iJETRM
International Journal of Engineering Technology Research & Management

ANALYSIS OF TEXT FILES ENCRYPTION-DECRYPTION METHODS

Prof. Ziad Alqadi, Dr Mohamad S. Khrisat
Albalqa applied university
Faculty of engineering technology
Amman-Jordan

ABSTRACT
Text file may contain secret or personal data which needs protection from hacking and preventing reading it by any third party. In this paper research we will introduce a symmetric method of text file encryption-decryption. This method will use a huge color image as a private key allowing us to encrypt-decrypt text files with large sizes by increasing the level of security because it is impossible to guess the image. The proposed method will be implemented and the obtained experimental results will be compared to DES and AES methods of encryption to prove the efficiency and security of the proposed method.

Keywords:
Text file, private key, encryption, decryption, MSE, PSNR, throughput, DES, AES.

INTRODUCTION

A **text file** is a computer file that only contains text and has no special formatting such as bold text, italic text, images. The text file is organized into a group of lines; each line ends with a new line (carriage return and line feed (10 and 13 ASCII code)). The text file may be confidential and contain highly confidential information, or it may be contain personal information which requires preventing any unauthorized person from viewing, reading, or understanding it. And to protect the text file from intruders, the encryption process is used to destroy the file completely so that it becomes unreadable, and the decryption process is to return the text file to its original status without losing any part of the information[23],[40]. [41].

Many methods based on data encryption standard (DES) and advanced encryption standard (AES) methods are used for text file encryption-decryption [16], [17]. These methods are symmetric by using the same private key by both the text sender and receiver. The text file is to be divided into fixed size blocks; each block is to be encrypted-decrypted separately using private key. These methods provide a good level of data security, but they can be hacked [18], [19]. [20].

In this paper research we will introduce a new method of text file encryption-decryption based on using a selected a huge color image as a private key, this image will be kept in secret by the sender and receiver[21], [22], [23].

The digital color image is represented by a three-dimensional matrix [1], [2], [3], where the first dimension is used to represent the red color and the second dimension is used to represent the green color, and the third dimension is used to represent the blue color, figure 1 shows Petra city image and the associated histogram as an example of RGB [6], [7], [8].

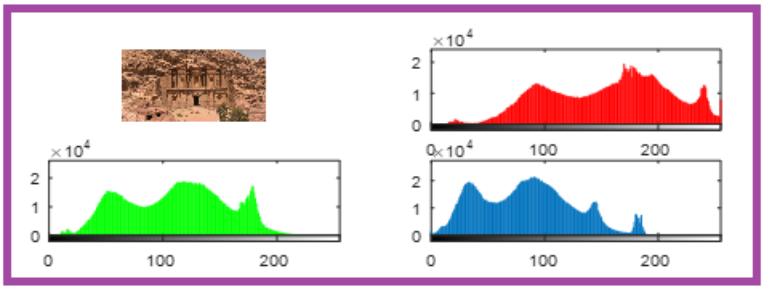

Figure 1: Color image example and histograms[4], [5]

iJETRM
International Journal of Engineering Technology Research & Management

Digital images are one of the most common types of data circulating through many social media[15], which facilitates the process of obtaining them and using them for various purposes, especially in the encryption and decryption process. The reasons for using the digital image in encoding and decoding can be summarized as follows:

- ✓ Ease of obtaining the digital image and the lowest costs[9].
- ✓ Ease of digital image processing. The large size of the digital image allows it to be used as a hard-to-crack key in the encryption and decryption process[10].
- ✓ The possibility of using part or parts of the image to form the private key.
- ✓ The image contains a large number of pixels with values ranging from zero to 255, which cover the ASCII code for all the symbols that the text file can contain. Ease of preserving the digital color image at the sender and receiver[11], [12].
- ✓ The ability to change the digital image and use an alternative image whenever the need arises[13], [14].

The process of encryption-decryption as shown in figure 2 must meet the following requirements[24], [25], [26]:

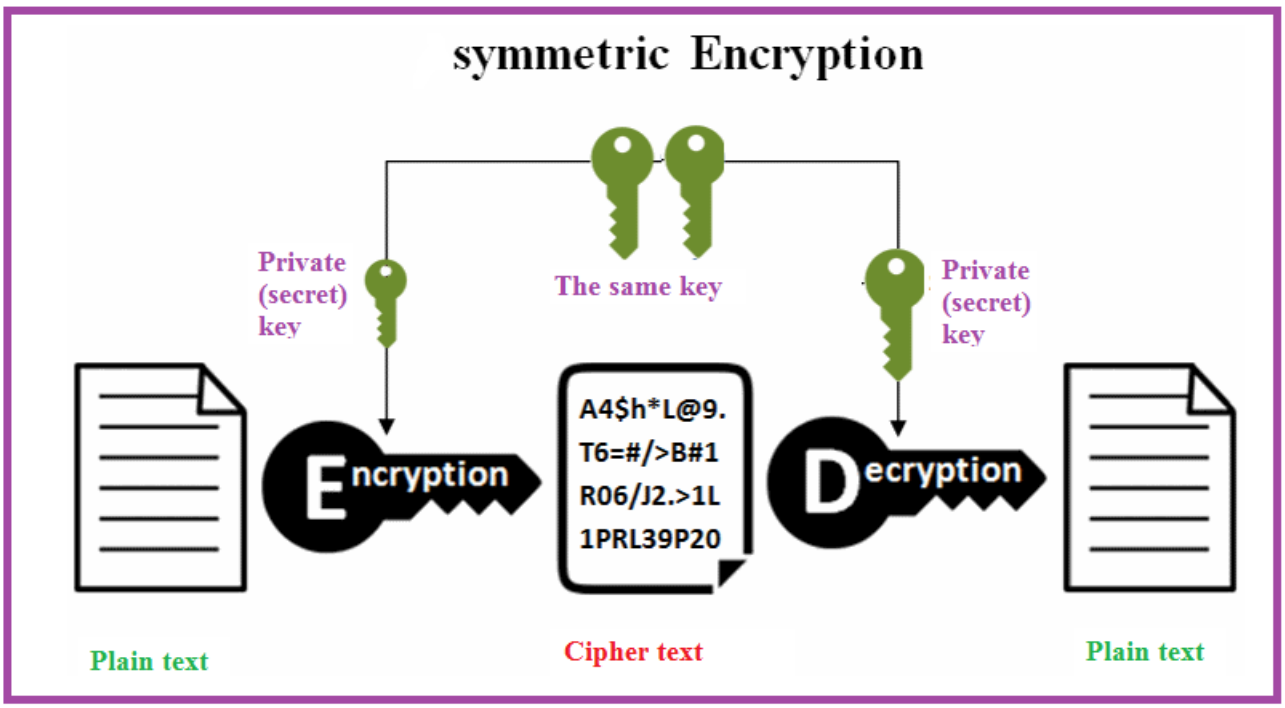

Figure 2: Encryption_decryption process

- The encryption process must destroy the source text file(plain text) making it unreadabale for any hacker[39], [40], so the mean square error (MSE) between the plain text and the encrypted one must very high, or the peak signal to noise ratio (PSNR) [41], [42]between the two files must be very low[27], [28].
- The dencryption process must retreive or recover the source text file(plain text), so the mean square error (MSE) between the plain text and the dencrypted one must be equal zero, or the peak signal to noise ratio (PSNR) between the two files must be infinite [29], [30], [31].
- The private key must be large, so it can not be guessed by any third part [32], [34], [35].
- The effecincy must be very high by providing a high throughput(maximizing the number of bytes encrypted or decrypted in a unit of time)[[36], [37], [38].

iJETRM
International Journal of Engineering Technology Research & Management

The proposed method of image encryption_decryption

The proposed method for encryption(as shown in figure 3) can be implemented applying the following steps:

1) Select a color image to be used as a private key.
2) Get the text file.
3) Reshape the text file to one row matrix.
4) Reshape the image to one row matrix.
5) From the image extract a private key with length equal text file length.
6) Apply XORing of text file and private key to get the encrypted text file.

The decryption phase can be implemeted applying the following steps:

1) Get the color image (key).
2) Get the encrypted text file.
3) Reshape the encrypted text file to one row matrix.
4) Reshape the image to one row matrix.
5) From the image extract a private key with length equal encrypted text file length.
6) Apply XORing of encrypted text file and private key to get the decrypted text file.

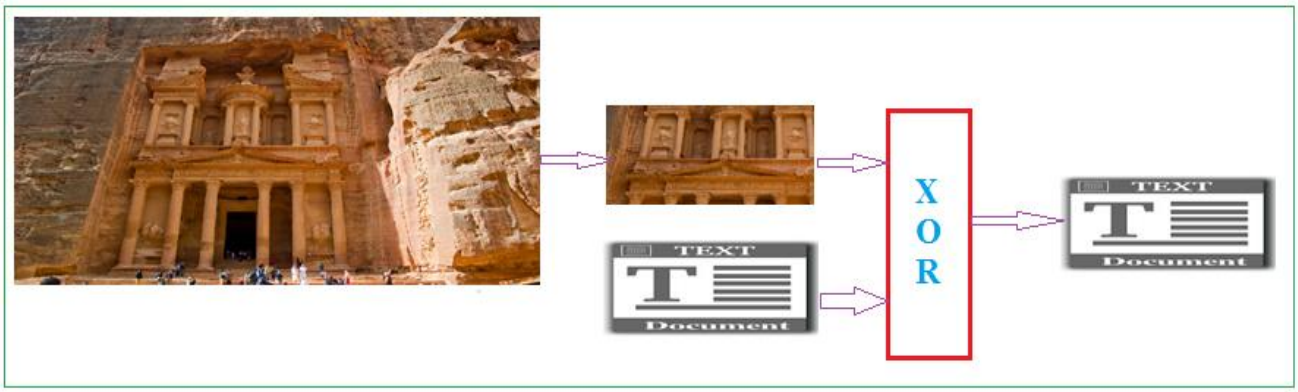

Figure 3: Proposed method(encryption phase)

Implementation and experimental results

Jordan Petra city image was selected to be used as a private key, the image size is equal 1080 * 1920* 3=6220800=6.2 MB, this image can be used to encrypt-decrypt text files with sizes up to 6 Mbyte(characters).
Deffirent test files with deffirent sizes were encrypted decrypted using this image, table 1 shows the obtained experimental results:

iJETRM
International Journal of Engineering Technology Research & Management

Table 1: Obtained experimental results

Text file size(byte)	Encryption time(seconds)	PSNR	MSE
3200	0.002618	19.5171	9.2355e+03
6400	0.002681	19.5263	9.2271e+03
25600	0.002905	19.7619	9.0122e+03
51200	0.001688	19.8752	8.9107e+03
102400	0.003379	19.9581	8.8372e+03
204800	0.004499	19.8487	8.9344e+03
409600	0.007618	19.6467	9.1166e+03
819200	0.010761	19.5026	9.2490e+03
1638400	0.025769	19.6123	9.1480e+03
3276800	0.027672	19.7627	9.0115e+03
Average: 653760	0.0090	Troughput=72640000 byte per second=72640 KB persecond	

From table 1 we can see the following facts:

- The MSE values between the original text file and the encrypted one are always very high, which mean that the encryption process destryed the original text file.
- The PSNR values between the original text file and the encrypted one are always small, which mean that the encryption process destryed the original text file.
- The decrypted text file was identical with the original text file (MSE always zero and PSNR always infinit).
- The average thoughput is very high comparing with DES and AES throughputs(see table 2), which means that the proposed method is very efficient.
- The proposed method is very secure because it uses a huge secret image as a key, and it is impossible to guess the key.

Table 2: DES and AES results

Input size(KB)	DES	AES
15	3.8	5.07
30	7.5	17.09
45	8.5	1.96
60	8.8	22.91
75	9.33	29.99
90	10.7	38.15
Average time	8.105	22.195
KB/sec	27.76	10.13

Figure 4 shows the relationship between the text file size and the encryption time, from this figure we can see that the encryption time is slowly incerasing when rapidly increasing text file size.

iJETRM
International Journal of Engineering Technology Research & Management

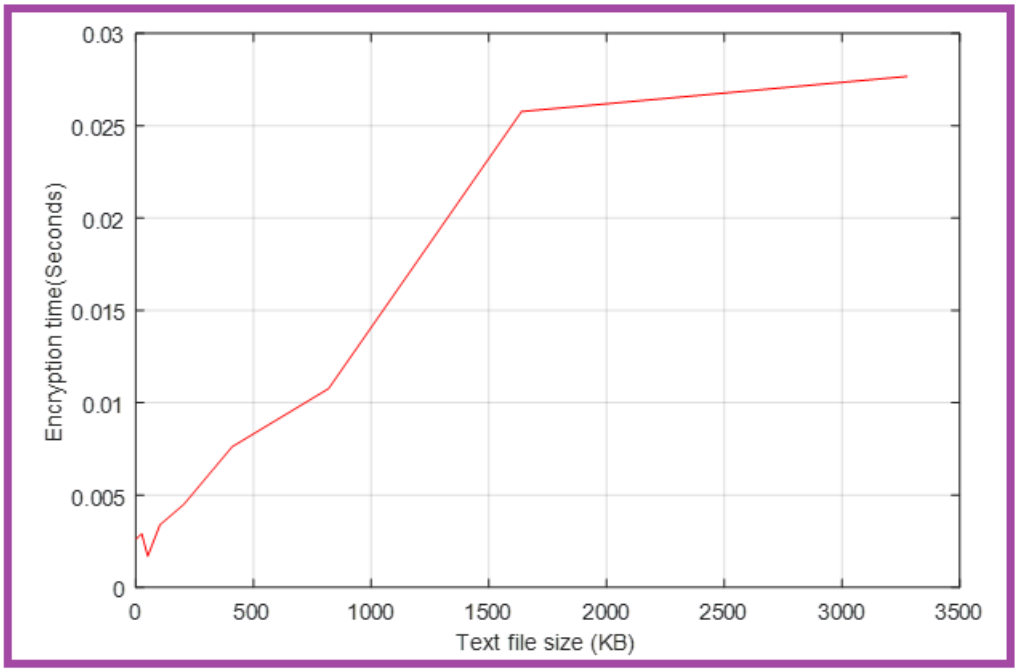

Figure 4: Encryption time as a function of text file size.

Table 3 shows comparisons between the proposed method features and DES and AES features.

Table 3: Comparisons with DES and AES

Feature	DES	AES	Proposed
Type	Symmetric	Symmetric	Symmetric
Data block size	Fixed	Fixed	Variable
Private key length	Fixed	Fixed	Variable
Key generation	Required	Required	No need
S-box	Required	Required	No need
Level of security	Low	High	Very high
Throughput	Medium	Low	Very high
Text file size	Good for small size	Good for small size	Good for any size

Conclusion

A simple and highly secure and efficient method of text files encryption-decryption was proposed, tested and implemented.

It was shown that requirements of good process of encryption-decryption were achieved by the proposed method, the method was compared with other standard methods of encryption-decryption such as DES and AES, it was shown that the proposed method increases the encryption process efficiency and at the same time it increases the level of security.

References

[1] 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.

[2] 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, vol. 153, issue 2, pp. 31-34, 2016.

[3] Qazem Jaber Ziad Alqadi, Jamil azza, Statistical analysis of methods used to enhance color image histogram, XX International scientific and technical conference, 2017.

[4] Bassam Subaih Ziad Alqadi, Hamdan Mazen, A Methodology to Analyze Objects in Digital Image using

iJETRM
International Journal of Engineering Technology Research & Management

Matlab, International Journal of Computer Science & Mobile Computing, vol. 5, issue 11, pp. 21-28, 2016.
[5]Mazen A.Hamdan Bassam M.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.
[6] 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.
[7] 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.
[8]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.
[9] Ziad Alqadi, Dr. Mohammad S. Khrisat, 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.
[10]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, pp. 60-66, 2017.
[11] 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.
[12]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.
[13] Yousf Eltous Ziad A. AlQadi, 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.
[14]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.
[15] 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
[16] Ziad Alqad, Majid Oraiqat, Hisham Almujafet, 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 8, pp. 30-48, 2019.
[17]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.
[18]Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, 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.
[19]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.
[20] 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.*
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] Belal Zahran Rashad J Rasras, Ziad Alqadi, Mutaz Rasmi Abu Sara, B Zahran, Developing new

iJETRM
International Journal of Engineering Technology Research & Management

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.
[26] Majed O Al-Dwairi, A Hendi, 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.
[27] Amjad Y Hendi, 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.
[28] 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.
[29] Ziad Alqad, Majid Oraiqat, Hisham Almujafet, 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.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] 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.

[35] Ziad alqadi, *Analysis of stream cipher security algorithm*, Journal of Information and Computing Science, vol. 2. Issue 4, pp. 288-298, 2007.
[36] 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.

[37] 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.
[38] 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.***
[39] 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.
[40] 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.
[41] 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.
[42] 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.