iJETRM
International Journal of Engineering Technology Research & Management

# USING LARGE COLOR IMAGE TO ENCRYPT-DECRYPT SMALLER ONES

Anwar Al Abadi,
Prof. Ziad A. Alqadi
Albalqa Applied University
Faculty of engineering technology
Jordan – Amman

**ABSTRACT**
Color images are some time used as a carrier which holds secret data, or sometime the image me be secret or has a private nature, for these reasons it requires protection by applying encryption-decryption. In this research paper we will introduce a very simple and highly efficient and secure method of image encryption. This method will be based on selecting and using a large image as a private key. To destroy the encrypted image an extra constant will be used, this constant will be enhancing the outputs of the proposed method and will be kept in secret.

**Keywords:**
Image key, secret constant, encryption, decryption, MSE, efficiency, security.

## INTRODUCTION

Color digital images are one of the most common types of digital data circulated through various social media [37], [39], [40].
The digital image may be of a personal nature or it may be confidential or carry confidential data or private secret messages[21], [38], [42] embedded in it, which requires protection from hacking or protection from intruders, which makes the importance of encrypting the digital image an urgent process[41].
Regardless of whether the digital image is secret or carries secret messages, it requires an encryption process for several reasons, the most important of which are:

- Most of the methods of hiding confidential data in digital images, which are based on the least sinifican bit (LSB) method, are not secure[16], [20], [21].
- The possibility that the text message is personal and contains private personal information[20], [23].
- The possibility that the digital image itself is secret or that it has a special character and is not allowed to anyone who is not authorized to understand it[24], [25], [26].
- Prevent the process of eavesdropping on text messages from spammers, regardless of the content of the text messagep27], [28].

And for the previous reasons, it is imperative to provide a way to protect the text message from the risk of intrusion or theft [27], [28], by destroying the message completely so that it becomes incomprehensible and unreadable and not even without benefit to any third party that has nothing to do with the text message[29], [30]. The process of destroying the text message is called the encryption process[22], [23], and it is usually carried out using one or more secret private keys, as shown in Figure 1

iJETRM
International Journal of Engineering Technology Research & Management

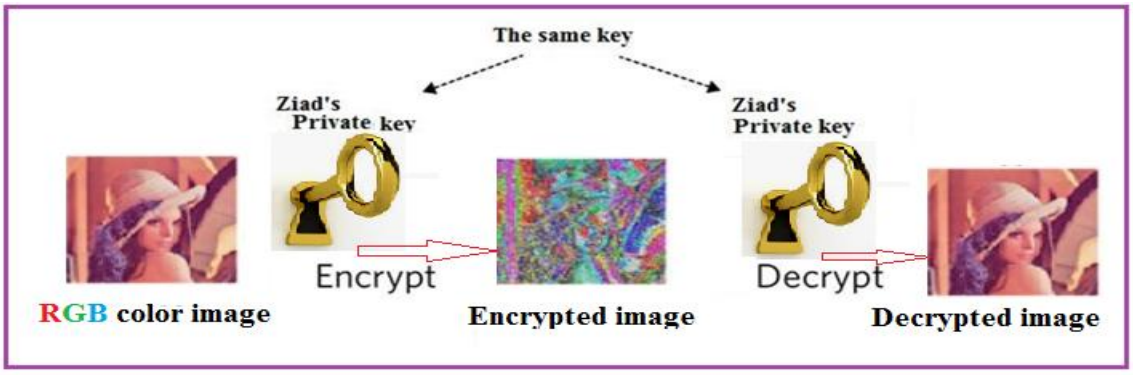


Figure 1: Image encryption-decryption process.

There are multiple ways to encrypt color image using international standards(data encrption standarad (DES) [16],[34], advanced enncryption standard (AES))[35], [36], where these methods depend on the use of a private key, and some of these methods are secure and some of them are not, and these methods require a long time for encryption and decryption, especially if the text message is long, this time is required to acomplish some task suck as key generation, rounds imaplementation and s-box implementation.

A good encryption-decryption method must satisfy the foloowing requirments:

- Effeciency by maximizing the method throughput( manipulated characters per second), this can be achieved by minimising the encryption-decryption times[24], [25].
- High level of security: by protecting data, and not allowing hackers to recover the private key[26], [27].
- Complete destruction of data during encryption by increasing the mean square error (MSE) between the original message and the encrypted message[28], [29].
- Retrieve the text message completely and without losing any data, so that MSE between the original message and the decrypted message is zero[30]. [31].

**Private(secret) key selection**

Data security [35], [36] in the encryption method depends entirely on the private key used in the encryption_decryption process, and the larger its size, the more difficult it is to find out this key by intruders[30], [31].

Most of the standard coding methods (based on DES and AES standards) use private keys of a specified length (for example, 256 bits) and these methods have drawbacks, the most important of which are[32], [33], [34]:

- The size of the private key is relatively small, which makes it possible to hack it.
- Most standard encryption methods need time to generate the available or private keys.
- Most of the standard methods require splitting a text message into a group of blocks, where the blocks are first encrypted and then the encrypted message is re-checked from the group of encrypted blocks, which increases the encryption time.

And to avoid the previous problems [35], [36], we suggest using a digital color phase that can be used as a master key, taking into account the following important things:

- The size of the digital color image used as a private key is large so that we can encrypt small and big color images.
- An agreement is made between the sender and the receiver on the digital image and each of them will preserve it.
- The digital image(private key) is not posted on social media.
- Agreeing to use part of the image to encrypt any color image.
- The possibility of replacing the digital image with another image if necessary.
- The large size of the image and not knowing it at all will make the process of hacking the private key impossible.

Color digital images [1], [2], [3] are one of the most common types of data circulating through social media and are considered one of the most used types of data in many vital and important applications for several reasons, the most important of which are [4], [5], [6]:

- ✓ Easy to obtain and without the lowest cost.[17].

iJETRM
International Journal of Engineering Technology Research & Management

- ✓ Ease of processing.[18], [19]
- ✓ The digital image provides an enormous volume of data that can be used for multiple purposes.

Digital color image is usually reperesented by a 3D matrix, 2D matrix for each color(red, green and blue colors)[7], [8], these matices provide a huge data source which can be used in variouus applivation such as speech encryption-decryption [9], [10] [11]], figure 2 shows an example of clor image and the associated histograms[12]:

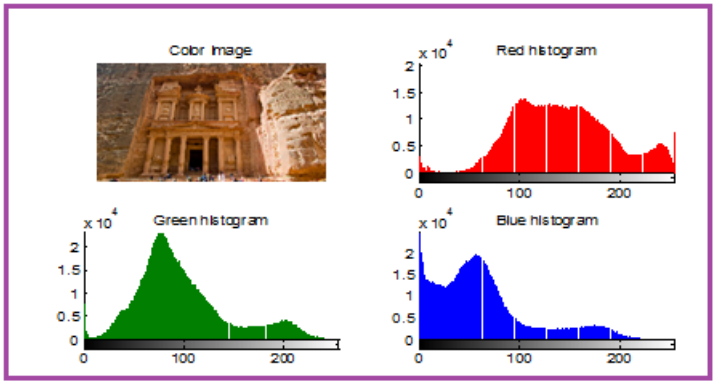


Figure 2: Huge color image(Private key) example and color histograms

The intensity of each color in RGB color image is within the range 0 to 255 [22], these values are not suitable for the proposed here method of encryption-decryption, so we need to convert the images from RGB color images to YIQ images, these images will have the intensity range within 0 and 1 [13], [14], [15] as shown in figure 3:

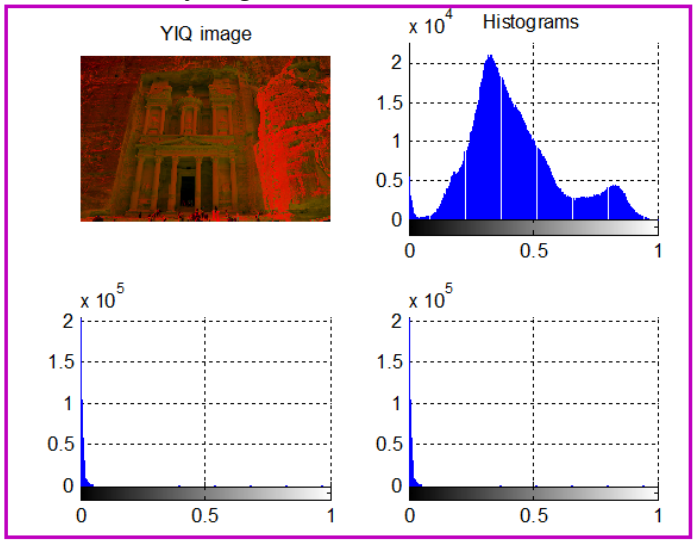


Figure 3: YIQ image

**The proposed method of image encryption_decryption**

The proposed method achieves a high level of data security and protection through the use of a large-sized[16], [17], colored digital image, which makes it difficult to detect because it is not sent, and this in turn eliminates the idea of generating the secret key in traditional methods, which increases the speed of encryption and decryption. In addition, the image to be encrypted, regardless of its size, is encrypted in one go, and this in turn leads to raising the efficiency of the method by reducing the time required for encryption and decryption.

The proposed method can be used to treat images with variable size starting from small images and ending with images with size equal the used color image as a private key, here we can select a part from the image key with size equal image size and apply adding .

The proposed method for encryption as shown in figure 4 can be implemented applying the following steps.

iJETRM
International Journal of Engineering Technology Research & Management

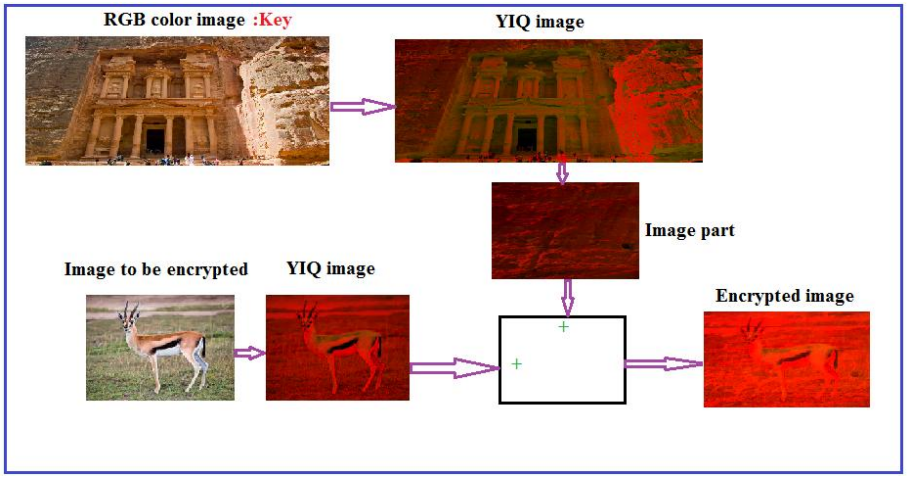


Figure 4: Encryption process diagram

1) Initial Step:

This step will be processed one time( every time we select an image as a private key), here the sender and reciever must agree on the image to be used as a private key for encryption-decryption, convert the image key to YIQ image.

2) Get the image to be encrypted.
3) Covert the image to YIQ image
4) Retreive the image size.
5) Select a part from the image key with size equal the image(to be encrypted) size.
6) Add the selected part to the image to get the encrypted image.
7) Convert the encrypted image back to RGB image.

To increase MSE and to decrease PSNR betwwen the original image and the encrypted one we can select a secret connstant to be added with the image key part to YIQ image as shown in figure 5:

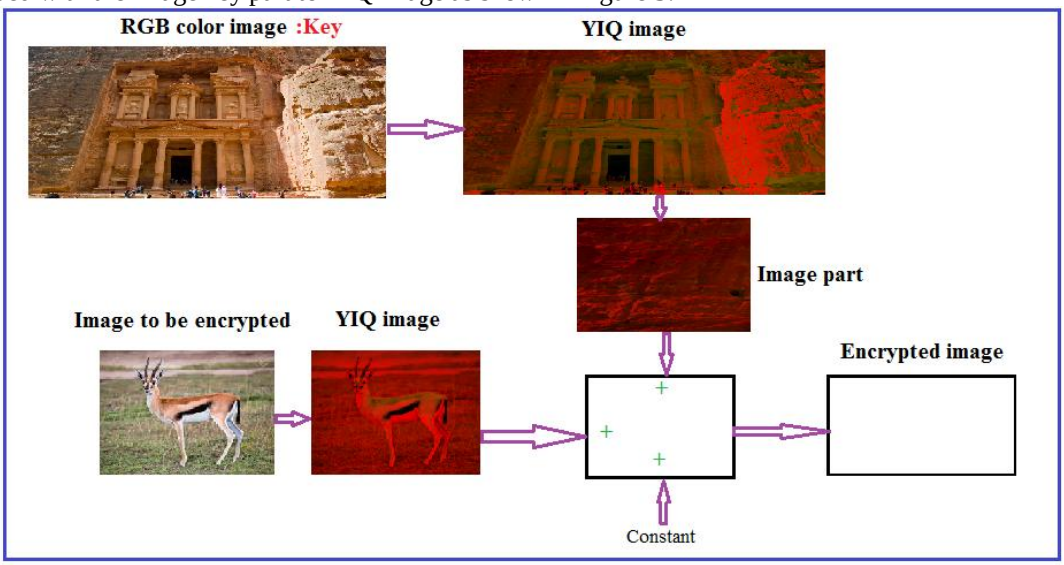


Figure 5: Encryption by adding a secret constant

The decryption process as shown in figure 6 will be implemented applying the following steps:

1) Get the image key.
2) Convert the image key to YIQ image.
3) Get the the encrypted image.
4) Convert the encrypted image to YIQ image.

iJETRM
International Journal of Engineering Technology Research & Management

5) Retreive the image size.
6) Select a part from the image key with size equal the image(to be encrypted) size.
7) Get the secrete constant.
8) Subtract the selected part and the constant from the encrypted image to get the decrypted one.
9) Convert the decrypted image back to RGB image.

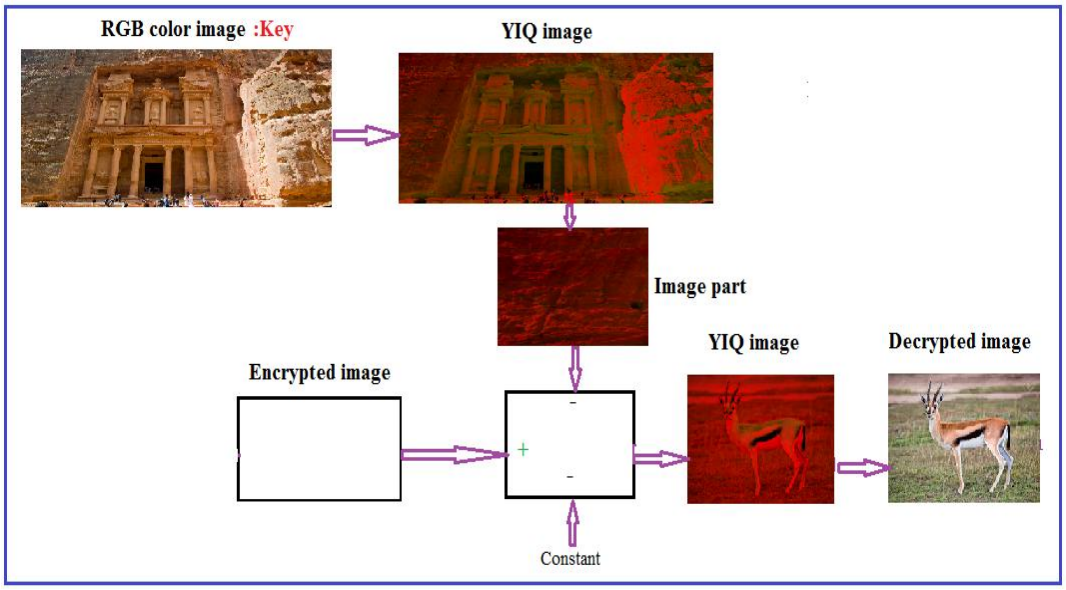


Figure 6: Decryption process diagram

**Implementation and experimental results**

Petra city (Jordainian city) image shown in figure 2 was selected to be used as a private key, the image size is 1071 * 1600* 3, which is equal 5140800 bytes, this image can be used to encrypt_decrypt images with sizes up to 5 M bytes.

The proposed method with the selected image key was implemented using deffirent images and without using the secret constant, figure 6 shows an image example, while table 1 shows the obtained experimental results:

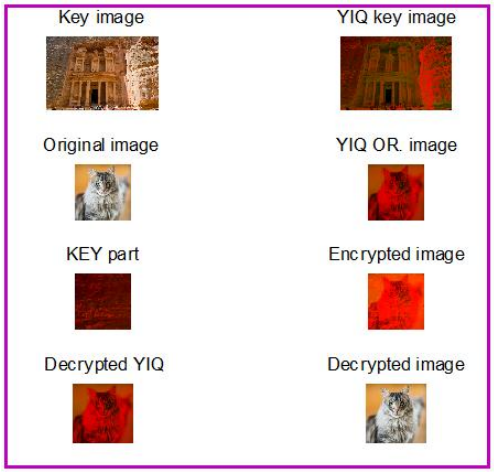


Figure 6: Implementation output sample

iJETRM
International Journal of Engineering Technology Research & Management

Table 1: Results of implementation withot using secret constant
Image key :Size=1071 *1600*3=5140800

| Image number | Size(byte) | Between original and encrypted | | Betrween original and decrypted | | |
|---|---|---|---|---|---|---|
| | | MSE | PSNR | MSE | PSNR | Encryprtion-decryption time(seconds) |
| 1 | 151875 | 0.0443 | 41.7115 | 0 | Inf | 0.014000 |
| 2 | 150738 | 0.0449 | 38.7655 | 0 | Inf | 0.014000 |
| 3 | 151050 | 0.0450 | 42.3375 | 0 | Inf | 0.014000 |
| 4 | 150750 | 0.0446 | 40.6817 | 0 | Inf | 0.014000 |
| 5 | 150975 | 0.0437 | 40.5875 | 0 | Inf | 0.013000 |
| 6 | 151680 | 0.0427 | 40.8994 | 0 | Inf | 0.015000 |
| 7 | 151515 | 0.0453 | 41.9991 | 0 | Inf | 0.014000 |
| 8 | 150975 | 0.0453 | 39.3903 | 0 | Inf | 0.014000 |
| 9 | 151218 | 0.0452 | 40.7869 | 0 | Inf | 0.014000 |
| 10 | 151008 | 0.0453 | 42.6509 | 0 | Inf | 0.015000 |

To decrease PSNR and to increase MSE between the original image and the encrypted one we can use a secret contanat to be addedd when encrypting and subtracted when decrypting, figure 7 shows an ouput implementation, while table 2 shows the obtsined experimental results:

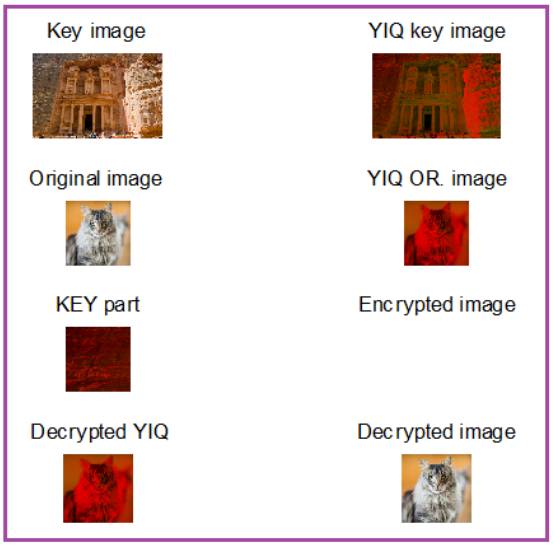


Figure 7: Sample output using secret constant

iJETRM
International Journal of Engineering Technology Research & Management

Table 2: Results of implementation using secret constant=5
Image key :Size=1071 *1600*3=5140800

| Image number | Size(byte) | Between original and encrypted | | Betrween original and decrypted | | |
|---|---|---|---|---|---|---|
| | | MSE | PSNR | MSE | PSNR | Encryprtion-decryption time(seconds) |
| 1 | 151875 | 26.3461 | 5.3122 | 0 | Inf | 0.014000 |
| 2 | 150738 | 26.3614 | 4.6304 | 0 | Inf | 0.014000 |
| 3 | 151050 | 26.3659 | 5.5057 | 0 | Inf | 0.014000 |
| 4 | 150750 | 26.3539 | 5.0704 | 0 | Inf | 0.014000 |
| 5 | 150975 | 26.3342 | 5.0064 | 0 | Inf | 0.013000 |
| 6 | 151680 | 26.3448 | 5.0198 | 0 | Inf | 0.015000 |
| 7 | 151515 | 26.3750 | 5.4304 | 0 | Inf | 0.014000 |
| 8 | 150975 | 26.3772 | 4.7914 | 0 | Inf | 0.014000 |
| 9 | 151218 | 26.3732 | 5.1230 | 0 | Inf | 0.014000 |
| 10 | 151008 | 26.3818 | 5.6009 | 0 | Inf | 0.015000 |

Defferent images with defferent ranges of sizes were used by the propoposed method, table 3 shows the the obtained experimental results using secret constant with value equal 1.5:
From table 3 we can see that the values of MSE and PSNR are good, and the proposed method meets the requirments of destruction the original imgae when encrypting and fully recovering the image when decrypting.

Table 3 : Results of encryption_decryption various images :K=1.5

| Image number | Size(byte) | Between original and encrypted | | Betrween original and decrypted | | |
|---|---|---|---|---|---|---|
| | | MSE | PSNR | MSE | PSNR | Encryprtion-decryption time(seconds) |
| 1 | 3686400 | 2.8629 | 13.7429 | 0 | Inf | 0.120000 |
| 2 | 3686400 | 2.8629 | 13.1417 | 0 | Inf | 0.119000 |
| 3 | 150849 | 2.6767 | 13.6905 | 0 | Inf | 0.013000 |
| 4 | 77976 | 2.6628 | 14.0842 | 0 | Inf | 0.012000 |
| 5 | 518400 | 2.7102 | 13.4645 | 0 | Inf | 0.026000 |
| 6 | 4326210 | 2.8904 | 12.9727 | 0 | Inf | 0.139000 |
| 7 | 122265 | 2.6815 | 12.6475 | 0 | Inf | 0.013000 |
| 8 | 518400 | 2.7102 | 13.5090 | 0 | Inf | 0.025000 |
| 9 | 150975 | 2.6949 | 13.9187 | 0 | Inf | 0.015000 |
| 10 | 150975 | 2.6949 | 13.4247 | 0 | Inf | 0.014000 |

An image with size equal 4326210 byte was selected and encrypted_decrypted using various values of secret constant, table 4 shows the obtained experimental results:

Table 4: Encrypting_decrypting an image using various values of the secret consant

| k | MSE | PSNR |
|---|---|---|
| 1 | 1.4529 | 16.5124 |
| 1.5 | 2.8904 | 12.9727 |
| 5 | 26.9530 | 5.2565 |
| 10 | 103.8282 | 2.8535 |
| 20 | 407.5785 | 1.4920 |
| 30 | 911.3287 | 1.0102 |
| 50 | 2518.8 | 0.6139 |
| 75 | 5653.2 | 0.4119 |
| 80 | 6430.1 | 0.3864 |
| 100 | 10038 | 0.3099 |

iJETRM
International Journal of Engineering Technology Research & Management

From table 4 we can see that increasing the value of the secret constant will decrease the value of PSNR between the original image and the encrypted one, at the same time it will increase the MSE value between the two images, figure 8 shows the relationship between the constant value and MSE, while figure 9 shows the relationship between the constant value and PSNR.

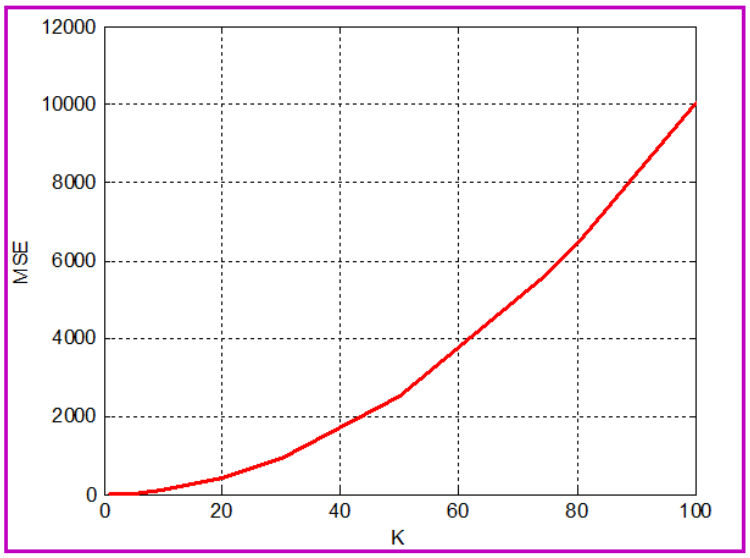


Figure 8: MSE and the secret constant

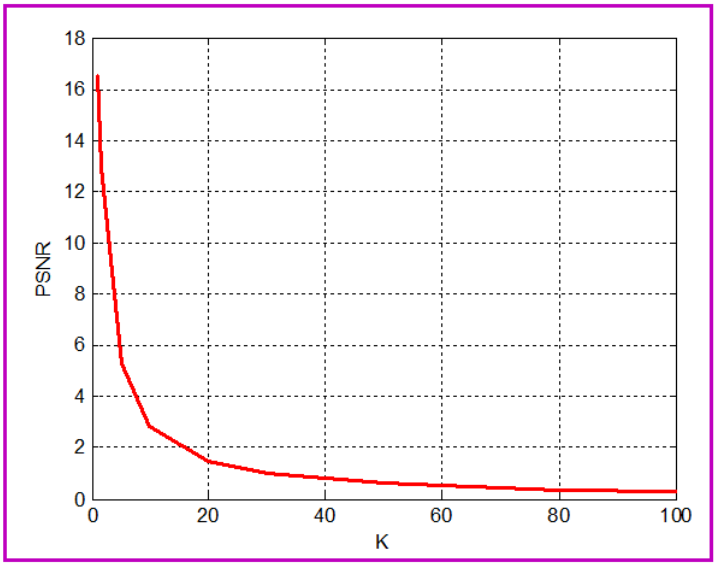


Figure 9: PSNR and the secret constan

**Conclusion**

A simple and highly secure method of color image encryption-decryption was proposed, tested and implemented. The obtained experimental results showed that the proposed method is efficient, requiring small time for encryption_decryption, very secure by using large color image and constant as a private keys. The private secret constant was used to apply fully distrction of the encrypted image making it un understandable by decresing PSNR and increasing MSE between the original image and the encrypted one.

The proposed method is very flixible and we can change the image key and the constant value any time we want by making an agreement between the sendedr and the reciever.

iJETRM
International Journal of Engineering Technology Research & Management

**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 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.*

iJETRM
International Journal of Engineering Technology Research & Management

*[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 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.*

iJETRM
International Journal of Engineering Technology Research & Management

*[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.*