secret
6.	Applications	Used for securing information against potential eavesdroppers	Used for securing information against potential eavesdroppers
7.	Security services offered	Confidentiality, Identification, Authentication	Confidentiality, Data Integrity Identification and authentication Non-repudiation
8.	Technology-specific problems	Steganalysis, Key distribution (except with keyless steganography	Key distribution, Law enforcement Cryptanalysis

Mostly classical steganography system relies on the encoding system's secrecy to secure the information. Although such a system might work for a time, once it is known, it is simple enough to expose the entire received media (e.g., images) passing by to check for hidden messages ultimately, such a steganographic system fails. The cryptography technique can be used to improve the security of secret information. As discuss earlier that in practical, no one standalone system is enough to provide the facility of a complete secure system but the concepts of combining the cryptography with steganography technique can provide two layer of security, where in case of failing the steganography system the secrete message remain safe because of encoding technique.

VI. CONCLUSION

This paper has present the investigation of two security approaches, namely cryptography and steganography. Where the cryptography only change the format of the information that cannot be understood by any unauthorized user, the steganography hide the complete information in the cover media, so no one can easily identify that any message is hidden in the presented content. However both of these techniques provide the security to information but the standalone approach based of either of these techniques is not so good for practice. Therefore to provide more security to the information at the time of communication over unsecured channel a novel advance technique for data security is needed. Future work can be done in way to combining the concepts of cryptography and stegnography, to provide more security to the secrete message.

REFERENCES

[1] Gaetan Le Guelvouit, “Trellis-Coded Quantization for Public-Key Steganography,” IEEE Internationalconference on Acostics, Speech and Signal Processing, pp.108-116, 2008.

[2] BabitaAhuja and, ManpreetKaur, “High Capacity Filter Based Steganography,” International Journalof Recent Trends in Engineering, vol. 1, no. 1, pp.672-674, May 2009.

[3] Debnath Bhattacharyya, Poulami Das, Samir kumarBandyopadhyay and Tai-hoon Kim, “TextSteganography: A Novel Approach,” International Journal of Advanced Science and Technology, vol.3, pp.79-85, February2009.

[4] Chin- Chen Chang, Yung- Chen Chou and Chia- Chen Lin, “A steganography scheme based on wetpaper codes suitable for uniformly distributed wet pixels,” IEEE International Symposium on circuitsand Systems, pp. 501-504, 2009.

[5] Atallah M. Al-Shatnawi “A New Method in Image Steganography with Improved Image Quality” Applied Mathematical Sciences, Vol. 6, 2012, no. 79, 3907 – 3915

[6] Dipesh G. Kamdar1, Dolly Patira, Dr. C. H. Vithalani “Dual Layer Data Hiding Using Cryptography and Steganography” International Journal of Scientific Engineering and Technology, Volume No.1, Issue No.4, pg :134-138, ISSN : 2277-1581, 01 Oct. 2012

[7] Neil F. Johnson and SushilJajodia, “Steganalysis: The Investigation of Hidden Information,” IEEEconference on Information Technology, pp. 113-116, 1998.

[8] ChristofPaar, “Applied cryptography and data security,” version 2.5, Ruhr-University at Bochum, Germany, Jan 2005.

[9] Moerland, T. 2003. Steganography and steganalysis. Leiden Institute of Advanced Computing Science http://www.liacs.nl/home/tmoerl/privtech.pdf, last accessed on 2006-05- 01.

[10] http://cs110.wellesley.edu/lectures/L18-encryption/handout.html

[11] http://www.powayusd.com/pusdtbes/cs/class7.htm

[12] Gisin, N. et al. 2002. Quantum cryptography. Reviews of Modern Physics, 74:145-196

[13] Marvel, L.M., Boncelet Jr., C.G. &Retter, C., “Spread Spectrum Steganography”, IEEE Transaction son image processing, 8:08, 1999

[14] Wang, H & Wang, S, “Cyber warfare: Steganography vs. Steganalysis”, Communications of the ACM,47:10, October 2004

[15] Mrs.Archana S. Vaidya, 2Pooja N. More., 3Rita K. Fegade., 4Madhuri A.Bhavsar., 5Pooja V. Raut “Image Steganography using DWT and Blowfish Algorithms” IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 8, Issue 6 (Jan. - Feb. 2013), PP 15-19

[16] Firas A. Jassim “A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method” International Journal of Computer Applications (0975–8887)Volume 72–No.17, June 2013