Advanced Computing: An International Journal (ACIJ), Vol.4, No.1, January 2013

TWO PHASE CLANDESTAIN IMAGE ENCRYPTION

V Hemanth[1,2], R Praveen Kumar[2]

[1] Assistant Professor
[2] Department of Computer Science and Engineering,
Sree Vidyanikethan Engineering College, Tirupati
{vhemanth87,praveenkumar.r07}@gmail.com

Abstract

In today's internet world is full of data steals and hackers. So, there is a essential to design a system that assists the internet users to interchange their secret and private data safely across the web. Information-hiding process in a Steganography system starts by identifying medium's redundant bits. The encryption process creates a stego medium by replacing these redundant bits with data from the hidden message. So, we propose a method for encrypting the image, which has two phases. In the first phase, Perform Circular Shift Operations on the image pixels and the number of rotations have been calculated based on the length of the password. In the second phase, the first phase has undergone some bitwise operations with a carriage image, by doing this; breaking of the cipher text is difficult.

1 Introduction

In today's information age, information sharing and transfer have increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat. Cryptography involves converting a message text into an unreadable cipher [7]. On the other hand, steganography embeds the message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an insecure communication channel and are vulnerable to intruder attacks [6]. Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion.

If we consider any organization attacks can happen in two ways that is "insider attacks", and "outsider attacks".

Insider attacks, can be initiated by authorized persons try to access other authorized person details that is within the organization.

Outsiders Attacks, can be initiated by unauthorized persons try to access other authorized person details that is different organizations.

Attacks are mainly classified into two types.

1. Active Attack
2. Passive Attack

DOI : 10.5121/acij.2013.4104

Active attacks, which the attacker changes the communication. He may create, forge, alter, replace, block or reroute messages [2]. Passive Attack, which the attacker only eavesdrops; he may read messages he is not supposed to see, but he does not alter messages [2].

Wire trapping, in olden days the communication media between two far users are done by telecommunication. The wiretapping is also called as telephone trapping, used for monitoring of telephone and Internet conversations by adversaries. Active wiretapping alters or otherwise affects it while passive wiretapping monitors or records the traffic [4].

Masquerade, is an attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain privileges than they are authorized. The authentication of a user's identity is based on a combination of something the user knows (e.g., a secret password), a physiological or learned characteristic of the user (e.g., a fingerprint, retinal pattern, hand geometry, keystroke rhythm, or voice), and a token the user possesses (e.g., a magnetic-stripe card, smart card, or metal key). Anybody with the correct combination of identification characteristics can masquerade as another individual.

Playback is another type of masquerade, in which user or computer responses or initiations of transactions are sneakily recorded and played back to the computer as though they came from the user. This fraud was curtailed when banks installed controls that placed encrypted message sequence numbers, times, and dates into each transmitted transaction and command.

Playback was suggested as a means of robbing ATMs by repeating cash dispensing commands to the machines through a wiretap. Different methodologies have been designed to transmit the data in secure mode. Apart from steganography and cryptography now a day's visual cryptography is placing a major role in transmitting the secret data [3].

In the section 2, discussed about the brief introduction about steganography, section 3, the algorithms of the proposed technique have been discussed. In section 4 the process of the technique has been explained and finally in section 5 and 6, results and the conclusion has been discussed respectively.

2 Steganography

Steganography is derived from Steganos (Greek word), which mean "covered" or "secret" and –graphy mean "writing" or "drawing". Therefore, steganography means, embedding secret information into the cover image. Steganography means concealing the information within the cover image. While communication if the message which is just encrypted is sent through covert channel, it will be easier to the intruder to decrypt the message. To avoid the intruder to decrypt the data, the information which is encrypted will be embedded into a image [6].

The main aim of Steganography, is to interchange messages secretly the complete information between sender and receiver without the knowledge of adversaries. Steganography method has failed, because when the carrier medium suspected by someone.

In Steganography there are different techniques are available to hide the secret information in an image. In the images the different representations are available. They are binary images, RGB images, Gray scale images etc. The images can be of different formats like jpeg, jpg, gif,bmp,tif etc. Large range of different images are available to implement Steganography. To implement different techniques on images first the image should be converted into pixel format, which is arranged in the form of a matrix. Pixel values are arranged in the matrix in r × c format. More the value of r and c clarity of the image will increase. The histogram is another way of representing the image. After and before embedding the secret information into the image there should be not much different in the histogram. If the variation in the histogram is more in cover image and stego image than the techniques used for embedding is not a good one.

The Steganography mainly concentrates on Carrier image, secret information and a Password. When the password is embedded into the image, that image is named as carrier image. The input image called as cover image is used for hiding the information.

The below diagram explains the basic model of the steganography, the message which has to be communicated can be in the form of plain text or image etc. in any format. The sender who wants to communicate will be embedding the message into an image and sends that image for communication. To have a secret and secure communication the plain text is now converted into a non- readable format and then communicated, this process of converting is called as encryption. To retrieve back the original plain text, decryption method has to be applied. In this process a key or a password places a major role in the process. In the diagram shown below a stego key is used and it is also be called as a password. By exchanging the key (password) the receiver can only be able to get back the original message. The secret message which is embedded in the cover object is further converted into stego- object.

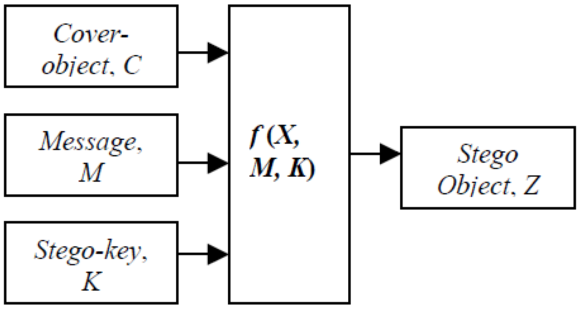


Figure 1 Basic Steganography Model

To provide secret communication between the sender and the receiver cryptography and steganography techniques are used. The main fact is that steganography and cryptography are not the same. Cryptography will be just converting the message into an unreadable format, and the untrusted third party can be able to know that that some communication is happening between the users. In steganography for an intruders will not be able to recognize that the existence of the message. By combining both cryptography and steganography, the intruder can be made confused. In cryptography by breaking the secret message, the original message can be retrieved back, but in steganography first to identify the message is a major task so by combining both the process the heights of security will be increased.

In cryptography, the plain text will be transformed into an unreadable format using a secret key, in cryptography the secrecy lies not in the algorithm but it lies in the key, because the algorithm is available publicly but not the key. Basically, cryptography has the ability of communicating the information between users in such a way that it is difficult to read the message. Cryptography provides confirmation for verifying the uniqueness of something or someone.

Steganography will not alter or change the secret message but it hides the secret message in a cover- image and the image helps it from by recognizing the secret information from the intruder. The existence of the message can be seen in cryptography but in steganography it has difficult identified the existence of the secret message. By combining both the process it will be difficult for an intruder to get back the original message. If the intruder is able to get the message from the image, then he has to apply cryptography to break the message to get the original message.

In cryptography, there are so many algorithms to encrypt the message like RSA, diffie hellman etc. in all this process the key places a major role. Converting the plain text into unreadable format is called as cipher text. Stream ciphers and block ciphers are available to convert the message into cipher text. In steganography, for embedding the message into an image there are so many techniques are available and the techniques have been explained in the section 2.1 in detail.

2.1 Steganography Techniques

Steganography plays a major role in securing the secret message in communicating with users. For embedding the message in a image there are so many techniques are available, some of the techniques are given below:

(i) Least significant bit insertion (LSB)

(ii) Masking and filtering

(iii) Transform techniques

Least significant bit (LSB) insertion is to embed the bits in an image file. It embeds the message bits directly into the LSB plane of the cover-image in a sequence. The resultant image is equivalent to cover image, the human eye cannot able to detect.

Masking and filtering techniques, it restricted to 24 bits and grayscale images, hide information by marking an image, it's similar to paper watermarking. It performs analysis of an image, it embeds the secret information in significant areas so that the hidden secret information is more important to the cover image than just hiding it in the noise level.

Transform techniques embed the message by using coefficients in a transform domain, that is the Discrete Cosine Transform, Discrete Fourier Transform, or Wavelet Transform. Transformation technique hides the secret information in specific areas of the cover-image, which make them robust to attack. Transformations applied over the image or to block throughout the image, or other variants.

3 Proposed algorithm

3.1 Encryption Algorithm:

Step 1: select the secret image and password

Step 2: perform circular shift operations on input image based on the formulae
Step 3: The resultant intermediate image goes to the next phase
Step4: Generate carrier image based on the input password
Step5: EXOR intermediate image and carrier image the resultant image is Encrypted image.

3.2 Decryption Algoritham:
Step 1: select the encrypted image and carrier image
Step 2: perform EXOR operation on encrypted image and carrier image.
Step 3: Intermediate image is generated.
Step 4: generate password using input carrier image
Step 5: perform circular shift operation on intermediate image using formulae

4 Proposed Technique

In the above technique which we have discussed is implemented for different images and passwords. For better quality of encryption, minimum effective length of the password (Ns) should be 4 characters.

4.1 Encryption Algorithm:

In this model, image is encrypted in two phases. In the first phase Circular shift operation [1] is performed on the input image. In the second phase, the input image is the output of the first phase, with the help of the carrier image and performs XOR operations on both the images, the subsequent image is randomized comparative to the input image.

In the first phase the inputs are the input image and a password. The input image is converted into its corresponding pixel decimal values and each pixel value is furthermore converted into 8 bit binary blocks. Now, Perform Right Circular Shift (RCS) operations on the eight bit block and perform Left Circular Shift (LCS) on the shifted bits [1]. Consider the password of minimum length is four characters and a maximum of fifteen characters. The number of LCS and RCS rotations on the bits is calculated using the formulae given below:

$$Ns = Lp \bmod P \qquad (1)$$

Where Ns be the number of shifts, Lp be the length of the password and P is a prime.

Assume Ns=4, Consider one of the pixel values from the input image and convert the pixel into its corresponding eight bit binary blocks. The bits are [B1 B2 B3 B4 B5 B6 B7 B8].

Pin(x,y)=[B1 B2 B3 B4 B5 B6 B7 B8]

Where Pin(x,y) be the input pixel value and x, y are the coordinates of the image.

On these bits perform four times LCS operation, After RCS □ [B5 B6 B7 B8 B1 B2 B3 B4]. When RCS operation is performed the bits are [B5 B6 B7 B8].

On the above 4 bits perform LCS operation times. Then the resultant of the LCS operation is [B7 B8 B5 B6].

After Performing LCS and RCS operation on the eight bit pixel value the resultant binary block is:

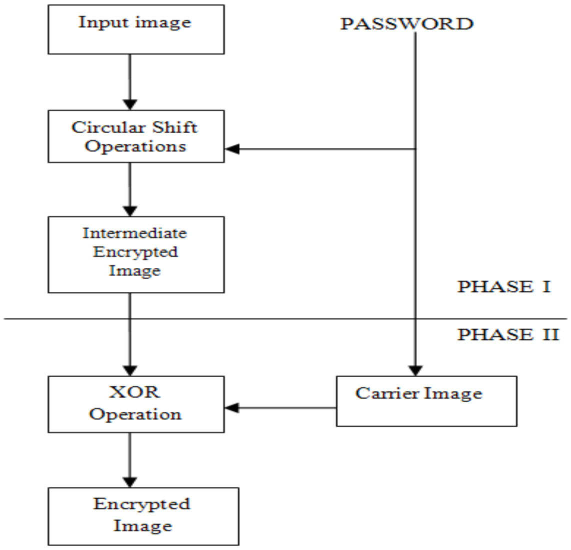
Pout(x, y) = [B7 B8 B5 B6 B1 B2 B3 B4]

Where, Pout(x, y) be the first phase output pixel value.

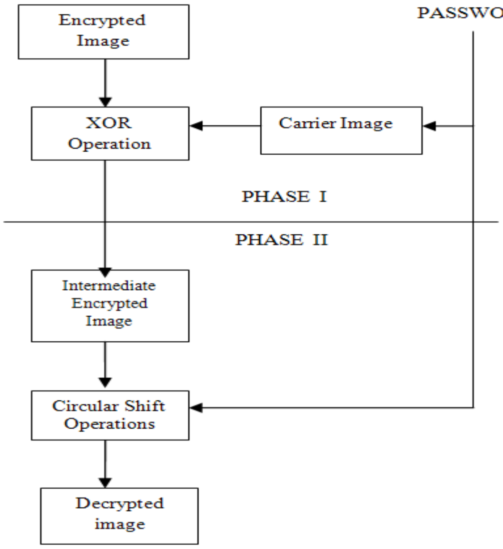
Convert each and every pixel using above method and the new pixel values are replaced with the old pixel values. By doing this an intermediate encrypted image has been generated.

In Second phase, a carriage image is generated from the password which has been given as input in the first phase. The ASCII value of each character of the password is arranged in a matrix, such a way that the matrix size and the input image size, both should be equal. Entering the ASCII values of the password in that matrix repeats until the entire matrix is filled to generate a carrier image which should be equal to the size of the input image. Bitwise exclusive OR operation is applied on the intermediate encrypted image generated in the first phase with the carrier image. By performing the XOR operation final the encrypted image has been generated.

4.2 Flow chart for Encryption Process:



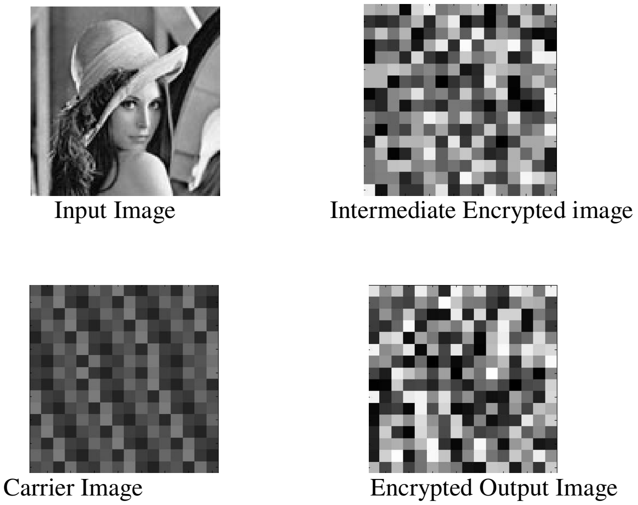
4.3 Flow chart for Decryption Process:



5 Results and Discussions

In the above technique which we have discussed is implemented for different images and passwords. For the good quality of encryption, minimum effective length of the password (Ns) should be 4 characters.

5.1 Results of encryption Process:



Phase I:

Input Image Intermediate Encrypted image

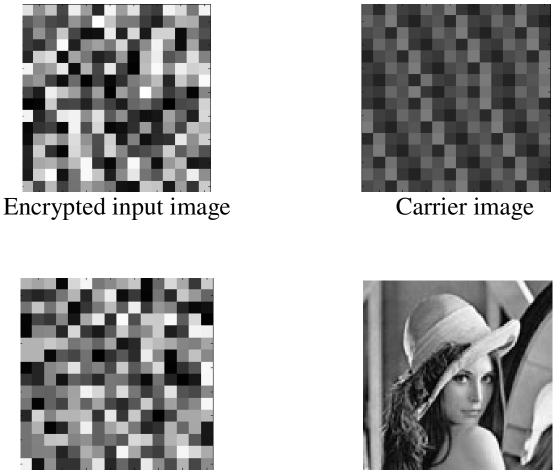
Phase II:

Carrier Image Encrypted Output Image

Figure 2: Encryption Results

While choosing the password care should be taken. The password should not contain the same characters .The password should contain minimum of four characters in which, at least one uppercase letter, one lower case letter, one special symbol and one numeric value [5]. Here we have taken the password as “V*r@8hP|7#K”.

5.2 Results for decryption Process:



Phase I:

Encrypted input image

Carrier image

Phase II:

Intermediate Decrypted image

Decrypted image

Figure 3: Decryption Results

5.3 Image analysis by using Histograms:

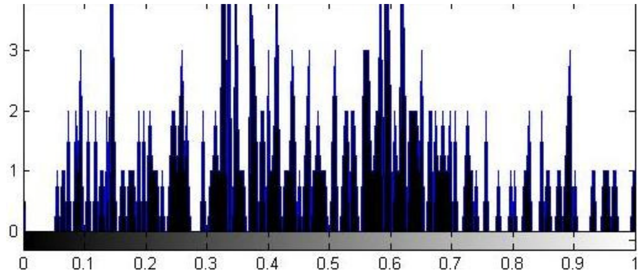


Figure 4: Histogram for input image

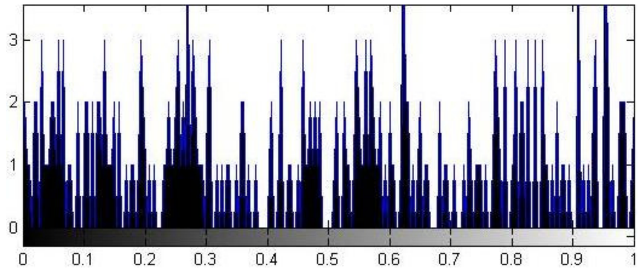


Figure 5: Histogram for output image

Histogram acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. By looking at the histogram for a specific image a viewer will be able to judge the entire tonal distribution at a glance. Comparing the input image histogram with the output image histogram, the pixel values are more randomized tonal distributed.

6 Conclusion

The proposed scheme, like two phase clandestine image encryption technique in stegnography is designed for encrypting a message by using a strong short length password. By introducing the second phase the steganalysis has become much more complex. By Introducing the carrier image which is generated from the password made the encryption process secure. The decryption process is quite difficult without the help of the carrier image. Without the knowledge of the password the intruder cannot generate the carriage image, so the decryption process is much more difficult.

References

1. Circular Shift, http://en.wikipedia.org/wiki/Circular_shift

2. Attack, https://www.owasp.org/index.php/Man-in-the-middle_attack

3. Robert F. Erbacher, Shashi Prakash, Chet Claar, Jason Couraud, "Intrusion Detection: Detecting Masquerade Attacks Using UNIX Command Lines," Proceedings of the 6th Security Conference, Las Vegas, NV, April 2007.

4. Rajaraman V. and A. Thangaraj, "Known-plaintext Attack on the Binary Symmetric Wiretap Channel," IEEE Globecom Physical Layer Security (PLS) Workshop, Dec 9, 2011

5. StrongPasswords,http://technet.microsoft.com/en-us/library/cc756109%28v=ws.10%29.aspx

6. Steganography, en.wikipedia.org/wiki/Steganography

7. Cryptography, www.cryptographyworld.com/