ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

Enhance Security in Steganography with cryptography

Chandra Prakash Shukla[1], Ramneet S Chadha[2], Abhishek Kumar[3]

Student,MTech(IT),CDAC Noida , India[1,3]

HOD,MTech(CSE),CDAC Noida, India[2]

Abstract: In many organizations like FBI and RAW share confidential and important data on any network. Hackers are always in wait for it. They hack the data and use it for their benefit. These peoples try to use these data to harm someone, they sale these important data to enemy countries. In either case, message sender or receiver has to pay the price. To protect from these undesirable acts, we can use Steganography and cryptography together to ensure security of the message. One of the most efficient and secure algorithms is RSA Algorithm for converting text message to cipher text. Steganography is the art and science of writing hidden messages in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden message and Cryptography is a mechanism to convert message or data in non readable form.

Keywords: Stego Object, Encryption, RSA Algo, Decryption, Cryptography, Steganography, Cipher Text.

I. INTRODUCTION

The widespread use of internet for communication has increased the attacks to users. The security of information is an important issue related to privacy and safety during storage and communication. Cryptography and Steganography are two popular ways of sending vital information in a secret way. Cryptography is the method of converting plaintext into cipher text. The messages are converted into an encrypted format using a key and then this cipher text is hidden into an image, audio or video file according to the user's choice. The encryption is done using Advanced Encryption Algorithm and the key is hashed using Secure Hash Algorithm.

II. WHAT IS CRYPTOGRAPHY

Cryptography (or *cryptology*; from Greek κρυπτός, "hidden, secret"; and γράφειν, graphein, "writing", or -λογία, -logia, "study", respectively)[2] is the practice and study of techniques for secure communication in the presence of third parties (called adversaries)[3]. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries [4] and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation [5]. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

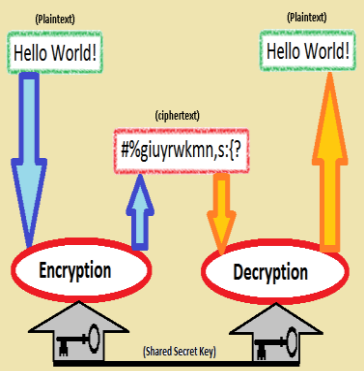

Fig.1 Cryptography Mechanism

A. *Symmetric-key cryptography*

1. *Advanced Encryption Standard:*-AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware.[8]Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

2. *Data Encryption Standard:*-DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is always quoted as such [6].

B. *Public-key cryptography*

Public-key cryptography, also known as **asymmetric cryptography**, refers to a cryptographic algorithm which requires two separate keys, one of which is *secret* (or *private*) and one of which is *public*. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature; whereas the private key is used to decrypt ciphertext or to create a digital signature. The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional ("symmetric")

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

cryptography which relies on the same key to perform both.

1. *RSA :-* **RSA** is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997. [9]

III. WHAT IS STEGANOGRAPHY

Steganography is the process of secretly embedding information inside a data source without changing its perceptual quality. Steganography comes from the Greek word steganos which literally means "covered" and graphia which means "writing", i.e. covered writing. The most common use of steganography is to hide a file inside another file [1].

A. Text steganography:

Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data [7].

B. Audio steganography:

When developing a method for audio steganography one of the first considerations is the likely environments, the sound signal will travel in environments between encoding and decoding. There are two main areas of modification. First the storage environment or digital representation of the signal that will be used and second the transmission pathway the signal might travel.

C. Image/Video steganography:

Images are often used as the popular cover objects in steganography. A message is embedded in a digital image through many embedding algorithms and a secret key. The resulting stego image is sending to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message because of steganography. Video Steganography is a technique to hide any kind of information file(image, audio, video) in Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements.

D. Data Hiding Techniques in IPv4 Header:

To securely transmit the data over the network the Vasudevan et al. [20] used the analogy of the jigsaw puzzle. They insinuate to fragment the data into variable sizes instead of fixed size like the jigsaw puzzle and append each fragment of data with a pre-shared message authentication code (MAC) and a sequence number so that the receiver can authenticate and combine the received fragments into a single message. At the sender side every data fragment is prefixed and suffixed with a binary „1" and then XOR"ed with a Random number called the one-time pad and transmitted over the network. When the receiver receives the message it performs the exact opposite process of that to the sender and retrieves the intended message [21].

IV. STEGANOGRAPHY WITH CRYPTOGRAPHY

A. Text Steganography with Cryptography:-

In this type combination we simply do not hide simple text message. We hide ciphertext message after encryption process, after that we can hide this cipher text message in any multimedia files like video, audio, and image.

Fig. 2 Text Steganography with Cryptography Mechanism

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 3, March 2014

B. Image Steganography with Cryptography:-

1. *Hide Encrypted Image in Multimedia Files:-* In this type combination we can hide an encrypted image into another image or other multimedia files like audio, video.

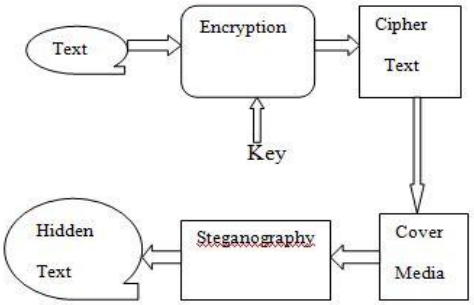

Fig.3 Encrypted images hide in Multimedia files mechanism

2. *Hide an Image into Cover image and then Encrypt the Cover image:-* We can hide a secrete image or picture into cover image and then we can encrypt the cover image and send via any network.

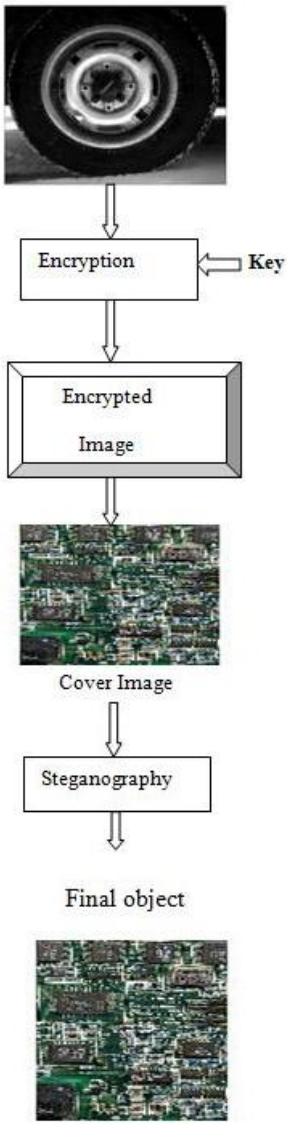

Fig.4 Hide an Image into Cover image and then Encrypt the Cover image Mechanism

C. Video Steganography with Cryptography

Video Steganography is a technique to hide any kind of files into a carrying Video file. The use of the video based Steganography can be more eligible than other multimedia files, because of its size and memory requirements [7]. We can hide a cipher text after encryption process in video. We can choose shorter key for encryption process which is not increase the size of cipher text then message size. In this process first we encrypt a text message into cipher text then we hide this cipher text into a video media. Because of video size and its memory requirement it can hide more text then other media.

1. Encrypted Message hide in Video Spatial Domain:-

Least Significant Bit approach is a most popular approach for hide in spatial domain. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover image. If we are using 24-bit colour, the amount of change will be minimal and invisible to the human eye.

For example a grid for 3 pixels of a 24 bit image can be as follows:

10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011

(Before) (After)

Now suppose we want to "hide" the following 9 bits of data : 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits underlined have been changed):

10010101 0000110**0** 11001001
1001011**1** 0000111**0** 1100101**1**
10011111 00010000 11001011

Here we can see that only some least significant bits are change during hide bits so we can hide large number of bits without less effect on visualization.

2. Encrypted Message hide in Video Frequency Domain:-

We can hide the bits of information in the DCT domain of the stego object. The hidden message is a stream of "1" and "0" giving a total number of 56 bits. The transform is applied to the image as a multiple factor of 8x8 blocks. DCT converts from spatial domain to frequency domain and message hiding in frequency domain is more robust than message hiding in spatial domain of stego object.

V. ADVANTAGE OF STEGANOGRAPHY WITH CRYPTOGRAPHY

Steganography especially combined with cryptography is a powerful tool which enables people to communicate without interferes of eavesdroppers even knowing there is a form of communication in the first place.

Cryptography can protect your data from thieves and impostors. You can encrypt the files on your hard disk so that even if your enemies gain physical access to your computer, they won't be able to access its data [10]. Cryptography can make it hard to forge email and hard to read other people's messages.

VI. CONCLUSION

In this paper we present combination of cryptography and steganography. Encryption only obscures a message's meaning, not its existence. Therefore, Steganography, a technique that hides the existence of a message, can be used to supplement encryption. This method can be used everywhere which requires transfer of sensitive data through network. It can be used to transfer the messages of RAW type security agnecies. It can be used in banks to secure account information from intruders. It can be used by companies to secure their confidential data from network.

REFERENCE

[1] Tsutomu Matsumoto, Junji Shikata, "Authenticated Encryption and Steganography in Unconditional Security Setting"
[2] Liddell and Scott's Greek-English Lexicon. Oxford University Press. (1984).
[3] Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. Handbook of Theoretical Computer Science 1. Elsevier.
[4] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.
[5] [a b c d e f g] AJ Menezes, PC van Oorschot, and SA Vanstone, Handbook of Applied Cryptography ISBN 0-8493-8523-7.
[6] en.wikipedia.org/wiki/
[7] A. Swathi, Dr. S.A.K Jilani, "Video Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5, September 2012.
[8] Khalil Challita, Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 199-208. The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).
[9] http://www.bristol.ac.uk/pace/graduation/honorary-degrees/hondeg08/cocks.html
[10] 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.
[11] Dipti Kapoor Sarmah, Neha Bajpai, "A new horizon in data security by Cryptography & Steganography", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (4) , 2010, 212-220.
[12] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography", www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 4, April 2013).