CRITICAL ENCRYPTION WITH STEGANOGRAPHY

GONDI BHARGAVESH, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING,K.L UNIVERSITY,GUNTUR,ANDHRAPRADESH,INDIA(sri274prince@gmail.com)

Abstract— Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. Steganography is often confused with cryptography because the both are used for used to protect important information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. In Steganography original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. On the other hand Cryptography basically means art of protecting information by converting it into unreadable format. Cryptography and Steganography are present in different domains of network security and often used as separate techniques to provide confidentiality and security of data. So in this paper we discuss how images can be used as a carrier for protecting the data and how encryption can be applied on the data hidden in the Stego image.

This paper will take in-depth look at this technology by introducing readers to various concepts of Steganography and Cryptography, a brief history of the above concepts and the technique in which both of the concepts can be applied for achieving confidentiality and authentication of the data.

Index Terms— Steganography, Cryptography, network security, confidentiality, security, Stego image, authentication.

1 INTRODUCTION

Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. A solution to this problem is steganography. The ancient art of hiding messages so that they are not detectable. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

Steganography is the technique of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the hidden message. It is taken from Greek word “STEGANOS” which means “Covered” and “GRAPHIE” which mean “Writing”. So, Steganography is a method of covering important information behind an image. In steganography, the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information hidden and may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image. When hiding information inside images the LSB (Least Significant Byte) method is usually used. When hiding information inside Audio files the technique usually used is low bit encoding which is somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. When only a small amount of information is hidden inside of video it generally isn’t noticeable at all however the more information that is hidden the more noticeable it becomes. So Steganography in Images is preferred. The figure below represents steganographic system. Here fE is steganographic function embedding and fE-1 is steganographic function extracting cover is the image were message is to be hidden and emb is the message that is to be hidden.

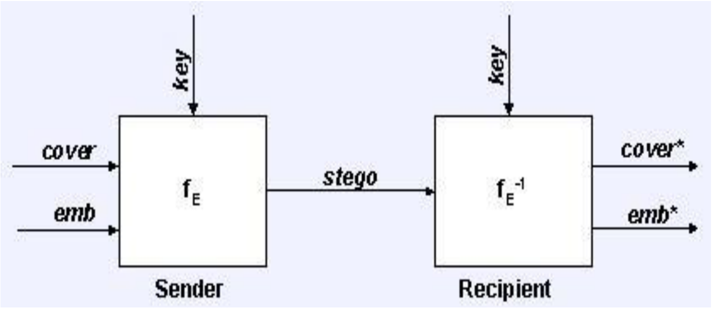

Figure: Graphical Version of the Steganographic System

The art of protecting information by transforming it into unreadable format is called Cryptography. The main feature of the Cryptography is generally the implementation of encryption and decryption techniques and involves the generation of the private key known only to the sender and receiver. Now days, cryptography has many commercial applications. However, the main purpose of the cryptography is used not only to provide confidentiality, but it can also provide solutions for other problems like: data integrity, authentication, non-repudiation etc. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver will be able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. The figure below represents conventional encryption.

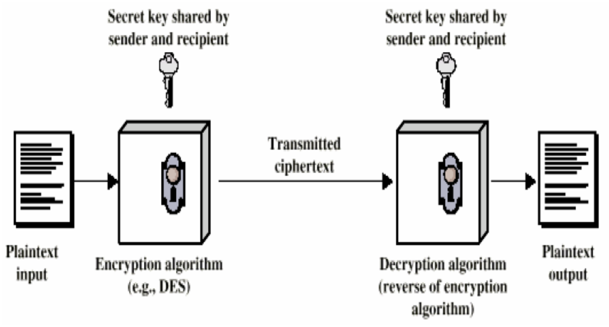
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure: Conventional encryption system

2 HISTORY OF STEGANOGRAPHY AND CRYPTOGRAPHY

2.1 Steganography

Steganography ancient origins can be traced back to 440 BC. It is believed that steganography was first practiced during the Golden Age in Greece. An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The wax was then reapplied to the wood, giving the appearance of a new, unused tablet. The resulting tablets could be innocently transported without anyone suspecting the presence of a message beneath the wax. This is the technique used by Demeratus who sent a warning about a forthcoming attack to Greece by writing it on a wooden panel and covering it in wax.

During World War 2 invisible ink was used to write information on pieces of paper so that the paper appeared to th average person as just being blank pieces of paper. In early World War 2 Steganographic technique such as invisible inks were used with much success as source of communication. Common sources for invisible inks are milk, vinegar, fruit juices and urine were used because each of these substances when heated they darken and become visible to the human eye.

2.2 Cryptography

One of the early techniques proposed was Caesar cipher technique which was proposed by Julius Caesar who enciphered his dispatches by writing D for A, E for B and so on. When Augustus Caesar ascended the throne, he changed the imperial cipher system so that C was now written for A, D for B, and so on. In modern terminology, we would say that he changed the key from *D* to *C*.

The Arabs generalized this idea to the monoalphabetic substitution, in which a keyword is used to permute the cipher alphabet. We will write the plaintext in lowercase letters and the cipher text in uppercase. But breaking ciphers of this kind is a straightforward pencil and paper puzzle. So for the reason of data security many encryption techniques emerged which provided both confidentiality and integrity.

3 CRYPTOGRAPHY AND STEGANOGRAPHY

3.1 Comparision between Cryptography and Steganography

Steganography and cryptography are closely related. Cryptography scrambles messages so it can't be understood and Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text, in steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in steganography is the stego-media. The message in steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

3.2 Combination of Cryptography and Steganography

Those who seek the ultimate in private communication can combine Cryptography and Steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

4 RELATED WORK

4.1 LSB INSERTION METHOD:

Least Significant Byte insertion method is probably the most well-known image Stenography technique. It is a common, simple approach to embed information in a graphical image file. Unfortunately, it is extremely vulnerable to attacks, such as image manipulation. A simple conversion from a GIF or BMP format to a lossy compression format such as JPEG can destroy the hidden information in the image. When applying LSB techniques to each bytes of an 8-bit image, one bit can be encoded to each pixel. Any changes in the pixel bits will be indiscernible to the human eye. The main advantage of LSB insertion is that data can be hidden in the last four least significant bits of pixel and still the human eye would be unable to notice it. Care needs to be taken in the selection of the cover image, so that changes to the data will not be visible in the stego-image.

4.2 RSA ALGORITHM:

Encrypting using RSA, we encrypt our data that is hidden in an image. Hackers cannot identify hidden data in images easily and at most they can get encrypted data from images which will not reveal any confidential information. Care should be taken during the selection of prime numbers, so that hacker will not able to reveal key to decrypt.

4.3 MD5 ALGORITHM*:*

MD5 algorithm provides data integrity. A Digital signature is sent along with encrypted data which is hidden in image. At receiver side, receiver first get data from image, decrypt it and then finds Digital signature attached behind the data and decrypts it using MD5 algorithm and compare it with original Digital signature. If they are same, data isn't tampered. Hence data integrity is maintained.

5 IMPLEMENTATION

The proposed work provides data integrity using MD5 algorithm. We create Digital Signature that is also sent along with encrypted data. At receiver side, receiver first gets data from image, decrypts it and then searches for the Digital Signature at the end of the actual data. Using MD5 hash algorithm the receiver decrypts the signature and checks whether it matches with original Digital signature. The challenge in this work was to find a way to provide confidentiality and data integrity that make man-in -middle attack difficult. Therefore, we applied an encryption using RSA algorithm and MD5 hash algorithm. The details regarding the approach are illustrated below:

- **STEP 1:**

  Here the data that is to be transmitted and the signature which is encrypted with MD5 hash algorithm are combined. The signature is encrypted with a different encryption algorithm to protect the integrity of the data. A care should be taken that the plain text and Signature are not to be encrypted with the same encryption technique.

- **STEP 2:**

  Applying RSA encryption to the whole information using sender's private key here sender and receiver generate their public and private keys using RSA algorithm. Then message bits are encrypted with sender's private key using RSA encryption **c = m^e (modulo n)**. We do this encryption to provide authentication that data is sent by intended user because intended user know his private key.

- **STEP 3:**

  Applying RSA encryption using receiver's public key here encrypted message is again encrypted with receiver's public key using RSA encryption **c = m^e (modulo n)**. We do this encryption to provide confidentiality that data is not read by any intruder without knowing private key.

- **STEP 4:**

  Using the Least Significant Byte technique the encrypted information which is in the form of text (.txt or .doc) can be hidden in the image (.jpg or .png). Another image will be produced which is similar to the previous image but the image will have the encrypted information.

- **STEP 5:**

  Then the image is to be kept in a folder and folder is to be compressed using WinRAR Achiever. For further security enhancement a security password can also be provided to the compressed folder. Then the compressed folder is again hidden in another image. The image obtained is this step is final and it is the source that is transferred to the end user.

6 ANALYSIS

6.1 USE OF RSA AND MD5 ALGORITHMS:

Two different algorithms are used for securing the data hidden in the image. The signature is encrypted with MD5 algorithm. The encrypted signature is attached to the data that is to be secured and then it is encrypted with RSA algorithm to secure the data. Even if the hacker manages to get the data then it would be of no use because it is present in encrypted format. The main reason for using two encryption techniques is that even if the hacker manages to crack the key and then morph the data then it would be easy for the person on the receiving side for identifying the change because there would be a specific change in the Digital signature. So this algorithm satisfies both confidentiality and integrity.

6.2 COMPARISION OF THE LSB AND ORGINAL IMAGE:

Compare the images shown below the Stego-image and original image can't be differentiated.

Figure representing stego image

Figure representing normal image

So if we notice there are no changes that are notable in the original-image and Stego-image. So by using LSB technique data integrity and hidden existence of the data, both can be achieved. LSB causes less degradation of data when compared to other techniques and is most commonly used technique for Steganography.

7 CONCLUSION

As steganography becomes more widely used in computing, there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. The use of benchmarking to evaluate techniques should become more common and a more standard definition of robustness is required to help overcome this. For a system to be considered robust it should have the following properties:

a) The quality of the media should not noticeably degrade upon addition of a secret data.

b) Secret data should be undetectable without secret knowledge, typically the key.

c) If multiple data are present they should not interfere with each other.

d) The secret data should survive attacks that don't degrade the perceived quality of the work.

This work presents a scheme that can transmit large quantities of secret information and provide secure communication between two communication parties. Both steganography and cryptography can be woven into this scheme to make the detection more complicated. Any kind of text data can be employed as secret message. The secret message employing the concept of steganography is sent over the network .In addition, the proposed procedure is simple and easy to implement. Also, the developed system has many practical, personal and militaristic applications for both point-to-point and point-to multi-point communications

REFERENCES

1) Aravind Kumar and Km. Pooja "Steganography- A Data Hiding Technique" in 2010 International Journal of Computer Applications.

2) Deepali "Steganography With Data Integrity" in International Journal Of Computational Engineering Research.

3) Nedal M. S. Kafri1 and Hani Y. Suleiman Bit-4 of Frequency Domain-DCT Steganography Technique in 2009 IEEE.

4) Sashikala Channali and Ajay Jadav "Steganography an Art Of Hiding Data" in International Journal of Computer Science and Engineering.