The Effect of the Smoothing Filter on an Image Encrypted By the Blowfish Algorithm Then Hiding It in A BMP Image

Nada Abdul Aziz Mustafa
Iraq, Baghdad, University of Baghdad, College of Languages
E-Mail:alilayan@yahoo.com

Abstract

This research includes the use of a combination of Cryptography and Steganography in order to increase the level of security, as this system encrypts the secret image before sending it through the internet to the recipient (by the Blowfish method). As The Blowfish method is known for its efficient security; nevertheless, the encrypting time is long. In this research we try to apply the smoothing filter on the secret image which decreases its size and consequently the encrypting and decrypting time are decreased. The secret image is hidden after encrypting it into another image called the cover image, by the use of one of these two methods "Two-LSB" or" Hiding most bits in blue pixels". Eventually we compare the results of the two methods to determine which one is better to be used according to the PSNR measures.

Keywords: *Smoothing Filter, Gaussian Filter, Cryptography, Blowfish, Steganography.*

1. Introduction

Cryptography and Steganography are two popular ways of sending vital information in a secret way [1]. The security of information is an important issue related to privacy and safety during storage and communication. There are several techniques used for hiding information in any medium. In cryptography, the longer the key size, the more secure it becomes, but the encryption time and decryption speed is slow. In order to overcome this problem in Blowfish algorithm we reduce the two S-boxes which increase the speed and provide a better security to the data. The salient features of Blowfish algorithm manipulates data in large blocks and uses very simple operations like addition and XOR addition [2].

Cryptography protects information by transforming it into unreadable format. Data from a source file is hidden by altering insignificant bits of information in a host file. The information hiding process in a steganographic system starts by identifying a cover medium's redundant bits [3]. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Steganography can be classified into image, audio and video steganography depending on the cover medium [1].

2. Smoothing Filter

Filtering is transforming the pixel intensity values to reveal certain image characteristics. Smoothing, also called blurring, is an important image processing operation which is necessary to reduce noises [4]. The most effective basic spatial filtering techniques for noise removal include: mean filtering, median filtering and Gaussian smoothing.

2.1. Gaussian Filter

The Gaussian smoothing operator is a 2-D, used to `blur' images and remove detail and noise, high pass filters and low pass filters are used to show some details in the image while hiding other details. Low pass filters blur the image which leads to noise reduction while high pass filter sharpen some image details, such as edges. In the case of Gaussian filtering, the frequency coefficients are not cut abruptly, but smoother cut of process is used instead [5]. Probably the most useful filter (although not the fastest).Gaussian filters may not preserve image brightness. 2-D Gaussian can be represented as:

$$G_0(x,y) = Ae^{\frac{-(x-\mu_x)^2}{2\sigma_x^2}+\frac{-(y-\mu_y)^2}{2\sigma_y^2}}$$

Where μ is the mean (the peak) and σ represents the variance (per each of the variables x and y). Central pixels have a higher weighting than those on the periphery. Larger values of σ produce a wider peak (greater blurring) [6].

3. Cryptography using Blowfish

Encryption and decryption of images using a secret-key block cipher is called "64-bits Blowfish", which is designed to increase security and improve performance.

This algorithm will be used as a variable key size up to 448 bits. The blowfish algorithm is safe against unauthorized attack and runs faster than the popular existing algorithms.

A colored image is usually represented in the RGB color space; each vector consists of three components, representing the intensity values in the Red, Green and Blue. The combination of these values delivers one particular color. A change in the intensity value will change the information stored in the picture, thus, performing some changes in intensity values enables us to encrypt the image and do the reverse in decryption [7]. All the changes in the intensity values are performed using a mathematical function [8]. The encryption algorithm produces a cipher image which is sent to the recipient through a communication channel. When the cipher image reaches the destination, the recipient enters the key and the original image is decrypted [9].

3.1. Encryption Process

Encryption process includes two inputs: the Data image as a plaintext and the encryption key. In this case, the original image data bit stream is divided into the blocks length of the Blowfish algorithm [7].the Image header is excluded in order to encrypt, and the start of the bitmap pixel or array begins right after the header of the file [10]. The byte elements of the array are stored in a row order from left to right, with each row representing one scan line of the image and the rows of the image are encrypted from top to bottom [8].

3.2. Decryption Process

The first block is entered to the decryption function and the same encryption key is used to decrypt the image, but the application of sub keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom [11]. The basic algorithm for the Blowfish method is illustrated as follows:

Divide X into two 32-bit halves XL and XR

For i=1 to 16:

XL = XL Pi

XR = F (XL) XR

Swap XL and XR

End for

Swap XL and XR

XR = XR P17

XL = XL P18

Recombine XL and XR

Output X (64-bit data block: cipher text) [9].

The same process is applied for decryption, except that the Sub-keys Pi must be supplied in a reverse order. The encrypted image is divided into the same block length of the Blowfish algorithm from top to bottom [10].

4. Steganography

Two types of a steganographic technique are used:

4.1. Two Least Significant Bit Replacement Method

24 bit color image is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye. The total number of color possible with 24-bit RGB image is $(2^8)^3 = 16,777,216$. In the case of 24 bit color image , each pixel is composed of RGB values and each of these colors requires 8-bit for its representation. [R (8 bits), G (8 bits), B (8 bits)][12]. we have to replace the last 2 - LSB of each of the RGB component and then embedding the first 2 MSB of first pixel of the secret image to the R component, then the next 2 MSB of the first pixel of the secret image to the G component and lastly, the next 2 MSB of the first pixel of the secret image to the B component[1].

A LSB-based Embedding Algorithm
Input -: cover C
for i = 1 to Length(c), **do**
$S_j \leftarrow C_j$
for i = 1 to Length(m), **do**
Compute index j_i where to store the i^{th} message bit of m
$S_{ji} \leftarrow LSB(C_{ji}) = m_i$
End for
Output -: Stego image S

A LSB-based Extracting Algorithm
Input -: Secret image s
for i = 1 to Length (m), **do**
Compute index j_i where to store the i^{th} message bit of m
$m_{ji} \leftarrow LSB(C_{ji})$
End for

In the extraction process, the embedded messages can be readily extracted without referring to the original cover-image from the given stego-image S [9]. The set of pixels storing the secret message bits are selected from the stego-image, using the same sequence as in the embedding process. Then LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits, Example 2-LSB Method for 24 Bit Color Image:

RGB first pixel can be represent as [11011100 11000110 10000111]

Embedding secret image [11001001]

we have to replace the last 2 - LSB of each of the RGB component and then embedding the first 2 MSB of the first pixel of the secret image to the R component, then the next 2 MSB of the first pixel of the secret image to the G component and lastly, the next 2 MSB of the first pixel of the secret image to the B component. In this way we get the stego image whose first pixel is: [11011**11** 11000**00** 100000**10**] [12].

In this method, the 6 bits of the secret image gets hidden by replacing only 2 bits of the RGB component so that the stego-image is visually indistinguishable from the original cover-image in the case of 24 bit.

4.2. Hiding Most of the Secret Image Bits in Blue Pixels

In this method the cover image is the 24 bit color image. At first, this cover image is split into its 3 planes (red, green, blue). The main aim of this method is to hide most of the secret image bits in the blue pixels rather than the red and green pixels. The blue pixels are chosen on the basis of a research that was conducted by Hecht**,** according to which 65% of all cones of human eyes are sensitive to red, 33% are sensitive to green, and only near about 2% are sensitive to blue, as a result visual perception of intensely blue objects is less distinct than the perception of objects of red and green[13].

Steps to be carried out in this technique:

1) Select the cover image, multiply the red pixels by 254 to make the last bit 0 : by "bitand(c(x,y,1), uint8(254))" command. Obtain the first MSB i.e. 8th bit of the secret image and then embed it in the last LSB of the red pixels.

2) Take the green pixels of the cover image and convert its last 2 LSBs to 0 by "bitand" command, multiplying each pixel with 252 : "bit and(c(x,y,2), uint8(252))". Obtain next to MSB i.e. 7th and 6th bit of the secret image and embed it into the green plane.

Lastly take the blue plane of the cover image and convert its last 3 LSBs to 0 by "bitand" command multiply each pixel by 248: "bitand(c(x,y,3), 248)". Obtain the next 3 MSB i.e. 5th , 4th and 3 rd bit of the secret image and embed it into the blue plane , so if the 24 bit color image first pixel is represented as: [11011100 11000110 10000111]

Then for embedding the secret image whose first pixel is [11001001], we follow the above step and get the stego image whose first pixel is [14]:

[11011101 11000110 10000010].

5. Testing

In the steganography technique: PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Squared Error) are standard measurement used in order to test the quality of the stego images. MSE measures the average of the squares of the errors [5]. The error is the amount by which the pixels value implied by the stego image differs from the cover image. PSNR, define ratio between the maximum possible power of a signal and the power of the corrupting noise that affects the fidelity of its representation. The signal in this case is the cover image, and the noise is the error introduced by bits of the secret image**,** increasing the value of PSNR, increases the quality of the stego image. The PSNR and MSE are then calculated as follows:

$$\text{PSNR} = 10 \log_{10} \frac{\text{MAX}^2}{\text{MSE}} (\text{db})$$

Where

$$\text{MSE} = \frac{1}{\text{MN}} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (\alpha_{i,j} - \beta_{i,j})^2$$

Here, $\alpha_{i,j}$ is the pixel of the cover image where the coordinate is (i, j), and $\beta_{i,j}$ is the pixel of the stego-image where the coordinate is (i, j). M and N represent the size of the image [14]. The use of "the hiding most of the secret image bits in blue pixels" method has shown to be better than two-LSB method, according to the PSNR measures.

6. Proposed system

The proposed system consists of two steps:

A- Sending the secret image.
B- Receiving the secret image.

A-The process of sending the secret image, includes the following steps, see fig1:

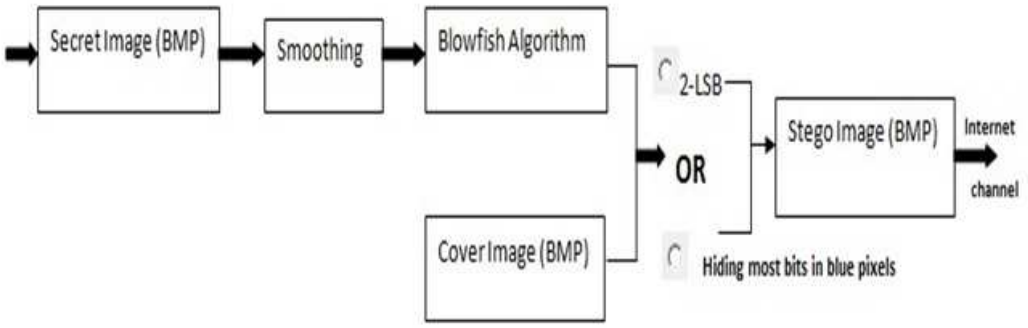

Figure 1. Shows the sending process of an image

1) Reading a BMP image (secret image).

2) Applying the smoothing filter (Gaussian filter) on this image in order to reduce its noise.

3) Encrypting the image by using the Blowfish method.

4) Selecting a BMP image (the cover image).

5) Encoding the first secret image into the BMP cover image, forming the Stego Image, through the use of either of these two methods (2- LSB or Hiding most of the secret image bits in blue pixels).

6) Sending the stego image BMP to the recipient through the internet, see fig 2:

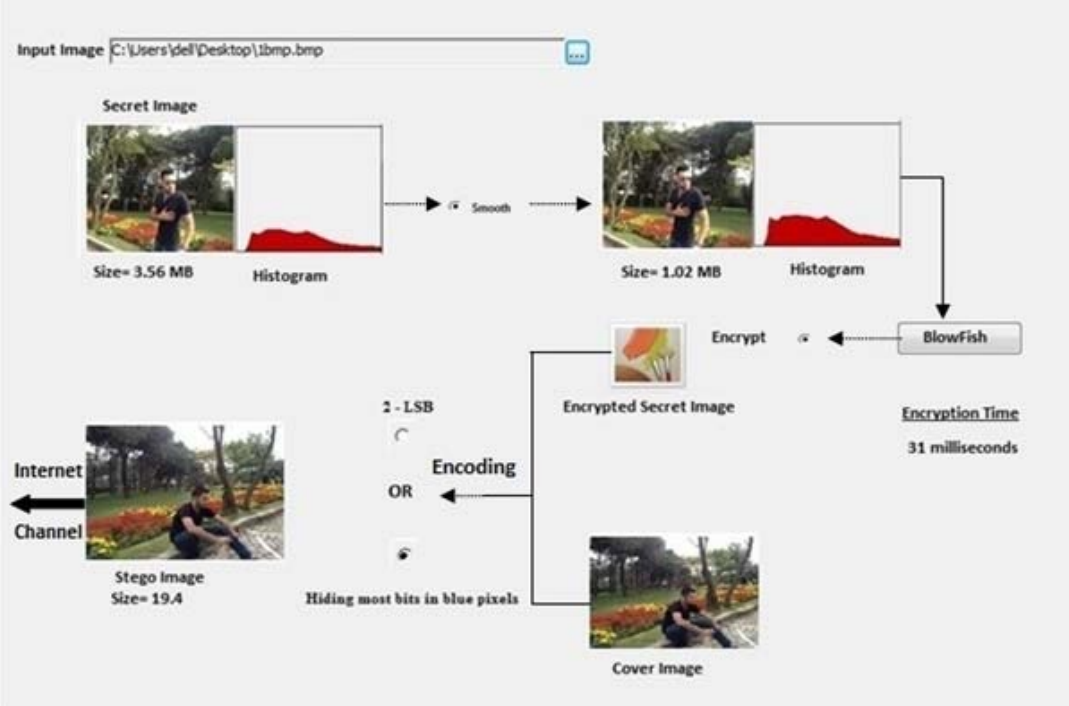

Figure 2. Shows the sending system

B-The process of receiving the secret image, includes the following steps, see fig3:

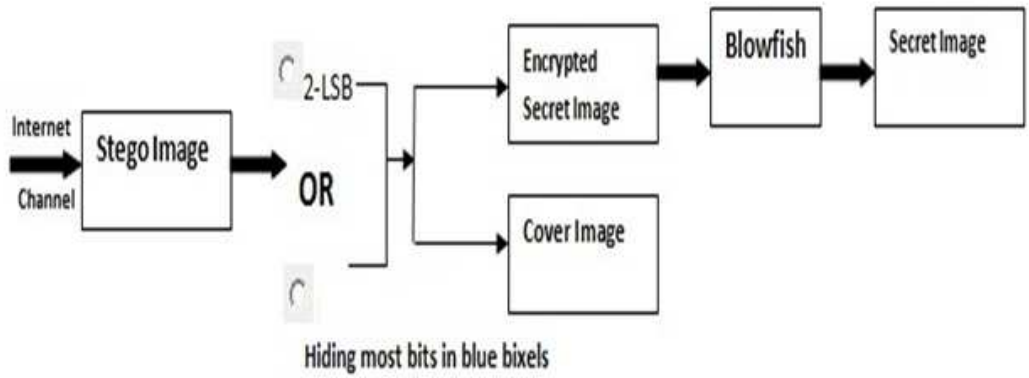

Figure 3. Shows the process of receiving the secret image

1) The stego image has been received.

2) Applying the decoding method to obtain the secret encrypted image (which had been encrypted using the Blowfish method).

3) Applying the decrypting method to obtain the original secret image, see fig4:

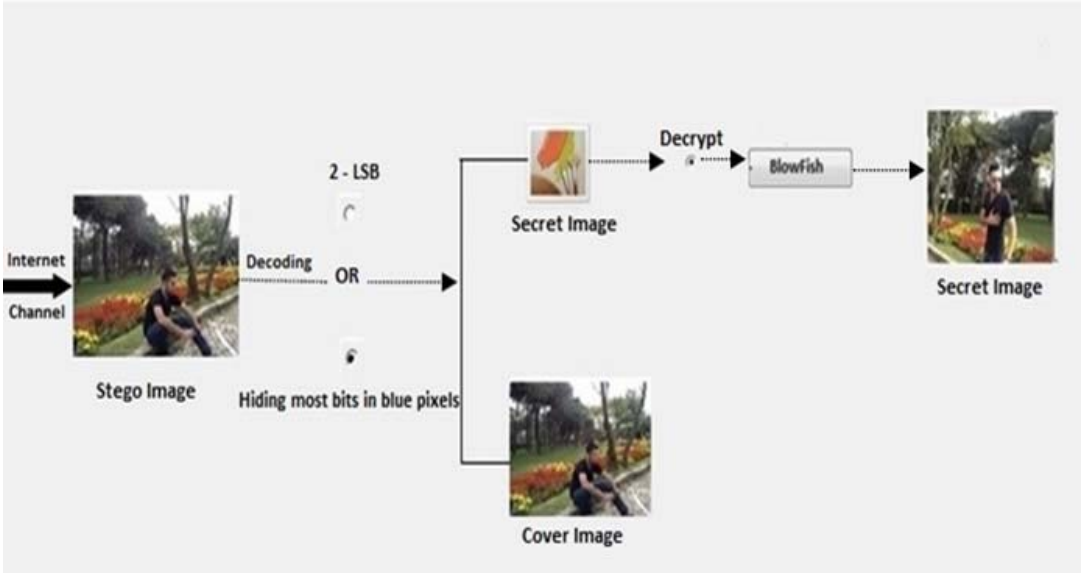

Figure 4. Shows the receiving system

7. Conclusion

1) Applying smoothing filter to a BMP image reduces the time required for encryption using the Blowfish method.
See fig5 and fig 6.

Figure 5. Shows the size of the original image before smoothing it, the encryption, and decryption time

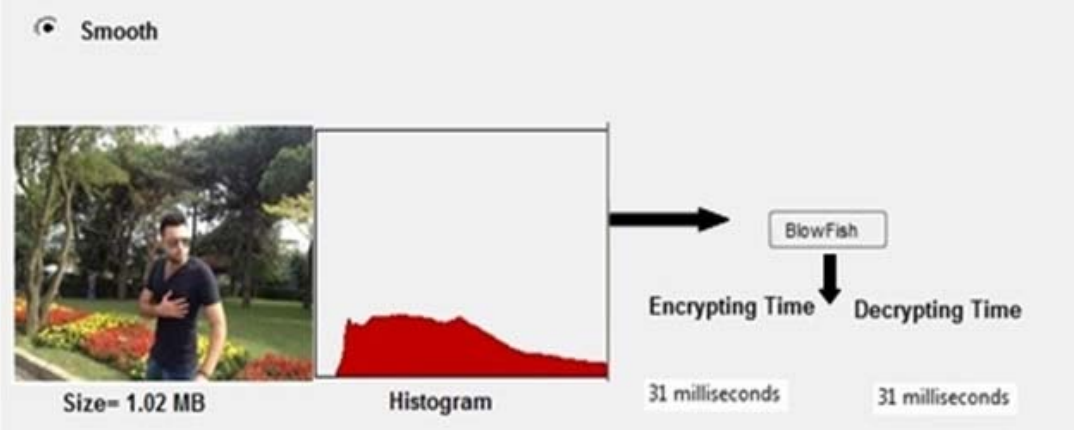

Figure 6. Shows the size of an image after smoothing it, the encryption, and decryption time

2) The use of Gaussian filter doesn't affect the image's properties. When smoothing an image, we don't only reduce the noise, but also the fine-scaled image details, which reduces the size of the image leading to a decrease in the time of encryption and decryption.

3) Two methods have been used in the steganography process, in which the use of "the hiding most of the secret image bits in blue pixels" method has shown to be better than two-LSB method, according to the PSNR measures, see table1.

Table 1. Shows the size, PSNR, encryption and decryption time

	Size	PSNR		Encrypted Time	Decrypted Time
		2-LSB	Hiding most bits in blue pixels		
Original Image	3.56 MB	40.23	48.04	78milliseconds	94milliseconds
Smoothing Image	1.02 MB	40.23	48.04	31milliseconds	31milliseconds

4) Combing steganography and cryptography increases security.
5) The Blowfish algorithm can be considered as an excellent standard encryption algorithm that cannot be broken until an attacker tries 28r+1 combination (where r is the number of rounds), if the number of rounds are increased then the blowfish algorithm becomes stronger. The longer the key size is, the more secure it becomes, but the encryption time and decryption speed is slow. In order to overcome this problem while encrypting an image by the Blowfish algorithm, the size of image is reduced.
6) A better robust visual cryptographic system can be obtained if the changes in an image are performed separately on Red, Green and Blue layers, because the intruder tries to know these basic intensity values when he goes for a complete analysis of the image. These intensity values are helpful to generate the original image. So if the encryption is done at this basic level, it will be hard to break the system.
7) During the encoding and decoding process, both the cover image and the stego image are shown, from this view and through the comparison between the two images ,one can conclude that the hiding process is not noticeable for the human eyes and doesn't affect the image quality. See figure 7 and figure 8

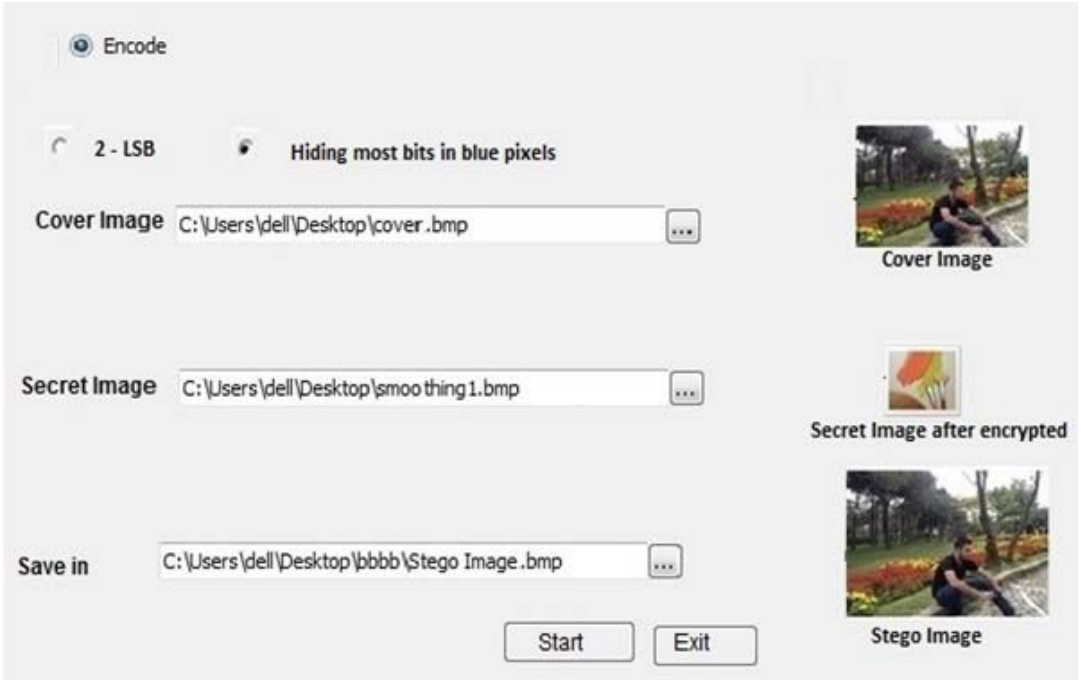

Figure 7. Shows the encoding system

Figure 8. Shows the decoding system

8. References

[1] Shery Elizabeth Thomas, Sumod Tom Philip;" Advanced Cryptographic Steganography Using Multimedia Files", International Conference on Electrical Engineering and Computer Science (ICEECS-2012), May 12th, 2012, Trivandrum and ISBN Number: 978-93-81693-58-2.

[2] Dr. J. Abdul Jaleel, Jisha Mary Thomas; "Guarding Images using a Symmetric key Cryptographic Technique: Blowfish Algorithm", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 2, August 2013, ISSN: 2277-3754, ISO 9001:2008 Certified.

[3] Niels Provos and Peter Honeyman;"Hide and Seek: An Introduction to Steganography", Published By the IEEE Computer Society,1540-7993/03/17.00, 2003 IEEE, IEEE Security & Privacy.

[4] S. Biswas, N. R. PAL and S. K. PAL; "Smoothing Of Digital Images Using The Concept of Diffusion Process", Machine Intelligence Unit, Indian Statistical Institute, 203 B.T. Road, Calcutta 700 035, India, (Received 23 March 1994; in revised form 5 June 1995; received for publication 3 July 1995), Copyright 1996 Pattern Recognition Society Printed in Great Britain, 0031-3203(94)00093-3.

[5] Ayush Dogra, Dr. Manjeet Singh Patterh; "Performance Comparison of Gaussian and Butterworth High Pass Filters", Punjabi University, Patiala (Punjab), India, International Journal of innovations in Engineering and Management, vol.2; No2: ISSN: 2319-3344(July- Dec.2013).

[6] P. Perona and J. Malik; "Scale-space and edge detection using anisotropic diffusion", University Of Michigan, IEEE Trans. Pattern Analysis and Machine Intelligence, 12:629– 639, 1990.

[7] Prof. Karamjeet Singh;" Image Encryption And Decryption Using Blowfish Algorithm In Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July -2013, ISSN 2229 -5518.

[8] B.SaiChandana, S.Anuradha; "A New Visual Cryptography Scheme for Color Images ", B.SaiChandana.et. al. / International Journal of Engineering Science and Technology, Vol. 2(6), 2010, 1997-2000.

[9] Jasdeep Singh Bhalla, Preeti Nagrath; "Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm", International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013, ISSN 2250-3153.

[10] Irfan.Landge, Burhanuddin Contractor; "Image encryption and decryption using blowfish algorithm", World Journal of Science and Technology 2012, 2(3):151-156ISSN: 2231 – 2587Available Online: www.worldjournalofscience.com.

[11] 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.

[12] Ankita Gangwar, Vishal Shrivastava; "Improved RGB -LSB Steganography Using Secret Key", International Journal of Computer Trends and Technology- volume4 Issue2- 2013.

[13] Shuchi Sharma, Uma Kumari; " A High Capacity Data-Hiding Technique Using Steganography", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 3, May – June 2013, ISSN 2278-6856.

[14] Deepesh Rawat, Vijaya Bhandari; "A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image", International Journal of Computer Applications (0975 – 8887), Volume 64– No.20, February 2013.