IOSR Journal of Engineering (IOSRJEN)
ISSN: 2250-3021 Volume 2, Issue 7(July 2012), PP 34-37
www.iosrjen.org

A Symmetric Key Based Steganography Algorithm for Secured Data Transfer

Sandipan Debnath[1,] Sudipta Kumar Dutta[2,] Mrinmoy Ghosh[3,] Anupam Mondal[4]
[1]*M.Tech (Computer Science & Engineering) Department of Computer Science, JIS College of Engineering, kalyani, Nadia- 741235*
[2]*M.Tech (Computer Science & Engineering) Department of Computer Science, JIS College of Engineering, kalyani, Nadia- 741235*
[3]*M.Tech (Computer Science & Engineering) Department of Computer Science, JIS College of Engineering, kalyani, Nadia- 741235*
[4]*Assistant Professor M.Tech (Computer Science & Engineering) Department of Computer Science, JIS College of Engineering, kalyani, Nadia- 741235*

ABSTRACT : - *Steganography is the art of hiding information efficiently into another media. It serves as a better way of securing message than cryptography which only conceals the content of the information. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. So the hidden message is difficult to detect without retrieval. In the recent years, we have plenty of security tools which are developed to protect the transmission of multimedia objects. But approaches for the security of text messages are comparatively less. In this paper, a new steganographic approach is proposed which imposes the concept of secrecy over privacy for text messages.*
Keywords: *- Steganography, encryption, decryption*

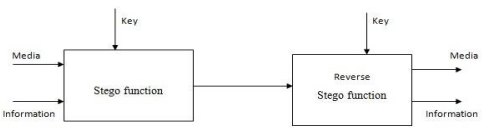
I. INTRODUCTION

In this paper we are mainly concern the data security based on Steganography concept. Already we are looking several types of different data hiding mechanism, but in this paper we are trying to design a new steganography concept with minimum complexity. Data hiding is one of the important part of cryptography, where basic concept of cryptography is based on append approach with original data and a key. But in this paper we are not interested with the basic cryptography concept. Already we are looking several different types of steganography approach based on image , audio and video. Here we are considering the data hiding mechanism within an image by using a new technique. By using this technique we are ensuring the transmission security by means of complicated manipulation over the actual information regarding the unauthentic access at the time of transmission from sender to receiver end. In this paper we are introducing our new steganography method named as, "Generation of Integrated Pictorial Information (GIPI)".

II. BACKGROUND:

For transferring a confidential data from sender to receiver end several different types of mechanisms are present. Now a days we are mainly concern different types of encryption and decryption algorithm (RSA, DES, IDEA, MD5 etc.) for sending original information from sender to receiver end. Steganography is another important approach, by which we can send information from sender to receiver end as hidden data. Already we are using so many numbers of steganography technique like image based steganography with bitmap image, LSB technique etc.In this paper, we are mainly concern secure data transfer by using combination of cryptography(symmetric key) and image steganography. We are applying here the stegofunction and key for secure data transfer. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message.

Hiding information into a media requires following elements [1]:



III. GIPI(Generation of Integrated Pictorial Information)

TECHNIQUE:

At first we are considering an image, where we can encrypt the original information. In this paper the original information first convert to ASCII value character wise, and calculate the length of information. If the information length is equal to 8 then we convert those ASCII value to octal representation, otherwise first translate the information length to multiple of 8, and then we apply the above mentioned technique. The initial gray scale image first convert to binary image and then decompose this image based on the length of the information. And merge the original information into the decomposed matrices by the following algorithm. Now we are sending this image and a key (dimension of decomposed matrix) towards the receiver end. Follow the reverse technique to decompose the image matrix received at the receiver end. And find the original information by the following algorithm.

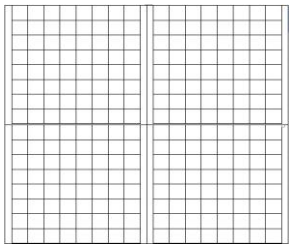
IV. Algorithm

1.1. Encryption Technique:

Step 1: Choose a block of information.
Step 2: Calculate the number of character along with space and store it in the variable I.
Step 3: Convert the total information into equivalent binary representation.
Step 4: Choose a gray scale image and convert it into binary image.
Step 5: if I is less than or equal to 8
Then the binary image will be completely logically decomposed into some 8x8 matrix blocks.Else
Chose a variable L where $L=2^n$ where $n>3$.
Calculate the specific value of L which is either exactly I or nearest greater than I and similarly logically decompose the binary image into some L x L matrix blocks completely.
Step 6: Convert the existing bit representation of each block of information to L bit.
Step 7: Put each first bit of every block of binary information into the first row of first decomposed block matrix sequentially.
Similarly put 2^{nd} bit of each block of information into 1^{st} row of 2^{nd} decomposed block matrix sequentially.
This process will be iterated until reaching to the last bit of each block of binary information.
Step 8: Convert the entire changed binary image to gray scale image.
Step 9: Forward this gray scale image along with the unique dimension of each logical decomposed matrix block to the receiver.

4.2 Decryption Technique:

Step 1: Convert the gray scale image to binary image.
Step 2: Logically decompose the binary image into some square matrix blocks completely, the unique dimension of those are forwarded by sender, say D.
Step 3: Construct a new matrix M, dimension of which is D.
Step 4: 1^{st} row of M contains the 1^{st} row of 1^{st} logical decomposed matrix into that binary image.
Similarly 2^{nd} row of M contains the 1^{st} row of 2^{nd} logical decomposed matrix into that binary image.
This process will be iterated until reaching to the D^{th} decomposed matrix.
Step 5: Retrieve the 1^{st} column of M.
Step 6: Convert the binary representation into equivalent decimal form.
Step 7: If the decimal no. is zero Then discard the no. Else Put the decimal no. into a new array. Iterate these steps until reaching to the last row of M.
Step 8: Convert each element of the array into equivalent character representation.These characters are the ultimate information was forwarded by the sender.



V. EXAMPLE

Suppose a word "IT" is required to transmit. Here number of character in the message is 2 and it is less than 8. To adjust it as a message of character length 8 it turns into "000000IT". Now converting only the characters into the message to their ASCII values and store into an array. The original message takes form as:

0	0	0	0	0	0	73	84

Now again each and every array elements are transformed into equivalent 8 bit binary form as the total character length of the message is now 8. The decimal values will be formed as:

0000	0000	0000	0000	0000	0000	0100	0101
0000	0000	0000	0000	0000	0000	1001	0100

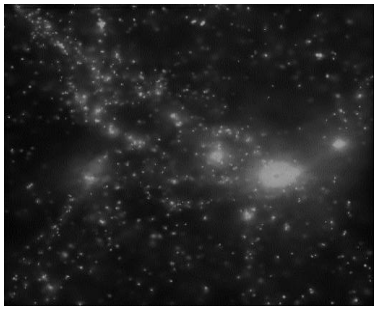
Now a gray scale image is chosen in which this binary message is merged:
Then that image is converted to equivalent binary image matrix. Suppose dimension of the image matrix is 256 x 256 (say). Then this matrix will be completely logically decomposed into some 8x 8 square matrices.
In the given diagram a specimen 16 x 16 matrix is taken and logically decomposed it into some 8 x8 square matrices as for example:

In such a way for a 256 x 256 matrix after logical decomposition 64 individual 8 x8 square matrices will be generated. We will consider only first 8 matrices, because the number of blocks into our original message is 8. Then the bit values of each block of the information are replaced into the chosen decomposed matrices in the following manner:

- 1st row of 1st matrix contains the 1st bit of each block of information. i.e. 00000000
- 1st row of 2nd matrix contains the 2nd bit of each block of information. i.e. 00000011

In such a way the 1st row of 8th matrix contains the 8th bit of each block of information. i.e. 00000010
Then the entire binary image again is converted into gray scale image and forward to the receiver along with number of blocks into our binary message i.e. 8. This is encryption process.

At the time of decryption this gray scale image again is converted into binary image matrix and is decomposed it as previous into some square matrices completely the dimension of each of which is 8 (as forwarded by sender). Then a new 8 x 8 matrix is constructed and inserted the value in following manner:



- 1st row contains the elements of 1st row of 1st decomposed matrix sequentially. . i.e. 00000000
- 2nd row contains the elements of 1st row of 2nd decomposed matrix sequentially. i.e. 00000011

In such a way 8th row contains the elements of 1st row of 8th decomposed matrix sequentially. i.e. 00000010

The new matrx will take form as:

0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1
0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	1	0

Now each and every column is checked and consider only the non-zero column(s) and convert them into equivalent character representation. i.e.

- 7^{th} column : 01001001, i.e "I"
- 8^{th} column :01010100 , i.e. "T"

So that is our required information. This is the ultimate decryption process.

VI. CONCLUSION:

In this paper, the ultimate focus is given on the privacy of information. So, to obtain this we have used the concept of cryptography along with steganography. The new algorithm is more efficient as here from the resultant image it is difficult to access the actual hidden message. Complicated encryption approach is also introducing further security over the hidden information. The new approach can be available to use on any type of the text to work with it, as the corresponding number system has to be chosen (ASCII).

REFERENCES

[1] Steganographic Techniques and their use in an Open-Systems Environment-Bret Dunbar, The Information Security Reading Room, SANS Institute 2002http://www.sans.org/reading- room/whitepapers/covert/677.php

[2] S.K.Bandyopadhyay, Debnath Bhattacharyya, Poulumi Das, S. Mukherjee, D. Ganguly, "A Tutorial Review on Steganography", IC3 Noida, pp. 106-114, August 2008.

[3] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4, April 2007.

[4] Sutaone, M.S., Khandare, M.V, "Image based steganography using LSB insertion technique", IEEE WMMN, pp. 146-151, January 2008.

[5] G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization", IJCSNS, Vol. 8, No. 1, pp. 228-233, January 2008.

Sandipan Debnath has passed his graduation in Mathematics Honours in 2007. After that he has completed his 1^{st} Post Graduation in Master of Computer Application in 2010. Now he is pursuading his 2^{nd} Post Graduation in M.Tech in Computer Science and Engineering, this paper is his first International journal. His main area of interest is Network Security.

Sudipta Kumar Dutta has completed his both Diploma and B.Tech in Computer Science and Engineering in the year 2007 and 2010 respectively. Recently he is pursuading his M.tech in Computer Science and Engineering. This paper is his first international journal. His area of interest is cryptography based Network Security.

Mrinmoy Ghosh has completed his B.Sc and M.C.A in 2007 and 2010 respectively. Now he is pursuading his M.Tech in Computer Science & Engineering. His area of interest to research is Cryptography and Network Security along with Mathematics. It is his 3^{rd} International Journal.

Anupam Modal is the Assistant Professor of JIS College of Engineering, West Bengal, India. He has completed his M.Tech from Kalyani University in 2007. His domain of research is Network Security & Ad-hoc Networking.