Blowfish and LSB Procedure to Secure Open Channel Communication

Neha Gupta[1] Parikshit Singla[2]
[2]Assistant Professor
[1, 2] Computer Science Department
[1, 2] Doon Valley Institute of Engineering & Technology Karnal, India

Abstract---Digital data communication has become an essential part of infrastructure nowadays, a lot of applications are Internet-based and it is important that communication be made secret. Cryptography and steganography are the two popular methods available to provide security. One distorts the message and the other hides the existence of message itself. Using cryptography, the data is transformed into some other gibberish form and in steganography,the data is embedded in an image file and the image file is transmitted.This paper focuses mainly on the strength of combining cryptography and stegnography methods to enhance the security of communication over an open channel.

Keywords: Steganography, Blowfish Encryption, Least Significant Bit, Cryptography.

I. INTRODUCTION

Now a days internet became common use. As the use of internet increases providing security to the information is also important thing. Information security means protecting information systems from unauthorized access, use, disruption, modification, recording or destruction. We have two methods to provide security to the information. They are: Cryptography and Steganography.

A. Cryptography:

Cryptography is now used in almost all network based applications to ensure security. Cryptography is "the art of writing in secret characters". Encrypting is the act of translating a 'normal message' to a message written with 'secret characters' called secret message or cipher text or encrypted message.

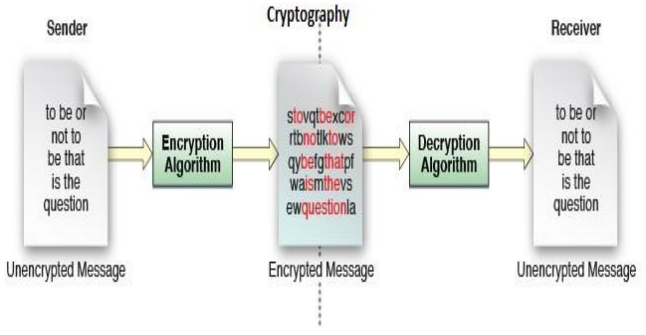

Fig. 1: Cryptography procedure

Decrypting is the act of translating a message written with 'secret characters' into a readable message or original message send by sender [1]. There are many cryptographic algorithms to ensure secure communication which involve algorithm and secure key in crypto system. There are symmetric key cryptography and asymmetric key cryptography. In crypto system, symmetric key is faster than asymmetric key in speed.A key-based algorithm uses an encryption key to encrypt the message. This means that the encrypted message is generated using not only the message, but also using a 'key': The receiver can then use a decryption key to decrypt the message. Again, this means that the decryption algorithm doesn't rely only on the encrypted message. It also needs a 'key'.Some algorithms use the same key to encrypt and decrypt, and some do not.

B. Steganography:

The term Steganography is forked from the Greek words "steganos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing" [2]. Steganography is an act of hiding of a message within another so that the presence of the hidden message is indiscernible. It does not modify original message but hides the message into a cover object and then cover object is transmiited. This technique relies on a message being encoded and hidden in a transport layer in such a way as to make the existence of the message unknown to an observer.It has many applications like online transaction, watermarking, military communication etc.

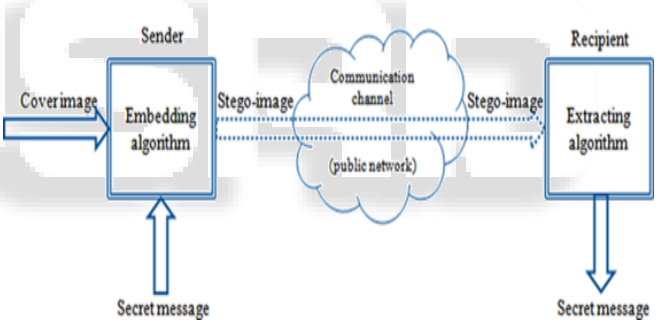

Fig 2: Stegnography procedure

In basic steganographic process, secret message is hidden into a cover media (can be an image, text, audio, video) to produce stego image. Original cover image and stego image looks exactly the same thereby an outside observer cannot detect that it can holds a secret mesaage. A secret key called stego key is also used to embed secret message into cover object and also use to extract secret message from stego image. A receiver can extract message with or without stego key that depends on hidden scheme. A pure steganographic system do not use stego key, it only uses secret key during encryption and decryption process whereas more secure steganographic system use the stego key.

II. RELATED WORK

Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. A number of approaches related with cryptography and LSB steganography and improved steganography present in the literature review of many authors.

Li Zhi, Sui Ai Fen states that spatial LSB Steganography results in the alteration of the smooth characteristics between adjoining pixels of the raw image. The relation between the length of embedded message and the gradient energy is theoretically analyzed [3].Through the analysis of the variation of the gradient energy, which results from the LSB Steganography in color and grayscale image, the secret message embedded in the target image is detected, and the length of the embedded message is estimated. The method is proved effective and accurate by simulation.

Deshpande Neeta emphasized strongly on image Steganography providing a strong focus on the LSB techniques in image Steganography. The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format [4]. This paper explains the LSB embedding technique and presents the evaluation results for 2,4,6 Least significant bits for a .png file and a .bmp file.

Dr. V. Vijayalakshmi proposed a modulo based image steganography algorithm for both colour and black-n-white images. The proposed algorithm was stimulated with secret data using Lena image as the cover image. The resultant stego image obtained after embedding of the secret message does not show any change when compared to original cover image.Histogram and statistical analysis were performed on the stego image and proved that the proposed method can effectively resist image steganalysis[5].

Ahmad T. Al-Taani proposed a novel Steganographic method for hiding information within the spatial domain of the gray scale image [6]. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. Experimental results, compared with other methods, showed that the proposed approach hide more information and gave a good visual quality stego image that can be seen by human eyes. They have compared the new method with two well-known methods, PVD and GLM methods.

Tingyuan Nie evaluated the performance of two symmetric key encryption algorithms: DES and Blowfish which commonly used for network data encryption. They first reviewed the basic algorithms and analyzed the security for both. Experimental results show that Blowfish algorithm runs faster than DES algorithm while both of them consume almost the same power [7]. It is proved that Blowfish algorithm maybe more suitable for wireless network which exchanges small size packets.

III. PROPOSED WORK

We have studied various simplifications in cryptography and steganograpgy. As each of these techniques have their own advantages and shortcomings. A better communication system can be presented by a combination of both the techniques cryptography and steganography. Here I am using Blowfish algorithm for encryption and decryption in cryptography and enhanced LSB algorithm for Image Steganography. Firstly we will discuss Blowfish encryption algoritm and then Lsb embedding procedure used in steganographic systems.

A. Blowfish Encryption Algorithm:

Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms[12]. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link. Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times [8]. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. The Feistel Network that makes up the body of Blowfish is designed to be as simple as possible, while still retaining the desirable cryptographic properties of the structure. A Feistel network is used within algorithm which is a general method of transforming any function into a permutation [9,11].It was invented by Horst Feistel and has been used in many block cipher designs. Below figures show brief about working of blowfish algorithm.

Subkeys: Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption. Figure 3 shows calculation of sub keys.The D-array consists of 18 32-bit subkeys: D1, D2,..., D18. There are four 32-bit S-boxes with 256 entries each:

S1,0, S1,1,..., S1,255; S2,0, S2,1,..., S2,255;
S3,0, S3,1,...,S3,255; S4,0, S4,1,..., S4,255.

B. The sub keys are calculated using Blowfish algorithm:

Step1: First initialize the P array and then the four S boxes in order with a fixed string. The string consist of hexadecimal digits of di.
P1 = 0 X 243f6288 P2 = 0 X 85a308d3
P3 = 0 X 13198a2e P4 = 0 X 03707344

Step2: XOR P1 with the first four 32 bits of key , XOR P2 with second 32 bits of key and so on for all bits of key (possibly up to P4). Repeatedly cycle through the key bits until the entire P array has been XOR ed with key bits.

Step3: Encrypt all the zero string with Blow fish algorithm using subkey described in step1 and 2.

Step4: Replace P1 and P2 with output of step 3.

Step5: Encrypt the output of step 3 using Blowfish with modified key.

Step6: Replace P3 and P4 with the output 5.

Step7: Continue the process of replacing all entries of P array and then all the four S boxes in order with the output of continuously changing Bluefish algorithm.

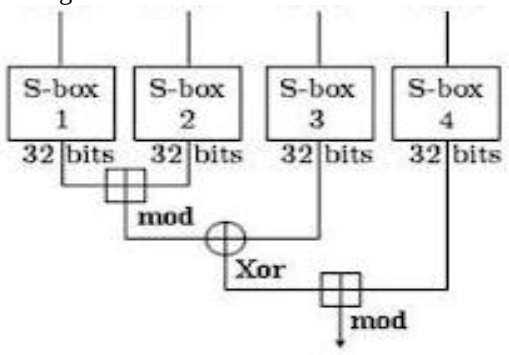

Fig. 3: Round Function of Fiestel Cipher

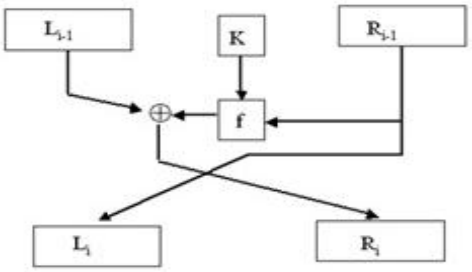

Fig. 4: Fiestel Network

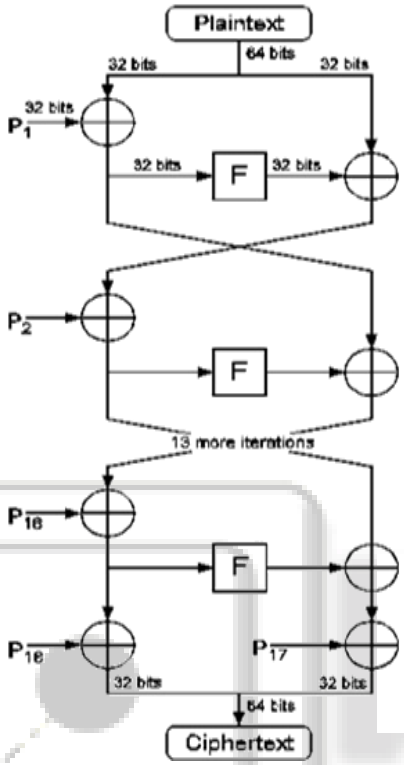

Fig. 5: Blowfish Encryption

Blowfish Encryption Algorithm: Blowfish is a Feistel network consisting of 16 rounds .The input is a 64-bit data element, X.

Step. 1 : Divide X into two 32-bit halves: XL, XR. Then, the following operations are performed form r=1 to 16.
Step. 2 : XL = XL ⊕ Pi
Step. 3 : XR = F (XL) ⊕ XR
Step. 4 : Swap XL and XR
Step. 5 : After 16 rounds Swap XL and XR (Undo the last swap) and then XR and XL are XORed with P17 and P18.
Step. 6 : XR = XR ⊕ P17
Step. 7 : XL = XL ⊕ P18
Step. 8 : Combine XL and XR

C. Least significant bit (LSB) Encoding Steganography :

LSB encoding is by far the most popular of the coding techniques used for digital images. By using the LSB of each byte (8 bits) in an image for a secret message, we can store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images[10]. As you can see, much more information can be stored in a 24-bit image file by changing a bit of each of red, green and blue component.
LSB example, suppose that we have three pixels (9 bytes) with the RGB encoding. When the number 301, can be which binary representation is 100101101 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following bits (where bits in bold have been changed).

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

Here the number 301 was embedded into the grid, only the 4 bits (in bold) needed to be changed as (0,0,1,0) according to the embedded message. On an average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of primary colour, changing the LSB of a pixel results in small changes in the intensity of the color. The difference between cover image and stego image will be hardly noticeable to human eye.

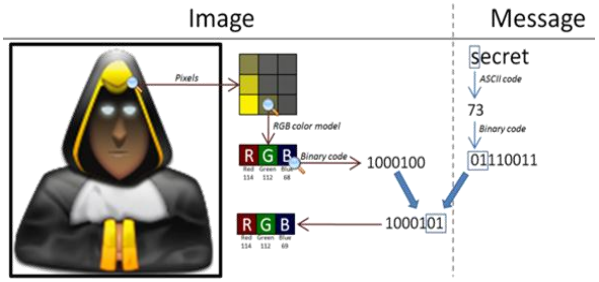

Fig. 6: Replace LSB of Color with message data

Here we use advanced LSB Steganography.In this firstly we will convert the image into grayscale image[14]. Conversion of a color image to grayscale can be done using several approaches. Different weighting of the primary colors effectively represents the effect of obtaining black-and-white image with color images. To convert a gray intensity value to RGB, simply set all the three primary color components red, green and blue. The method adopted in current work for experimental evaluation is to obtain the RGB values of individual pixels and to take the average to be normalized to fit in the scale 0 to 255.

D. LSB Based Steganography Algorithm to embed text message:-

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Peak signal to noise ratio (PSNR) of the stego image.

E. Advanced LSB Algorithm to embed text message:-

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary
Step 3: Convert color cover image into gray scale image and find LSB to hide data.
Step 4: Calculate LSB of each pixels of color image using LSB of gray scale image.
Step 5: Replace LSB of cover image with each bit of secret message one by one.
Step 6: Write stego image.

Step 7: Calculate the Peak signal to noise ratio (PSNR) of the stego image.

F. Algorithm to extract text message:

Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

IV. IMPLEMENTATION

The propose work is implemented in JAVA as it is an object oriented and platform independent language used for many programming desktop application. It consists of a virtual machine and set of libraries which are needed to allow the use of file systems, networks, graphical interfaces, etc. Java's inherent network programming capability makes it suitable for distributed programming. Start with blowfish encryption algorithm of cryptography that converts a secret message text file into cipher text file, then enter into stegnography area which is used to hide cipher text file into a cover image. Same secret key is used for both encryption and decryption process.

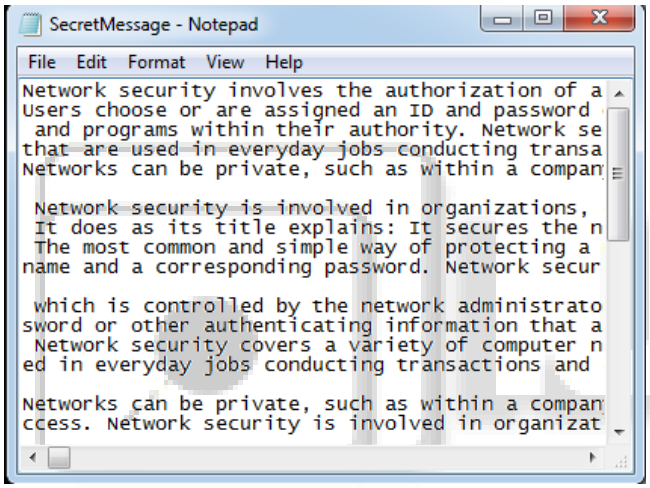

Fig 7: Original Message

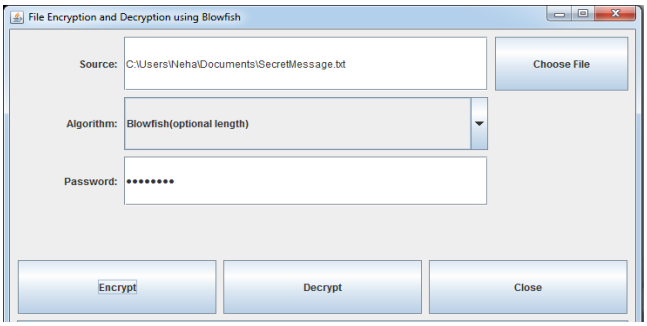

Fig. 8: Blowfish Encryption applied on Message

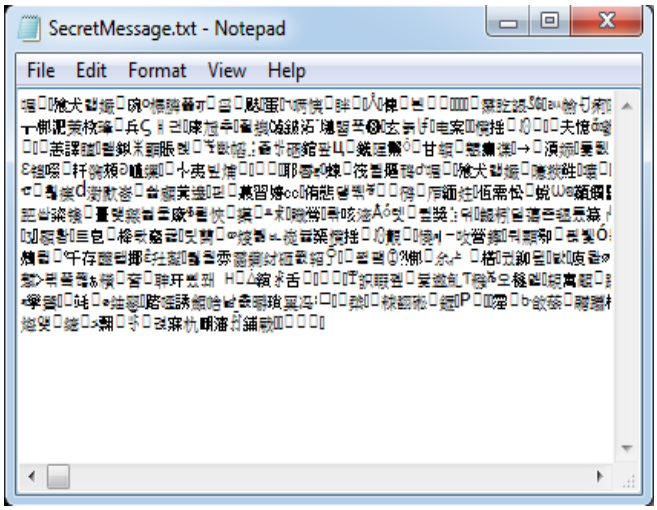

Fig. 9: Message Conversion after Encryption.

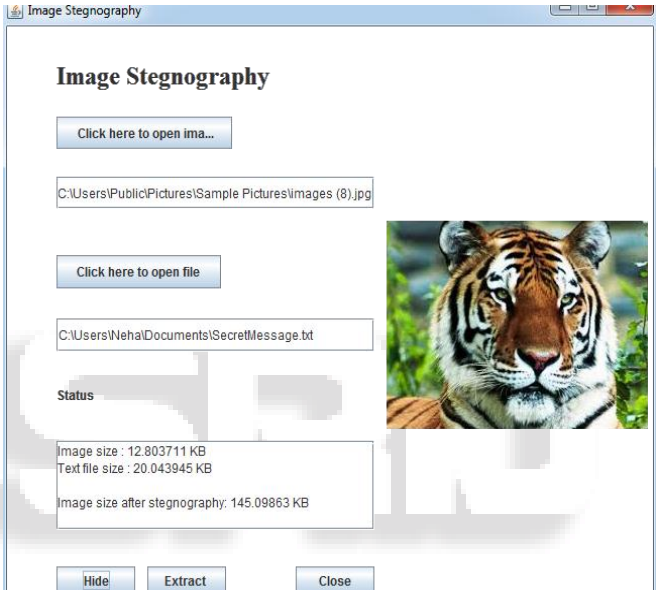

Fig. 10: Encrypted Message Hide into Cover Image.

Likewise, Hidden message is extracted using Lsb steganography and decrypted using Blowfish decryption process.

V. RESULT AND DISCUSSION

Survey shows that security is most important aspect of information world. For security purpose we use encryption schemes but our encryption scheme cannot provife security completely. So in order to rely on encryption we need a better approach. Cryptography and steganography are used for enhancing security. Neither of these schemes alone can provide security efficiently. Steganography hides the data whereas cryptography scrambles the data.

Sr. No	Parameter	Only Cryptography	Only Steganography	Combination of Cryptography and Steganography
1	Visibility of Text	Visible (encrypted text)	Not Visible	Not Visible
2	Security	Less	Less	More
3	Key Required	Yes	May or May not be	Yes
4	Encryption of Plain Text	Yes	No	Yes

Table. 1 : Comparison Parameter

Sr. No	Image name	Image size	PSNR	Algorithm used
1	parrot.png	130.9414	7.679916778540448	LSB
2	parrot.png	130.9414	13. 6799167785404	Advanced LSB
3	sunset.png	3804.1064	7.65225355973709	LSB
4	sunset.png	3804.1064	15.6522535597379	Advanced LSB
5	trees.png	5423.49	7.60711947409527	LSB
6	trees.png	5423.49	10.60711947409527	Advanced LSB

Table. 2: PSNR value comparison of stego images using simple LSB and Advanced LSB approach



Stego Images after Data Embedding



Image1:parrot Image2:sunset Image3:trees

Table. 3: Original Cover Images before Data Embedding

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image. For steganography firstly we have used LSB technique but performance of this LSB technique is not good in terms of PSNR so we have use an enhanced LSB method which will improve the overall performance in terms of security and PSNR. Also the capacity of embedding data in image is increased in advanced lsb procedure.Table 3 shows the difference between cover image and stego image that reflects both images looks same before and after steganography technique applied to images. Using both cryptography and steganography, security of open channel communication increases. Even if an attacker get able to detect hidden data in image, he is not able to get original data file because it is in encrypted form.

VI. Conclusion

In today's era most of the information travels over the internet. Some of the messages are very confidential and require additional protection from intruders. For increasing the security I have used a combination of cryptography and steganography. Cryptography will make the text unreadable, for this, I have used Blowfish cryptography algorithm and for hiding this encrypted text I have used LSB steganography algorithm which has proven to be a better security then earlier algorithms. In order to break blowfish algorithm attacker has to spend a lot of time and effort for trying several attacks and getting the original message. This approach is easy to implement and can be used in real life like in business world where some information need to be keep secret. Using this approach,we get better psnr value of stego image as compared to original image. Original cover image and stego image looks exactly the same, thereby it does not attract the attention of intruder that image may contain hidden data. This scheme results in increase in security level that require for reliable communication over interenet.

References

[1] Atul Kahate (2009), Cryptography and Network Security, second edition, McGraw-Hill.
[2] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf.
[3] Li Zhi,Sui Ai Fen "Detection of Random LSB Image Steganography", Vehicular Technology Conference, 2004. VTC2004-Fall. 2004
[4] Deshpande Neeta, Kamalapur Snehal "Implementation of LSB Steganography and Its Evaluation for Various Bits, Digital Information Management", 2006 1st International Conference
[5] Dr. V. Vijayalakshmi, Dr. G. Zayaraz, and V. Nagaraj "A Modulo Based LSB Steganography Method" International Conference on Control, Automation, Communication and Energy Conservation 2009, June 2009
[6] Ahmad T. Al-Taani and Abdullah M. AL-Is "A Novel Steganographic Method for Gray-Level Images" International Journal of Computer and Information Engineering 3:1 2009
[7] Tingyuan Nie, Chuanwang Song, Xulong Zhi "Performance Evaluation of DES and Blowfish Algorithms" IEEE2010.
[8] B. Schneier, Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[9] H. Feistel, "Cryptography and Computer Privacy," Scientific American.
[10] B. Karthikeyan, S. Ramakrishnan, V. Vaithiyanathan, S. Sruti, and M. Gomathymeenakshi "An Improved Steganographic Technique Using LSB Replacement on a Scanned Path Image" International Journal of Network Security, Vol.16, No.1, Sep.2012
[11] Komal Patel, Sumit Utareja and Hitesh Gupta Information hiding using Least Significant Bit Steganography and Blowfish Algorithm , February 2013
[12] Jawahar Thakur1, Nagesh Kumar2 DES, AES AND BLOWFISH Symmetric key cryptography simulation based performance analysis December 2011
[13] http://en.wikipedia.org/wiki/Steganography
[14] M.B. Ould MEDENI El Mamoun SOUIDI "A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution" Multimedia Computing and Systems (ICMCS), 2011 International Conference IEEE
[15] http://en.wikipedia.org/wiki/Blowfish_(cipher)

