*International Journal of Engineering & Technology*, 7 (4) (2018) 3674-3677

International Journal of Engineering & Technology

*Website: www.sciencepubco.com/index.php/IJET*
*doi: 10.14419/ijet.v7i4.20951*
***Research paper***

# Multilevel hiding text security using hybrid technique steganography and cryptography

**Noor Hasan Hassoon [1], Rajaa Ahmed Ali [2], Hazim Noman Abed [2] *, Adel Abdul-Jabbar Alkhazraji [2]**

*[1] Computer Science Department, College of Education for pure Science, University of Diyala, Diyala, Iraq*
*[2] Computer Science Department, College of Science, University of Diyala, Diyala, Iraq*
**Corresponding author E-mail: Hazim_numan@sciences.uodiyala.edu.iq*

## Abstract

Information security in the recent decades has become one of the main topics in communication systems. Security of information depended on strength of the keys in the Cryptographic and Steganographic processes. In this paper, a few techniques are used to implement both steganography and cryptography. The process of hiding data in this research goes through several processes, as follows: the first process is to encrypt a secret message through the use of Blowfish algorithm to generate the key that will be used in the encryption process and XOR it with a secret message. The second process, hiding positions are determined by using the edge detection algorithm to a cover image. After that, the bats algorithm will be applied to the cover image resulted by edge detection to choose random hiding positions in edge detection image. The last stage is to embed the secret message in a cover image using the least significant bit. Fig2 shows the opera-tions achieved on the secret message.

***Keywords***: *Blowfish; Bats algorithm; Cryptography; Edge detection; LSB; Steganography.*

## 1. Introduction

Information security in the recent decades has become one of the main topics in communication systems. Security requirements with time progress have been changing quickly. Information security was mainly delivered through administrative and physical methods before the rise of computer and network communications services. However, with the starter of using of the computer, internet and the use of distributed systems, there was a need to use automated tools to protect the information stored on the computer as well as to protect the data during their transmission. Therefore, a high level of security is required to protect the information from several forms of attacks [1-2].
One of the methods of hiding the existence of information from others is steganography [3]. It is the technique and science of safe communication [4]. The core objective of steganography is to protect the data during their transmission through the internet [5]. Various files host the data in steganography such as video, audio, image, text [6]. Different steganography methods exist for hiding data in the image with less difficulty than others taking into consideration strong and weak points. Steganography is used with cryptography in order to increase the security of data transfer [7].
Cryptography is the science of keep information by making it unreadable to others and called as cipher text or secret message [8]. The secret message or ciphertext can only be readable by the recipient of the message who owns a secret key to decrypt the ciphertext into plaintext [9].
Many of the algorithms in literature are offered for hiding data. One of the easiest and used techniques is the Least Significant Bit (LSB) algorithm [10]. This algorithm is used to hide the information in steganography by swaps the bit of least significant in the cover file based on the bit of secret message. This method is very effective because it does not cause a significant change in the quality of the cover file [7].

### 1.1. Blowfish algorithm

Actually, the Blowfish algorithm is a block cipher with a symmetric key that encodes data in 64-bit blocks. It comprises16 rounds, each round involves XOR operation and a function. Each round has two parts data encryption and key expansion. key expansion usually is used to generate elementary contents of one array while data encoding uses a 16 iterate Feistel network techniques. Figure 1 illustrates the works of blowfish algorithm. Key and plaintext are considered the inputs of the algorithm. 64-bit plaintext is separated to two equal halves and at each iterated the key is extended and kept in 18 p array and provide the 32-bit key as input, and XOR with previous iterated data [11].
Then, for j = 1 to 14:

yL = yL XOR Pj

yR = F(yL) XOR yR

Exchange yL and yR
After the 16-round, exchange yL and yR again for backing down the last exchange.

Then, yR = yR XOR P15 and yL = yL XOR P16.

In conclusion, re-combine yL and yR to obtain the cipher text.
decoding is precisely the similar as encoding, but that P1, P2,P3..., P18 are used in the opposite order[11].

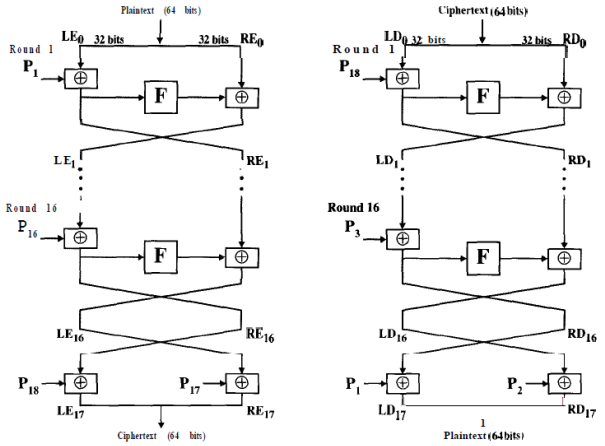



**Fig. 1:** Blowfish Encryption and Decryption Algorithm.

### 1.2. Edge detection

The proposed embedding method utilizes Sobel edge detector on every 3 × 3 non-overlapping block of the cover image. To conduct detection in edge detection methods, operators are utilized where Sobel operator is a mutually perpendicular gradient vector field operator. Gradient is an assessing of change of a pixel with its adjacent pixels [20]. Sobel detection is a gray weighted technique of the next to points in 2 directions. It founds edges of the point depending on its next to points. Gradient of point v(j,i) of a position j,i consist of two first derivatives in j-direction and i-direction such that it utilizes 3 × 3 neighboring of the point:

$$Gj = \{v(j+1, i-1) + 2v(j+1, i) + v(j+1, i+1)\} - \{v(j-1, i-1) + 2v(j-1, i) + v(j-1, i+1)\}$$

$$Gi = \{f(j-1, i+1) + 2v(j, i+1) + v(j+1, i+1)\} - \{v(j-1, i-1) + 2v(j, i-1) + v(j+1, i-1)\} \quad (1)$$

The gradient vector field is determined for each point v(j,i) is given below:

$$\text{Gradient vector field } (j, i) = |Gj| + |Gi| \quad (2)$$

$$\begin{vmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{vmatrix} \begin{vmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{vmatrix} \quad (3)$$

Figure 2 explains the algorithm of the Sobel edge detection algorithm. This algorithm is given to edge detection to be used with our proposed technique. Next portion explains the hiding of data and the process of extraction of the presented method [12]

```
Input: image[][], w, h  (w and h are the width and height of the image respectively)
Output: Gradient[][]

G_x = new double[w][h];
G_y = new double[w][h];
Gradient = new double[w][h];

for (x = 0; x < w; x+=3) {
      for (y = 0; y < h; y+=3) {
        if (x = 0 || x = w - 1 || y = 0 || y == h - 1)
            G_x[x][y] = G_y[x][y] = Gradient[x][y] = 0  // Image boundary
        end if
        else
            G_x[x][y] = image[x + 1][y - 1] + 2 * image[x + 1][y]+ image[x + 1][y+ 1]
                        -image[x - 1][y - 1] – 2 * image[x - 1][y] - image[x - 1][y + 1]
            G_y[x][y] = image[x - 1][y + 1] + 2 * image[x][y + 1]+ image[x + 1][y + 1]
                        -image[x - 1][y - 1] – 2* image[x][y - 1] - image[x + 1][y - 1]
            Gradient [x][y] = abs(G_x[x][y]) + abs(G_y[x][y])
        end else
      end for
end for
```

**Fig. 2:** Algorithm of Sobel Edge Detection.

### 1.3. Bats algorithm

Bats algorithm is an optimization algorithm depends on the echolocation behavior of bats when searching for preys. The main contribution in the bat search algorithm was presented by Yang in 2010 and the simulations were completed under numerous perfect rules [13].

1) Each bat uses echolocation features to search for preys and avoid obstacles.
2) Each bat flies with a velocity $v_i$ at position $x_i$ with a fixed frequency $f_{min}$, varying wave length $\lambda$ and loudness $L_0$ to search for prey. Automatically bats can alter the frequency of their emitted pulses and the frequency of pulse emission r in a range of [0, 1], according to the proximity of the goal.
3) The loudness $L_m$ can differ from a large positive value $L_0$ to a least constant value $L_{min}$.

Through the optimization procedure, the position and the velocity of the bat i at the time t should be well-defined and updated. The new position $x_i^{t+1}$ and velocity $v_i^{t+1}$ at the time t+1 are given by the Eqs. (1), (2) and (3):

$$Fi = f_{min} + (f_{max} - f_{min})\,\beta \quad (1)$$

$$v_i^{t+1} = v_i^t + (x_i^t - x_*)\,f_i \quad (2)$$

$$x_i^{t+1} = x_i^t + v_i^{t+1} \quad (3)$$

Where fi denotes the pulse rate emitted via the bat i which is drawn uniformly from (fmin, fmax). β is a random number in a range of [0, 1] and x∗ is the existing global best position (i.e., solution), which results after matching all the solutions between all the bats. When the solution is nominated between the existing best solutions, a new solution for each bat is produced locally using random walk, this procedure can be understood as a local search, it can be denoted by Eq. (4):

$$X\,new = xold + \epsilon L^t \quad (4)$$

Where ϵ is a random number in [−1, 1], $L^t$ is the loudness and $x_{old}$ denotes a random solution selected from the existing ideal solution. Typically, through the search process, when a bat finds a prey, the loudness decreases and the pulse emission gradually increases. Assuming that $L_{min} = 0$ means that a bat has found his prey (i.e., solution), the loudness $L_i$ and pulse emission $r_i$ are updated according to Eqs. (5) and (6):

$$L_i^{t+1} = \beta L_i^t \quad (5)$$

$$r_i^{t+1} = r_i^0\,[1 - \exp(-\gamma t)] \quad (6)$$

Where β is a random number in [−1, 1], while γ is a positive constant. In conclusion, we can simply conclude that when time → ∞, the loudness → 0 and $r_i^t \rightarrow r_i^0$ [14].

## 2. Related work

So far, several types of research have been done in the steganography field. Basically, the literature review offers a mean to investigate for researches and provide an idea of what has been done till now. In this study, the researchers review some papers which interrelated to our study as follows.

Chauhan, S. et al. [1] proposed the technique of uses together cryptography and steganography. The cryptography method used to encrypt the message is content-based encoding algorithm and the steganography method used are raster scan and the least significant bit method. In this study, encoded data is hiding various rate in RGB plane concurrently. This technique can approximately hide 16-KB, 260-KB, and 480-KB in a cover image with size respectively (128*128) pixels, (512*512) pixels, and (800*600)

pixels. Compared the results of this proposed algorithm with the presented algorithm gives more PSNR and less MSE value.
Joshi, K., & Yadav, R. [7] proposed a modern method of hiding data to overcomes the restriction of the presented technique. In this method, the message is firstly encoded by using the algorithm of transposition then using the gray image to hidden the ciphertext using a new technique (LSB-S). The capacity of the proposed technique for data hiding is 100% as all the pixel can hold data bit. 256*256 pixels is the total number can be hidden in an image which means 65536 bit. In the study, the meddlesome does not obtain the message even he extract all LSB bits. As well the alteration in the value of the pixel is only minus one or plus one which indicates good MSE and PSNR.
Ahmed, D. E., & Khalifa, O. O. [15] presented a model for steganography and cryptography. In this model, Elliptic curve cryptography (ECC) is using to encryption the secret message after selecting the suitable curve and defines their parameters, and a binary version of the secret message can then be obtained which is attached into the cover image by using LSB algorithm. When the receiver gets the cover image can abstract the secret message by applying the inverse function(E-if) followed by the decryption key to collect the secret message. The model is most common robust against attacks such as statistical attacks.
Samidha, D., & Agrawal, D. [16] presented a new technique to hide data in images depend on random bit steganography and spatial domain steganography additionally with existing methods of image steganography. the researchers using many techniques to hide data in pixels like layout management schemes, Least Significant Bit (LSB). When random pixels are chosen, the secret message can be hidden in random bits, which are denoted in the bytes of binary form. Various parameters from an image when choosing these pixels are considered for example physical location of pixels, the color of pixels etc. depended on these parameters they can conclude some more methods of image steganography.
Hazim N. [17] presented a new technique for hidden data security using steganography and cryptography. The encrypted message in cryptography was generated by XOR the QR code with a secret message. While the embedded process in steganography was done via using the LSB method and using the bats algorithm in order to select the hidden location.
With the advance of the technology and using the internet, the number of attacks is grown up. Therefore is necessary to pay attention to data security. In this study a multi-level of a technique for data security by using the properties of steganography and cryptography.

# 3. The proposed method

## 3.1. Proposed architecture

Information hiding is one of the main topics in information security. In this paper, a few techniques are used to implement both steganography and cryptography. The process of hiding data in this research goes through several processes, as follows: the first process is to encrypt a secret message through the use of Blowfish algorithm to generate a key that will be used in the encryption process by XOR a plaintext with the key. The second process, hiding positions are determined by using the edge detection algorithm to a cover image. After that, the bats algorithm will be applied to the cover image resulted by edge detection to choose random hiding position in edge detection image. The last stage is to embed the secret message in a cover image using the least significant bit. Figure 3 shows the operations achieved on the secret message.

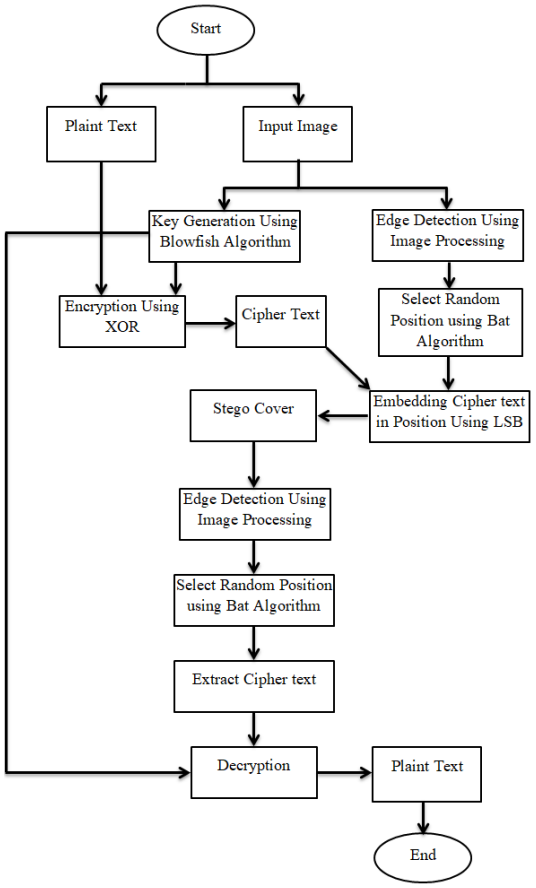



**Fig. 2:** Architecture of Proposed Technique.

## 3.2. Proposed algorithms

This section presents the key generation, embedded as well as extracted algorithms

### 3.2.1. Key generation and encryption algorithm

Input: Color Image, Plaintext.
Output: Key
Method:
Step1: Load BMP color image.
Step2: Key generation using the blowfish algorithm after convert input image into a binary image and divide it into to 64-bit blocks as a plaintext.
Step3: Load plaintext with different size and divide it into blocks in the same size as the key.
Step4: Apply XOR between step2 and step3 to generate a ciphertext.

### 3.2.2. Embedded algorithm

Input: Color cover image, Ciphertext.
Output: Stego Image.
Method:
Step1: Load BMP color image.
Step2: Apply edge detection using Sobel filter.
Step3: Apply bat algorithm on the output of step2 to choose random positions.
Step4: Embedding ciphertext using the LSB technique to generate steganography image.

### 3.2.3. Extracted algorithm

Input: Stego Image.
Output: Plaintext.
Method:
Step1: Apply edge detection on stego image using Sobel filter.
Step2: Apply bat algorithm on step1 to select random positions.

Step3: Extract the ciphertext using LSB.
Step 4: Apply XOR between step3 and the key to getting the plaintext.

## 4. Experimental results and results evaluation

The experiments in this study develop a schema based on the proposed algorithm. The different sizes of the cover with different size of the secret message been tested. Also, in order to determine the quality of the method used for information hiding, there are some measures for comparing the original image and cover results image has been adopted [17].
The NC, as described in the equation below, can calculate the resemblance between d (original secret image) and d* (extracted secret image):

$$\mathrm{corr}(d, d^*) = \frac{\sum_{i=1}^{N}(d_i-\bar{d})(d_i^*-\bar{d})}{\sqrt{\sum_{i=1}^{N}(d_i-\bar{d})}\sqrt{\sum_{i=1}^{N}(d_i^*-\bar{d})}}, \quad (1)$$

Where $d_i$ and $d_i^*$ are the original and modified data, respectively, and $\bar{d}$ is the average of the original data.
MSE measures the mean squares error between the original image and the steganography image.

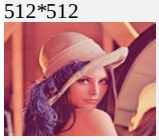
$$\mathrm{MSE} = \frac{1}{MM}\sum_{i=1}^{M}\sum_{j=1}^{M}(A - A_s)^2, \quad (2)$$

Where A and $A_s$ are the steganography images and original host, respectively.
The PSNR is used to estimate the steganography image quality. The PSNR is defined as follows:

$$\mathrm{PSNR} = 10\log\frac{255^2}{\mathrm{MSE}} \quad (3)$$

Table 1 illustrates the results of the steps of the implemented schema as well as the measures for comparing between the original image and cover results image.

**Table1:** Results Evaluation of Implemented Schema

| Cover Image Details | Text Message Size (Byte) | Stego Image | | Original Cover Image |
|---|---|---|---|---|
| 512*512  | 608 | PSNR | 80. 8394 | NC0.9875 |
| | | MSE | 5. 1977 | |
| 400*400  | 500 | PSNR | 79. 3400 | NC0.9721 |
| | | MSE | 9. 0495 | |
| 300*300  | 400 | PSNR | 78. 9720 | NC0.8759 |
| | | MSE | 1. 5410 | |
| 256*256  | 300 | PSNR | 78. 2502 | NC0.9240 |
| | | MSE | 1. 9194 | |

## 5. Conclusion

In this paper, the researcher proposed a new architecture for hiding information used cryptography and steganography. The process of hiding information in this research was done via several processes. Firstly, the secret message was encrypted by used blowfish algorithm to generate the secret key and XOR it with plaintext. Secondly, the hiding position was selected via used edge detection then bats algorithm. While the LSB was used to embed the data in an image. In the end, many parameters have been adopted to improve the quality of the proposed method. These parameters show our method offer the highest performance in regards to data transmission

## References


[1] Chauhan, Shivani, Janmejai Kumar, and Amit Doegar. "Multiple layer text security using variable block size cryptography and image steganography." In Computational Intelligence & Communication Technology (CICT), 2017 3rd International Conference on, pp. 1-7. IEEE, 2017.
[2] William, Stallings. "Cryptography and network security: principles and practice." Prentice-Hall, Inc (1999): 23-50.
[3] Johnson, Neil F., and Sushil Jajodia. "Exploring Steganography: Seeing the unseen." Computer 31, no. 2 (1998). https://doi.org/10.1109/MC.1998.4655281.
[4] Atawneh, Samer, and Putra Sumari. "Hybrid and blind steganographic method for digital Images based on DWT and chaotic map." Journal of Communications 8, no. 11 (2013): 690-699. https://doi.org/10.12720/jcm.8.11.690-699.
[5] Macrakis, Kristie. "Confessing secrets: Secret communication and the origins of modern science." Intelligence and National Security 25, no. 2 (2010): 183-197. https://doi.org/10.1080/02684527.2010.489275.
[6] Luo, Xiangyang, Fenlin Liu, Chunfang Yang, Shiguo Lian, and Ying Zeng. "Steganalysis of adaptive image steganography in multiple gray code bit-planes." Multimedia Tools and Applications 57, no. 3 (2012): 651-667. https://doi.org/10.1007/s11042-010-0663-3.
[7] Joshi, Kamaldeep, and Rajkumar Yadav. "A new LSB-S image steganography method blend with Cryptography for secret communication." In Image Information Processing (ICIIP), 2015 Third International Conference on, pp. 86-90. IEEE, 2015. https://doi.org/10.1109/ICIIP.2015.7414745.
[8] Albayaty, Ismael Salih, Ahmed Luay Ahmed, Noor Hasan Hassoon, and Hazim Noman Abed. "Hiding Information in an Image Based on Bats Algorithm." Iraqi Journal of Information Technology 8, no. 2 .(2018): 128-141
[9] Saritha, M., Vishwanath M. Khadabadi, and M. Sushravya. "Image and text steganography with cryptography using MATLAB." In Signal Processing, Communication, Power and Embedded System (SCOPES), 2016 International Conference on, pp. 584-587. IEEE, 2016.
[10] Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." Signal processing 90, no. 3 (2010): 727-752. https://doi.org/10.1016/j.sigpro.2009.08.010.
[11] Manku, Saikumar, and K. Vasanth. "Blowfish encryption algorithm for information security." ARPN Journal of Engineering and Applied Sciences 10, no. 10 (2015): 4717-4719.
[12] Smitha, G. L., and E. Baburaj. "Sobel edge detection technique implementation for image steganography analysis." Biomedical Research 29 (2018).
[13] Yang, Xin-She. "A new metaheuristic bat-inspired algorithm." In Nature inspired cooperative strategies for optimization (NICSO 2010), pp. 65-74. Springer, Berlin, Heidelberg, 2010. https://doi.org/10.1007/978-3-642-12538-6_6.
[14] Taha, Anass, Mohamed Hachimi, and Ali Moudden. "A discrete Bat Algorithm for the vehicle routing problem with time windows." In Logistics and Supply Chain Management (LOGISTIQUA), 2017 International Colloquium on, pp. 65-70. IEEE, 2017.
[15] Ahmed, Diaa EM, and Othman O. Khalifa. "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography." In 2014 International Conference on Computer & Communication Engineering (ICCCE), pp. 288-291. IEEE, 2014.
[16] Samidha, Diwedi, and Dipesh Agrawal. "Random image steganography in spatial domain." In Emerging trends in VLSI, embedded system, nano electronics and telecommunication system (ICEVENT), 2013 international conference on, pp. 1-3. IEEE, 2013.
[17] Abed, Hazim Noman. "Robust and Secured Image Steganography using LSB and Encryption with QR Code." Journal of AL-Qadisiyah for computer science and mathematics 9, no. 2 (2017): 1-9.