International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 80-85
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

DATA HIDING IN IMAGE USING LSB WITH DES CRYPTOGRAPHY

Krati Yadav
GLBITM

Swapnil Rajput
GLBITM

ABSTRACT - To increase the security of messages sent over the internet steganography is used. This paper discussed a technique used 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 steg analysis to recover data. Before hiding the data in an image the application first encrypts it.

Keywords *- Steganography, LSB (least significant bit), Encryption, Decryption, DES (Data Encryption Standard), ANSI (American National Standards Institute) Data Security*

I. 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 Steganos" = cover "Graphie" = writing its ancient origins can be traced back to 440 BC. 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 cipher text 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. But steganography is concern with the hiding of text in information like image, text, audio, and video.[5]

II. TYPE OF STENOGRAPHY

There are 4 different types of steganography

1. Text

2. Image

3. Audio

4. Video

5. 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 used for hiding process of data because this is quite simple and secure way to transfer the information over the internet. Image steganography has following types: [10]

* Transform domain

1) Jpeg

2) Spread Spectrum

3) Patch Work

* Image domain

1) LSB and MSB in BMP

2) LSB and MSB in JPG

III. STENOGRAPHY ALGORITHM

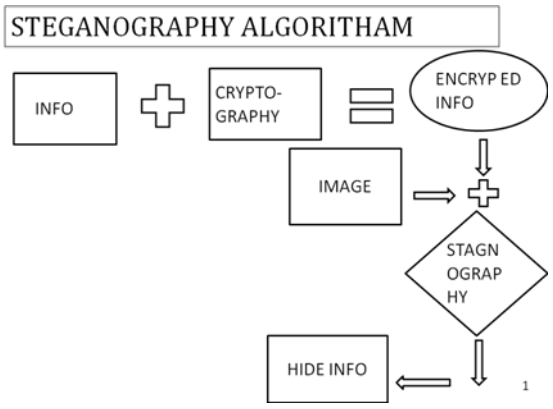


Figure 1: Steganography Algorithm

IV. CRPTOGRAPHY ALGORITHM

Normal text message: - Pirate4

Key:-hello

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 80-85
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

1. Change the key and data in to ASCII format. Eg. hello is changed in B[5]={8, 5, 9, 9, 13}

   Pirate49 is changed in A [20] = {16, 9, 18, 1, 20, 5, and 4}

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

   E.g. Pirate4 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.

   Pirate4 Pirate 4xxx

   A[20]={ 16, 9,18,1,20,5,4,24,24,24}

   m = length of key

4.1 Encryption algorithm

1. Take two arrays flagtxt and flagkey of size of length of text and key and fill it with zeros.
2. Repeat this process till the length of key.

A: 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
```

B: Process of hiding of key

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

C: Change the array A and B in to character form

```
E.g.
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 while
    end for
```

4.2 Decryption Algorithm

(This is reverse process of encryption)

A: Change the encrypted data in ASCII format

E.g.

A [20] = {20, 143, 29, 231, 256}

B [20] = {10, 2, 230, 19, 23}

B: 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]
```

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 80-85
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

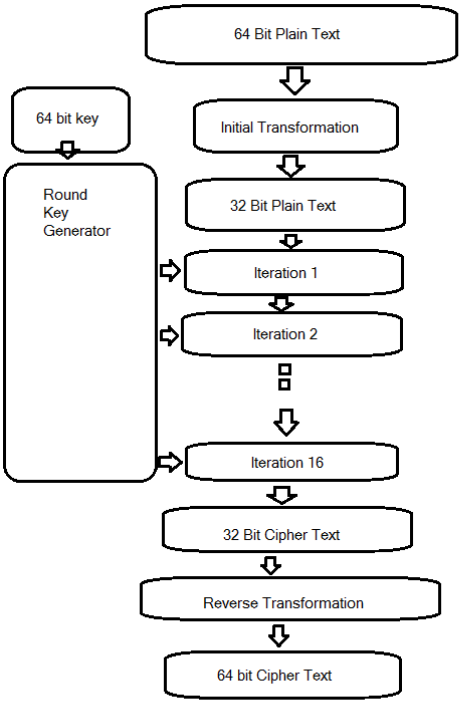
```
        end for
        j=1
        for i=1 to n
                if(j>m)
                        j=1
                        a[i]=a[i]-b[j]
                end if
        end for
end for
```

V. DES ENCRYPTION ALGORITHM

The Data Encryption Standard is symmetric-key algorithm for the encryption. It is developed by IBM in 1970. DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits.[7] DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.
The key is nominally stored or transmitted as 8 bytes, each with odd parity. According to ANSI X3.92-1981 (Now, known as ANSI INCITS 92-1981), section 3.5: One bit in each 8-bit byte of the KEY may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16... 64 are for use in ensuring that each byte is of odd parity.

Like other block ciphers, DES by itself is not a secure means of encryption but must instead be used in a mode of operation. FIPS-81 specifies several modes for use with DES. Further comments on the usage of DES are contained in FIPS-74.[8]

Decryption uses the same structure as encryption but with the keys used in reverse order. (This has the advantage that the same hardware or software can be used in both directions.)



Working of DES

Figure 2: Working of DES

VI. 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. [9]

• 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 .e.g.

11111000 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.

6.1 Steps to Insert Data in Image

For pages other than the first page, start

- Take an input image.
- Find out the pixel values.
- 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.

- Insert the data values in pixels eg. For example a grid for 3 pixels of a 24-bit image can be as follows:

00101101 00011100 11011100

10100110 11000100 00001100

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 80-85
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

11010010 10101101 01100011

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:

00101101 00011101 11011100

10100110 11000101 00001101

11010010 10101100 01100011

At the top of the page, and continue in double-column format. The two columns on the last page should be as close to equal length as possible.

VII. RESULTS

Figure 3: Original Image

Fig. 4 Output Image

VIII. COMPARISON BETWEEN VARIOUS STENOGRAPHY ALGORITHM

NO	BASE	Steganography without cryptography	Steganography with DES cryptography technique	Steganography with Other cryptography technique
1.	Security	One level security	Two level security	Two level security
2.	Key size	No key present	Fixed size of key	Random size of key
3.	Steps involve in encryption of data	No step	Fixed step	Depend on the key size
4.	Brute force attack	No need	Very hard to attack	Can possible

Images of LSB Based Steganography

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 80-85
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

Fig. 5 Original Image

Fig. 6 Stegano Image

Images of MSB Based Steganography

Fig. 7 Original Image

Fig. 8 Stegano Image

Images of LSB Based Steganography: with color Image

Fig. 9 Original Image

Fig. 10 Output Image

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 80-85
Published Online December – January. 2016 in IJEAST (http://www.ijeast.com)

Images of MSB Based Steganography: with color Image

Fig. 11 Original Image

Fig. 12 Output Image

IX. 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. Often stegnography is used in conjunction to cryptography so that message remains unreadable even if detected. This paper is to create across platform that can effectively encrypt a message and hide it inside a digital image file. The encryption algorithm is the DES algorithm which converts readable message into unreadable.

X. REFERENCES

[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 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]. 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.
[6]. [5]. Dr. Ekta Walia, Payal Jain,Navdeep “ An Analysis of LSB & DCT based Steganography
[7]. [6]. Joshua Michael Buchanan,”Creating a robust form of steagonography”
[8]. [7]. Vijay kumar sharma ,vishal shrivastava” a steganography algorithm for hiding image in Image by improved lsb substitution by imizeDetection
[9]. [8]. V. Lokeswara Reddy, Dr. A. Subramanyam” Implementation of LSB Steganography and its Evaluation for Various File Formats” Int. J. dvanced Networking and Applications 868 Volume: 02, Issue: 05, Pages: 868-872 (2011)
[10]. Neeta Deshpande, Kamalapur Sneha, Daisy Jacobs, “Implementation of LSB Steganography and Its Evaluation for various Bits‖ Digital Information Management”, 2006 1st International Conference on. 06/01/2007; DOI: 10.1109/ICDIM.2007.369349