Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1035 – 1039

RESEARCH ARTICLE

A NOVEL STEGANOGRAPHIC APPROACH FOR IMAGE ENHANCEMENT USING LEAST SIGNIFICANT BIT

Dr. Deepti Sharma[1], Ms. Anshu Sharma[2]

[1]H.O.D, Department of Computer Science Engineering, AITM, PALWAL, INDIA

[2]Lecturer, Department of Computer Science Engineering, Lingayas University, Faridabad, INDIA

[1] deeptiguria@gmail.com, [2] anshu.atri25@gmail.com

Abstract

Steganography means the process of hiding information by embedding messages within other. 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, Cipher

1. INTRODUCTION

1.1 INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. The terms information security, computer security and information assurance are being used frequently interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information. However, there are some subtle differences between them.

1.2 INFORMATION HIDING TECHNIQUES

The introduction of the various processes of the last decades have continuously pointed out towards the security requirement levels, especially since the massive utilization of personal computers, networks and the internet with its availability. Many techniques have been developed for avoiding theft of data, controlling quantities of possible copies.
These techniques used for data hiding are:
(i) Cryptography
(ii) Steganography

2. CRYPTOGRAPHY

Cryptography[1] is the practice and study of hiding information. The word is derived from the Greek kryptos, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. In modern times, cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies. It‘s examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography.

2.1 Symmetric-key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way).

- **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time.
- **Cipher text:** This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts.
- **Decryption Algorithm:** This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

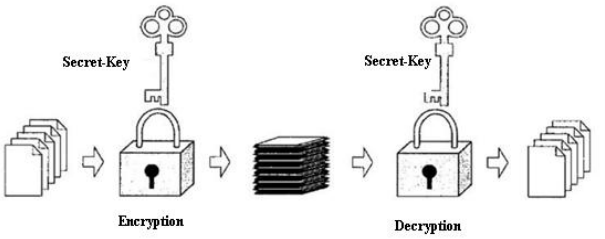

Figure 1: General Cryptography Concept Symmetric-key Cryptography

2.2 Public-key Cryptography

It is also called asymmetric-key cryptography. This kind of cryptography is mainly used for authentication and non-repudiation. Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others.

2.3 Limitations

If one only uses cryptography to protect information, data are not readable, but existence of secret is evident. Therefore, one can easily notice that some sort of data has been transferred and thus, he can alter data or can interrupt that data, so that data should not reach right user.

3. STEGANOGRAPHY

Steganography[2] 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.
"Steganos" = covered "Graphie" = writing

Its ancient origins can be traced back to 440 BC.1In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who used steganography first time.[5]

The goal of Steganography[3] 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 cipher text invisible to unauthorized users.

Two other technologies that are closely related to Steganography are watermarking and finger printing. These technologies are mainly concerned with the protection of intellectual property. But Steganography is concern with the hiding of text in information like image, text, audio, and video.

3.1 Type of Steganography:

There are 5 different types of Steganography

i. Text
ii. Image
iii. Audio

iv. Video
v. 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
c. 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.

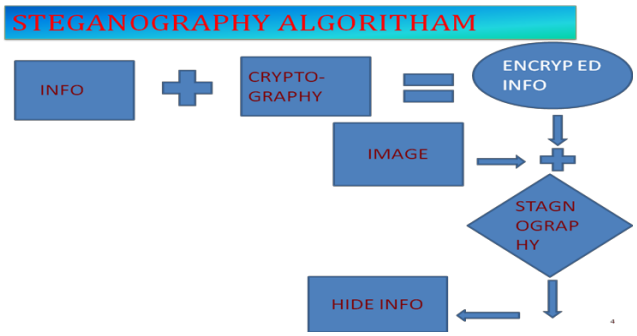

Figure 2: Steganography Algorithm

- **CRYPTOGRAPHY ALGORITHM**

Normal text message:- Surbhi Key:-hello
Eg. hello is changed in B[5]={8, 5, 9, 9, 13} surbhi is changed in A[20]={21, 1,20,2,8,9}

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

Eg. Surbhi has 6 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 one letter left so we pad ***p*** letter (x or y or z) for padding to make exact length pairs.

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 Algorithm: - 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 1or 0 after hiding the information.
b. Change in intensity is either 0 or 1 because the change at last bit .e.g.
   1111100**0** 11111001

The change is only one bit so that the intensity of image is not affected 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

4. 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.

5. CONCLUSION

This paper is an introduction about various information security method and image Steganography. Here we are using symmetric encryption algorithm to provide more security. Research in this field has already begun. Next to Steganography, one of the most active fields of research is hiding text using image Steganograhy and using various other image quality parameters.

REFERENCES

[1] W. Stallings, ―Cryptography and Network Security: Principles and Practice, N
Prentice- Hall, New Jersey, 1999
[2] J. Caldwell, ―Steganography, United States Air Force, http:// www.stsc.hill.af.mil
/crosstalk/2003/06/caldwell.pdf, June 2003.
[3] Eric Cole, Ronald D. Krutz, "Hiding in Plain Sight: Steganography and the Art of Covert Communication",
Wiley Publishing Inc. (2003).
[4] David Kahn,"The History of Steganography", Proc. of First
Int. Workshop on Information Hiding,
[5] 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.

