Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm

Komal Patel
Patel Institute of Technology
Ratibad, Bhopal

Sumit Utareja
Patel Institute of Technology
Ratibad, Bhopal

Hitesh Gupta
Patel Institute of Technology
Ratibad, Bhopal

ABSTRACT
Security is the most challenging aspects in the World Wide Web. In present time information sharing and transfer has increased exponentially. So to find out best solution this is providing necessary protection of our data against malicious attacks from intruders.
Cryptography and Steganography are the two major techniques for secret communication. Cryptography converts information from its original form (plaintext) into unreadable form (cipher text); where as in steganography the secret message is hidden into the cover medium. There are many different techniques are available for cryptography and stagnography. In this paper two techniques BLOWFISH algorithm for cryptography and LSB approach for stagnography are used. First encryption of data is done by using BLOWFISH algorithm which is one of the most powerful techniques and then hide encrypted message using LSB approach. Our proposed model gives two layers of security for secret data.

Keywords
Cryptography, Stenography, LSB, BLOWFISH, Encryption, Decryption.

1. INTRODUCTION
In today's information age, the technologies have developed so much that most of the users prefer internet to transfer data from one end to another across the world. So privacy in digital communication is basic requirement when confidential information is being shared between two users. To provide security, various steganography and cryptography techniques have been used in the past research.

CRYPTOGRAPHY:
Cryptography is the science that studies the mathematical techniques for keeping message secure and free from attacks [2]. For that information is transforming into an unreadable form which is called cipher text. Only those users who know secret key can decrypt the message into their original form. Cryptography system can be classified into two parts first is Symmetric – key Cryptography and second is public – key cryptography.

1. Symmetric – key cryptography :
In symmetric key cryptography system sender and receiver share a single key which is used to encrypt and decrypt a message. It is also called secret key cryptography. The algorithms used for symmetric – key cryptography is called symmetric- key algorithms. There are two types of symmetric algorithms such as stream cipher and block cipher. Stream ciphers encrypt the bits of information one at a time and Block ciphers encrypt the information by breaking down into blocks.
List of Symmetric Algorithms

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

2. Public- key cryptography:
In public key cryptography there is pair of keys one is secret key and other is public key. In which one is used for encrypting the plain text, and the other is used for decrypting the cipher text
List of public – key algorithms

- Diffie-Hellman
- RSA
- DSA etc.

STEGANOGRAPHY:
Steganography is the art and science of hiding communication [1].
Throughout history Steganography has been used to secretly communicate information between people.
Some examples of use of Steganography of past times are:

1. During World War 2, invisible ink was used to write information on pieces of paper so that the paper appeared to the average person as just blank pieces of paper. Liquids such as milk, vinegar and fruit juices were used, because when each one of these substances is heated they darken and become visible to the human eye.
2. In Ancient Greece they used to select messengers and shave their head, they would then write a message on their head. Once the message had been written the hair was allowed to grow back. After the hair grew back the messenger was sent to deliver the message, the recipient would shave off the messengers hair to see the secrete message.
3. Another method used in Greece was where someone would peel wax off a tablet that was

So stagnography is chosen, because this system includes not only imperceptibility but also un-delectability by any steganolysis tool.
This paper is dividing into six sections, first section is general introduction about cryptography and stegnography, second section is the literature survey, third section is our proposed work, forth section is result analysis, Conclusion and references where I have completed my research work.

2. LITERATURE SURVEY
From the study of research paper and other, it is concluded that in [4] only hide the text information is. There is no use of

cryptography on this paper. It is also analyzed that [3, 5, 6, 10] used LSB for hiding data it is easy to implement and has high capacity. In [5] there is no clarification about the configuration of machine and platform where all the experiment is calculating. [5] There is no specification which symmetric algorithm used. [3] Used permutation techniques for encryption but Permutation techniques are attractive due to their efficiency. But the drawbacks of these techniques are evident in terms of generated key and security. [8, 10] used AES and [9] used S-DES algorithm for encryption. But from [11] it is concluded that after comparison between AES, DES, 3DESand Blowfish in terms of Encryption time, Decryption time and Throughput Blowfish has better performance. Also from [7] we conclude comparison between AES, DES and BLOWFISH basis of parameters like as speed, block size, and key size prove that BLOWFISH has a better performance than other common encryption algorithm

The above cases showing that using the existing algorithm like S-DES algorithm, AES and other algorithm which is mentioned in [8, 9 and 10] resulted in a lower encryption time decryption time, throughput, speed, block size and a lower key size.

3. PROPOSED WORK

Proposed Architecture

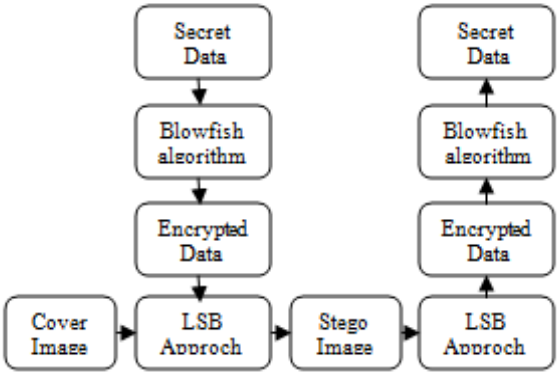


Fig. 1- Block diagram of proposed system

In proposed system the secret data is encrypted by using BLOWFISH algorithm then LSB approch is used to hide encrypted data. This process gives Stego image in which secret data is hidden into cover image. To get original data first LSB approch is applied to stego image which gives encrypted data then to it BLOWFISH algorithm is applied to encrypted data which convert encrypted data into our secret data.

Blowfish algorithm:-

Graphical representation of blowfish algorithm is given below figure 2.

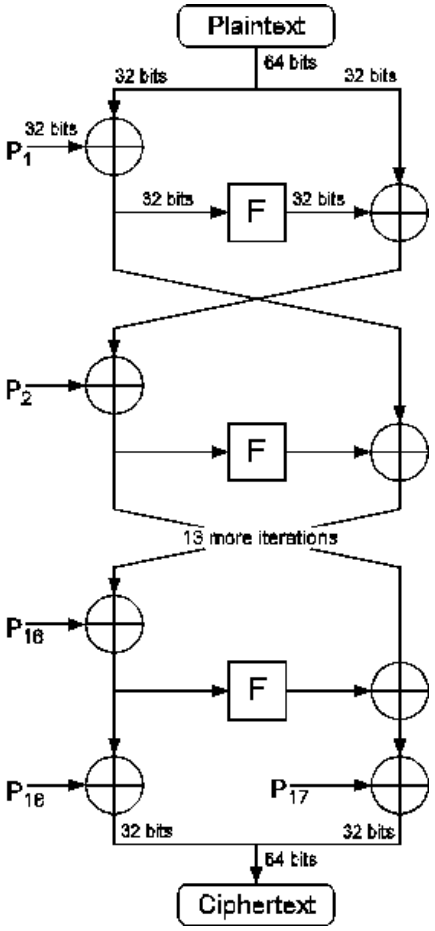


Fig.2 Blowfish algorithm

In blowfish algorithm a 64-bit plaintext message is first divided into 32 bits. The "left" 32 bits are XORed with the first element of a P-array to create a value, run through a transformation function called F, then XORed with the "right" 32 bits of the message to produce a new value. Then swap the "left" half of the message and the "right" half of the message, and the process is repeated 15 more times with successive members of the P-array. The resulting “right” half and “left” half are then XORed with the last two entries in the P-array (entries 17 and 18), and produce the 64-bit ciphertext

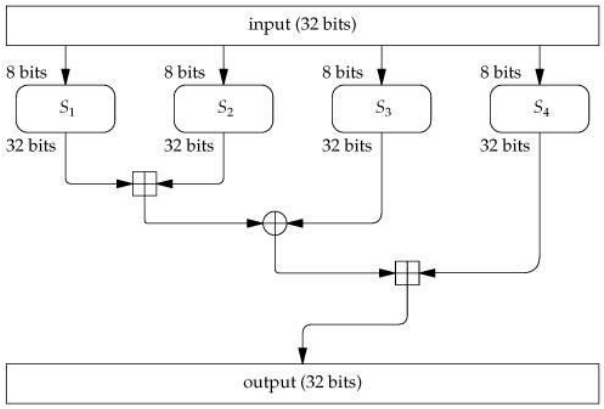


Fig:-3 Graphical representation of F.

In Figure 3 the function divides a 32-bit input into four bytes and uses those as indices into an S-array. The lookup results

are then added and XORed together to produce the 32 bits output.

LSB approach:-

Images created from pixels i.e. If any pixel created by using these three colors red, green and blue are called as RGB. Each color of a pixel is one byte information that shows the density of that color. It is known that in 8 bits the first bit is Most-Significant-Bit (MSB) and the last bit Least-Significant-Bit (LSB). Here LSB bit is used for hiding encrypted information inside the image. So if only last layer of information is used, then the last bits of the pixels has to be changed, in other hands we have 3 bits in each pixel so we have 3*height*width bits memory to write our information. But before hiding the data name of data (file) and size of data has to be written. This can do by assigning first bit of memory. Using each 3 pixel of image to save a byte of data.

(00101101	**00011101**	**11011100)**
(10100110	**11000101**	**00001100)**
(11010010	**10101100**	**01100011)**

4. RESULTS ANALYSIS

We are using C#.Net language to implementation my proposed work. The screen shots of my work are given below.

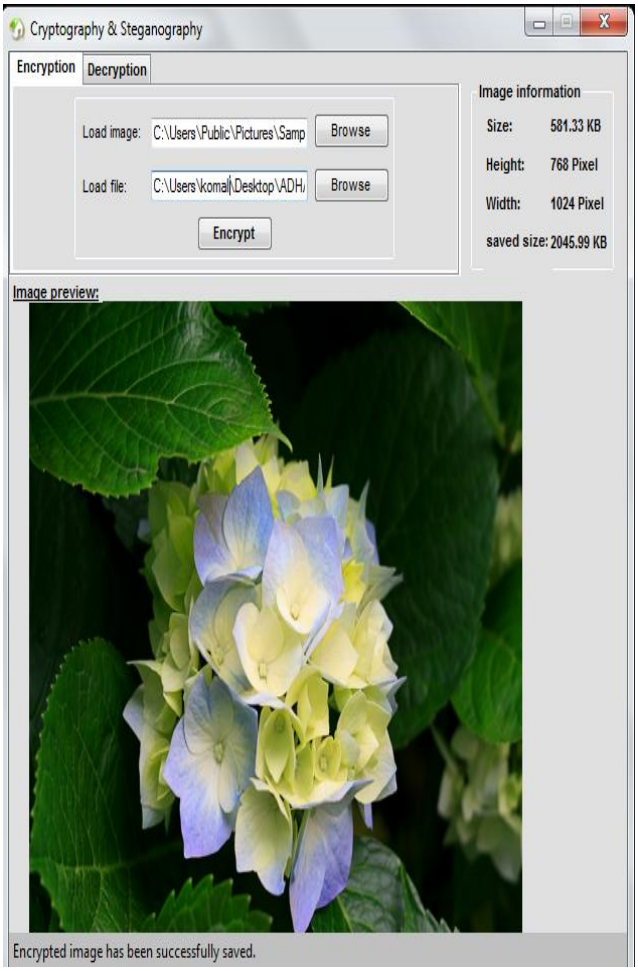


Fig 4: Snapshot of encryption window

In fig.4, encryption window is given. In this image, the information has to be hidden and then select file which is to secured from browse button. When the image is select image it automatically displays image information in top right corner. When you press encrypt button text file is encrypted and hide into image and saved into your preferred location.

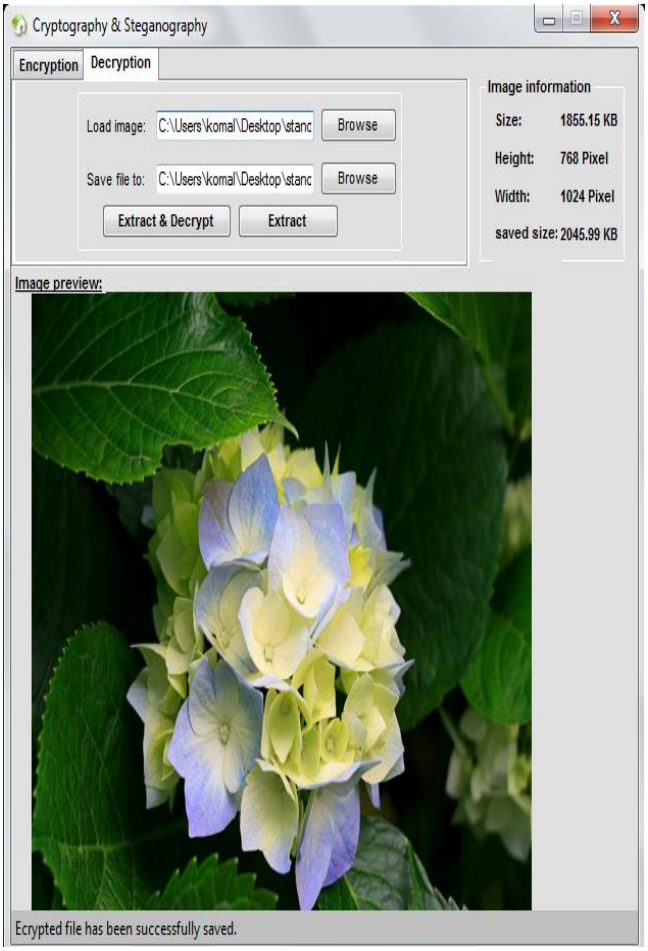
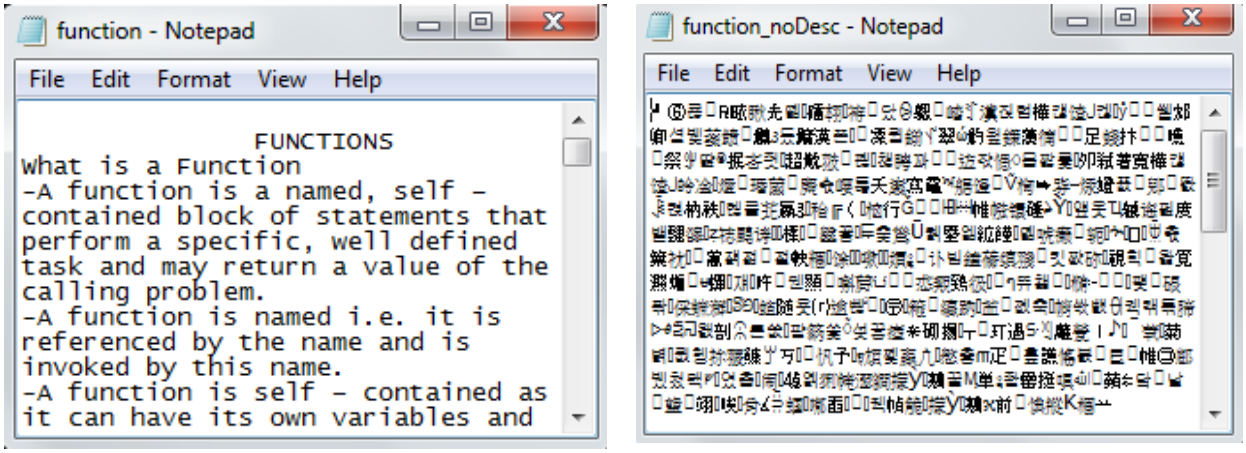


Fig 5: Snapshot of decryption window

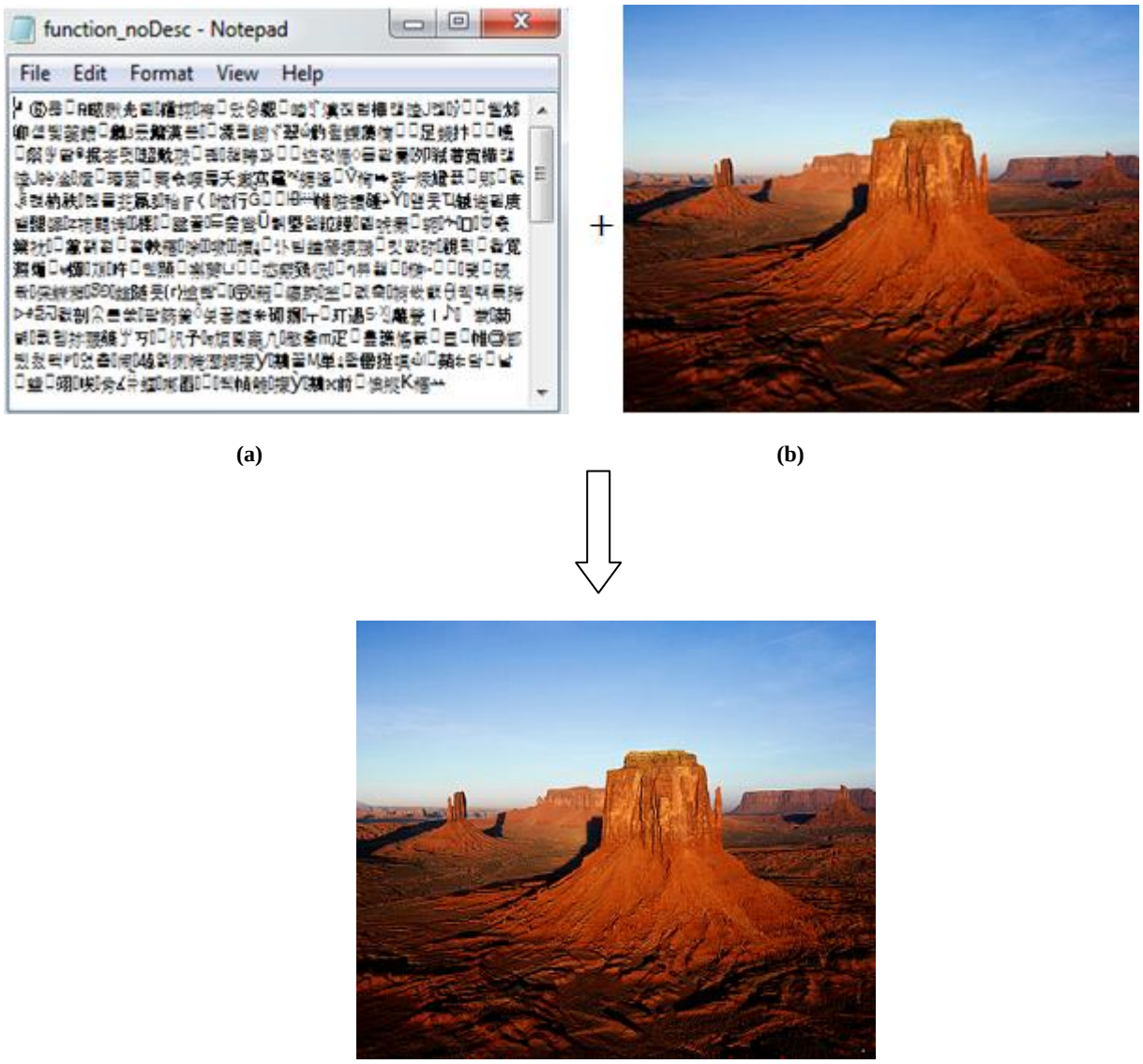
In fig. 5 decryption window is given in which first of all select the image which is Encrypted and has hidden information file by using browse button. Then preferred location is selected where original information is to be saved. In this window there are two buttons one is extract & decrypt and other is extract. When extract & decrypt button is pressed it saves original file and image into location and then when extract button is pressed it saves encrypted file and image into preferred location.

Fig 6 and Fig. 7 shows the resulted images.



(a) **(b)**

Fig .6 (a) original texts file. (b) Encrypted text file using blowfish algorithm.



(a) **(b)**

(C)

Fig. 7 (a) encrypted text file. (b) Cover image. (c) Stego image

5. CONCLUSION

Cryptography and steganography are two major techniques of data security. In the proposed system these two techniques are used for providing higher security. First the information is encrypted by using Blowfish algorithm which is better than DES and AES algorithm then the encrypted information is hidden by using LSB approach. The entire work is done in .net framework. So our techniques provide two layers of security for secret data. It is very hard for unauthorized user to find out your secret information. Finally we can conclude that the proposed technique is effective for secret data communication.

6. REFERENCES

[1] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security and Privacy Mag.", 2003, vol. 1, no. 3, pp. 32–44.

[2] William Stallings, "Cryptography and Network Security: Principles and practices", Pearson education, Third Edition, ISBN 81-7808-902-5.

[3] Harshitha K M and Dr. P. A. Vijaya , *"secure data hiding algorithm using encrypted secret message"* in International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012.

[4] M.Grace Vennice, Prof.Tv.Rao, M.Swapna, Prof.J.Sasi kiran, " *Hiding the Text Information using Stegnography*" , in nternational Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 1, Jan-Feb 2012.

[5] Mr. Vikas Tyagi, " *Data Hiding in Image using least significant bit with cryptography*", in International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012

[6] Shailender Gupta, Ankur Goyal , Bharat Bhushan, *" Information Hiding Using Least Significant Bit Steganography and Cryptography" ,* in I.J.Modern Education and Computer Science, june 2012

[7] Jawahar Thakur, Nagesh Kumar*, " DES, AES and Blowfish : symmetric key cryptography algorithms simulation based performance analysis" ,*in International Journal of Emerging Technology and Advanced Engineering Volume 1, Issue 2, December 2011.

[8] Dipti Kapoor Sarmah, Neha Bajpai , "*Proposed System for data hiding using Cryptography and Steganography "* in international gournal of computer applications,2010.

[9] Ankita Agaral , "*Security Enhancement Scheme for Image Steganography using S-DES Technique" in* International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 4, April 2012.

[10] Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R. , " *A Novel Security Scheme for Secret Data using Cryptography and Steganography"* in I. J. Computer Network and Information Security, March 2012.

[11] Gurjeevan Singh, Ashwani Kr. Singla, K.S. Sandha , *"Superiority of Blowfish Algorithm in Wireless Networks",* in International Journal of Computer Applications Volume 44– No11, April 2012