ISSN No. 0976-5697

Volume 8, No. 3, March – April 2017

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Combined Strength of Steganography and Cryptography- A Literature Survey

Aiswarya Baby
P.G Scholar
Department of Computer Science & Engineering
FISAT, Mookkannoor, Kerala, India

Hema Krishnan
Assistant Professor
Department of Computer Science & Engineering
FISAT, Mookkannoor, Kerala, India

Abstract: Cryptography and steganography are the 2 popular methods available to provide security. The objective of cryptography is data protection and the objective of steganography is secret communication. Cryptography converts the data into cipher text that can be in unreadable format to normal user where steganography hides the existence of message by embedding data into some other digital media. Both of them has their own vulnerabilities. Crypto-steganography combination overcomes each other's weakness and make difficult for intruders to attack or steal sensitive information. This paper focus on the strength of combining cryptography with steganography and various works in the area of combination of these 2 techniques are discussed.

Keywords: Cryptography; Steganography; Cipher, Stego image; Advanced Encryption Standard; Least Significant Bit

I. INTRODUCTION

Computer and internet are the major media that connects different parts of the world as one global virtual world in this modern era. That's why we can exchange lots of information easily at any distance within seconds of time. But the confidential data need to be transferred should be kept confidential till the destination. Rapid enlargement in number of attack recorded during electronic exchange of information has certainly called for more robust method for securing data transfer.

Information security has grown as a prominent issue in our digital life. The network security is becoming more significant as the volume of data being exchanged over net increases day by day [1]. One of the reasons why attackers become successful in intrusion is that they have an opportunity to read and understand most information from system. The most important motive for attacker to benefit from intrusion is value of confidential data he can obtain by attacking the system. Hackers may expose the data, alter it, distort it or employ it for more difficult attacks. The solution for this problem has led to the development of cryptography and steganography. By combining cryptography and steganography in one system we can ensure enhanced security [2].

Cryptography and steganography is not capable of protecting the data alone. To improve information security and to maintain secrecy and privacy of data, steganography and cryptography alone is not sufficient. Cryptography can be used where steganography is inefficient and steganography can be used where cryptography is inefficient. Thus a new approach of combining both techniques has been proposed by many researchers for secure storage and transmission of data [3].

The remainder of this paper is organized as follows: Section II introduces a brief note on cryptography and steganography. Related works in the literature of combining cryptography and steganography are analyzed in Section III. Finally, a brief conclusion is given in Section IV.

II. BACKGROUND DETAILS

A. *Cryptography*

Cryptography is one among many aspects of building security. It is a powerful tool used to protect information in computer systems. When we use the browser for home banking we use a number of cryptographic algorithms for protecting the confidential data. Even the computer passwords are protected by cryptographic hash functions. When we send an email, it is also encrypted by SSL. Modern cryptography concerns itself with confidentiality (information cannot be processed by anyone for whom it was not intended), integrity (information cannot be altered), and authentication (sender and receiver can confirm their identity).The aim of cryptography is to store and transmit data in a particular form so that only those for whom it is intended can read and process it. To achieve this the data is scrambled into cipher text, an unreadable format.

Modern cryptography is a mix of mathematics, computer science, and electrical engineering and it has been around of 1000's of years. It is at the heart of worldwide communication network today. Cryptanalysis is the art of breaking into secure communication. Cryptography relies on two component: an algorithm and a key. The 2 key terms associated with cryptography is encryption and decryption. Encryption is the process of scrambling the plain text into cipher text, an unreadable format and decryption is just the reverse of encryption.

Cryptographic system can be classified based on,

1) Methodology for transforming plain text to cipher text: It includes substitution technique and transposition technique. In substitution technique, plain text is mapped into another element and in transposition technique, plain text is rearranged. The first well known cipher, a substitution cipher was used by Julius Caesar around 58 BC. It is now referred as Caesar cipher.

2) Methodology for number of keys used : It includes secret key cryptography, public key cryptography and hash function. Secret key cryptography [4] method employs a single key for both encryption and decryption. The sender uses a 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. Since a single key is used for both function, this cryptography is also called symmetric key cryptography. This is faster compared to asymmetric key cryptography. Here the keys must be known to both sender and the receiver. The difficulty of this approach is the distribution of the key. The secret key cryptographic algorithm in use today includes DES, AES, CAST-128/256, Blowfish, Rivest cipher etc.

Public key cryptography [5] uses 2 different keys public key, and private key. This is a property which set this scheme different than symmetric encryption. If encryption is done using sender's public key then decryption should be done using receiver's private key and vice versa. Public key cryptography algorithm that is in use today for a key exchange /digital signature include RSA, Diffie-Hellman, DSA, ElGamal, ECC etc.

Hash function also called message digest and 1-way encrypt are algorithm that use no key. A fixed length hash value is computed based upon the plain text that makes it impossible for either contents or length of plain text to be recovered. Hash algorithm are used to provide digital fingerprint of a files contents. Examples includes MD, SHA, RIPEMD, Tiger etc.

3) Methodology for processing plain text: In block cipher technique [6] processing or encoding of the plain text is done as a fixed length block one by one. A block example could be 64 or 128 bits in size. The same key is used to encrypt each of the blocks. A pad is added to short length blocks. It is usually more complex and slower in operation and examples of block cipher are Lucifer, IDEA, RC5 etc.

In stream cipher technique [6] processing or encoding of plain text is done bit by bit. The block size here is simply one bit. A different key is used to encrypt each of bits. Bits are processed one by one in as in a chain. It is simple and much faster than block cipher. Examples of stream cipher are FISH, ISAAC, RC4 etc.

B. Steganography

Steganography derived from 2 Greek words 'steganos' which means either secret or covered and 'graphein' which means writing or drawing. In this case steganography literally means covered writing. The Greeks would actually use this method to transmit secret messages more than 2000 years ago. Normally in those days they wrote on tablet covered with wax. The first recorded use of the word steganography came up from 15th century book called steganographia, disguised as a book on magic. This was written by Johannes Trithemius [7].

Steganography means hiding a secret message within another message. In digital computing there are many opportunities for steganography. Steganography is the practice of concealing information or files within non secret data. The file containing the secret data is called the carrier. The modified carrier looks like original carrier. Best's carriers are images, audio, video files since everybody can send receive download them. Steganography is not encryption. The data is hidden not encrypted.

Steganography techniques can be generally classified as,

1) Spatial domain technique: In spatial domain steganography bits in the pixels values are changed in order to hide the data. Spatial domain techniques can be classified into Least Significant Bit (LSB), Pixel value Differencing (PVD), Random Pixel Embedding method, histogram Shifting method, Texture Based method etc. LSB is the widely used simplest method where there is less chance for degradation of original image.

2) Transform domain technique: Transform domain embeds information in transform space. In this domain, the image is transformed from spatial domain to frequency domain by using any transforms and after a transformation process, the embedding process will be done in proper transform coefficients. The process of embedding data in the frequency of a signal is much stronger than embedding principles that operate in the time domain. Transform domain techniques include DFT, DCT, DWT and they are less exposed to compression, cropping etc [8].

3) Distortion technique: This technique store message by distorting the cover slightly and detecting the change from the original. The decoder function uses the original cover image during decoding process to find the difference between original and distorted cover image in order to restore secret message [8].

4) Masking and filtering: This technique is usually restricted to grayscale and 24-bit images. It doesn't hide the data in noise level but embeds it in significant areas. Masking adds redundancy to the hidden information. This method is more robust than LSB modification with respect to compression and different kinds of image processing since the information is hidden in the visible parts of the image.

III. RELATED WORKS

This section gives an analysis on the various works that have been proposed in the area of combination of steganography and cryptography.

In [9] authors proposed a model for security enhancing in image steganography that uses the neural network and visual cryptography. Visual cryptography is a renowned technique to protect data which is image based. The secret data is encrypted using AES algorithm. The cover image is divided into blocks and energy coefficient for each block is identified using IWT. The neural network is used to identify the best location in host image in order to embed the secret data. LSB embedding technique is used to embed the secret data into high energy locations of cover image. Inverse IWT is applied on stego image in order to negate the effects of IWT. Later stego image is brought back to original shape by

using data re-arrangement process. During decryption the 2 shares of image are retrieved and inverse visual cryptography is applied and later message is extracted and decrypted.

In [10] authors proposed a technique for protection of image in open wireless channel. The secret image is embedded in the cover image using LSB technique from spatial domain. Then the stego image is divided into 8*8 blocks. The divided stego image is encrypted by double random phase encoding. Double random phase encoding transforms the image into white stationary noise. In the first phase of double random phase the image is multiplied by first random phase mask. Then the, multiplied image is transferred from time domain to frequency domain by applying fourier transform. In the final phase the image is convolved with the second random phase mask.

In [11] authors presented an enhanced safe data transfer scheme in smart Internet of Things (IoT) environment. They proposed a technique that employ an integrated approach of steganography and cryptography during data transfer between IoT device & home server and home server & cloud server. The sensed data from IoT device is encrypted and embedded in the cover image along with message digest of sensed data and send to the home server for authentication purpose. At the home server the embedded message digest and encrypted data version is extracted. The received digest is compared with newly computed digest to ensure data integrity and authentication. The same procedure is carried out between home server and cloud server.

In [12] authors integrated RSA cryptography and audio steganography. The secret message is converted to cipher text using RSA algorithm and the cipher text is hidden in audio using LSB audio technique. By combining steganography and cryptography it produces the higher level of security.

In [13] authors proposed a new method of image steganography on gray images combined with cryptography. The secret message is encrypted using Vernam cipher and the message is embedded in the cover image using LSB with shifting. Here the sender and the receiver shares one time pad key for Vernam cipher. The authors claim that data hiding capacity of their method has increased to 100%.

In [14] authors presented 2 new approaches to secure data. In the first approach each byte of the secret image is encrypted using S-DES algorithm to produce an array of encrypted pixels. Each element of array is then divided into 2 parts where first part contains first 4 MSB's and second part contains remaining LSB's. Then each pixel value is converted with alphabets from A to P where A is assigned to 0000 and P to 1111. The output will be an encrypted image containing text. The encrypted image is then embedded in cover image by XOR method. In the second approach they simply encrypted the secret image using S-DES algorithm and embed it in the cover image as stated above.

In [15] authors has given a hybrid approach for image security that provides good encryption quality. The secret image is encrypted using blowfish algorithm to produce the cipher image. Then the encrypted image is embedded using LSB technique in the cover image. Blowfish algorithm is lossless and highly secured encryption technique.

In [16] authors proposed a method that increase the security of data transfer by combining cryptography and steganography. Mp3 file is taken as the cover media and the secret message is encrypted using AES algorithm using a key that has been processed by MD5 hash function. The secret message was inserted in the homogeneous frame in mp3 files with addition of a key code. The MD5 algorithm is a widely used cryptographic hash function used to verify data integrity.

In [17] authors came up with space domain steganography. Secret image and carrier image are taken of same size. Pseudo random noise sequence of both image is generated which is dependent on key. A single plane(R or G or B) is selected from both the images. Given plane of the carrier image (CI) is divided into set of 16 pixels and then selection of the pixels are done in the similar manner as they appear. Similarly given plane of secret image (SI) is sliced into a set of 16 pixels based upon column select sequence and row select sequence sequences.Then selected pixel will be ciphered using second key and then embedded into the carrier image.

IV. CONCLUSION

The use of internet for communication purpose has rapidly increased and it magnified the attacks to users. Protecting the data is a big challenge for computer users. Cryptography and Steganography are widely used techniques to ensure security. Both techniques have many applications in computer science and other related fields. Both methods provide security in their own ways, but to add multiple layers of security it is always a good practice to use combination of these techniques. The concepts of steganography, cryptography and their applications in the security of digital data communication across network is studied in this paper and technical survey of recent methods which combined steganography and cryptography is presented.

V. REFERENCES

[1] JidagamVenkataKarthik, B.Venkateshwar Reddy, "Authentication of Secret Information in Image Steganography", International Journal of Latest Trends in Engineering & Technology, ISSN: 2278-621X, Vol. 3(1), Sep 2013, pp. 97-104.

[2] Dhawal Seth, L. Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010, pp. 3-6.

[3] Shristi Mishra, Prateeksha Pandey "A Review on Steganography Techniques Using Cryptography", International Journal of Advance Research In Science And Engineering, Vol. No.4, Special Issue (01), March 2015.

[4] Garry. C. Kessler, "An Overview of Cryptography", Handbook on Local Area Networks (Auerbach, Sept. 1998).
[5] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15, 2010.
[6] https://www.securityconsulting.net.au/block-cipher-stream-cipher-comparison/
[7] https://en.wikipedia.org/wiki/Steganography
[8] Mehdi Hussain and MureedHussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013.
[9] K.S. Seethalakshmi, Usha. B, Sangeetha. K. N, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography", IEEE Int. Conf.Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016.
[10] SadafBukhari, Muhammad ShoaibArif, M.R. Anjum, and SamiaDilbar, "Enhancing security of images by Steganography and Cryptography techniques", IEEE Int. Conf. Innovative Computing Technology (INTECH), 2016.
[11] Ria Das, Indrajit Das, "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques", IEEE Int. Conf. on Research in Computational Intelligence and Communication Networks (ICRCICN), 2016.
[12] AnkitGambhir and SibaramKhara, "Integrating RSA Cryptography & Audio Steganography", IEEE ICCCA, 2016.
[13] Kamaldeep Joshi, RajkumarYadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE ICIIP, 2015.
[14] Vipul Shanna and Madhusudan "Two New Approaches for Image Steganography Using Cryptography" IEEE Int. Conf. Image Information Processing, 2015.
[15] MoreshMukhedkar, PrajktaPowar and Peter Gaikwad, "Secure non real time image encryption algorithm development using cryptography & Steganography", IEEE INDICON, 2015.
[16] RiniIndrayani, HanungAdiNugroho, RisanuriHidayat, IrfanPratama, "Increasing the Security of MP3 Steganography Using AES Encryption and MD5 Hash Function", International Conference on Science and Technology-Computer (ICST), IEEE, 2016.
[17] Nikhil Patel, ShwetaMeena, "LSB Based Image Steganography Using Dynamic Key Cryptography", International Conference on Emerging Trends in Communication Technologies (ETCT), 2016.

