Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-7, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Combined Technique of Cryptography and Steganography to provide Double Security

Bharti Sharma
Department of Computer Science & Technology, Vivekananda Global University, Jaipur, India

Abstract: *Information security is the most important area of research now-a day. Cryptography and steganography technologies are used to provide the security to the sensitive data. Cryptography is an art of hiding and verification. It provides security and preventing from unauthorized access to sensitive data and enable verifiability of data in a communication. In this paper we focused on steganography techniques along with cryptography. Steganography plays an important role in information security. Steganography mean hiding sensitive information within cover media. The information can be in the form of a text, an image, a video or an audio which is to be hidden using any cover media like image, text, audio or video.*

Keywords: *Cryptography, Steganography, Message Hiding, Cover media*.

1. Introduction

With the advent of internet data security is the critical issue in information security. Today's we can exchange lots of information within seconds of time with the help of computer and internet media that connects peoples of the world. But secret data should be kept confidential till the destination. There are two techniques cryptography and steganography that provides security to the sensitive information. Cryptography technology uses a mathematical function to protect sensitive data. It is just changed the data into cipher text but doesn't hide the existence of data so that people can easily detect the sensitive information by applying inversing techniques. On the other hand steganography technique uses a cover media for hiding data. It also hides the existence of secret data so that human eyes can't be able to detect secret information. But both technologies are not capable to protect data alone. To overcome each other problems, combination of steganography and cryptography is used [3].

1.1 Cryptography

Cryptography is a method used to protect sensitive information by converting data into cipher text [1]. The various aspects in data security are:

- Confidentiality: the information can be read only by authorized persons.
- Authentication: The originality of the message is identified correctly.
- Integrity: An unauthorized person can't be able to modify stored or transmitted information.
- Non-Repudiation: It assures that both sender and receiver of the message can't be able to deny the transmission.
- Access control: It requires that access may be controlled by intended receiver.
- Availability: The components of computer system are available to authorized persons whenever needed.

Fig1. Process of Encryption.

1.2 Steganography

Steganography is a technique of hiding sensitive information within any cover media like text, image, audio & video. There are mainly four types of steganography technologies [2].

1) Text Steganography
2) Image Steganography
3) Audio Steganography
4) Video Steganography

Text Steganography: A steganography Technique that uses text as a cover media for hiding secret information is known as the text steganography technique. This technique is difficult to use because

Text files have a small amount of redundant data to hide secret information.

Image Steganography: A steganography technique that uses image as a cover media for hiding secret information is known as image steganography technique. This is the most widely used technique because it hides the existence of secret information so that a human can't able to detect the secret information.

Video Steganography: A steganography technique that uses Video as a cover media for hiding secret information is known as Video Steganography.
Audio Steganography: A steganography technique that uses audio as a cover media for hiding secret information is known as audio steganography technique. But it is not used so much because human can detect even a minute change in an audio quality by the human ears.

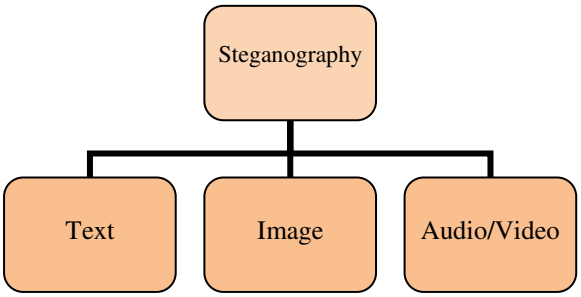

Fig2. Types of Steganography

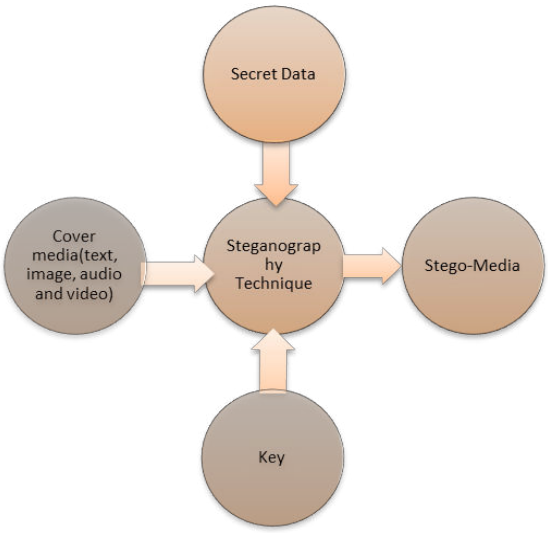

Fig3. Steganography Process

2. Techniques used in Cryptography and Steganography

There are so many cryptography and steganography technologies available for hiding secret information such as human eyes can't able to detect it.

2.1 Cryptography techniques

In cryptography technique a data is converting into cipher but it doesn't hide the existence of secret data. It can be broadly classified into three categories:

1. Symmetric key cryptography.
2. Asymmetric key cryptography.
3. Key-less cryptography.

2.1.1 Symmetric key cryptography technique: In this technique both sender and receiver uses a secret shared key for converting plain text into cipher text. Symmetric algorithms are includes: Information Encryption Standard (DES), Triple-DES, and Advanced Encryption Standard (AES) and Blowfish Algorithm [4].

1) Data Encryption Standard (DES)

Data encryption standard mechanism uses a 56-bit key to generate a 64-bit long plain text block to cipher text block. Data encryption standard algorithms take the fixed size plain text block stream, & generate the same size cipher text block stream through a series of complicated operations. Another advanced version of DES algorithm is triple data encryption standard (3DES). Triple DES is the same process as DES but it uses 192 bits key on 64 bits plaintext data.

2) Advanced Encryption Standard(AES)

Advanced encryption standard algorithm is used to overcome the problem of DES algorithm. It uses 128 bits plain text data and a key size of 128, 192, 256 bits. DES uses a Feistel network for encryption but it does not encrypt an entire block per iteration. The key length is defined by the number of internal round of the cipher text. For 128 bits key, Number of round is 10 in AES algorithm.

3) Blowfish

Blowfish algorithm is invented by Bruce Schneier in 1993. Bruce Schneier designed blowfish algorithm for general purpose use and as a alternative to DES (Data Encryption Standard). It has a 64 bit block size and variable length key from 32 bits to 448 bits. It uses a Feistel network for encryption process. Blowfish algorithm uses a large number of dependent S boxes. The S boxes take 8 bit input and produce 32 bit as output.

2.1.2 Asymmetric key cryptography technique: In Asymmetric key cryptography technique both sender and receiver uses a different keys to perform cryptography algorithm for providing security to sensitive data. Asymmetric key algorithm includes: RSA, Diffie-Hellman Key Exchange, Elliptic Curve cryptography, Digital Signature Standard.

1) RSA

RSA algorithm is invented by Ronald Rivest, Adi Shamir, and Leonard Adleman. It can be used for Digital Signature, key Exchange, and Encryption of small plain text data. The RSA algorithm uses a variable size plain text block and variable size key. The key-pair is generated by two prime numbers chooses from large number n according to special rules [5]. The algorithm is as follows:

A. First generate two Random prime numbers p and q.
B. Then calculate n= p x q, it is a key length which is expressed in bits.
C. Calculate Euler's totient function φ (n) = (p - 1) x (q - 1).
D. Calculate e based on the following conditions:

- $1 < e < \varphi(n)$
- GCD (e, φ (n)) = 1 that is e and φ (n) are co-prime.
- Also ensure that e must have a short bit-length and small Hamming weight.

E. At the last step, find d by using the following relation:

- (e x d) mod n=1, private key (d, n) and public key (e, n).

Message Encryption: Encryption is done at the sender's side that uses a public key to convert plain text into cipher text.

- Cipher text $C = M^e$ Mod (n) where C is the cypher text generated after encryption.

Message Decryption: Decryption is done at the receiver's side that uses a private key to convert cipher text into plain text.

- $M= C^d$ mod (n) Where M is the plain text generated after decryption.

2) Diffie-Hellman Key Exchange

Diffie-Hellman is a simple public key encryption algorithm. It is used only for key-exchange, not for digital signature or authentication. In Diffie-Hellman Key Exchange Algorithm, two users has to establish the authenticity by generating a secret key using public key scheme based on discrete logarithmic [7].
The algorithm is as follow:

- Select two elements: first select a prime number P and an integer r. r is the root of prime number P.
- In the second step, sender selects a random number XA which is less than P. The random number XA is private. By using XA, Sender will generate YA= rXA mod P. which is public.
- After sender key generation, receiver selects a random number XB which is less than p. the random number XB is private. Receiver will compute YB=rXB mod P. which is public.
- Both sender and receiver calculate the secret key which is identical. Sender's secret key K= (YB) XA mode P, receiver's secret key K= (YA) XB mode P.

3) Elliptic Curve Cryptography

Elliptic curve cryptography is a public key cryptography algorithm purposed by Victor Miller and Neal Koblitz in 1985. It is based upon elliptic curve arithmetic. It is used to develop a variety of schemes including key exchange, digital signature and encryption. The security of elliptic curve cryptography (ECC) based on ECCLP (Elliptic Curve Cryptography Logarithm Problem). It is used in wireless communications like sensor networks, PDAs, smart cards, and mobile phones [6].
The General equation of ECC is:
$y2 + axy + by = x3 + cx2 + dx + e$
Where x, y are belongs to set of real number and a, b, c, d, e are real numbers.

4) Digital Signature Standard

Digital signature standard provides an authentication to users by attaching a code that act as a signature. It is an NIST standard and uses secure hash algorithm to provide security to the sensitive information [8]. Signature is formed by taking the hash code of the message and encrypting the message by sender's private key. It provides the integrity of the message.

2.2 Steganography Techniques

In steganography technique the secrete message is hidden inside the cover media (text, image, audio and video). It also hides the existence of the secret message so human eyes can't able to detect the secret message.

Steganography technique can be classified in six categories [9]:

2.2.1 Substitution Method: In substitution method (Spatial Domain Method) secret data is directly embedded into cover media. In this technique the secret message bits are embedded into the least significant bits of cover media known as LSBs. By using LSB technique, secret message bits are embedded into the pixels of image. Some Time these pixels can be selected randomly. Thus it provides security to secret data but human can easily detect the secret

information because it directly embeds the secret information into an image [11].

2.2.2 Transform Domain Method: In Transform Domain method secret message can't be embedded directly into the image cover. First the image cover is transformed into frequency domain form spatial domain. The transformation can be achieved by using DCT (discrete cosine transformation), DFT (discrete Fourier transformation), and DWT (discrete wavelet transformation) [11].

2.2.3 Spread Spectrum: Spread spectrum techniques adopt ideas from spread spectrum communication.

2.2.4 Statistical Method: Statistical methods encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.

2.2.5 Distortion Method: Distortion techniques store information by signal distortion and measure the deviation from the original cover in the decoding step.

2.2.6 Cover Generation: Cover generation methods encode information in the way a cover for secret communication is created.

3. Literature Survey

For secure transmission of data various cryptography and steganography techniques have been purposed by many researchers. The basic technique for providing multilayered security to data, Researchers purposed a combination of cryptography and steganography technique.

Palak Mahajan, Heena Gupta [10] implemented image steganography algorithm to provide security to secret data while allowing maximum capacity to hide secret data inside an image. To achieve this objective initially the image is transformed from spatial domain to frequency domain using discrete wavelet transform technique. To increase the capacity, Huffman encoding is applied on secret message. Then compressed secret data is embedded into cover image by using RC4 based LSB embedding algorithm.

Rig Das, Thamrichon Tuithung [11] purposed an image steganography method based on Huffman encoding. Two 8-bit gray level images are used as a cover image (P x Q) and as a secret image (M x N). LSB steganography technique is used to embed secret image into cover image for providing more security to secret data because it can't be detected without knowing the decoding rule and Huffman table.

Aiswarya Baby, Hema Krishnan [3] purposed a combination of cryptography and steganography technique to achieve multilayered security. Cryptography and Steganography is not capable to provide security to data alone. To achieve this goal, researcher first applied AES algorithm on secret data and then embed it into cover image by using LSB image steganography algorithm. The combination of cryptography and steganography technology provides multilayered security to secret data by doing double security.

4. Purposed Method:

To improve the security of secret data, combination of steganography and cryptography has been purposed. In this technique a secret data is embedded into the cover media by using steganography technique and encryption is done over secret data by using cryptography technique. This multilayer security provides a more security to sensitive data so that human can't able to detect it. The diagram of this purposed system is given in fig.4.

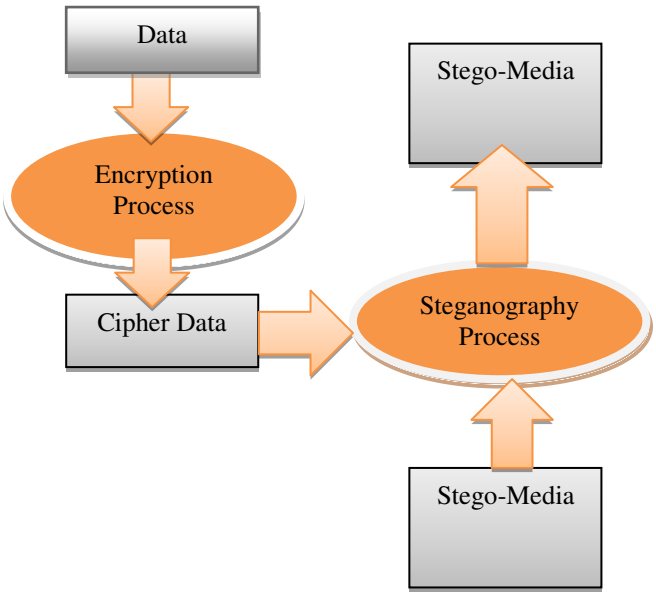

Fig4. Purposed System architecture

5. Conclusion

At some stage human needs a secure communication to provide security to their sensitive information. Both cryptography and steganography technologies provides confidentiality to secret data. Cryptography hides secret data by encrypting plain data into cipher data but it doesn't hide the existence of the secret data so human can easily detect the hidden

information. On the other hand steganography hides an existence of secret data but it has also some limitations. To overcome these limitations of cryptography and steganography, combination of cryptography and steganography technology is used to provide multilayer security to secret data.

6. References

[1] Prof. Mukund, R. Joshi, Renuka Avinash Karkade, "Network Security with Cryptography", International Journal of Computer Science & Mobile Computing, Vol.4 Issue.1, January- 2015, pg. 201-204.

[2] Sikha, Vidhu Kiran Dutt, "Steganography: "The Art of Hiding Text in Image using Matlab", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 9, September 2014, pg. 822-823.

[3] Aiswarya Baby, Hema Krishnan, "Combined Strength of Cryptography and Steganography: A Literature Survey", International Journal of Advanced Research in computer Science, Volume 8, No. 3, March – April 2017.

[4] Jawahar Thakur, Nagesh Kumar, "DES,AES and Blow Fish: Symmetric key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced, ISSN 2250-2459, Volume 1, Issue 2, December 2011.

[5] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj Vincent PM, "An Algorithm to Enhance Security in RSA", IEEE, July 4-6, 2013.

[6] Prof. Suraj R. Pardeshi, Prof. Vikul J. Pawar, Prof. kailash D. Kharat of Government College of Engineering, "Enhancing Information Security in Cloud Computing Environment using Cryptographic Techniques".

[7]https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange.

[8]https://www.cse.unr.edu/~bebis/CS477/Papers/DigitalSignatures.pdf.

[9] C. P. Sumathi, T. Santanam and G. Umamaheswari, "A Study Of various Steganography Techniques used for Information hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[10] Palak Mahajan, Heena Gupta, "Improvisation of Security in Image Steganography using DWT, Huffman Encoding & RC4 based LSB Embedding", IEEE, 978-9-3805-4421-2, 2016.

[11] Rig Das, Thamrichon Tuithung, "A Novel steganography Method for Image Based on Huffman Encoding", IEEE, 978-1-4577-0748-3, 2012.