IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016), PP 130-139
www.iosrjournals.org

Data Security using Cryptography and Steganography

Ms. Arati Appaso Pujari[1], Mrs. Sunita Sunil Shinde[2]
[1] *(Department of Electronics and Telecommunication, ADCET, Ashta, India)*
[2] *(Department of Electronics and Telecommunication, ADCET, Ashta, India)*

Abstract: *As use of computer networks and internet is growing very fast and admiring day by day, information security is become a major concern in computer networks. There is always risk in violation of network security which leads a need of an efficient and simple way of securing the electronic documents from being read or used by people other than who are authorized to do it. Encryption is one of the security technique widely used to ensure secrecy. Encryption is an entirely mathematical process that takes in data, performs some predefined mathematical operations on the data, and then outputs the result. Blowfish is one of the superlative encryption algorithms because it requires less execution time, memory and has high throughput. However if any eavesdropper detects the presence of encrypted data he or she can try several attacks in order to get the original data. So there is a need to provide a two layer approach for better security. That's why this work presents a security system using combination of cryptography and steganography to enhance the security.*

Keywords: *Blowfish, Cryptography, Decryption, Encryption, Security, Steganography.*

I. Introduction

Today's world is of Computer and Internet. The Internet is a global system of interconnected computer networks to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. With the rapid growth of internet, there is need to protect the sensitive data from unauthorized access. Because of these reasons the need for information security is stronger than ever. Mechanisms which commonly employed for privacy are controlling access to the computer system or media (e.g.: via passwords), employing an access control mechanism (such as profiling), restricting physical access (e.g.: keeping media locked away or preventing access to the computer itself).

Cryptography is one of the main categories of computer security. In Cryptography the original message is transformed into non readable message. That is cryptography hides information from prying eyes.

Encryption algorithms are of two types asymmetric and symmetric. Asymmetric encryption algorithms are almost 1000 times slower than symmetric encryption algorithms, because they require more computational processing power. So symmetric encryption algorithms are commonly used now days.

Blowfish encryption algorithm is one of the symmetric algorithms which requires less execution time, memory and has high throughput as compared to others.

But cryptography is not capable of hiding the presence of data alone and it cannot protect data effectively. Any eavesdropper 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 there is a need to provide a two layer approach for providing an improved and better security. Steganography is concerned with security of transmitting data and allows communicating secretly by hiding the data within data (text/image). So for further enhancement of the data security, this system uses Blowfish algorithm along with steganography technique.

Data is encrypted by blowfish algorithm and obtained encrypted data is hidden inside a different image by using the steganography. So eavesdropper will not be aware of the presence of some secret information behind the image noticeable to eyes. So there is very low probability of acquiring that secret message. Even though the secret message is acquired by the attackers, the message is in encrypted form.

So again difficulty in acquiring secret message is increased. This paper is organized into four sections. Section II presents the techniques used in this work, while in section III implementation and result is discussed. In section for the work is concluded.

II. Techniques Used

Neither cryptography, nor steganography can alone make the data secure efficiently, so a better technique is developed by combining these two techniques. Blowfish Encryption Algorithm is used for encrypting the message to be hidden inside the image for making it non readable and secure. After encryption, LSB technique of steganography is used for further enhancing the security.

1. Cryptography

Cryptography [4, 11, 12] is the art and science of achieving security by encoding message to make them non readable form. In cryptography the original message is transformed into non readable message by applying some mathematical operations. The basic idea behind the cryptography is: at sender side it converts plaintext into cipher text by using encryption algorithms, Cipher text is transmitted over the transmission medium and finally at receiver side cipher text is converted back to the original plain text by using decryption algorithm. Fig.1 shows this idea behind cryptography.

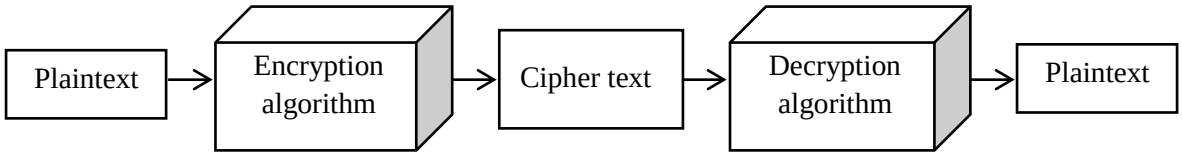

Fig. 1 Encryption and decryption Process

Many encryption algorithms are extensively available and are categorized into asymmetric and symmetric encryption algorithms. Symmetric key encryption uses same key to encrypt and decrypt data while in asymmetric key encryption two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption. Asymmetric encryption algorithms are almost 1000 times slower than symmetric encryption algorithms, because they require more computational processing power [1]. Symmetric algorithms are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish Encryption Algorithm, International Data Encryption Algorithm and Triple Data Encryption Standard etc. Out of these algorithms, Blowfish algorithm is used in this system because it is one of the superlative encryption algorithms which requires less execution time, memory and has high throughput.

1.1 Blowfish Encryption Algorithm

Blowfish is symmetric block cipher designed in 1993 by Bruce Schneier. Blowfish has a 64 bit block size data and variable key length from 32 up to 448 bits. It is a 16 round Fiestel cipher and uses a large key dependent S-boxes [4, 11, 12]. Fig.2 shows the general action of Blowfish algorithm.

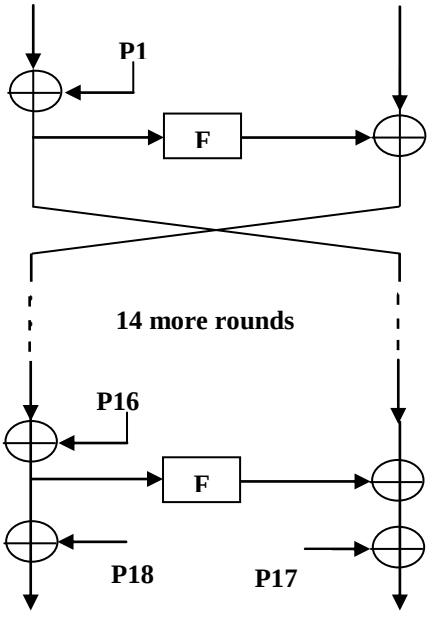

Fig. 2 General structure of Blowfish algorithm

2. Steganography

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists. The goal of Steganography is to mask the very presence of

communication making the true message not discernible to the observer. Steganography is very close to cryptography with some differences.

There are 4 different types of steganography such as Text steganography, Audio/Video steganography, Image steganography**.** Image steganography is widely used 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
a. Image domain
i. LSB and MSB in BMP
ii. LSB and MSB in JPG

After hiding Message image in Carrier image by steganography method results in Stego- Image while encrypting. This is shown in Fig. 3. At the decryption side, again by using steganography, carrier image and message image is separated out from Stego-image. This method is shown in Fig.4.

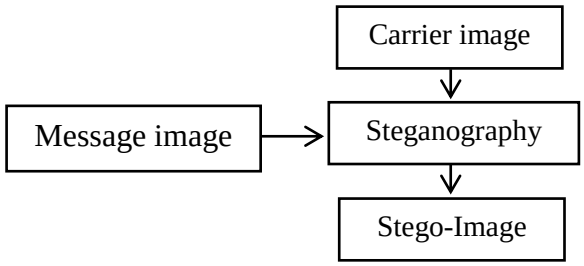

Fig. 3 Steganography process at sender side

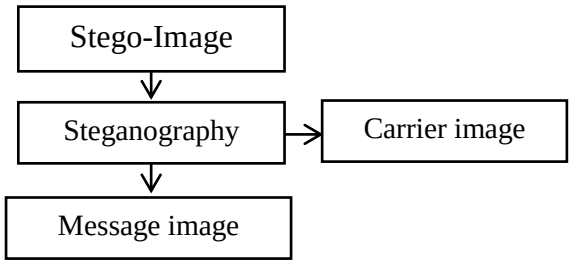

Fig. 4 Steganography process at receiver side

2.1 LSB technique

The Least Significant Bit (LSB) 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. In LSB technique intensities of message image and cover image are obtained. After that LSB bit of cover image is replaced by LSB bit of message image. Least significant bit for the patching of data is used because the intensity of image is only changed by 1 or 0 after hiding the information. The change is only one bit so that the intensity of image is not affected too much and we can easily transfer the data. This results in LSB is most efficient (in term of data hiding) method of image steganography.

Example

Consider a mask of 3X3 for Message image is as shown below:

00010111	10100101	00110011
01111000	10100000	00000111
01010111	00111110	00010000

and a mask of 3X3 for Message image is as shown below:

00011100	10110111	10100000
10000001	10000011	11111011
00110010	11001100	00111101

Then by applying LSB steganography the mask for Stego image will be

0001011**0**	10100101	0011001**0**
0111100**1**	1010000**1**	00000111
0101011**0**	00111110	0001000**1**

III. Implementation And Results

The above described work is implemented in MATLAB (Version 7.11.0.584[R2010b], 64-bit). Firstly blowfish symmetric key encryption algorithm is used which converts a text file in to a cipher text file. After that cipher text is enclosed into other image by a new layer of security called steganography. Developed work gives combination of two layers of security so the work is divided into three parts: implementation of blowfish algorithm, implementation of steganography and implementation of blowfish algorithm along with steganography.

1. Blowfish Algorithm (First layer of security system)

This level convert secret message into encrypted (Non readable) form by using blowfish encryption algorithm and in reverse original message is obtained from encrypted message by using blowfish decryption algorithm. These steps are shown in the snapshots from Fig. 5 to 7.

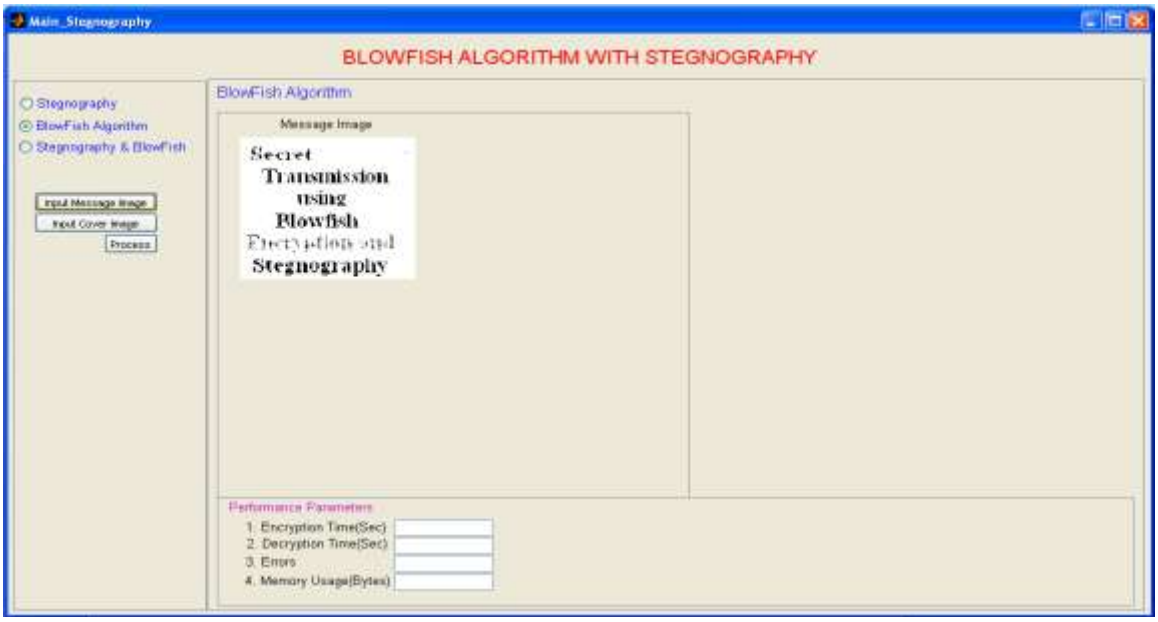

Fig. 5 Selection of message image (Blowfish algorithm)

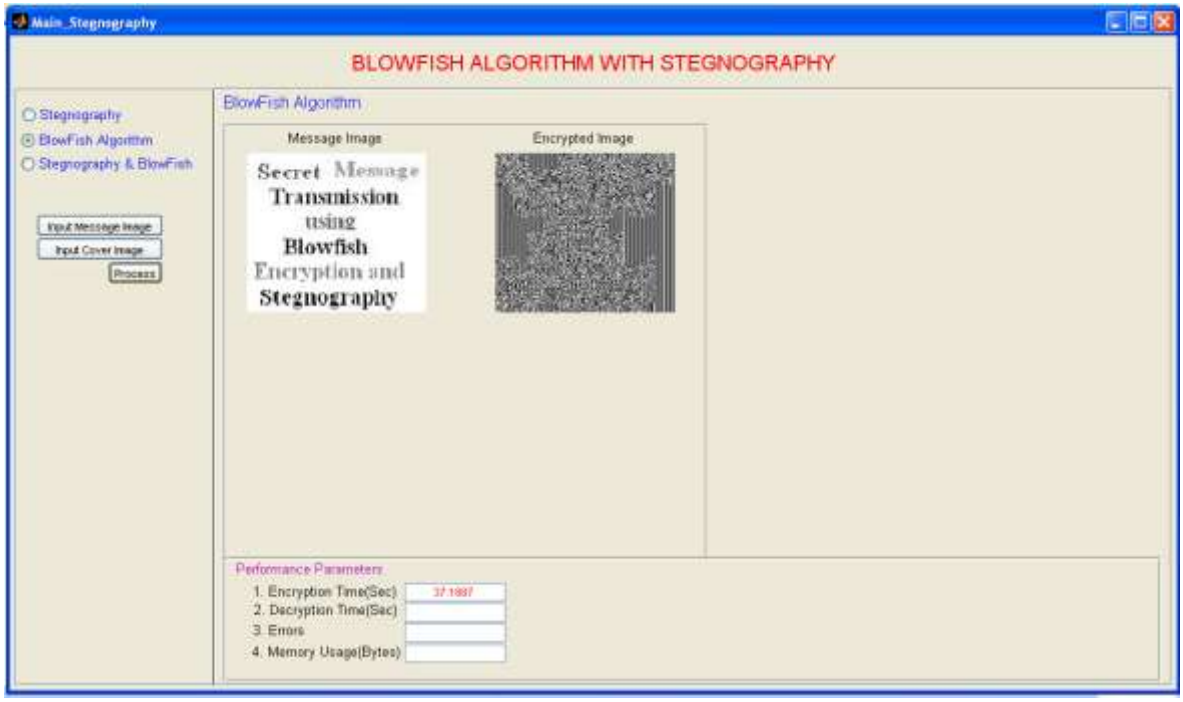

Fig. 6 Encrypted form of message image (Blowfish algorithm)

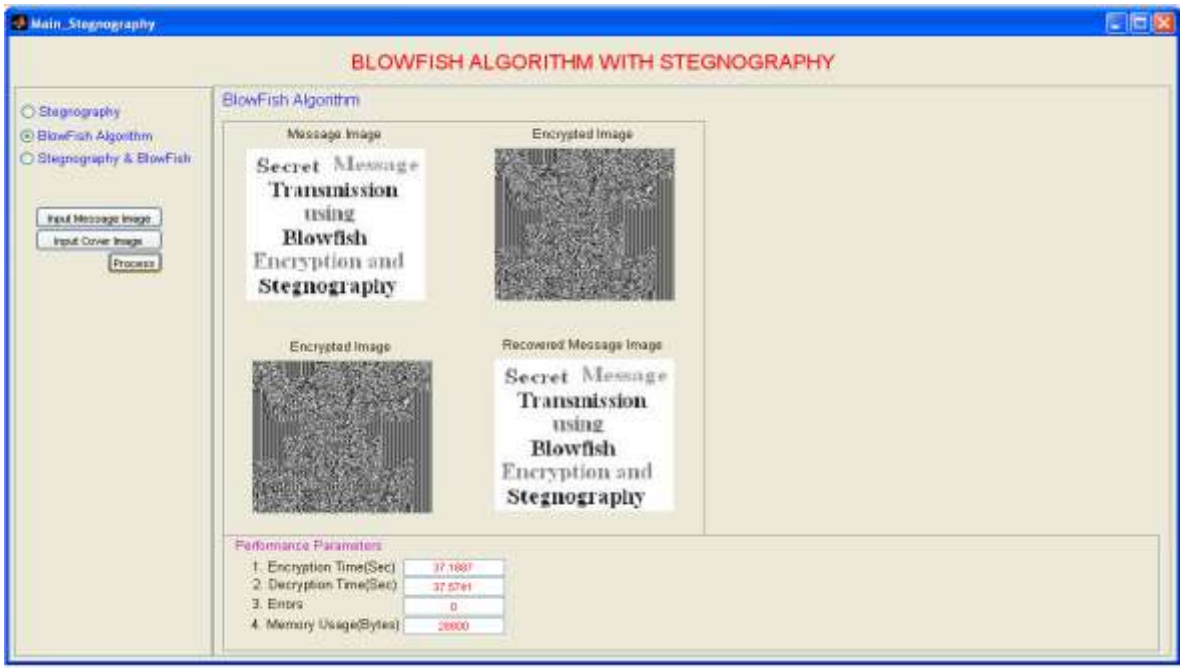

Fig. 7 Recovered message image by decryption algorithm (Blowfish algorithm)

2. Steganography (Second layer of security system)

In this level Secret message image to be transmitted and cover image used to hide the secret message image is selcted. Steganography encryption algorithm is performed to hide this secret message. The image hidding secret message image within cover image is Stego-image. In decryption the reverse operation is performed. Stego-image is the input for decryption and performing steganography original message image and cover image is retrived from stego image. Fig. 8 to 10 illustrates this method of steganography.

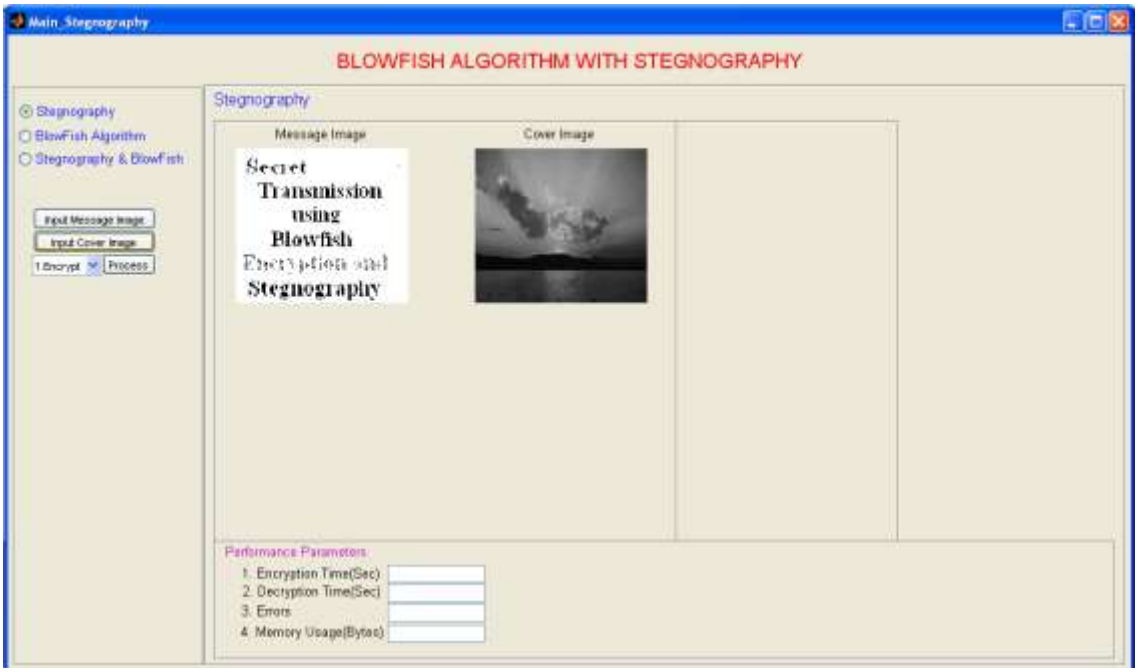

Fig. 8 Selection of message image and cover image (Steganography)

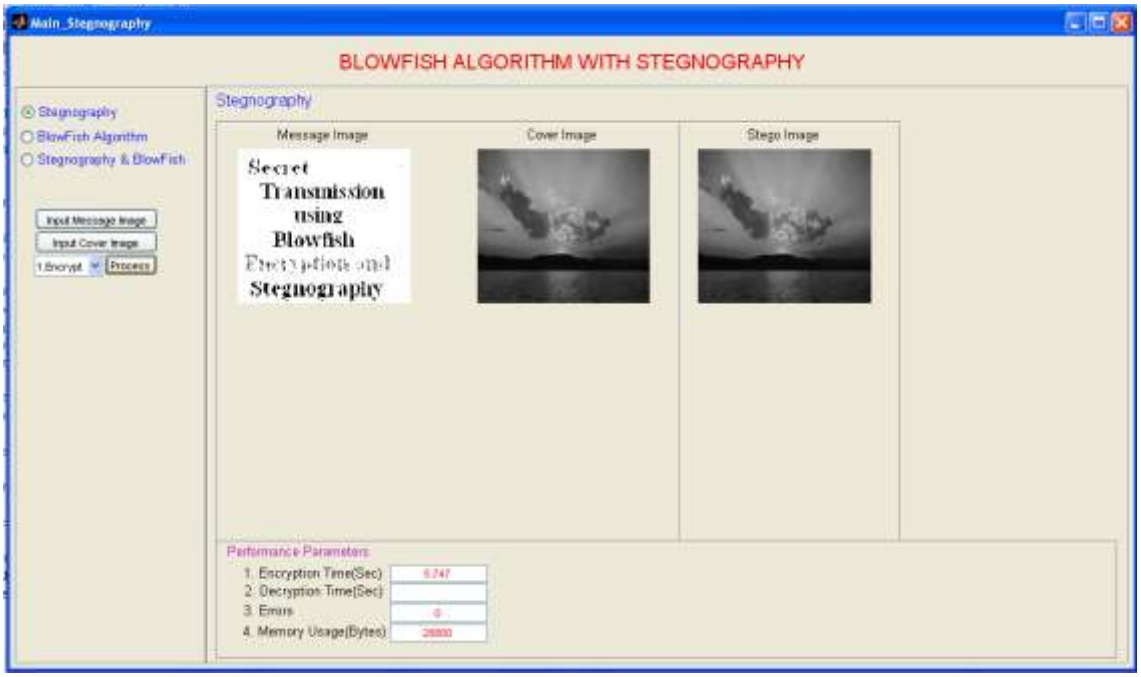

Fig. 9 Hiding of message image into cover image-Stego image (Steganography)

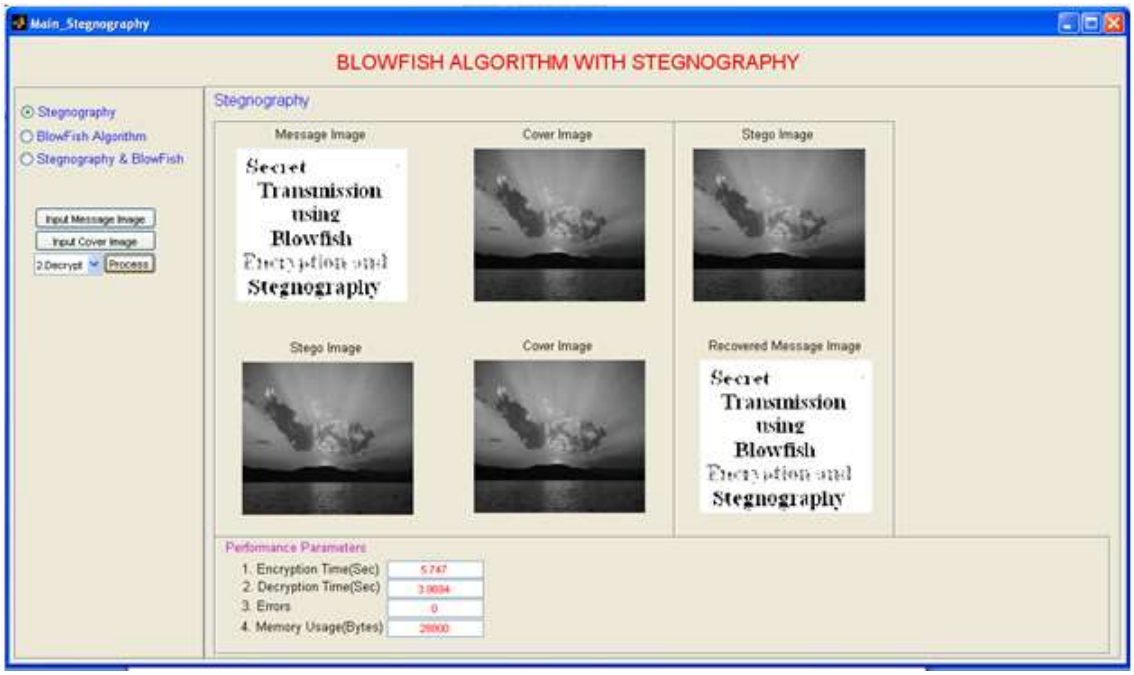

Fig. 10 Retrieved Message image and cover image from Stego image (Steganography)

3. Blowfish Algorithm along with Steganography (Combination of two layers)

This is the final stage of developed work which gives the combined effect of above mentioned two layers of security. In this stage encrypted message is hidden into cover image by steganography as discussed in following steps:

- The secret (message) image to be transmitted and cover image to hide the message image is selected (Fig.11).
- Secret image is transformed into non-readable form by performing blowfish encryption (Fig.12).
- Encrypted image is then hidden into cover image by using steganography which will results in Stego-image (Fig.13).
- At the receiver side reverse operation will be performed. First encrypted message image and cover image will be separated from Stego image by applying reverse steganography. (Fig.13)
- Finally blowfish decryption algorithm will be performed to obtain original message image (Fig.14)

Fig. 11 Selection of message image and cover image (Blowfish + Steganography)

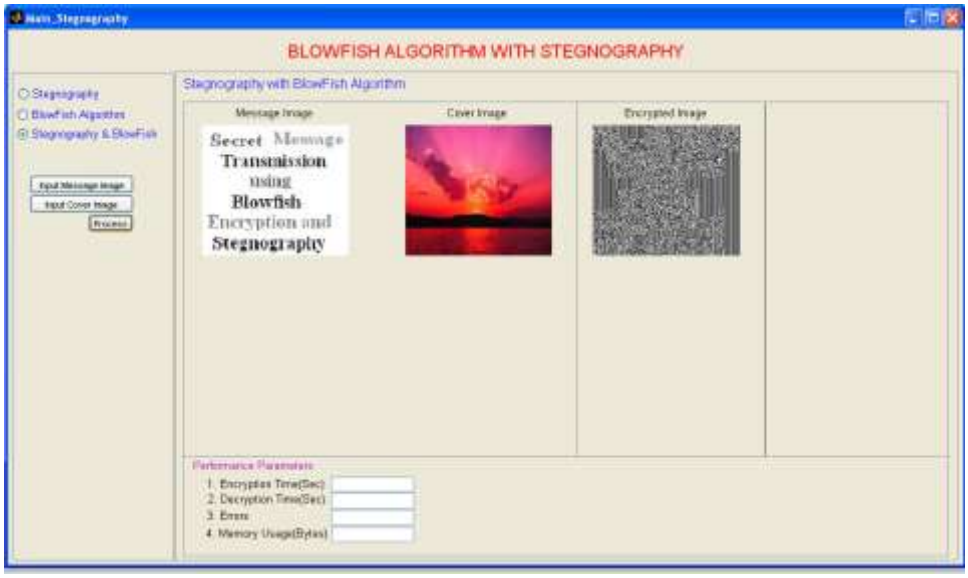

Fig. 12 Encrypted form of message image by blowfish encryption

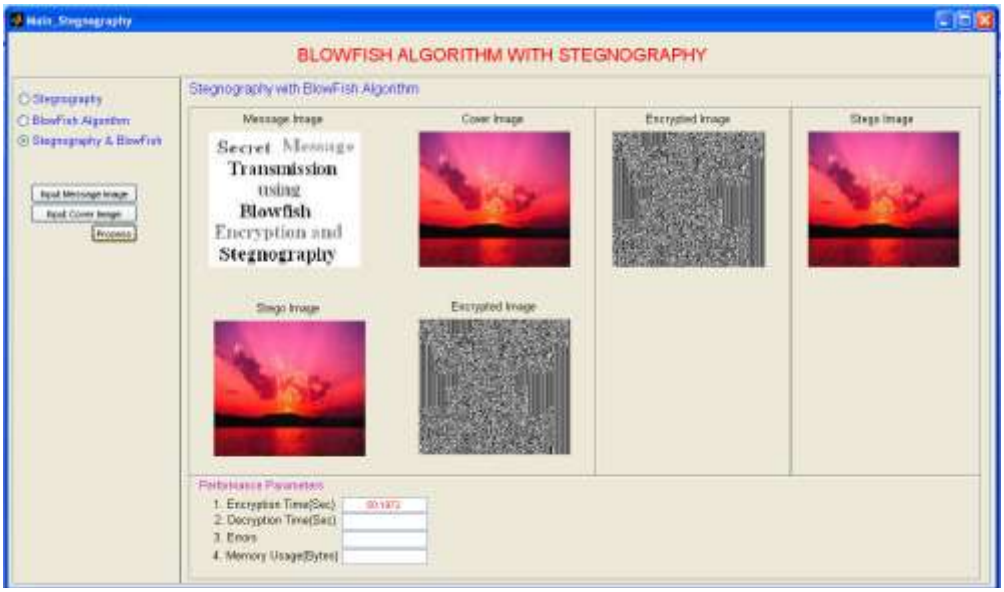

Fig. 13 Encrypted message hidden into cover image (Blowfish + Steganography)

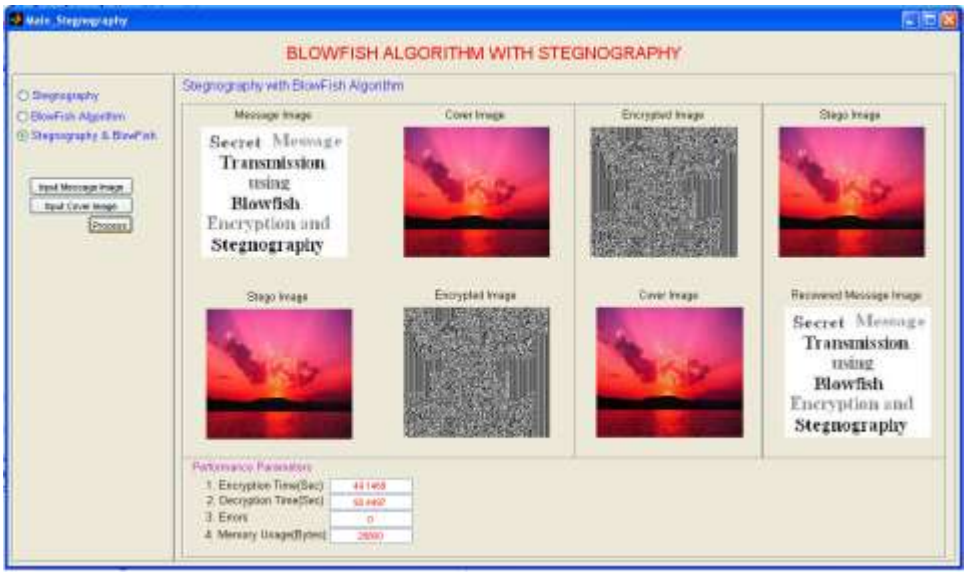

Fig. 14 Snapshot showing result (Blowfish + Steganography)

IV. Performance analysis of proposed system

The ten images of different size are used to conduct the experiments, where analysis of Steganography, Blowfish and combination of Blowfish and Steganography algorithms are performed. The experiments are carried out on MATLAB 7.11.0 (R2010b) version. The performance of these algorithms is evaluated based on metrics such as execution time, memory required for implementation and throughput.

Execution time (or) Computation time is defined as total time by the algorithm for encryption and decryption for a particular length of data. It is used to calculate the throughput. Throughput of the algorithm is calculated by dividing total plaintext size in bytes to average execution time in seconds. As throughput value is increased, the power consumption of the algorithm is decreased. It is used to know better performance of the algorithm.

The following tasks are performed

- Evaluation of Encryption and Decryption time for same dimension images
- Evaluation of Encryption and Decryption time for different dimension images
- Evaluation of throughput

4.1 Evaluation of Encryption and Decryption time for same dimension images

By analyzing Table 1 it can be stated that encryption and decryption time for different images having same dimensions (180x160) remains same for the same algorithm irrespective of their sizes. Which means that execution time of any algorithm is depend on dimension of images.

It is observed that Blowfish algorithm performs 1.4 times faster than Blowfish + Steganography algorithm. Even though Blowfish is 1.4 times faster than Blowfish + Steganography algorithm, Blowfish along with Steganography gives two layers of security. The analysis of Encryption and Decryption Time among Steganography, Blowfish and Steganography+Blowfish for identical dimension images is shown in Table 1

4.2 Evaluation of Encryption and Decryption time for different dimension images

Analysis of Encryption and Decryption Time among Steganography, Blowfish and Steganography+Blowfish for different dimension images is shown in Table 2 and Table 3. By observing these tables it can be stated that as dimension changes encryption and decryption time for different images having different dimensions changes for same algorithm. As dimension changes execution time increases with increase in size of plaintext. For this case also Blowfish algorithm performs 1.4 times faster than Blowfish + Steganography algorithm.

Table 1 Analysis of Encryption and Decryption Time among Steganography, Blowfish and Steganography+Blowfish for identical dimension images (180X160)

Message Image (Bytes)	Cover Image (Bytes)	Algorithm					
		Steganography		Blowfish		Steganography+Blowfish	
		Encryption Time(Sec)	Decryption Time(Sec)	Encryption Time(Sec)	Decryption Time(Sec)	Encryption Time(Sec)	Decryption Time(Sec)
4792	20480	5.3	3.7	36.1	36.4	47.7	48.7
5939	20480	5.4	3.8	36.3	36.6	47.8	49.6
6553	20480	5.3	3.8	36.6	35.6	47.9	48.8
6563	20480	5.4	3.8	35.5	35.5	48.1	48.9
7106	20480	5.4	3.9	35.7	35.5	47.9	48.9
7168	20480	5.3	3.8	35.6	35.6	47.7	48.8
7229	20480	5.4	3.8	35.8	35.7	48.0	48.8
7393	20480	5.6	3.8	36.2	36.0	48.4	48.9
8151	20480	5.7	3.9	35.7	35.7	47.8	48.8
10956	20480	5.3	3.8	35.8	36.1	47.8	48.8
20480	4792	5.2	3.1	36.1	35.8	47.5	48.9
20480	5939	5.4	3.8	35.6	35.5	47.9	48.7
20480	6553	5.4	3.8	35.6	35.4	47.6	48.5
20480	6563	5.3	3.8	35.5	35.7	47.7	49.1
20480	7106	5.3	3.8	35.4	35.5	48.2	49.3
20480	7168	5.3	3.9	35.5	35.5	48.0	49.1
20480	7229	5.3	3.8	35.4	35.4	47.8	49.0
20480	7393	5.3	3.8	35.4	36.0	47.7	48.6
20480	8151	5.3	3.8	35.4	36.0	47.6	48.5
20480	10956	5.4	3.8	35.4	36.2	47.5	48.6

Table 2 Analysis of Encryption and Decryption Time among Steganography, Blowfish and Steganography+Blowfish for different dimension images

Dimensions	Message Image (Bytes)	Cover Image (Bytes)	Algorithm					
			Steganography		Blowfish		Steganography+Blowfish	
			Encryption Time(Sec)	Decryption Time(Sec)	Encryption Time(Sec)	Decryption Time(Sec)	Encryption Time(Sec)	Decryption Time(Sec)
120 x 110	4771	2631	2.52	1.97	16.55	17.06	22.47	22.50
140 x 124	5386	3215	3.31	2.37	21.08	21.04	28.75	28.97
180 x 160	5099	21913	5.48	4.19	35.52	35.83	48.70	49.39
300 x 198	11673	9902	12.02	8.05	78.94	79.58	102.99	108.10
300 x 225	16793	14438	13.09	9.16	87.45	88.96	119.69	119.22
300 x 271	13926	20172	15.83	10.98	102.27	102.40	144.34	148.64
280 x 300	16793	16588	16.36	11.61	106.88	105.85	143.90	148.44
600 x 400	16384	20889	44.46	32.60	296.79	294.93	399.52	407.56

Table 3 Analysis of Execution Time among Steganography, Blowfish and Steganography+Blowfish for different dimension images

Dimensions	Message Image (Bytes)	Cover Image (Bytes)	Total size of plain text (Bytes)	Execution Time (Sec)		
				Steganography	Blowfish	Steganography+Blowfish
120 x 110	4771	2631	7402	4.5	33.6	45.0
140 x 124	5386	3215	8601	5.7	42.1	57.7
180 x 160	5099	21913	27012	9.7	71.4	98.1
300 x 198	11673	9902	21575	20.1	158.5	211.1
300 x 225	16793	14438	31231	22.3	176.4	238.9
300 x 271	13926	20172	34098	26.8	204.7	293.0
280 x 300	16793	16588	33381	28.0	212.7	292.3
600 x 400	16384	20889	37273	77.1	591.7	807.1

4.3 Evaluation of Throughput

Throughput of the Steganography is 1033.9 while throughput of the Blowfish algorithm is 134.5. Means Steganography performs approximately 7 times faster than Blowfish. Blowfish performs only 1.4 times faster than combination of Blowfish and Steganography but combination gives two layers security approach. This Analyzed Throughput among Steganography, Blowfish and Steganography+Blowfish is shown in Table 4

Table 4 Analysis of Throughput among
Steganography, Blowfish and Steganography+Blowfish

Algorithm	Throughput (bytes/sec)
Steganography	1033.9
Blowfish	134.5
Steganography + Blowfish	98.2

IV Conclusion

To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. So in this work blowfish algorithm along with steganography is implemented to secure sensitive data by making difficult to detect the presence of hidden message. Two layer approach of security is implemented and some conclusions are made as listed below.

- Blowfish algorithm is one of the superlative encryption algorithms because it requires less execution time, memory and has high throughput.
- Same dimension images require same execution time for same algorithm.
- Images with different dimensions require different execution time for same algorithm. This execution time changes with change in dimensions. Hence with increase in dimensions execution time for the algorithm also increases.
- Steganography performs seven times faster than Blowfish while alone blowfish algorithm performs 1.4 times faster than combination of Blowfish and Steganography.
- Although blowfish algorithm performs 1.4 times faster than combination of Blowfish and Steganography, the combination provides two layer approach of security and will provide much efficient and reliable security.

References

Journal Papers:

[1]. Russell K. Meyers and Ahmed H. Desoky, "An Implementation of the Blowfish Cryptosystem", IEEE conference 2008

[2]. Ajit Singh and Swati Malik, "Securing Data by Using Cryptography with Steganography", International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013

[3]. SumedhaKaushik and AnkurSinghal, "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 12, December 2012

[4]. Dr. A. Suruliandi and A. Ramesh, "Performance Analysis of Encryption Algorithms for Information Security", International Conference on Circuits, Power and Computing Technologies 2013

[5]. PratapChnadraMandal, "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012

[6]. Jawahar Thakur and Nagesh Kumar, "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Emerging Technology and Advanced Engineering Volume 1, Issue 2, December 2011

[7]. Pia Singh and Prof. Karamjeet Singh, "Image Encryption and Decryption using Blowfish Algorithm in Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013

[8]. B. Schneier, "The blowfish encryption algorithm - one year later," Dr. Dobb's Journal, 1995.

[9]. Nicholas Hopper, Luis von Ahn, and John Langford, Provably Secure Steganography", IEEE TRANSACTIONS ON COMPUTERS, VOL. 58, NO. 5, MAY 2009.

[10]. Mr .VikasTyagi, Mr. Atulkumar, Roshan Patel, SachinTyagi and Saurabh Singh Gangwar, "IMAGE STEGANOGRAPHY USING LEAST SIGNIFICANT BIT WITHCRYPTOGRAPHY", Journal of Global Research in Computer Science, Volume 3, No. 3, March 2012

Books:

[11]. Cryptography & Network Security by Atul Kahate-Tata McGraw-Hill Publishing Company Ltd, New Delhi

[12]. Cryptography and Network Security by William Stallings-Prentice-Hall of India Private Ltd, New Delhi.