Hiding a Secret Message Encrypted by S-DES Algorithm

Nada Abdul Aziz Mustafa
University of Bagdad, Collage of Languages,
Information Technology Unit
nada@colang.uobaghdad.edu.iq
Orcid.org/0000-0001-6683-3687

DOI: http://dx.doi.org/10.31642/JoKMC/2018/100213

Received Jun. 11, 2023. Accepted for publication Jul. 14, 2023

***Abstract*—-** *Nowadays, it is quite usual to transmit data through the internet, making safe online communication essential and transmitting data over internet channels requires maintaining its confidentiality and ensuring the integrity of the transmitted data from unauthorized individuals. The two most common techniques for supplying security are cryptography and steganography. Data is converted from a readable format into an unreadable one using cryptography. Steganography is the technique of hiding sensitive information in digital media including image, audio, and video. In our proposed system, both encryption and hiding techniques will be utilized. This study presents encryption using the S-DES algorithm, which generates a new key in each cycle to increases the complexity of the algorithm detection. An additional shared key between the sender and the receiver is added which is applied before starting the encryption process, that key must be hex-decimal in order to increase the level of security and give enough time to delay the guessing of the secret text by the attackers. The secret message data is concealed using one of the two techniques: either least significant bit (3-LSB) steganography or hiding in green and blue bits. To expedite the concealment process, the cover image is enhanced by applying a median filter, the median filter removes noise from the image while preserving its details. Finally, comparing the results of the two methods to determine which is better for the cover image in terms of PSNR metrics and hiding process time.*

Keywords—Cryptography, S-DES algorithm, Steganography, Information hiding, LSB algorithm, Stego-analysis, Stego-object, Median filter.

I. INTRODUCTION

The two important processes for transmitting data more securely over the Internet are encryption and steganography. Encryption is to obscure the meaning of a message, while steganography is to hide its existence [1]. Both methods are used together to prevent attackers from stealing or sabotaging data, thus increasing the level of security [2]. In encryption, the structure of the data is changed by using one of the encryption algorithms and the plain text is converted into a ciphered text to be sent securely to the recipient, who decrypts the message to get the original text [3]. There are two types of encryption: symmetric cryptography and asymmetric. In symmetric, both the sender and the recipient share a single key which is used for encryption and decryption [4]. In asymmetric two keys are used, one is a private key to decrypt the message and the second is a public key to encrypt the message [5]. In steganography, the data structure is preserved to prevent suspicion of the existence of confidential data hidden in the medium used for concealment, which may be a photo or a video [6]. Furthermore, steganography can be defined as a procedure of hiding a secret text message in an image or hiding an image within an image [7]. Based on that, the cover image should not raise any suspicion and should closely resemble the original image to the human eye as much as possible [8], after images are utilized as the carrier in steganography, they are normally handled by changing more than bit of the byte, which formed the pixels of the image [9]. Cryptography is considered a technique of sending a text message in a different form as the envisioned receiver could read and procedure it [10]. For cryptography, the message is named plain text and a masked text message is called cipher text [11], the procedure of changing a plain text into cipher text is called encryption and the opposite procedure is named decryption [12]. For steganography, the procedure of embedding a secret text message inside the cover image is named encoding and the opposite procedure is named decoding [13].

II. SIMPLIFIED DATA ENCRYPTION STANDARD (S-DES)

The S-DES algorithm is a symmetric encryption algorithm that uses the same key for encryption and decryption [8]. Encryption using the S-DES algorithm consists of two stages, the first stage is a key generation, and the second stage is the text encryption [14], see Fig.1.

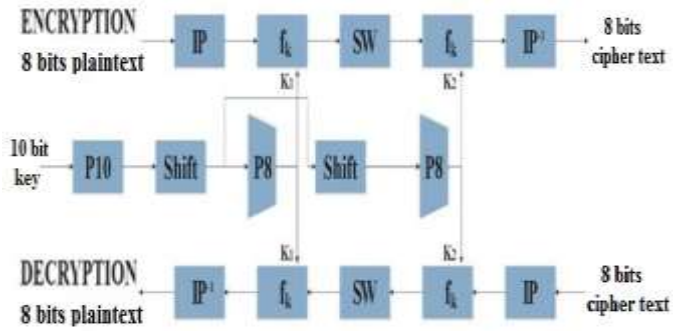


Fig.1. Show the S- DES algorithm

This algorithm relies on the use of a key consisting of 10 bits shared between the sender and the receiver. The key becomes two keys, each one is consisting of 8 bits used for encryption and decryption [15].

III. MEDIAN FILTERING

A nonlinear technique for removing noise from images is known as median filtering. It is commonly used for being very good at eliminating noise while maintaining edges, and it is especially good at eliminating "salt and pepper" noise[16]. The median filter operates by going pixel-by-pixel across the image and replacing each value with the median value of nearby pixels. The median is determined by inserting the pixel under consideration in place of the middle (median) pixel value after numerically ordering all of the pixel values from the window [17]. The median filter does not produce new, irrational pixel values when it crosses an edge because the median value must really be the value of one of the pixels in the neighborhood. As a result, the median filter preserves sharp edges far better than the mean filter [18], see Fig.2.

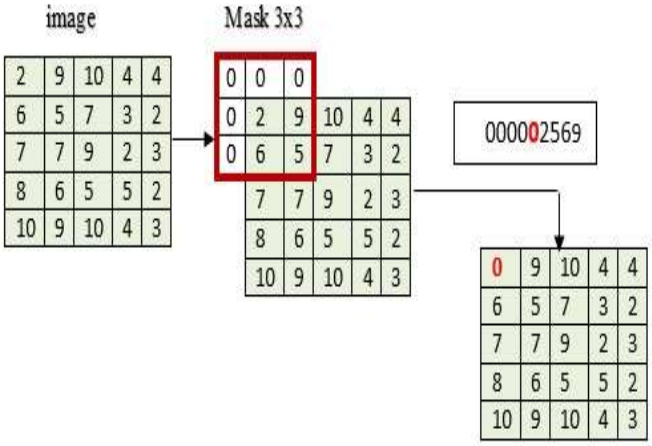


Fig.2. Example of 2D median filtering with a 3 x 3 sampling window

IV. HIDING TEXT IN AN IMAGE BY USING THE 3-LSB ALGORITHM

In the less important parts of the BMP image, the message bits will be hidden, taking advantage of the unimportant data by replacing it with the important data to be hidden [19]. This is called Steganography (3-LSB). The image will not be affected and there will be no doubt that important data is hidden inside it [20], see Table 1.

Table 1. The difference between LSB and MSB

data	Method	result	Affected
101	LSB	100	Affected by 1
101	MSB	128	Affected by 128 (1*2^7)

To hide a message in an image, the unimportant image data in the image pixels will be replaced by the important secret message data [21], each pixel contains red, green, and blue elements and each color has a value between 0 and 255, if the size of an image(cover image) = 500*400 = 200000, 3 colors for each pixel = 200000*3 = 600000, each character (for secret message) can be represented by 8 bits= 600000/8 then this image can hide 75000 characters.

V. SYSTEM PROPOSED

The proposed system approach is to encrypt the text of the message by using the S- DES algorithm then using one of the two following hiding techniques: the 3- LSB or hiding the secret message bits in green and blue in an image (BMP) after applying a median filter to reduce the noise in it.

The cover image is initially divided into three planes (red, green, and blue), the technique works by hiding the important data (secret message) in the green and blue color pixels rather than in the red ones. Hecht's study, which found that just a small percentage of human eye cones, nearly 2%, are sensitive to blue, 33% are sensitive to green, and 65% of all cones are sensitive to red, had led to the selection of hiding 2 bits in green and 3 bits in blue [22]. For the 24 bits color image, the first pixel is represented as:

[11011100 11000110 10000111] and the first secret message [00011101] the result:

Red Green Blue

[11011100 11000100 10000011].

The proposed approach can be divided into seven main phases: message encryption by using (S-DES), use median filter, hiding cipher text in the image, extracting secret text messages from stego-object, decrypting the cipher text. The steps of the proposed system are:

The sender

1) Input hex-decimal key, encrypting the secret message (file type txt) by using the S-DES block cipher algorithm.
2) Using the BMP format (the cover image), a median filter is applied.
3) Hiding the encrypted secret message in the cover image using hide 2-bits in green and 3-bits in blue pixels, then sending the stego image to the recipient.

The recipient

4) Search across image pixels to find 8 consecutive zeros then extract an encrypted secret message from the stego image.
5) Input hex-decimal key, decrypt the secret message by using (S-DES), every 8 bits is converted into a letter, and the process continues until all the letters of the hidden encrypted secret message are collected, see Fig.3.

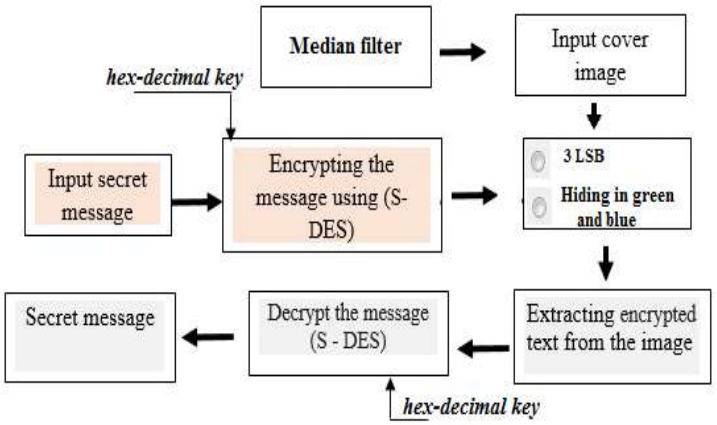


Fig.3.The proposed system technique

To encrypt the message by using the S-DES algorithm a file type txt (secret message) is selected then the key is added which must be hex-decimal, to increase the security.

After removing noise with median filtering, two bits in the green color channel and three bits in the blue color channel are hidden to conceal secret message data in the image (BMP) see Fig.4 and Fig.5.

Fig.4. File before and after encryption using S-DES

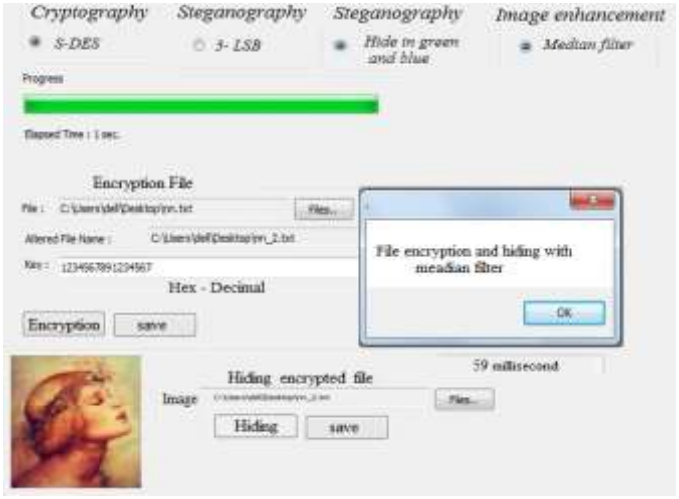


Fig.5. Encrypted the message using the S-DES algorithm and hiding it in green and blue with median filtering.

By employing the reverse method, the encrypted secret message is extracted from the image, and then the decryption algorithm is applied to retrieve the original text (secret message), see Fig.6.

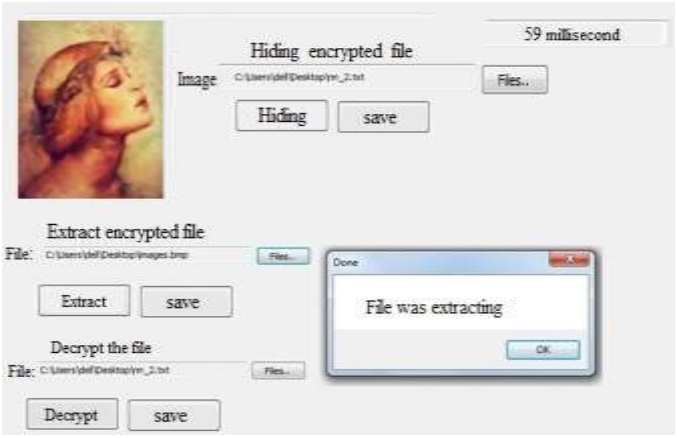
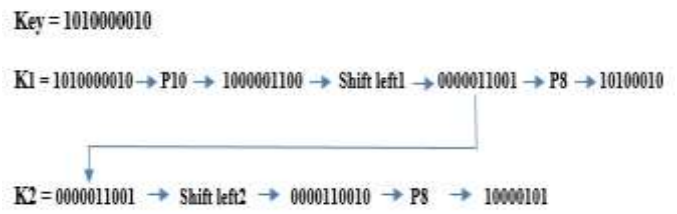


Fig.6. Extracting a file from a BMP image

The S-DES algorithm consists of two stages, a key generation and the text encryption, for example to key generation, suppose key value =1010000010, P10= (3 5 2 7 4 10 1 9 8 6) and
P8= (6 3 7 4 8 5 10 9).
Find K1 and K2:
1. Key = 1010000010 (10 bits)
2. Key passes through the p10 =1000001100
3. Key shift left 1 =0000011001
4. Key passes through the p8 =10100010= Key 1
Find key 2
1. Key shift left1=0000011001, Shift left2 =0000110010,
2. Passes through the p8 = 10000101 = key 2.
The execution path of the key generation process are:



The Function (fk) it is considered the most complex in the S-DES algorithm because it goes through the stages of permutation and replacement, the execution path of the permutation and replacement process are:
Apply (IP) initial permutation on the message=8 bits then divide the message into L0 and R0, afterwards find L1 and R1. L1=R0, R1=f (L, R) = (L0 XOR F (R0, K1), R0) the R0=4 digit and the K1=8 digit. E/P must be used then. R0 XOR K1 followed by using S- box array to convert R0 from 8 bits to 4 bits. Concatenate R0+L0 (Reverse) and permutation (IP^1).
For example to message encryption, suppose
IP= (2 6 3 1 4 8 5 7)
IP^-1= (4 1 3 5 7 2 8 6)
E/P= (4 1 2 3 2 3 4 1)
S/p= (4 1 3 5 7 2 8 6) and S-BOX array = (S0, S1) defined as follows:

$$S0 = \begin{pmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{pmatrix} \quad S1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{pmatrix}$$

Let the message be 11011001, the steps of encrypting the message by using S-DES are as follows:
1. Apply IP (Initial permutation on message).
Message after IP=10011110 (to change the location)
2. Divide the message into L, R---- L0=1001, R0=1110
3. Find L1, R1---- L1=R0= 1110
R1= fk (L, R) = (L XOR F(R, SK), R)
Using E/P to make the R= 8 bits = 01111101
R1=f (L, R) = (L0 XOR 01111101, R0)
R1=f (L, R) = (1001 XOR 01111101, R0) (using S-BOX array to change R into 4 bits), the
R1=f (L, R) = (1001 XOR 1111, R0) = (0110 XOR 1110) = 1000
4. R1+L1= 10001110
5. Permutation (IP^-1) = 01011001
The output of the encrypted message = 01011001.

To hide the output of the encrypted message:
First pixel (image): [**10010100 01000110 10000100**]
Encrypted message = 01 011 001
Hiding message: [**10010100 01000101 10000011**]

VI. EXPERIMENTAL RESULTS

The complexity of the S-DES encryption algorithm has been increased by using an additional key (Hexadecimal) and the system was applied to an image it has a noisy, the hiding time on the image was calculated in two stages: the first stage without applying the median filter, and the second stage with the use of the median filter. The result was the acceleration of the hiding process through the application of the median filter, see Fig.7.

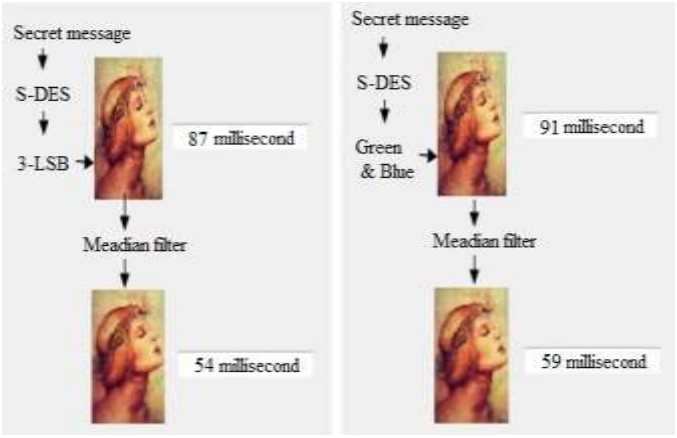


Fig.7. Hiding time

VII. CONCLUSION

By using median filtering in an image, the fine-scaled visual features are removed, in addition to the noise, which decreases the size of the image and speeds up the hiding processes and in addition to maintaining the image quality. In the steganography procedure, there are two approaches that have been utilized, and the PSNR measurements have revealed that the usage of "the hiding the secret message bits in green and blue pixels" method is superior to the 3-LSB method, see Table 2 and Fig.7. If alterations to a picture are made individually, to the green, and blue layers, a more reliable visual cryptography system may be achieved since the intruder tries to determine these fundamental intensity values when he does a thorough examination of the image. Less distortion is implied by a higher PSNR number, a PSNR score of 40 dB or more is considered to be extremely good, see Table 2.

Table 2. The performance evaluation findings encrypted time and PSNR score

Cover image	PSNR			Encrypted time	
	3-LSB	Hiding in Green and Blue	distortion	3-LSB	Hiding in Green and Blue
Original image	41.28	44.31	More than 40 (Less distortion) **Then Good PSNR score**	87 milliseconds	91 milliseconds
Median filter Image	41.39	44.35		54 milliseconds	59 milliseconds

The right technique may be chosen based on the findings, whether a strong security is required with difficult data detection or decreases encryption time. Increasing the complexity in the algorithm used for hiding always increases the difficulty of detecting hidden data, but at the expense of execution speed.

The use of encryption with steganography gave a strong result in protecting the secret file to be sent over the Internet, the reason for this is that encryption is supported by Authentication, Data integrity, Confidentiality, and Non-repudiation, while steganography supports Authentication and Confidentiality. The system power level is implemented in two phases: the first stage is using the S-DES algorithm, this algorithm is characterized by speed and efficiency and the use of different keys in each session in addition to the keys of the S-DES algorithm, a hexadecimal key is added to which gives enough time to delay the guessing of the secret text by the attackers. The second stage is to disguise the cipher text in an image to prevent suspicion of an important secret message. To minimize noise and hasten the concealing process, the median filter is used to the cover image and the cover image is in BMP format helps to provide a large area to hide confidential data.

The usage of the hiding in green and blue channels has proven to be efficient in matching the original image and due to the high sensitivity of the human eye to the color red, the bits in the red color channel were avoided and not used.

REFERENCES

[1] Ahmed AL-Shaaby, Talal AlKharobi, Cryptography and Steganography: New Approach, Transactions on Networks and Communications, Volume 5 No. 6, December (2017); pp: 25-38

[2] Rawaa Hamza Ali, Jamal Mohamed Kadhim1, Text-based Steganography using Huffman Compression and AES Encryption Algorithm, Iraqi Journal of Science, 2021, Vol. 62, No. 11,pp: 4110-4120DOI: 10.24996/ijs.2021.62.11.31.

[3] Pria Bharti, Roopali Soni, New Approach of Data Hiding in Images Using Cryptography and steganography, International Journal of Computer Applications,Vol.58, No.18, 2012, pp1-5.

[4] Muna M. Hummady, Ameer Hussein Morad, Enhancement of System Security by Using LSB and RSA Algorithms, Al-Khwarizmi Engineering Journal, Vol. 18, No. 1, March 2022, P. P. 26-37.

[5] Venkata Sai Manoj, Cryptography and Steganography, International Journal of Computer Applications (0975 8887), Volume 1 No.12.

[6] Nada Abdul Aziz Mustafa, Text Hiding In Text Using Invisible Character, International Journal of Electrical and Computer Engineering, 2020. 10(4): p. 3550.

[7] 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. 2013. 64(20).

[8] Rasha H.Ali, Steganography in Audio Using Wavelet and DES, Baghdad Science Journal, Vol.12 (2) Jun 7, 2015

[9] Elaf Ali Abbood, Rusul Mohammed Neamah, Shaymaa Abdulkadhm, Text in Image Hiding using Developed LSB and Random Method, International Journal of Electrical & Computer Engineering (2088-8708), 2018. 8(4).

[10] Dipti Kapoor Sarmah, Neha bajpai, Proposed System for Data Hiding Using Cryptography and Steganography, International Journal of Computer Applications (0975 8887), Volume 8 No. 9, October 2010.

[11] Shailender Gupta, Ankur Goyal, Bharat Bhushan, Information Hiding Using Least Significant Bit Steganography and Cryptography, International Journal of Modern Education and Computer Science, 2012. 4(6): p. 27.

[12] Safwat Helmy Hamad, Amal Khalifa, Ahmed Atito Elhadad, S. Z. Rida, A Modified Play fair Cipher for Encrypting Digital Images, J. of Commun. & Comput. Eng. ISSN 2090-6234, Volume 3, Issue 2, 2013, Pages 1:9.

[13] Huda Dheyauldeen Najeeb, Israa Tahseen Ali, A proposal of Multimedia Steganography Algorithm based on Improved Least Significant Bit (LSB) Method, Journal of Science, 2017, Vol. 58, No.4B, pp: 2188-2199DOI:10.24996/ ijs.2017.58.4B.22.

[14] Keshav Raj1, Bharti Sharma1, Neeraj Kumar, Dr. Dalveer Kaur, Differential Cryptanalysis on S-DES, International Journal of Management & Information Technology, Volume 1, No 2, July, 2012.

[15] Sanjay Kumar, Sandeep Srivastava, Image Encryption using Simplified Data Encryption Standard (S-DES), International Journal of Computer Applications (0975 – 8887), Volume 104 – No.2, October 2014.

[16] Youlian Zhu, Cheng Huang, Improved Adaptive Median Filtering, Computer Engineering and Applications. 2010, vol.46, no. 3, pp. 175-176.

[17] Chao Wang, Zhongfu Ye, Salt-and-pepper noise removal by adaptive median filter and TV in painting, Journal of University of Science and Technology of China, 2008, vol.38, no. 3, pp. 282-287.

[18] Guohong Liu, Wenming Guo, Application of improved arthmetic of median filtering denoising, Computer Engineering and Applications, 2010, vol.46, no.10, pp.187-189.

[19] Mohammed Abbas Fadhil Al-Husainy, Diaa Mohammed Uliyan, A Secret-Key Image Steganography Technique using Random Chain Codes, International Journal of Technology, 2019. 10(4): p. 731-740.

[20] Manoj, I. V. S., Cryptography and Steganography, International Journal of Computer Applications (09758887), Vol.1, No.12, 2010, pp 63-68.

[21] Reyam Jassim Essa, Nada A.Z. Abdullah, Rawaa Dawoud AL-Dabbagh, Steganography Technique using Genetic Algorithm. Iraqi Journal of Science, 2018, Vol. 59, No.3A, pp: 1312- 1325, DOI: 10.24996Lijs. 2018.59.3A.19

[22] Soumendu Chakraborty, Anand Singh Jalal, Charul Bhatnagar, LSB Based Non Blind Predictive Edge Adaptive Image Steganography, Multimedia Tools and Applications, vol-76, no-6, pp. 7973–7987, (2017). (Springer) ISSN/ISBN: 1573-7721.