International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 12, December 2021, pg.46 – 61

Crypto-Steganographic Method to Protect Secret Messages

Dr. Mohamad Tariq Barakat; Dr. Rushdi Abu Zneit; Prof. Ziad A. Alqadi

Albalqa Applied University, Jordan

Faculty of Engineering Technology

Electrical Engineering Department

DOI: 10.47760/ijcsmc.2021.v10i12.007

Abstract: Multiple methods are used to hide secret messages in digital color images, and the most important and most common is the least significant bit (LSB) method. The LSB method is a known and exposed method, and anyone with programming experience can retrieve the secret message embedded in the digital image. In this paper research we will add some enhancements to improve the security level of LSB method to protect the embedded secret message from being hacked. A simple method of secret message cryptography will be used to encrypt the secret message before bedding it using LSB method. The method will be based on using color image as an image_key; this image_key will be resized to generate the needed secret private key used to encrypt-decrypt secret message. The length and the contents of the generated private key will dynamically change depending on the message length and the selected image_key. The selected image_key will be kept in secret without transmission and will be known only by the sender and receiver and it can be changed any time when needed. The proposed crypto_steganographic method will be implemented to show how it will increase the level o secret message protection.

Keywords: Cryptography, steganography, image_key, PK, MSE, PSNR, efficiency.

Introduction

Text messages are now being circulated through various social media in a very large way, and many of these messages may be private or carry confidential information, which requires protecting them from penetration or attempting to read them and tamper with them by unauthorized persons [1-3]. Multiple methods are used to protect text messages and from these methods data steganography and data cryptography methods [1-10].

Data steganography as shown in figure 1 means hiding the secret message in a covering digital color image [5-10], the process of message hiding must not make big changes in the covering images and these changes must not be determined by human naked eyes [11-17]. The small changes between the stego_image (covering image) and the source image can be measured by mean square error (MSE) and/or peak signal to noise ratio (PSNR)[17], [18], here

MSE must be closed to zero, while PSNR value must be very high, these quality parameters can be calculated using equations 1 and 2 as shown below [49-56].

Figure 1: Data steganography process

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \|f(i,j) - g(i,j)\|^2 \quad (1)$$

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right) \quad (2)$$

Where: f and g are the images to be compared for quality.

The second method used to protect confidential messages is data cryptography [18-25] which means data encrypting and decrypting [26-30]. The data encryption process is implemented using a private and secret key known to the sender and receiver, and as shown in the figure 2, where some special operations are implemented on the data and the private key to generate destructive and distorted data that no third party can understand or benefit from. As for the decryption process, the data is processed using the same private key to generate data that exactly matches the original data that was encrypted. Here MSE between the original data and the encrypted one must be very high (PSNR must be very low) (this means fully destruction o the data), while MSE between the decrypted data and the original one must equal zero (PSNR must be infinite)(this means fully data recovery) [31-40].

It should be noted here that in order to raise the level of protection for confidential text messages, the following can be done [41-50]:

- Applying cryptography the steganography to protect the embedded in the covering image data.

- Using a color image as an image_key to generate the necessary PK (as shown in figure 3), this image is known only by the sender and receiver and must be kept in secret without transmission.

Figure 2: Data cryptography process

Figure 3: Using secret image as an image_key

The most popular method of data steganography is least significant bit (LSB) method [29], [41], [51], this method is very simple and provides a good values for the quality parameters MSE and PSNR, but it is not secure and can be easily hacked, this method can be implemented applying the steps shown in figure 4, these steps are illustrated in the example shown in figure 5:

Figure 4: LSB implementation[51]

Figure 5: LSB example

The proposed method

The proposed method is based in cryptography followed by steganography to protect the secret message when sending the message and steganography followed by cryptography when receiving the message. The cryptography is based on using a secret color image as an image_key, this image_key must kept in secret and used to generate the PK required for data cryptography[32-37].

The length and contents of PK depends on the image_key, the selected color channel and the message length. Changing the message or changing the image_key and the selected color channel will change the PK length and contents as shown in the figures 6 thru 10:

Figure 6: Using image 1 as an image_key and selecting red color to generate PK

Figure 7: Using image 1 as an image_key and selecting green color to generate PK

Figure 8: Using image 1 as an image_key and selecting blue color to generate PK

Figure 9: Using image 5 as an image_key and selecting red color to generate PK

Figure 10: Using image 5 as an image_key and selecting red color to generate PK for another message

The proposed method for data hiding can be implemented as shown in figure 11 applying the following steps:

Figure 11: Proposed method of data hiding

- *Select the image_key.*
- *Select the color channel.*
- *Select the secret message.*
- *Resize the color channel to the message size to get the PK.*
- *Encrypt the message applying XORing of the message and the PK.*
- *Apply LSB method to hide the encrypted message.*

The extraction process can be implemented as shown in figure 12 applying the following steps:

Figure 12: Proposed method of data extraction

- *Get the stego image*
- *Apply LSB to get the encrypted image.*
- *Select the image_key,*
- *Select the color channel from the image_key.*
- *Resize the color channel to the message size to get PK.*
- *Apply XORing of the PK and the encrypted message to get the original secret message.*

Implementation and Experimental Results

The proposed method was programmed using Matlab, and this method was implemented using the selected digital color images shown in the figures 13 and 14, table 1 show the main features of these images.

Table 1: Used images information

Image number	Dimensions			Size(byte)
1	151	333	3	150849
2	152	171	3	77976
3	360	480	3	518400
4	1071	1600	3	5140800
5	981	1470	3	4326210
6	165	247	3	122265
7	360	480	3	518400
8	183	275	3	150975
9	183	275	3	150975
10	201	251	3	151353
11	600	1050	3	1890000
12	1144	1783	3	6119256

Figure 13: Used images 1 to 6

Figure 14: Used images 7 to 12

Figure 15 shows an output example of the proposed method implementation:

Figure 15: Implementation output example

Image 5 was selected as an image_key, image 12 was selected as a stego_image, and table 2 shows the results of processing various messages with various lengths.

Table 2: Processing various messages using image 5 as image_key, image 12 as stego_image

Message length(byte)	MSE	PSNR	Encryption time(second)	Hiding time(second)	Total time(second)
10	5.8831e-006	231.2596	0.0400	0.0412	0.0812
20	1.3073e-005	223.2745	0.0400	0.0420	0.0820
30	1.9610e-005	219.2199	0.0400	0.0427	0.0827
40	2.4676e-005	216.9220	0.0400	0.0433	0.0833
50	3.2520e-005	214.1617	0.0473	0.0510	0.0983
100	6.5204e-005	207.2052	0.0480	0.0512	0.0992
200	1.2992e-004	200.3114	0.0482	0.0522	0.1004
400	2.5232e-004	193.6735	0.0484	0.0649	0.1132
500	3.2504e-004	191.1409	0.0488	0.0707	0.1195
600	3.8289e-004	189.5029	0.0507	0.0774	0.1282
800	5.3242e-004	186.2061	0.0532	0.0903	0.1435
1000	6.4926e-004	184.2220	0.0533	0.1097	0.1630

The same messages were processed using image 2 as a stego_image; table 3 shows the obtained results:

Table 3: A5 image_key, a2 stego_image

Message length(byte)	MSE	PSNR	Encryption time(second)	Hiding time(second)	Total time(second)
10	5.3863e-004	186.0901	0.0474	0.0021	0.0495
20	9.2336e-004	180.7002	0.0488	0.0025	0.0514
30	0.0014	176.5534	0.0496	0.0032	0.0528
40	0.0019	173.2280	0.0484	0.0048	0.0531
50	0.0025	170.6857	0.0496	0.0040	0.0536
100	0.0051	163.6023	0.0491	0.0078	0.0569
200	0.0102	156.6708	0.0478	0.0142	0.0620
400	0.0200	149.9488	0.0482	0.0270	0.0752
500	0.0250	147.7212	0.0490	0.0340	0.0830

600	0.0294	146.0863	0.0489	0.0401	0.0890
800	0.0383	143.4432	0.0486	0.0548	0.1033
1000	0.0473	141.3357	0.0561	0.0654	0.1215

To show the effects of image size, a message of 500 bytes was treated using various images as a stego_image; table 4 shows the obtained experimental results.

Table 4: Image 4 key, message size =500 byte

Stego_image	MSE	PSNR	Encryption time(second)	Hiding time(second)	Total time(second)
1	0.0134	153.9720	0.0526	0.0322	0.0847
2	0.0250	147.7212	0.0521	0.0322	0.0843
3	0.0039	166.2770	0.0518	0.0377	0.0895
4	3.8846e-004	189.3585	0.0509	0.0654	0.1163
5	4.5074e-004	187.8714	0.0517	0.0598	0.1115
6	0.0161	152.1170	0.0513	0.0335	0.0848
7	0.0039	166.3713	0.0503	0.0367	0.0870
8	0.0128	154.4316	0.0511	0.0339	0.0851
9	0.0134	153.9654	0.0557	0.0342	0.0900
10	0.0131	154.1401	0.0517	0.0336	0.0853
11	9.3492e-004	180.5758	0.0511	0.0453	0.0963
12	3.3386e-004	190.8730	0.0527	0.0780	0.1307

Red: Small stego_image size, Green: Big stego_image size

Each message was encrypted-decrypted using an image_key, the values of obtained MSE and PSNR were acceptable, table 5 shows the results of encryption various messages using image 4 as an image_key:

Table 5: Messages encryption results using image 4 as an image_key

Message length	MSE	PSNR
10	1.2047e+004	15.9775
20	1.0915e+004	17.6890
30	1.2961e+004	15.8918
40	1.2934e+004	15.9917
50	1.2927e+004	16.1548
100	1.2359e+004	16.6039
200	1.3457e+004	15.7529
400	1.2833e+004	16.2272
500	1.2915e+004	16.1638
600	1.2772e+004	16.2753
800	1.3037e+004	16.0699
1000	1.2931e+004	16.1514

Results Discussion

Adding the encryption and decryption process does not negatively affect the LSB quality of the images by obtaining excellent values for MSE and PSNR as shown in figures 16 and 17

Figure 16: Covering image and histograms

Figure 17: Stego_image and histograms

The added time as a result of the encryption and decryption process is very little, so the efficiency of the LSB method will not be affected much.

The proposed method increases the degree of protection of the hidden data in the digital image for the following reasons:

- The digital image used as a private key is a large image and is difficult to hack.
- The digital image used as a private key is confidential and is not circulated and is kept by the sender and receiver and is agreed upon.
- The possibility of replacing the key image at any moment.
- The color used in the image for encoding is confidential
- The private key changes dynamically depending on the text message and image used.

The time to hide the text message increases with the increase in its size, and the same is true for the MSE value, but the values remain good and acceptable, as shown in the figure 18:

Figure 18: Relationships of message length and MSE, PSNR and hiding time (big stego_image)

Decreasing the stego_image size will decrease the value of PSNR, the hiding time and will increase the value of MSE, but the obtained values are acceptable (see figure 19)

Figure 19: Relationships of message length and MSE, PSNR and hiding time (smaller stego_image)

Conclusion

LSB is one of the most popular methods of data steganography, this method is very simple and capable to hide long secret messages in a stego_image. LSB is not secure and it can be easily hacked. A cryptography procedures were added to LSB to protect the secret message and raise the LSB data protection degree. The added procedures use a digital color image as an image_key to generate the PK. The private key length and contents will dynamically change when the message length changes and when the image_key changes. The proposed method was implemented and tested and the obtained experimental results showed that the proposed method enhanced the security of LSB method with minimum cost in time and without affecting the image quality parameters.

References

- [1] E. Fujisaki and T. Okamoto, Secure Integration of Asymmetric and Symmetric Encryption Schemes, J Cryptol, vol. 26, pp. 80-101, 2013.
- [2] K. Kurosawa and T. Takagi, "Some RSA-Based Encryption Schemes with Tight Security Reduction" in Advances in Cryptology - ASIACRYPT 2003. ASIA CRYPT 2003, Lecture Notes in Computer Science, Berlin, and Heidelberg: Springer, vol. 2894, 2003.
- [3] Musbah J. Aqel, Ziad A. Alqadi, Ibraheim M. El Emary, Analysis of Stream Cipher Security Algorithm, Journal of Information and Computing Science Vol. 2, No. 4, 2007, pp. 288-298.
- [4] Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, pp. 3228-3235, 2019.
- [5] Dr. Hatim Zaini Prof. Ziad Alqadi, SIMPLE, EFFICIENT AND HIGHLY SECURE METHOD FOR TEXT FILES CRYPTOGRAPHY, World Journal of Engineering Research and Technology, vol. 7, issue 6, 2021.
- [6] Dr. Mohammad S. Khraisat Prof. Ziad Alqadi, ANALYSIS OF TEXT FILES ENCRYPTION-DECRYPTION METHODS, IJETRM, vol. 5, issue 3, pp. 48-54, 2021.
- [7] Prof. Ziad Alqadi, EFFICIENT AND HIGHLY SECURE METHOD OF MESSAGE ENCRYPTION, IJETRM, vol. 5, issue 2, pp. 58-64, 2021.
- [8] Dr. Jihad Nader; Dr. Mohammad S. Khraisat; Prof. Ziad Alqadi, A Survey of RGB Color Image Encryption Methods, IJCSMC, Vol. 9, Issue 6, pp.106 –113, 2020.
- [9] Ziad Alqad, Majid Oraiqat, Hisham Almujafer, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.
- [10] Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, optimized true-color image processing, World Applied Sciences Journal, vol. 8, issue 10, pp. 1175-1182, 2010.
- [11] Jamil Al Azzeh, Hussein Alhatamleh, Ziad A Alqadi, Mohammad Khalil Abuzalata, creating a Color Map be used to Convert a Gray Image to Color Image, International Journal of Computer Applications, vol. 153, issue 2, pp. 31-34, 2016.
- [12] Qazem Jaber Ziad Alqadi, Jamil azza, Statistical analysis of methods used to enhance color image histogram, XX International scientific and technical conference, 2017.
- [13] Bassam Subaih Ziad Alqadi, Hamdan Mazen, A Methodology to Analyze Objects in Digital Image using Mat lab, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 21-28, 2016.
- [14] Mazen A. Hamdan Bassam Subaih, Prof. Ziad A. Alqadi, Extracting Isolated Words from an Image of Text, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 29-36, 2016.
- [15] 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.
- [16] Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, pp. 1220-1225, 2019.
- [17] Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.
- [18] Ziad Alqadi, Dr. Mohammad S. Khraisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, VALUABLE WAVELET PACKET INFORMATION TO ANALYZE COLOR IMAGES FEATURES, International Journal of Current Advanced Research, vol. 9, issue 2, pp. 2319, 2020.

- [19] Ziad Alqadi, M Essayed Hussein, Window Averaging Method to Create a Feature Vector for RGB Color Image, International Journal of Computer Science and Mobile Computing, vol. 6, issue 2, pp. 60-66, 2017.
- [20] Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, suggested Method to Create Color Image Features Vector, Journal of Engineering and Applied Sciences, vol. 14, issue 1, pp. 2203-2207, 2019.
- [21] Ahmad Sharadqh Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, vol. 8, issue 8, pp. 50-56, 2019.
- [22] Yousf Eltous Ziad A. Al Qadi, Ghazi M. Qaryouti, Mohammad Abuzalata, ANALYSIS OF DIGITAL SIGNAL FEATURES EXTRACTION BASED ON KMEANS CLUSTERING, International Journal of Engineering Technology Research & Management, vol. 4, issue 1, pp. 66-75, 2020.
- [23] Ziad A Alqadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp.48-55, 2020.
- [24] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2019.
- [25] Ziad Alqadi, Majid Oriana, Husham Almujafer, Salah Al-Saleh, Hind Al Husband, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 8, pp. 30-48, 2019.
- [26] Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.
- [27] Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqh, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8, issue 5, pp. 2780-2787, 2018.
- [28] Jihad Nader Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.
- [29] 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.
- [30] Ziad Alqadi, Ahmad Sharadqh, Naseem Asad, Ismail Shayeb, Jamil Al-Azzeh, Belal Ayyoub, 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.
- [31] Musbah Aqel Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences, vol. 6, issue 1, pp.45-52, 2009.
- [32] Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, vol. 5, issue 5, pp. 465-470, 2016.
- [33] Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, International Journal of Engineering and Technology, vol. 7, issue 3, pp. 104-107, 2018.
- [34] Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED), International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 6, pp.3228-3235, 2019.
- [35] Majed O Al-Dwairi, A Hindi, Z Alqadi, an efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.
- [36] Amjad Y Hindi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, A novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp. 232-238, 2019.
- [37] Ziad A Alqadi, Accurate Method for RGB Image Encryption, International Journal of Computer Science and Mobile Computing, vol. 9, issue 1, pp. 12-21, 2020.
- [38] Ziad Alqadi, Majid Oraiqat, Hisham Almujafer, Salah Al-Saleh, Hind Al Husban, Soubhi Al-Rimawi, A New Approach for Data Cryptography, International Journal of Computer Science and Mobile Computing, vol. 8, issue 9, pp. 30-48, 2019.
- [39] Jamil Al-Azzeh, Ziad Alqadi, Qazem Jaber, A Simple, Accurate and Highly Secure Method to Encrypt-Decrypt Digital Images, JOIV: International Journal on Informatics Visualization, vol. 3, issue 3, pp. 262-265, 2019.
- [40] Dr Saleh a Khawatreh Dr Majed, Omar Dwairi, 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.

- [41] Mutaz Rasmi Abu Sara Rashad J. Rasras, Ziad A. Alqadi, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages, *Engineering, Technology & Applied Science Research*, vol. 9, issue 1, pp. 3681-3684, 2019.
- [42] Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein, A Comparison BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 8, issue 5, pp. 125-131, 2016.
- [43] PROF. ZIAD A. ALQADI, A SIMPLE METHOD TO ENCRYPT-DECRYPT SPEECH SIGNAL, *International Journal of Engineering Technology Research & Management*, vol. 5, issue 2, pp. 44-52, 2021.
- [44] Ziad Alqadi, Analysis of stream cipher security algorithm, *Journal of Information and Computing Science*, vol. 2, Issue 4, pp. 288-298, 2007.
- [45] 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.
- [46] 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.
- [47] Amjad Y Hindi, Majed O Dwairi, Ziad A Alqadi, A Novel Technique for Data Steganography, *Engineering, Technology & Applied Science Research*, vol. 9, issue 6, pp. 4942-4945, 2019.
- [48] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, issue 5, pp. 4092-4098, 2019.
- [49] 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.
- [50] Akram A Moustafa, Ziad A Alqadi, A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image, *Journal of Computer Science*, vol. 5, issue 5, pp. 355-362, 2009.
- [51] Rushdi Abu Zneit, Jamil Al-Azzeh, Ziad Alqadi, Belal Ayyoub, Ahmad Sharadqh, Using Color Image as a Stego-Media to Hide Short Secret Messages, *International Journal of Computer Science and Mobile Computing*, vol. 8, issue 6, pp. 106-123, 2019.
- [52] 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.
- [53] Mohammed Ashraf Al Zudool, Saleh Khawatreh, Ziad A. Alqadi, Efficient Methods used to Extract Color Image Features, *IJCSMC*, vol. 6, issue 12, pp. 7-14, 2017.
- [54] ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, *World Applied Sciences Journal*, vol. 5, issue 2, pp. 211-214, 2008.
- [55] Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, issue 5, pp. 4092-4098, 2019.
- [56] Ziad Alqadi, A practical approach of selecting the edge detector parameters to achieve a good edge map of the gray image, *Journal of Computer Science*, vol. 5, issue 5, pp. 355-362, 2009.