Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Securing Data by Using Cryptography with Steganography

Ajit Singh*
SES, BPS Mahila Vishwavidhyalaya
India.

Swati Malik
SES, BPS Mahila Vishwavidhyalaya
India.

Abstract— Securing data is a challenging issue in today's era. Most of the data travel over the internet and it becomes difficult to make data secure. So Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So here we are using a combination of steganography and cryptography for improving the security.

Keywords— Cryptography, Steganography, Fiestel Network, attack, evedropper.

I. INTRODUCTION

Cryptography is a part of information security. It is an art of securing the data. It is mainly concerned with storing and transmitting the information safely over the insecure medium like Internet by encoding text data into a form non recognizable format with the help of various encryption algorithms and only the intended user will be able to convert it into original text. The process which converts original data into the unreadable form is called encryption process. Cryptography is not capable of hiding the presence of data alone and it cannot protect data effectively. Any eveddropper can easily detect the presence of encrypted data and can try several attacks in order to get the original data. So in order to further enhance the security we want to provide a two layer approach for providing an improved and better security. Steganography is also concerned with security of transmitting data but with a different objective. Steganography allows people to communicate secretly by hiding the data within data.

A. Cryptography

Cryptography is that branch of science which is concerned with the mathematical techniques for keeping message secure and free from attacks. Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text [1]. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish alled cipher text. You use Encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption [2].

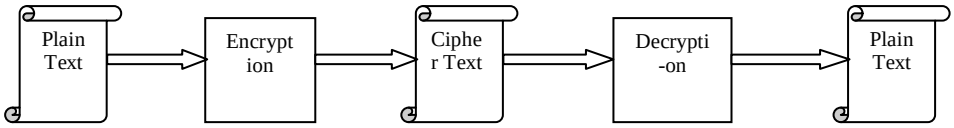

Fig.1 Encryption and decryption

There are two types of encryption algorithms: symmetric encryption algorithm and asymmetric encryption algorithm. In Symmetric key encryption sender and receiver will have the same key for the process of encryption and decryption of data. In asymmetric key encryption algorithm different keys are used at sending and receiving site for encryption and decryption.

List of Symmetric Algorithms

- Data Encryption Standard(DES)
- Advanced Encryption Standard (AES)
- Blowfish Encryption Algorithm
- International Data Encryption Algorithm
- Triple Data Encryption Standard etc.

List of Asymmetric algorithms

- Diffie-Hellman

- RSA
- DSA etc.

B. Steganography

Steganography is the art of passing information using original files in a manner that the existence of the message is unknown. The term steganography is arrived from Greek word means, "Covered Writing". The carrier files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been hidden inside a digital Picture, Video or Audio file. Images can be more than what we see with our Human Visual System (HVS); hence, they can convey more than merely 1000 words [3].

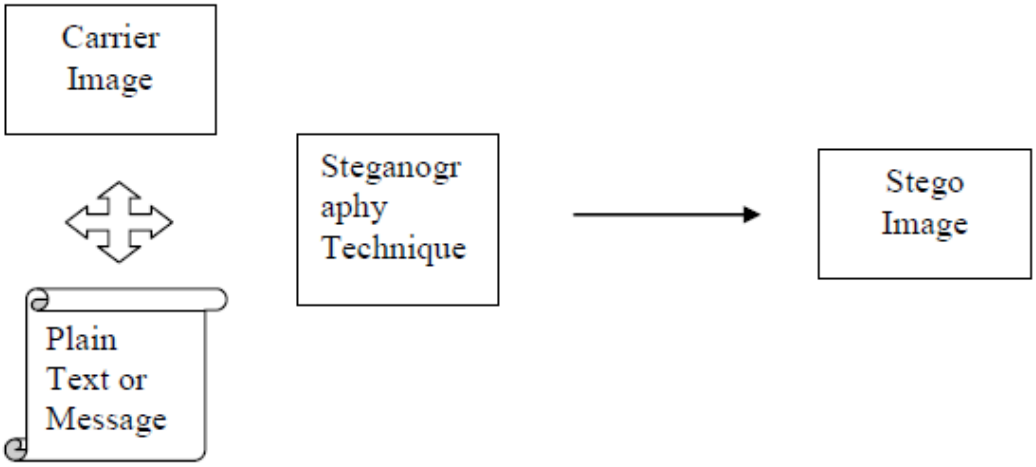

Fig.2 Basic process of Steganography

Almost any plain text, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image. With the continued growth of strong graphics power in computers and the research being put into image based Steganography, this field will continue to grow at a very rapid pace.

Before diving into steganography techniques for digital images, a brief explanation of digital image architecture should be explained [4].

As Duncan Sellars [5] explains, "To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the images raster data." When dealing with images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages, as we will explain below. 8-bit images are a good format to use because of their relatively small size. The problem is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color will be harder to detect after the image has been encoded with the hidden message. 24-bit images offer much more flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go beyond the human visual system (HVS), which makes it very difficult to detect once a secret message, has been encoded. The other benefit is that a much larger amount of hidden data can be encoded into a 24-bit digital image as compared to an 8-bit digital image. The one major problem with 24-bit digital images is their large size (usually in MB) makes them more suspect than the much smaller 8-bit digital images (usually in KB) when sent over an open system such as the Internet. We will now discuss a few of popular digital image encoding techniques used today. They are least significant bit (LSB) encoding and masking and filtering techniques. Least significant bit (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. As you can see, much more information can be stored in a 24-bit image file. Depending on the color palette used for the cover image (i.e., all gray), it is possible to take 2 LSB's from one byte without the human visual system (HVS) being able to tell the difference. The only problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (i.e., changing from .GIF to .JPEG).

Masking and filtering techniques for digital image encoding such as Digital Watermarking (i.e.- integrating a company's logo) are more popular with lossy compression techniques such as (.JPEG). This technique actually extends an image data by masking the secret data over the original data as opposed to hiding information inside of the data. The beauty of Masking and filtering techniques are that they are hard to detect manipulations in the image which makes there possible uses very robust. As a side note, there are many other techniques that are more secure and robust ways to use digital images in Steganography.

C. Types Of Attacks Attacks and analysis of hidden information may take several forms: detecting, extracting, and disabling, destroying or modifying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography-based information streams). The possible attacks on a stego media can be one of the following[3]:

1. Stego-only attack: Only the steganography medium is available for analysis.
2. Known-cover attack: The carrier, i.e. the original cover and steganography media are both available for analysis.
3. Known-message attack: The hidden message is known.
4. Chosen-steganography attack: The steganography medium and tool (or algorithms) are both known.
5. Chosen-message attack: Known message and steganography tools (or algorithms) are used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms.

II. PROPOSED WORK

No Niether cryptography, or steganography can alone make the data secure efficiently So a better technique is developed by combining these two techniques. A combination of steganography and cryptography is used which will take advantage of both the techniques. We are using Blowfish Encryption Algorithm for encrypting the message to be hidden inside the image for making it non readable and secure. After encryption we will apply LSB technique of steganography for further enhancing the security. Below we will first explain Blowfish Encryption Algorithm and then the LSB technique.

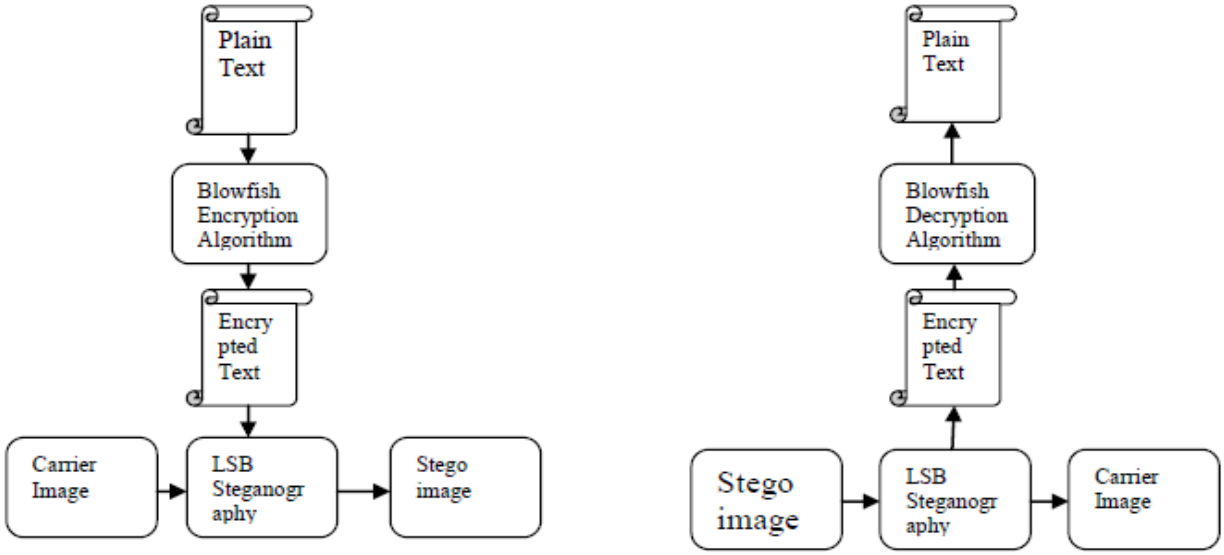

Fig. 3 Proposed Work

A. Blowfish Encryption Algorithm

Blowfish is a symmetric key block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits. Blowfish was designed in 1993 by **Bruce Schneier** as a fast, free alternative to existing encryption algorithms [6]. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm is a **Feistel Network**, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA [7]. In paper [9] and [10] it is clearly shown that how blowfish encryption algorithm is better then other symmetric algorithms.

B. Description of Algorithm

Blowfish has a variable-length key and 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data- encryption part. Key expansion converts a key of at most 448 bits into several subkey arrays totalling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of permutation depending on key, and a data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round.

1. Subkeys

Blowfish uses a large number of subkeys. These keys must be precomputed before any data encryption or decryption.[9]

- 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.

The sub keys are calculated using Bluesfish 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.

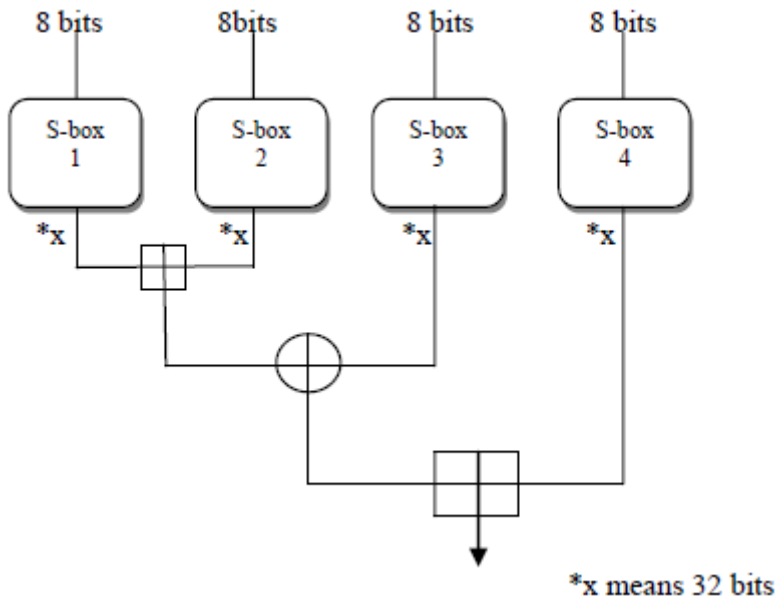

Fig 4 Round Function of Fiestel Cipher

C. Encryption

Blowfish is a Feistel network consisting of 16 rounds. The input is a 64-bit data element, X. Divide X into two 32-bit halves: XL, XR. Then, the following operations are performed form r=1 to 16.

$XL = XL \oplus Pi$

$XR = F(XL) \oplus XR$

Swap XL and XR

After 16 rounds Swap XL and XR (Undo the last swap.) and then XR and XL are XORed with P17 and P18.

$XR = XR \oplus P17$

$XL = XL \oplus P18$

Lastly recombine XL and XR. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. Implementations of Blowfish that require the fastest

D. The LSB Steganography

In this technique, least significant bit i.e. the eighth bit inside an image is changed to a bit of the secret message[11]. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components, since they are each represented by a byte. An 800×600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. As an example, suppose that we have three pixels (9 bytes) with the RGB encoding.

10010101 00001101 11001001
10010110 00001111 11001011
10011111 00010000 11001011

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 0000110**0** 1100100**0**
1001011**1** 0000111**0** 11001011
10011111 00010000 11001011

Here the number 301was embedded into the grid, only the 4 bits needed to be changed 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 human eye cannot detect these changes thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the LSB without noticing the difference [12].

III. IMPLEMENTATION AND RESULT

The above described work is implemented in JAVA. Firstly blowfish symmetric key encryption algorithm is used whoch converts a text file in to a cipher text file. After that for adding a new layer of security called steganography for further enhancing the security of communication process.

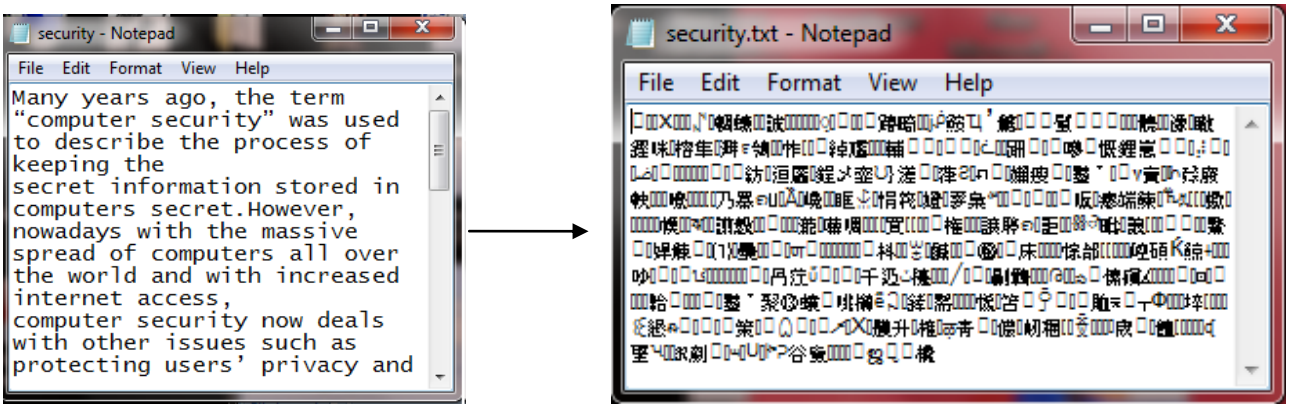

Fig.5 Encryption by using Blowfish Encryption Algorithm

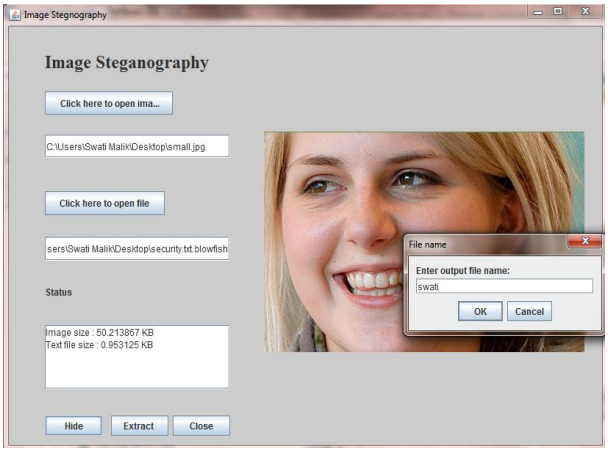

Fig. 6Using LSB Steganography Hiding the encrypted file

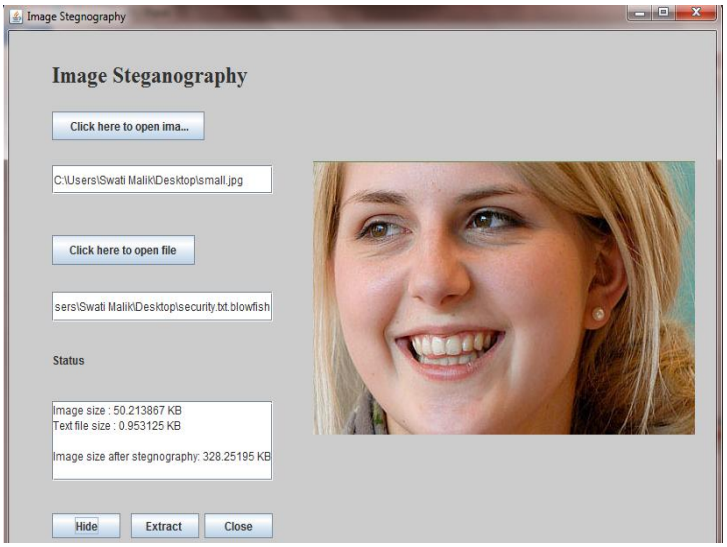

Fig.7 After Steganography

IV. CONCLUSION

In this paper two layers of security i.e. cryptography and steganography are used which makes it difficult to detect the presence of hidden message. But in some cases if the evedropper has attacked the carrier of message then he will not be able to get the original message as all the relevant data here is in encrypted form. For cryptography Blowfish algorithm is used which is much better than AES and DES. In order to break blowfish algorithm he has to spend a lot of time and effort for trying several attacks and getting the original message. Although both of these techniques are easy to implement but there combination will provide much efficient and reliable security.

ACKNOWLEDGMENT

Author would like to give her sincere gratitude to guide Mr. Ajit Singh who encouraged and guided her throughout this paper.

References

[1] Ajit Singh, Aarti Nandal, Swati Malik "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security "IJARCSSE Dec,2012
[2] Atul Kahate (2009), *Cryptography and Network Security*, second edition, McGraw-Hill.
[3] Vijay Kumar Sharma ,Vishal Shrivastav" A steganography algorithm for hiding image in image by improved LSB substitution by minimize detection "Journal of Theoretical and Applied Information Technology 15th February 2012.
[4] www.sans.org/reading_room/whitepapers/covert/detailed-steganographic-techniques-open-systems environment677
[5] Sellars, D., "An Introduction to Steganography", www.cs.uct.ac.za/CS400W/NIS/papers99/dsellars/stego.html)
[6] http://en.wikipedia.org/wiki/Blowfish_(cipher)
[7] https://www.schneier.com/blowfish.html
[8] Cryptography and information security by V.K. Pachghare
[9] Tingyuan Nie, Chuanwang Song, Xulong Zhi "Performance Evaluation of DES and Blowfish Algorithms" IEEE 2010.
[10] Gurjeevan Singh Ashwani Kr. Singla K.S. Sandha Superiority of Blowfish Algorithm in Wireless Networks International Journal of Computer Applications (0975 – 8887) Volume 44– No11, April 2012
[11] Lokeswara Reddy Dr. A. Subramanyam Dr.P. Chenna Reddy" Implementation of LSB Steganography and its Evaluation for Various File Formats" Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872 (2011)
[12] Deshpande Neeta, Kamalapur Snehal, DaisyJacobs "Implementation of LSB Steganography and Its Evaluation for Various Bits" Digital Information Management, 2006 1st International conference.pp 173-178,2007

