Volume 3, No. 3, March 2012

Journal of Global Research in Computer Science

RESEARCH PAPER

Available Online at www.jgrcs.info

ISSN-2229-371X

IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITH CRYPTOGRAPHY

Mr . Vikas Tyagi[*1], Mr. Atul kumar[2], Roshan Patel[3], Sachin Tyagi[4], Saurabh Singh Gangwar[5]
[*1]Assistant Professor IMS Engineering college, Ghaziabad
[*1]Itengg.vikas@gmail.com
[2]Assistant Professor IMS Engineering college, Ghaziabad.
[2]Atul0411@yahoo.com
[3, 4, 5] Student IMS Engineering College, Ghaziabad
Student IMS Engineering college, Ghaziabad.
[3]Roshanraj.singh@gmail.com
[4]Sachintech.tyagi@gmail.com
[5]saurabhsinghgangwar@gmail.com

Abstract: - To increase the security of messages sent over the internet steganography is used. This paper discussed a technique based on the LSB(least significant bit) and a new encryption algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it.

Keywords:- Steganography, LSB(least significant bit), Encryption, Decryption.

INTRODUCTION

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. It is the art of concealing a message in a cover without leaving a remarkable track on the original message. It Pronounced "ste-g&-'nä-gr&-fE" and Derived from Greek roots[7]
"Steganos" = covere "Graphie" = writing

Its ancient origins can be traced back to 440 BC.[1]In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who used steganography first time.[3]

The goal of Steganography[1] is to mask the very presence of communication making the true message not discernible to the observer. As steganography has very close to cryptography and its applications, we can with advantage highlight the main differences. Cryptography is about concealing the content of the message. At the same time encrypted data package is itself evidence of the existence of valuable information. Steganography goes a step further and makes the ciphertext invisible to unauthorized users.[4]

Two other technologies that are closely related to steganography are watermarking and fingerprinting . These technologies are mainly concerned with the protection of intellectual property.[6] But steganography is concern with the hiding of text in another information like image, text, audio, video.

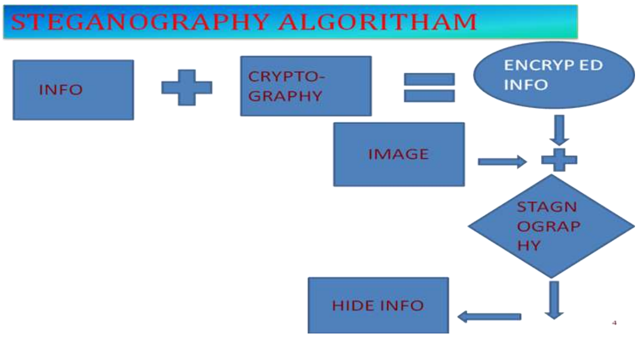
Type of steganograpy:

There are 4 different types of steganography .[6]
Text
- a. Image
- b. Audio
- c. Video
- d. Protocol

Text steganography using digital files is not used very often since text files have a very small amount of redundant data.
Audio/Video steganography is very complex in use.
Image steganography is widely use for hiding process of data. Because it is quite simple and secure way to transfer the information over the internet.
Image steganography has following types:

- a. Transform domain
- i. Jpeg
- b. Spread spectrum
- ii. Patch work
- a. Image domain
- i. LSB and MSB in BMP
- ii. LSB and MSB in JPG

It is most efficient (in term of data hiding) method of image steganography.
Because the intensity of image is only change by 1 or 0 after hiding the information.
Change in intensity is either 0 or 1 because the change at last bit.



CRYPTOGRAPHY ALGORITHAM

Normal text message:- Saurabh
Key:-hello
- a. Change the key and data in to ASCII format.

Eg. hello is changed in B[5]={8, 5, 9, 9, 13}
sauarbh is changed in A[20]={19, 1,21,1,18,2,8}

b. Pad the Normal message according to the length of the key .

Eg. Saurabh has 7 char. In it and the key has 5 letters ,so first five letter of message will change according to the key but in the end we have only two letter left so we pad ***p*** letter (x or y or z) for padding to make exact length pairs.

Saurabh Saura ***bhxxx***
A[20]={19,1,21,1,18,2,8,24,24,24}
m = length of key

Encryption Algorithm:

a. take two arrays flagtxt and flagkey of size of length of text and key and fill it with zeros.
b. Do this process till the length of key

Process for encryption of data by the key:

```
for  k=1 to m
 J=1
for  i=1 to n        ( n is length of padded text)
{
      if( j>m)
   {      j=1
         a[i] =a[i] +  b[j]
          j++
         }
          else
                   { a[i] =a[i] +  b[j]
          j++
            }
End for
```

Process of hiding of key:

```
Do
  for  j=1 to m-1
  b[j]=b[j]+b[j+1]
end for
b[m]=b[m]+b[1]
End for
```

Change the array A and B in to character form:

```
Eg.
For i=1 to n
while a[i]>256
a[i]=a[i]-256
flagtxt[i]+=1
end while
end for
for i=1 to m
while b[i]>256
b[i]=b[i]-256
flagkey[i]+=1
end if
end for
```

Decryption Algoritham:- this is reverse process of encryption

Change the encrypted data in ASCII format:

Eg
A[20]={20,143,29,231,256}
B[20]={10,2,230,19,23}

Decryption of data and key:

```
for  i=1 to n ( n is length of padded text)
while flagtxt[i]!=0
a[i]=a[i]+256
flagtxt[i]--
end while
end for

for  i=1 to m
while flagkey[i]!=0
b[i]=b[i]+256
flagkey[i]--
end while
end for

for  k=1 to m
b[m]=b[m]-b[1]

for  j=m-1 to 1

b[j]=b[j]-b[j+1]

end for

j=1
for i=1 to n
if(j>m)
j=1
a[i]=a[i]-b[j]
end if
end for
end for
```

ADVANTAGE OF ALGORITHM-

a. This algorithm use random size of key .
b. Because of this random size the middle person can't predict the size of key and data**.**
c. The number of times execution of loop is not fixed so that more secure algorithm.
d. This is more secure and easy to implement.

DISADVANTAGE OF ALGORITHM-

a. Key distribution.

COMPLEXITY OF ALGORITHM-

Complexity of algorithm is depend on size of key and text it is approximately equal to O(mn) where m and n is size of key and text respectively.

PIXEL PROCESSING

After the converting our information in secret code or encrypted form we need to patch that data in the image. We use least significant bit for the patching of data because of following reason.

a. Because the intensity of image is only change by 1 or 0 after hiding the information.
b. Change in intensity is either 0 or 1 because the change at last bit .e.g.

1111100**<u>0</u>** → 11111001

The change is only one bit so that the intensity of image is not effected too much and we can easily transfer the data.

***Steps To Insert Data In Image** :-*

a. Take an input image.
b. Find out the pixel values.
c. Select the pixel on which we want to insert data.

This process of selection of pixel is done as user's choice he may choose pixel continuous or alternate or at a fixed distance.

i. Insert the data values in pixels eg.

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

0010110**1** 0001110**0** 1101110**0**
1010011**0** 1100010**0** 0000110**0**
1101001**0** 1010110**1** 0110001**1**

When the number **200**, which binary representation is **11001000**, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

0010110**1** 0001110**1** 1101110**0**
1010011**0** 1100010**1** 0000110**1**
1101001**0** 1010110**0** 01100011

DISCUSSION AND FUTURE WORK

In today's world, we often listen a popular term"Hacking". Hacking is nothing but an unauthorized access of data which can be collected at the time of data transmission. With respect to steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem. In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down.

CONCLUSION

This paper is a short introduction to the world of steganography. We have shown how the simplest methods work and how they can be explored. We have used symmetric encryption algo to provide more security. Research in this field has already begun. Next to steganography, one of the most active fields of research is mass detection tools for hidden contents. The problems are really big. At first, known statistical tests are fragile and for many embedding schemes we still do not know which properties to test. At second, the today traffic in public networks is so overwhelming, that is too hard to rigorously check each file.

REFERENCE

[1]. Eric Cole, Ronald D. Krutz, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley Publishing Inc. (2003).

[2]. David Kahn, "The History of Steganography", Proc. of First Int. Workshop on Information Hiding,

[3]. Cambridge,UK, May30-June1 1996, Lecture notes in Computer Science, Vol.1174, Ross Anderson(Ed.), pp.1-7 Benderr, D. Gruhl, N. Morimoto and A.Lu, "Techniques for Data Hiding", IBM System's Journal, Volume 35, Issue 3 and 4, 1996, p.p., 313-336.

[4]. Artz, D, 'Digital Steganography: Hiding data within Data', IEEE Internet Computing, May/June 2001.

[5]. Wang, Y., Moulin, P. , 'Steganalysis of Block- DCT Image Steganography', BeckmanInstitute, CSL & ECE Department, University of Illinois at Urbana-Champaign, 2003.

Short Bio Data for the Author

Mr. Vikas Tyagi Assistant Professor IMS Engineering college, Ghaziabad

Mr. Atul kumar Assistant Professor IMS Engineering College, Ghaziabad.

Roshan Patel Student IMS Engineering College, Ghaziabad

Sachin Tyagi Student IMS Engineering College, Ghaziabad

Saurabh Singh Gangwar Student IMS Engineering College, Ghaziabad