ISSN:0975-9646
Deepa S et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,3905-3909

A Novel Method for Secured Communication by Merging Steganography with Encryption Technique

Deepa S[1], Umarani R[2]

[1]*Department of Computer Science, Periyar University College of Arts & Science, Mettur Dam, Tamilnadu, India*
[2]*Department of Computer Science, Sri Sarada College for Women, Salem, Tamilnadu, India*

***Abstract*-- A security solution in communication network is a great demand. Information security deals with confidentiality, integrity and availability of data. Information hiding technique is a new kind of secret communication technology. Steganography, derived from Greek, literally means "covered writing". Steganography is the process of hiding a secret message within an ordinary message & extracting it at its destination. Anyone else viewing the message will fail to know that it has hidden data. Cryptography, derived from a Greek word literally means "secret writing". Cryptography is the process of securing a data by encryption. It is the science of using mathematics to encrypt and decrypt data. The scope of this paper is to achieve higher level of secured communication, by combining steganography and cryptography properties in such a way to make it harder for a steganalyst to retrieve the plain text of the secret message from a stego-object.**

***Keywords*-- Steganography, Steganalysis, Image Steganography, LSB, Cryptography**

I. FRAMEWORK OF STEGANOGRAPHY

Hiding information into a media requires following elements: The cover media that will hold the hidden data, the secret message, may be plain text, cipher text or any type of data, the stego function, an optional stego-key or password may be used to hide and unhide the message.

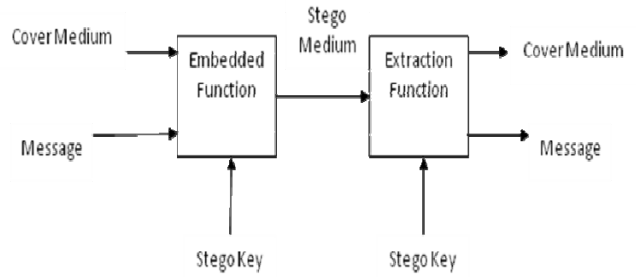

Fig 1: Steganography Flow

Cover-medium + hidden-data + stego-key = stego-medium

II. CLASSIFICATION OF STEGANOGRAPHY

There are only three ways to hide a digital message in a digital cover media.

1) *Injection*: The secret message is directly embedded in the host medium.

2) *Substitution:* Normal data is replaced or substituted with the secret data.

3) *Propagation:* A cover is generated for the sole purpose of concealing a secret message. It Create a file with the intent of hiding information.

III. CATEGORIES OF STEGANOGRAPHY

Steganography Techniques can be categorised into the following:

A. Substitution Systems

Replace redundant or unneeded bits of a cover with the bits from the secret message.

B. Transform Domain Techniques

Embed secret information in significant areas of the cover object.

C. Spread Spectrum Techniques

Means of transmission in which the signal occupies a bandwidth in excess of the minimum necessary to send the information.

D. Statistical Methods

Encode information by changing several statistical properties of a cover and use hypothesis testing in the extraction process.

E. Distortion Techniques

It Create a change in a cover object to hide information. Some steganography applications generate a digital object, only for the purpose of being a cover for secret communication.

IV. TYPES OF STEGANOGRAPHY

The two types of Steganography are

A. Linguistic Steganography

Any form of steganography that uses language in the cover. Two most basic categories are Open codes – the openly readable text is mostly well constructed. Text semagrams – works with graphical modification of text.

B. Technical Steganography

Technical steganography is a method where a tool, a device or a method is used to conceal the message.

V. EMBEDDING METHODS

The embedding methods of steganography to hide a message:

1) *Least Significant Bit:* It is a Substitution method of steganography where the right most bit in a binary notation is replaced with a bit from the embedded message.

2) *Transform Techniques:* Embeds the secret data in the cover during the transformation process.

3) *Spread-spectrum Encoding:* Method of hiding a small or narrow band signal, a message, in a larger cover signal.

4) *Perceptual Masking:* Occurs when one signal or sound becomes imperceptible to the observer because of the presence of another signal.

VI. STEGANOGRAPHY APPLIED TO MEDIA

The methods of Steganography are quite varied to different media.

A. Still Images: Pictures

LSB insertion and spread spectrum techniques are commonly used. Texture block is another method that uses low-bit rate data hiding and is accomplished by copying a region from a random texture pattern in a picture to an area of similar texture resulting in a pair of identically "textured" regions in a picture.

B. Moving Images: Video

Steganography, when applied to a video file such as an .avi or .mpg, typically uses Discrete Cosine Transform (DCT) manipulation, meaning that as the video is compressed or decompressed, secret data can be added during the transformation process.

C. Audio Files

The following are various audio file methods:

1) *LSB Insertion:* The bit with the least impact on the binary data is replaced with a bit from the embedded message.

2) *Differential Phase Variation:* The sound file is divided into blocks, and the initial phase of the sound file is modified with the secret message, preserving the following relative phase shifts. This is an effective method given it has a low signal-to-noise ratio.

3) *Spread spectrum schemes:* The method of hiding a small- or narrow-band signal, the secret message, in a large- or wide-band cover.

4) *Adding echo to the audio signal:* A slight echo is added to the signal using two different delays to encode the 1 and 0 bits. The echo is too slight to be perceived by the human ear.

D. Text Files

Three methods exist for text files:

- Open-space - The use of white space, between words or sentences, to hide data.
- Syntactic - Uses modification of the word order or punctuation to hide a message.
- Semantic - Uses synonyms to encode a secret message.
-

E. Steganographic File Systems

A steganographic file system is a method of storing files in such a way that it encrypts data and hides it so well that it can't be proven it's there.

A steganographic file system can

1) Hide users' documents in other seemingly random files.

2) Allow the owner to give names and passwords for some files while keeping others secret.

3) Behave like a second layer of secrecy. Encrypted files are out in the open and visible, but not understandable. Stego files aren't even visible, and an outsider can't look for files that "aren't there."

F. Hiding in Disk Space

Three main methods exist for hiding data in disk space: unused sectors, hidden partitions, and slack space.

1) *Unused Sectors:* Similar to the method used in the section, "Steganographic File Systems," tools that hide data in unused sectors, such as S-tools, will take the file and spread the bits out throughout the free space on the floppy. Though undetectable in the normal Windows viewer, the file is still there.

2) *Hidden Partitions:* A hidden partition on a hard drive is another way of hiding information, sometimes large amounts, in plain sight. This method isn't terribly robust since a close examination of the hard drive, independent of the operating system, will usually reveal that the drive is bigger than the OS is letting on.

3) *Slack Space:* Slack space is a type of unused space in a disk. Even if the actual data being stored requires less storage than the cluster size, an entire cluster is reserved for the file. The unused space is called the *slack space*. If minimum space allocated is 32 kb and the file is 6 kb, then 26 kb is left unused and considered unavailable by the operating system. This unused space (slack space) could be used to hide information without showing up in any directory or file system.

VII. PRINCIPLES OF STEGANOGRAPHY

The three core principles that are used to measure the effectiveness of given steganography technique are

1) *Amount of Data:* Steganography is all about hiding as much information within a file as possible.

2) *Ease of Detection:* When hiding information, we want to make sure it is very difficult for someone to detect.

3) *Ease of Removal:* In some situations, even if someone cannot detect whether data is hidden within a file, they can still try to remove any data.

VIII. ATTACKS

Steganalysis is an attempt to detect the existence of hidden information. Attacks available to steganlayst are

Stego-only Attack – Only stego media is available for analysis.

Known-cover Attack – The original cover media and stego media both are available for analysis.

Known-message Attack – Hidden message and the stego medium are available.

Chosen-stego Attack – The steganography tool (algorithm) and stego-object are known.

Chosen-message Attack – The steganalyst generates a stego-object using some steganography tool or algorithm of a chosen message.

Known-stego Attack – The cover media, stego media as well as the steganography tool or algorithm, are known.

IX. DETECTION

The detection methods are

Statistical Tests – This test can reveal that an image has been modified by determining that its statistical properties deviate from a norm

Stegdetect – It is an automated tool for detecting steganographic content in images.

Stegbreak – It is a program that uses dictionary guessing to break the encoding password.

Visible Noise – Some images may become quite degraded with even small amounts of embedded information. This "visible noise" will give away the existence of hidden information.

Appended Spaces & Invisible Characters – This is a technique of hiding data in spaces within text.

Color Palettes – The palette modification creates a detectable steganography signature.

TCP/IP Packet Capture – To determine where a forged packet originated is to put a sniffer on the inbound side of the server.

Repetitive Patterns (Patchwork) – The Patchwork algorithm allows for the detection of a single, specific bit in an image.

X. IMAGE STEGANOGRAPHY

The most cover media used for steganography is image. The reason is that the large amount of redundant data present in the images that can be easily altered to hide secret messages inside them. Work performed on steganography in image can be classified into 3 major groups:

1) *Temporal Method:* The data is added to quantities of luminosity of pixels in the image. (Ex: LSB)

2) *Spatial Domain Method:* It is the calculation of conversion of frequency of the image and adding information in the frequency domain. (Ex: DFT, DCT)

3) *Fractal Method:* In this method, blocks of the image that contain repeated patterns are selected and information is saved in them.

A good technique of image steganography aims at three aspects

- *Capacity* - The maximum data that can be stored inside cover image.
- Transparency - Visual quality of stego image after data hiding.
- *Robustness* - Security against attacks.

A computer image is an array of points called pixels (which are represented as light intensity). Digital images are stored in either 8-bit or 24-bit pixels. For large file size image compression techniques are used. Two forms of compression are

- *Lossy compression* - Provides high compression rates, but at the expense of data image integrity loss (Ex: JPEG).
- *Lossless compression* - Does not lose image integrity. (Ex: BMP, GIF).

A common image might be 640 * 480 pixels and use 256 colors (8 bits per pixel). In an 8-bit image, each pixel is represented by 8 bits as 11001101. The 4 bits to the left are MSB and 4 bits to the right are LSB. Changes to the MSB will result in a drastic change in the color and the image quality, while changes in the LSB will have minimum impact. So hiding data in any 2 bits of LSB, the human eye will not detect it. For ex., if the bit pattern 11001101 is changed to 11001100 it will look the same. So steganography uses these LSB's to store the secret data.

A. MODIFICATION OF LSB OF A COVER IMAGE IN 'BITMAP' FORMAT

In this method binary equivalent of the message (to be hidden) is distributed among the LSB of each pixel. For Ex. To hide the character 'A' into an 8-bit color image eight consecutive pixels from top let corner of the image are taken.

The equivalent binary bit pattern of those pixels may be 00100111 11101001 11001000 00100111 11001000 11101001 11001000 00100111

Each bit of binary equivalence of letter 'A' i.e. 01100101 are copied serially (from the left hand side) to the LSB of equivalent binary patter of pixels, results with the bit pattern 00100111 11101001 11001001 00100111 11001000 11101001 00110111 00100111

XI CRYPTOGRAPHY

Cryptography is the process of encrypting the data.

Encryption is defined as the process of transformation of plaintext into an unreadable form (cipher text) so that the original plaintext cannot be obtained without using the inverse decryption process.

In Symmetric cipher model the encryption algorithm performs various substitutions and transformations on the plaintext.

Decryption returns the information to readable form with the help of a key provided by the encryption process. It takes the cipher text and the secret key and produces the original plaintext.

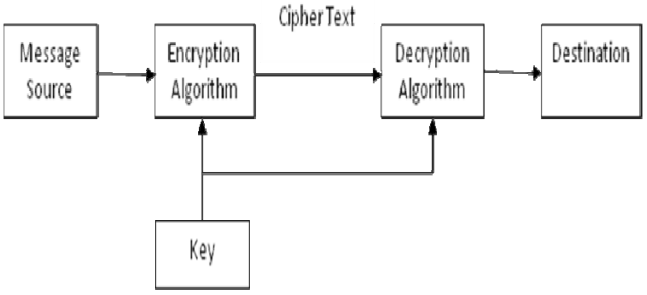

Fig 2: Crytographic Flow

The process of attempting to break a cryptosystem is called cryptanalysis.

XII METHODOLOGY

A blend of the two technologies cryptography and steganography can provide a high level security system.

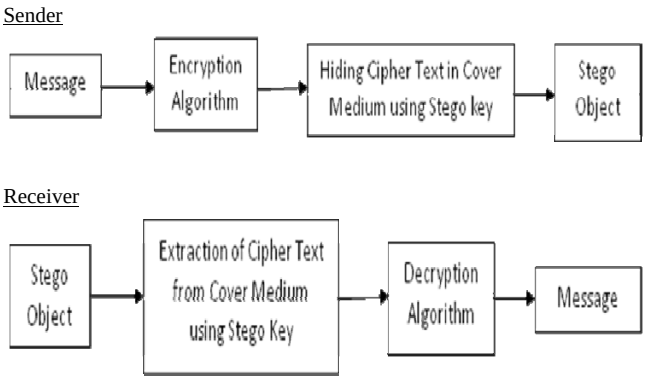

Fig 3: Secure Communication

Cryptography technique to be used is Substitution by means of XOR and NOT operation.

Steganography technique to be used to hide data is Least Significant Bit (LSB).

The cover medium considered is image.

A. Substitution Technique

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbol.

B. Least Significant Bit

Substitution method of steganography where the right most bit in a binary notation is replaced with a bit from the embedded message.

C. Image

A computer image is an array of points called pixels (which are represented as light intensity).

Digital images are stored in either 8-bit or 24-bit pixels.

A usual digital image of 640 * 480 pixels can approximately hide 300KB data & high resolution image can approximately hide 2.3 MB data.

In an 8-bit image, each pixel is represented by 8 bits as 11001101.

In this method binary equivalent of the message (to be hidden) is distributed among the LSB of each pixel.

XIII PROPOSED METHOD

A. Embed a Secret Message in an Image

1) Read the data character wise

2) Convert each character into its equivalent ASCII code

3) ASCII code is converted to binary and XOR ed with 01011110 (key value)

4) To the result NOT operation is performed

5) The stream of 8 bits is embedded into LSB of each pixel of the image

B. Extract the Message from the image

1) Extract LSB of the pixels of the stego image

2) Perform NOT operation to the bits

3) The resultant bits are XOR ed with the same key as of encryption

4) Finally decrypt each 8 bits to ASCII code and then generate the equivalent ASCII character

XIV. CONCLUSION

Security has always been important in electronic applications. The key advantage of stego is the ability to communicate without anyone knowing the true content of communication. Steganography techniques used to hide secret messages in stego objects are explained. The Steganography methods applied to different media are discussed. Steganalysis is the technique to detect steganography or defeat steganography. Possible attacks & detection are analyzed. The image steganography is most widely used because of its large redundant data. Least Significant Bit is the simplest way to embed information in an image file.

In proposed method a message is encrypted before being hidden in order to achieve a better level of secrecy. It achieves a very high level of confidentiality because a steganalyst will not be able to recover the plain text even if he suspects the presence of hidden information in stego-object.

Further Proceedings is to implement the proposed methodology and to build a new system that can withstand the attacks of cryptanalyst and steganalayst. Also experiment using different algorithm for encryption and decryption and test this method for different number of cover images.

REFERENCES

[1]. William Stallings, *Cryptography and Network Security*, Principles and Practices, Fourth Edition, Pearson Prentice Hall.

[2]. Stefan Katzenbeisser and Fabien A.P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, 2000 citation.

[3]. Greg Kipper, *Investigator Guide to Steganography*, Auebach publications, 2004 citation.

[4]. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, *Digital Watermarking and Steganography*, Second edition.

[5]. Shiguo Lian and Yan Zhang, *Handbook of Research on Secure Multimedia Distribution*, IGI Global, 2009 citation.

[6]. Jack Wiles and Anthony Reyes, *Cybercrime and Digital Forensics*, Syngress Publishing, 2007 citation.

[7]. Mohammed Abbas Fadhil, "A Novel Steganography-Cryptography System", WCECS Vol I, October 2010, USA.

[8]. Mohammed Abbas Fadhil Al-Husainy, "A new image Steganography Based on Decimal-Digits Representation", Computer and Information Science Vol. 4, No.6, Nov 2011.

[9]. Sujay Narayana and Gaurav Prasad, "Two New Approaches for Secured Image Steganography using Cryptographic Techniques and Type Conversions", Signal & Image Processing: An International Journal (SIPIJ) Vol.1, No.2, December 2010.

[10]. Er. Prajaya Talwar, "Implementation of Image Steganography using Least Significant Bit Insertion Technique", IJMIE Vol.1. Issue 6, Nov 2011.

[11]. R. Vendateswaran and Dr. V. Sundaram, "Novel information security model using proposed e-cipher method with combining the features of cryptic-steganography", IJCSI, Vol.8. Issue 5, No.2, September 2011.

[12]. C. Parthasarathy, G. Ramesh kumar, Dr. S.K. Srivatsa, "Secure Communication with Flipping Substitute Permutation Algorithm for Electronic Copy right Management System", IJCSIS, Vol9. No.5, May 2011.

[13]. Rajkumar Yadav, "Analysis of Various Image Steganography Techniques Based Upon PSNR Metri", International Journal of P2P Network Trends and Technology, Vol 1 Issue 2 – 2011.

[14]. Kamaldeep, "Relative Antropy Based Analysis of Image Steganography Techniques", International Journal of P2P Network Trends and Technology, Vol 1 Issue 3 – 2011.