Research Article *ISSN: 2319-507X*
Shital Patil, IJPRET, 2012; Volume 1(8): 9-15 *IJPRET*

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CRYPTOGRAPHY, STEGANOGRAPHY &NETWORK SECURITIES

SHITAL C. PATIL[1], PROF. R. R. KEOLE[2]

1. PG Students H.V.P.M's college of Engg. & Tech., Amravati, India.
2. Faculty in H.V.P.M's college of Engg. & Tech., Amravati, India.

Accepted Date:
27/02/2013

Publish Date:
01/04/2013

Keywords

Cryptography,
Steganography,
Authentication,
Security Techniques

Corresponding Author

Ms. Shital C. Patil

Abstract

This paper presents a classification of network security techniques such as: secrecy, authentication and Non-repudiation. The secrecy techniques are of two categories: cryptography and steganography. Cryptographyis, traditionally, the study of means of converting information from its normal, comprehensible form into an incomprehensible format, rendering it unreadable without secret knowledge, the art of encryption. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. Authentication is the act of confirming the truth of an attribute of a datum or entity.If both cryptography and steganography are used then the communication becomes two fold secured.

ISSN: 2319-507X
IJPRET

1. INTRODUCTION

During the last few decades there is a tremendous development in information and communication technology. So security in communication through internet has become a concern. Network security problems can be categorized roughly into four areas: secrecy, authentication, non-repudiation and integrity control. Secrecy, also called confidentiality concerns with keeping the information away from the unauthorized users. That means unauthorized users should not be able to read and/or understand the information on transit.

There are mainly two techniques to achieve secrecy. Those are: cryptography and steganography. Cryptography is a technique in which the secret information is transformed to a new form such that the intruder can not understand information. The Cryptographic algorithms are again two types. They are: symmetric key cryptography and public key cryptography. Steganography is a technique of converting communication in which the intruder can not suspect that communication is going on [1].The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden a data. It is not to keep others from knowing hidden information even exist. If a steganography method causes someone to suspect the carrier medium then the method has failed [2].

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packing and labeling claims to be.

Non-repudiation refers to a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement or contract [1].

2. CRYPTOGRAPHY

Cryptography is the art of protecting information by encrypting it into an unreadable format, called cipher text. Only those who possess a secret *key* can

ISSN: 2319-507X
IJPRET

decipher(or decrypt) the message into plain text.

2.1. Symmetric Key Cryptography

This is the traditional cryptography known as private key cryptography too. The sender uses a key and the encryption procedure to encrypt the message (plain text) into cipher text. The receiver uses the decryption procedure and the key to decrypt the cipher text to message. The key at sender is same as the key at the receiver. The encryption and decryption procedures except the key are known to the adversary, so the protection of the data or message depends on the key only. Fig.1 is a diagrammatical representation of Symmetric Key Cryptography . There are a good number of symmetric key algorithms. Some well known algorithms are: DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), Triple-DES, AES (Advanced Encryption Standard), RC6 [1].

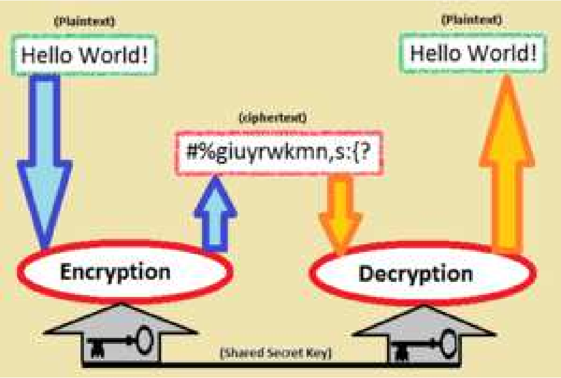

Figure 1: Symmetric Key Cryptography

2.2. Public Key Cryptography

In 1976 Diffie and Hellman developed a two key crypto system, called public key cryptography. The distinguishing technique used in public-key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys – a public encryption key and a private decryption key. The publicly available encrypting-key is widely distributed, while the private decrypting-key is known only to its proprietor, the recipient. Messages are encrypted with the recipient's public key, and can be decrypted only with the corresponding private key. Some well known public key algorithms are: RSA

(Rivest, Shamir and Adelman), Diffie-Hellman etc [1].

3. STEGANOGRAPHY

Steganography is a technique for invisible communication. This is achieved by hiding information inside another information, thus hiding the existence of the communicated information.The word steganography is ofGreek origin and means "concealed writing" from the Greek words steganos means "covered or protected", and grapheimeans "writing".The advantage of steganography over cryptography alone is that messages do not attract attention to themselves.

Modern techniques of steganography

Steganographic techniques are based on the four types of cover files i.e. text, image, audio and video files.

3.1 Text Steganography: [3]

In this technique the message is hidden within a plain text file using differentschemes like use of selected characters, extra white spaces of the cover text etc.

•Use of selected characters of cover Text.

Sender sends a series of integer number (Key) to the recipient with a prioragreement that the secret message is hidden within the respective position ofsubsequent words of the cover text. For example the series is ‘1, 1, 2, 3, 4, 2, 4,’and the cover text is “**At**eam o**f** fi**v**e men j**o**ined tod**a**y”. So the hiddenmessage is “Atfvoa”. A “0” in the number series will indicate a blank space inthe recovered message. The word in the received cover text will be skipped if thenumber of characters in that word is less than the respective number in theseries (Key) which shall also be skipped during the process of message unhide.

•Use of extra white space characters of cover text.

A number of extra blank spaces are inserted between consecutive words of covertext. This numbers are mapped to a hidden message through an index of alookup table.

3.2 Image Steganography:

The most widely used technique today is hiding of secret messages into a digitalimage. This steganography technique exploits the weakness of the human visualsystem (HVS). HVS cannot detect the variation in luminance of color vectors athigher frequency side of the visual spectrum. A picture can be represented by a

collection of color pixels. The individual pixels can be represented by their opticalcharacteristics like 'brightness', 'chroma' etc. Each of these characteristics can bedigitally expressed in terms of 1s and 0s.For example: a 24-bit bitmap will have 8 bits, representing each of the threecolor values (red, green, and blue) at each pixel [4].If we consider just the bluethere will be 2^8different values of blue. The difference between 11111111 and11111110 in the value for blue intensity is likely to be undetectable by thehuman eye. Hence, if the terminal recipient of the data is nothing but humanvisual system (HVS) then the Least Significant Bit (LSB) can be used forsomething else other than color information.

3.3 Audio Steganography[5,6,7]

In audio steganography, secret message is embedded into digitized audio signalwhich result slight altering of binary sequence of the corresponding audio file.There are several methods are available for audio steganography. Some of themare LSB Coding, Phase Coding, Spread Spectrum,Echo Hiding etc.

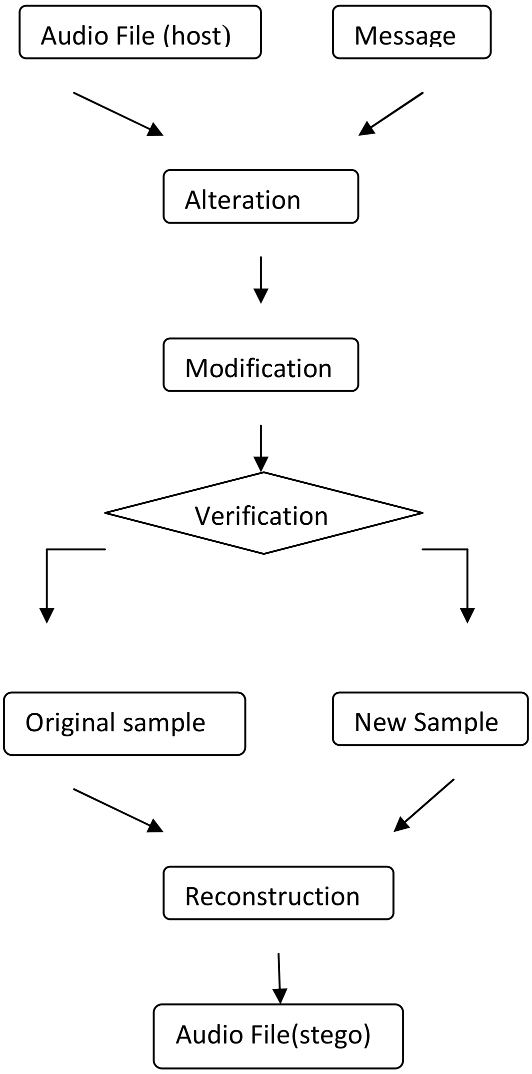

Fig 2 : Audio Steganography

3.4 Video Steganography

Video files generally consist of images and sounds, so most of the relevant techniques for hiding data intoimages and audio are also applicable to video media. In the case of video steganography sender sends the secretmessage to the recipient using a video sequence as cover media. Optional secret key 'K' can also be used duringembedding the secret message to the cover media to produce 'stego-video'. After that the stego-video iscommunicated over public channel to the receiver. At the receiving end, receiver uses the secret key along with extraction algorithm to extract

the secret.

4. APPLICATIONS

4.1. Applications of Cryptography:

Cryptography is used for securing transmission of messages, protection of data, and to provide privacy and security in any situation where information is not intended for public consumption. Examples include political campaign plans, extramarital affairs, cover-ups, ecommerce, business transactions, and private communications.

4.2. Applications of steganography:

Usage in modern printers: Steganography is used by some modern printers, including HP and XEROX brand color laser printers. Tiny yellow dots are added to each page. The dots are barely visible and contain encoded printer serial numbers, as well as date and time stamps.

Alleged use by intelligence services: In 2010, the Federal Bureau ofInvestigation revealed that the Russian foreign intelligence service uses customized steganography software for embedding encrypted text messages inside image files for certain communications with "illegal agents" (agents under non-diplomatic cover) stationed abroad.

To Control Terrorist Activities: How to control terrorist activities is a big question before many countries. The government and anti-terrorism offices can communicate secretly to monitor or stop the terrorist activities. If they are communicating openly terrorists can be careful and change their plans.

5. CONCLUSION

This paper presents a classification of network security techniques and the recent research work in the field of steganography. Cryptography like Steganography is a very useful technique to achieve secrecy in communication. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies andpass messages covertly.

REFERENCES

1. Gandharba Swain, Saroj Kumar Lanka, “A Quick review of Network Security and Steganography”, International Journal of Electronics and Computer Science Engineering, (IJECS- 2012),2012

2. M.I.Khalil, “Image Steganography: hiding Short Audio Message within Digital Images” ,(JCS&T, 2011), 2011.

3. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, “ Steganography and Stegnalysis: Different Approaches”, http://arxiv.org/ftp/arxiv/papers/111/358.pdf

4. Babloo Shaha and Suchi Sharma, “ Steganographic Techniques of Data Hiding using Digital Images” , Defence Science Journal, vol 62, No.1, 2012.

5. Bhavsar Jaimin H, Imaran Khan, “ Techniques of Steganography And Steganalysis”, http://ssrn.com/abstract=2029407.

6. Udit Budhiaa andDeepa Kundur, “Digital video steganalysis exploiting collusion sensitivity” - Sensors, Command Control, Communications and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense, Edward M.Carapezza, ed., Proc. SPIE (vol. 5403), Orlando, Florida, April 2004. http://www.ece.tamu.edu/~deepa/pdf/BudKun04.pdf

7. Methods of Audio Steganography, Internet Publication, www.snotmonkey.com