ISSN: 2454-1907
International Journal of Engineering Technologies and Management Research
September 2020, Vol 7(09), 31 – 38
DOI: https://doi.org/10.29121/ijetmr.v7.i9.2020.782

# DATA STEGANOGRAPHY USING EMBEDDED PRIVATE KEY

Dr. Mohammad S. Khrisat [1], N Prof. Ziad Alqadi [*2] ✉

[1, *2] Computer Engineering, Albalqa Applied University, Jordan

DOI: https://doi.org/10.29121/ijetmr.v7.i9.2020.782

**Article Citation:** Dr. Mohammad S. Khrisat, and N Prof. Ziad Alqadi. (2020). DATA STEGANOGRAPHY USING EMBEDDED PRIVATE KEY. International Journal of Engineering Technologies and Management Research, 7(9), 31-38. https://doi.org/10.29121/ijetmr.v7.i9.2020.782

**Published Date:** 21 September 2020

**Keywords:**
Embedded Key
LSB2
Covering Image
Holding Image
PK
MSE
PSNR

## ABSTRACT

LSB2 method of data steganography is one of the most popular methods used to hide secret messages in digital color image. This method keeps the quality of the holding image high but it is not secure and it can be easily hacked.

In this paper a method of improving the security of LSB2 method will be proposed, tested and implemented. The added security issues are simple and do require extra memory and time for execution. An embedded key will be extracted from the holding image to encrypt the message, this key will be variable and depends on the selected covering image, selected message length and selected position in the image where to extract the embedded key; the selected position and message length will form a private key to enhance LSB2 security.

## 1. INTRODUCTION

Color digital images are one of the most common and widely used types of data, as they are circulated among multiple categories of users [1], [2], [3]. These images have important characteristics that make them a desirable medium for hiding confidential or personal text messages [4], [5], [6]. Among the most important characteristics are:

- Ease of obtaining and ease of handling.
- Its large size and the possibility of using this large volume of data to hide text messages.

The digital color image is represented by a three-dimensional matrix [7], [8], [9], where the first dimension represents the red color matrix; the second one represents the green color matrix, while the third dimension represents the blue color , figure 1 shows a color image example with the histogram of each color dimension histogram [10], [11], [12] :

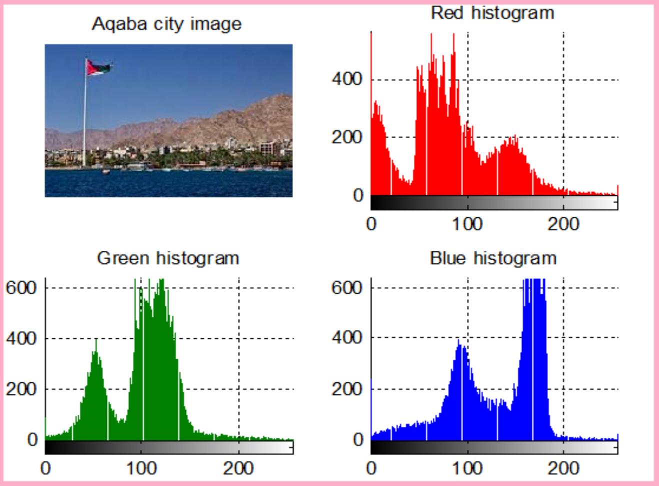


**Figure 1:** Digital color image example

The process of re-dyeing the digital image is an easy process [13], [14], [15], since the image can be converted into a single column or into a single row, and this is what we will adopt in this research paper [15], [17], [18], figure 2 shows the histogram of the image shown in figure 1 after reshaping it into one row matrix:

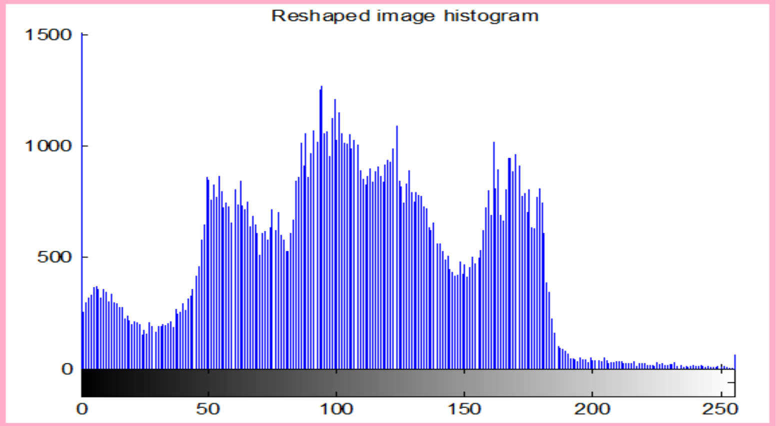


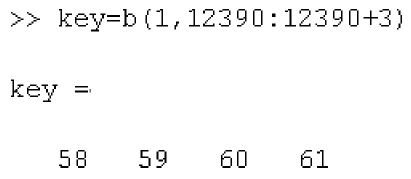
**Figure 2:** Histogram of the one row image

## 2. EMBEDDED KEY

Image position is the starting index of the row image where to get the key used to encrypt the secret message applying XOR operation of the message and the extracted (embedded key). The position P will form a part of the private key of data steganography; the other part will be the secret message length.

The value of the position P will be within the range of one to image size subtracted by the message length for example if the reshaped image size = 122265, then the P may take any value within the range 1 to 122165 when the secret message length =100 characters.

For example if want to hide the message 'Ziad' in the previous image, and we select P=12390, then the extracted embedded key will equal:

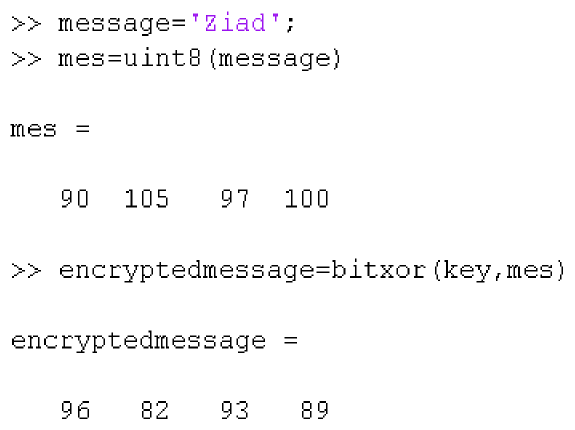


```
>> key=b(1,12390:12390+3)

key =

    58    59    60    61
```

This key can be used now to encrypt the secret message as follows:



```
>> message='Ziad';
>> mes=uint8(message)

mes =

    90   105    97   100

>> encryptedmessage=bitxor(key,mes)

encryptedmessage =

    96    82    93    89
```

The encrypted message then will be hidden in the image applying LSB2 method of data steganography.

Here we have to notice that the embedded key values are variables and they depend on the selected covering image and on the selected secret position P.

## 3. DATA STEGANOGRAPHY

Data steganography as shown in figure 3 is the process of hiding confidential data in the digital image so that the concealment process does not distort the image or change its features, and that no change is noticed with the naked eye. The quality of the holding image must be much closed to quality of the covering image, so the mean square error (MSE) between the covering image and the holding image must be closed to zero, or the peak-to-signal-noise ratio (PSNR) between the two images must be very high.

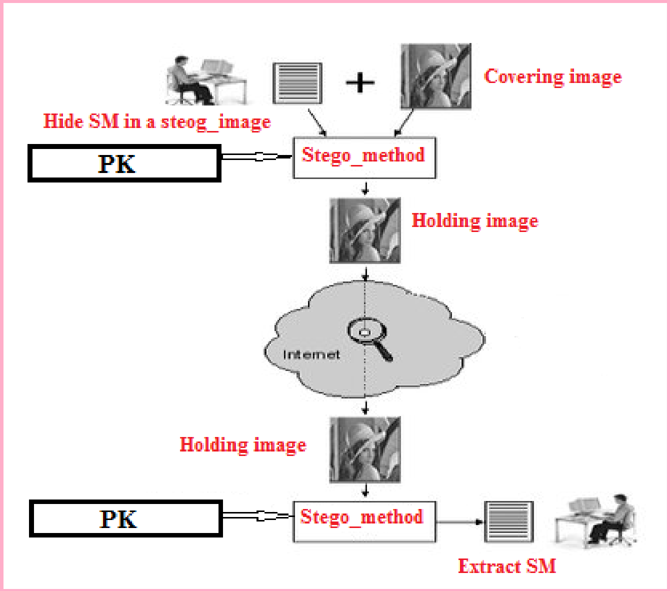


**Figure 3:** Data steganography process

Many methods were proposed for data steganography [19], [20], [21], most of them are based on least significant bit (LSB) method of data hiding, and here in this paper we will use LSB2 method because it has good features such as doubling the hiding capacity, providing low value for MSE and high value for PSNR [22], [23], [24].

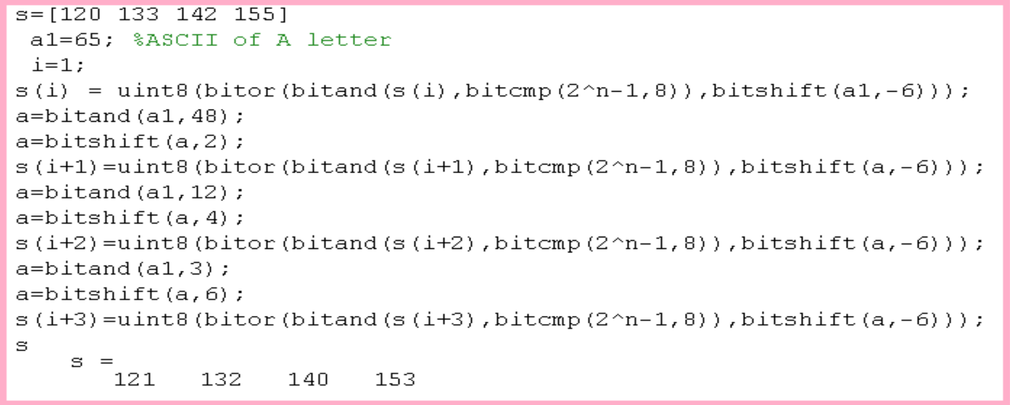
LSB2 method [25] can be implemented by using the least two significant bits to hold data from the secret message as shown in table 1

**Table 1:** Hiding process using LSB2 (Hiding character A)

| Covering image bytes(decimal) | 190 | 200 | 143 | 166 |
|---|---|---|---|---|
| Covering image bytes (Binary) | **10111110** | **11001000** | **10001111** | **10100110** |
| **Message A (one character) =65** | **01000001** | | | |
| Holding image bytes(decimal) | **10111101** | **11001000** | **10001100** | **10100101** |
| Holding image bytes (Binary) | **189 (-1)** | **200(no change)** | **140(-3)** | **165(-1)** |

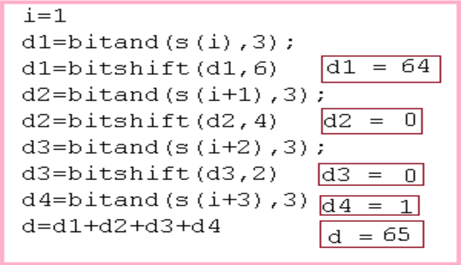
From table 1 we can see that LSB2 method of data hiding adds minor changes to the covering image, and the change ranges (if there is any) from +3 to -3, these changes in the pixels colors cannot be noticed by the human eyes [26], [27].

The process of data hiding and data extracting using LSB2 method is very simple, figure 4 shows the process if hiding, while figure 5 shows the process of data extracting:



```
s=[120 133 142 155]
 a1=65; %ASCII of A letter
 i=1;
s(i) = uint8(bitor(bitand(s(i),bitcmp(2^n-1,8)),bitshift(a1,-6)));
a=bitand(a1,48);
a=bitshift(a,2);
s(i+1)=uint8(bitor(bitand(s(i+1),bitcmp(2^n-1,8)),bitshift(a,-6)));
a=bitand(a1,12);
a=bitshift(a,4);
s(i+2)=uint8(bitor(bitand(s(i+2),bitcmp(2^n-1,8)),bitshift(a,-6)));
a=bitand(a1,3);
a=bitshift(a,6);
s(i+3)=uint8(bitor(bitand(s(i+3),bitcmp(2^n-1,8)),bitshift(a,-6)));
s
    s =
       121    132    140    153
```

**Figure 4:** LSB2 hiding process



```
i=1
d1=bitand(s(i),3);
d1=bitshift(d1,6)        d1 = 64
d2=bitand(s(i+1),3);
d2=bitshift(d2,4)        d2 = 0
d3=bitand(s(i+2),3);
d3=bitshift(d3,2)        d3 = 0
d4=bitand(s(i+3),3)      d4 = 1
d=d1+d2+d3+d4            d = 65
```

**Figure 5:** LSB2 extraction process

## 4. THE PROPOSED METHOD

The secret message hiding process as shown in figure 6 can be implemented applying the following steps:

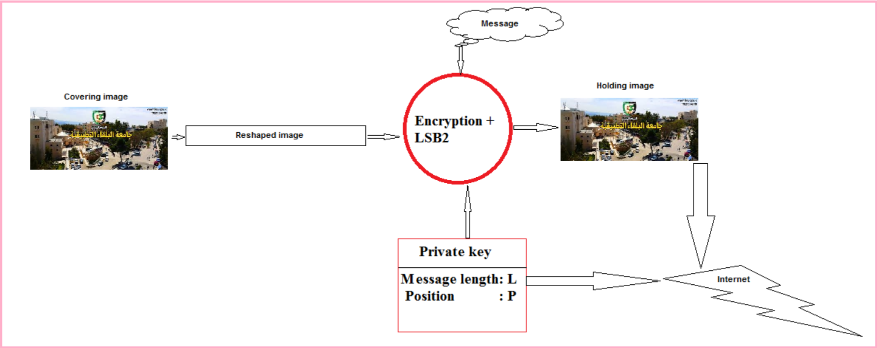


**Figure 6:** Hiding process

1) Get the covering image.
2) Reshape the covering image into one row matrix.
3) Get the secret message and find the secrete message length (L).
4) Select the position P where to start extracting the embedded key from the image.
5) Retrieve the embedded key.
6) Apply XORing using the message and the embedded key to get the encrypted version of the message.
7) Apply LSB2 method to hide the encrypted message.
8) Reshape back the image to 3D matrix to get the holding image.

The extraction process can be implemented applying the following steps:

1) Get the holding image.
2) Reshape the holding image into one row matrix.
3) Get the message length (L).
4) Apply LSB2 method to extract the encrypted message.
5) Get the position P.
6) Retrieve the embedded key using L and P.
7) Apply XORing using the encrypted message and the embedded key to get the original message.

## 5. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The quality of the holding (stego) image (which means that the changes that have occurred to her cannot be noticed with the naked eye, and it is not possible to suspect that the image contains confidential information) can be achieved by [28], [29], [30]:

- Keeping low value of mean square error (MSE) between the covering and the holding images.
- Keeping High value of peak signal to noise ratio (PSNR) between the covering and the holding images.

The proposed method was implemented using various color images. A short message of 80-character length was hidden and extracted using each of the selected images; table 2 shows the results of implementation.

**Table 2:** Obtained result by hiding a message with 100-character length

| Image # | Image size(byte) | MSE | PSNR | Hiding time (Seconds) | Extraction time (Seconds) |
|---|---|---|---|---|---|
| 1 | 150849 | 0.0058 | 162.3120 | 0.0019 | 0.0011 |
| 2 | 77976 | 0.0128 | 154.4093 | 0.0019 | 0.0011 |
| 3 | 518400 | 0.0019 | 173.6787 | 0.0019 | 0.0011 |
| 4 | 5140800 | 0.00019394 | 196.3050 | 0.0032 | 0.0011 |
| 5 | 4326210 | 0.00022260 | 194.9268 | 0.0030 | 0.0011 |
| 6 | 122265 | 0.0072 | 160.1769 | 0.0019 | 0.0011 |
| 7 | 518400 | 0.0018 | 173.9728 | 0.0019 | 0.0011 |
| 8 | 150975 | 0.0066 | 161.0164 | 0.0019 | 0.0011 |
| 9 | 150975 | 0.0058 | 162.2861 | 0.0019 | 0.0011 |
| 10 | 151353 | 0.0063 | 161.5238 | 0.0019 | 0.0011 |
| 11 | 1890000 | 0.00049841 | 186.8661 | 0.0020 | 0.0011 |
| 12 | 6119256 | 0.00015737 | 198.3942 | 0.0034 | 0.0011 |

From table 2 we can see that the proposed method does not add any negative effects on LSB2 method by keeping MSE low and PSNR high, and here we can recommend using images with big sizes to increase PSNR and at the same time decrease MSE between the covering and the holding images.

The previous experiment was repeated but for a message of 1600 character length, table 3 shows the obtained results.

**Table 3:** Obtained result by hiding a message with 1600-character length

| Image # | Image size(byte) | MSE | PSNR | Hiding time (Seconds) | Extraction time (Seconds) |
|---|---|---|---|---|---|
| 1 | 150849 | 0.0948 | 134.3862 | 0.0150 | 0.0140 |
| 2 | 77976 | 0.2005 | 126.8967 | 0.0150 | 0.0140 |
| 3 | 518400 | 0.0287 | 146.3305 | 0.0150 | 0.0140 |
| 4 | 5140800 | 0.0029 | 169.2741 | 0.0160 | 0.0160 |
| 5 | 4326210 | 0.0034 | 167.5254 | 0.0160 | 0.0160 |
| 6 | 122265 | 0.1203 | 132.0019 | 0.0150 | 0.0140 |
| 7 | 518400 | 0.0291 | 146.2070 | 0.0150 | 0.0140 |
| 8 | 150975 | 0.0954 | 134.3269 | 0.0150 | 0.0140 |
| 9 | 150975 | 0.0970 | 134.1520 | 0.0150 | 0.0140 |
| 10 | 151353 | 0.1001 | 133.8368 | 0.0150 | 0.0140 |
| 11 | 1890000 | 0.0082 | 158.8737 | 0.0160 | 0.0160 |
| 12 | 6119256 | 0.0024 | 171.0184 | 0.0170 | 0.0160 |

From table 3 we can see that the proposed method does not add any negative effects on LSB2 method even for long messages by keeping MSE low and PSNR high, and here we can recommend using images with big sizes to increase PSNR and at the same time decrease MSE between the covering and the holding images, and here the changes in the holding image cannot be noticed by human eyes as shown in figures 7 and 8.

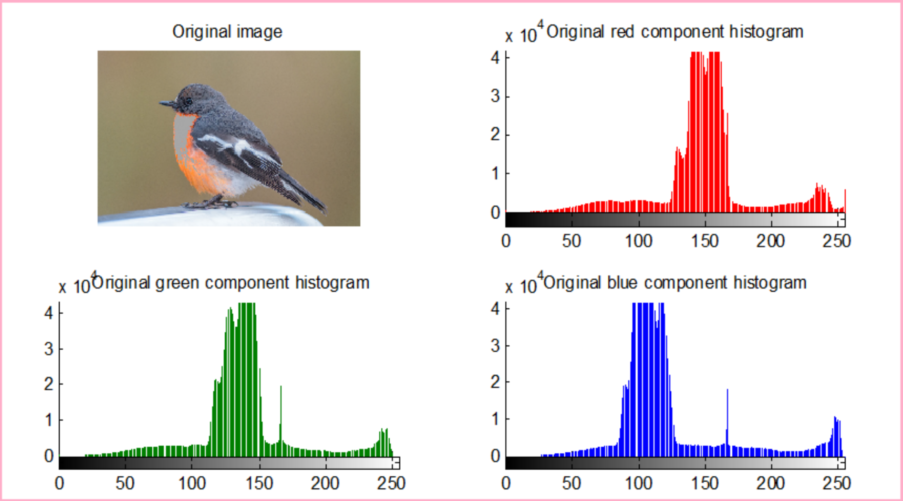


**Figure 7:** Covering big size image

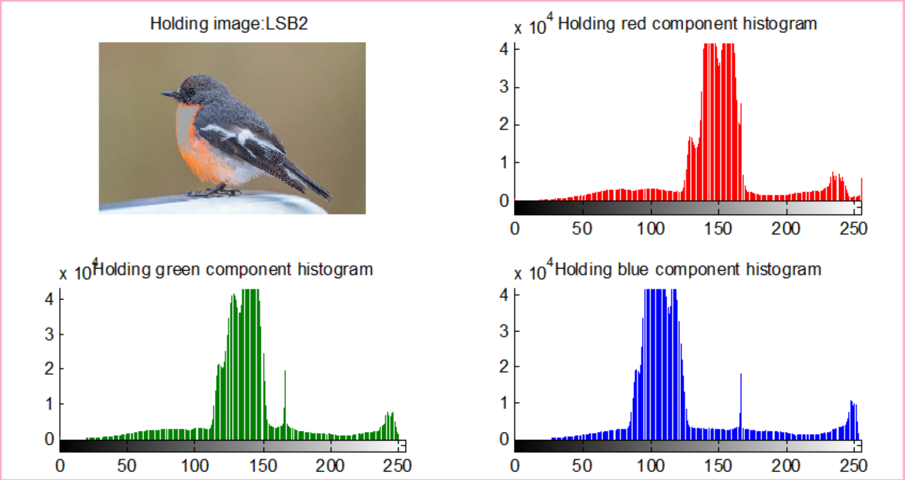


**Figure 8:** Image holding 1600-character message

## 6. CONCLUSION

A method of improving the security of LSB2 method of data steganography was proposed, tested and implemented. The obtained experimental results showed that the proposed method does not negatively affect LSB2 method by keeping MSE low and PSNR high. The proposed method uses an embedded key to encrypt the message, the values of this key are variable and they depend on the selected image, selected message length and selected position from where to extract the embedded key, the method uses the image position and the message length as a private key to secure LSB2 method.

## SOURCES OF FUNDING

None.

## CONFLICT OF INTEREST

None.

## ACKNOWLEDGMENT

None.

## REFERENCES

[1] Jamil Al-Azzeh, Ziad Alqadi, Mohammed Abuzalata, Performance Analysis of Artificial Neural Networks used for Color Image Recognition and Retrieving, international Journal of Computer Science and Mobile computing, vol. 8. Issue 2, pp. 20-33, 2-19.

[2] Ziad AlQadi, M Elsayyed Hussein, Window Averaging Method to Create a Feature Victor for RGB Color Image, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, 2017.

[3] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.

[4] Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, optimized true-color image processing, World Applied Sciences Journal, vol. 10, issue 8, pp. 1175-1182, 2010.

[5] A. A. Moustafa, Z. A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.

[6] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata, creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications, November 2016, Volume 153, Issue 2.

[7] AlQaisi Aws and AlTarawneh Mokhled and Alqadi Ziad A. and Sharadqah Ahmad A, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, volume 17, number 3, pages1220—1225, year 2019.

[8] Al-Azzeh J., Zahran B., Alqadi Ziad, Ayyoub B. and Abu-Zaher, M., A novel zero-error method to create a secret tag for an image, Journal of Theoretical and Applied Information Technology, volume 96, number13, pages 4081-4091, year 2018.

[9] Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, Creating Human Speech Identifier using WPT, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 117-123, 2020.

[10] Amjad Hindi, Majed Omar Dwairi, Ziad Alqadi, Analysis of Digital Signals using Wavelet Packet Tree, IJCSMC, vol. 9, issue 2, pp. 96-103, 2020.

[11] Prof. Mohammed Abu Zalata Dr. Ghazi. M. Qaryouti, Dr.Saleh Khawatreh, Prof. Ziad A.A. Alqadi, Optimal Color Image Recognition System (OCIRS), International Journal of Advanced Computer Science and Technology, vol. 7, issue 1, pp. 91-99, 2017.

[12] Dr. Amjad Hindi, Dr. Majed Omar Dwairi, Prof. Ziad Alqadi, Analysis of Procedures used to build an Optimal Fingerprint Recognition System, International Journal of Computer Science and Mobile Computing, vol. 9, issue 2, pp. 21 – 37, 2020.

[13] Prof. Ziad Alqadi Dr. Mohammad S. Khrisat, Prof. Yousif Eltous, Dr. Saleh A. Khawatreh, Dr. Majed Omar Dwairi, Building Face Recognition System (FRS), International Journal of Computer Science and Mobile Computing, vol. 9, issue 6, pp. 15-24, 2020.

[14] AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.

[15] Ziad Alqadi, Bilal Zahran, Jihad Nader, Estimation and Tuning of FIR Lowpass Digital Filter Parameters, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 7, issue 2, pp. 18-23, 2017.

[16] Musbah Aqel Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, vol. 6, issue 1, pp. 45-52, 2009.

[17] Jamil Al-Azzeh Naseem Asad, Ziad Alqadi, Ismail Shayeb, Qazem Jaber, Simple Procedures to Create HSCS, International Journal of Engineering Research and Management (IJERM), vol. 7, issue 5, pp. 6-10, 2020.

[18] BILAL ZAHRAN, JAMIL AL-AZZEH, ZIAD ALQADI, MOHD–ASHRAF ALZOGHOUL, SALEH KHAWATREH, A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES, Journal of Theoretical and Applied Information Technology, vol. 96, issue 10, pp. 3014-3024, 20, 2018.

[19] Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETES TEXT IN WAVE FILE, International Journal of Computer Applications, 2016.

[20] Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, IJCSMC, vol. 8, issue 6, pp. 106-123, 2019.

[21] Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Improving the security of LSB image steganography, JOIV: International Journal on Informatics Visualization, vol. 3, issue 4, pp. 384-387, 2019.

[22] Belal Ayyoub Ziad Alqadi, Ahmad Sharadqh, Naseem Asad Ismail Shayeb, Jamil Al-Azzeh, A highly secure method of secret message encoding, International Journal of Research in Advanced Engineering and Technology, vol. 5, issue 3, pp. 82-87, 2019.

[23] Ahmad Sharadqh Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 306 – 319, 2019.

[24] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.

[25] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Ahmad Sharadqh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 306-319, 2019.

[26] Mohammad S Khrisat, Ziad Alqadi, Saleh A Khawatreh, Improving WPT color image decomposition, International Journal of Computer Science and Information Security (IJCSIS), vol. 12, issue 7, pp. 13-21, 2020.

[27] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, two ways to improve WPT decomposition used for image features extraction, European journal for scientific research, vol. 157, issue 2, pp. 195-205, 2020.

[28] Ziad Alqad, Majid Oraiqat, Hisham Almujafet, Salah Al-Saleh, Hind Al Husban, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.

[29] Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Digital color image encryption-decryption using segmentation and reordering, International Journal of Latest Research in Engineering and Technology (IJLRET), vol. 6, issue 5, pp. 6-12, 2020.

[30] Rashad J Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh, Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 14-26, 2019.