World Journal of Engineering Research and Technology

WJERT

www.wjert.org

Impact Factor Value: 5.924

COLOR IMAGE CRYPTOGRAPHY USING HUGE RANDOM PRIVATE KEY

Dr. Hatim Ghazi Zaini*[1] and Prof. Ziad AlQadi[2]

[1]Taif University, Computer and Information Technology College, KSA.

[2]Albalqa Applied University, Faculty of engineering technology, Jordan.

Article Received on 05/03/2021 **Article Revised on 25/03/2021** **Article Accepted on 15/04/2021**

***Corresponding Author**
Dr. Hatim Ghazi Zaini
Taif University, Computer and Information Technology College, KSA.

ABSTRACT

Image cryptography is a very needed process to protect the image from any third patry, and to protect the data imbeded in the image. In tis paper research we will introduce a method of image encryption decryption base on using a huge private key of ranadm numbers. The image is to devided into blocks with defined earlier size, these blocks are to be converted to YIQ to form the YIQ image, then thes blockis are to be encrypted using subkeys obtained from the private key. Various experemeint will done to chech the effeciency and accuaracy of the proposed method.

KEYWORDS: Cryptography, huge random private key, MSE, PSNR, protection, throughput.

INTRODUCTION

Color digital images.[1,2,3] are one of the most common and used types of digital data at the present time.[4,5] as this spread is due to several reasons, the most important of which are.[6,7,8]

- The spread of smart phones, which can be used easily to capture high-resolution images at a very low cost.[9,10]
- Ease of circulating digital images through various social media platforms.[11,12]
- The ability to use digital images by a large variety of users.[13,14]
- The large size of the digital image saves huge amounts of data.[15,16]
- The use of digital images in many vital and important applications for humans.[17,18]

Many applications that deal with digital images require the cryptography(encryption-decryption) process for several reasons, the most important of which are:

- The digital image may be confidential so that no unauthorized third party is allowed to view and understand it.[20]
- The digital image may be personal, which means that it is protected from disingenuous people.[21]
- The digital image may be carrying important private information.[41,42] or confidentiality, which requires protection from intruders for fear of being able to retrieve the information embeded in the digital image.[22,23]

To protect the digital image and the data contained in it, an encryption process.[24,25] can be used, the encryption process is used to completely destroy the original data so that it becomes incomprehensible or clear to any third party who is not authorized to the image or to the data included in the image.

The encryption and decryption process.[24,25,26] (see figure 1)is carried out using a private and secret key so that it is difficult to decipher or obtain it, as it is possible here to agree between the sender and the receiver on a secret large-sized and random key that does not need a generating process and is stored with them with the possibility of changing it if the need arises.[27,28]

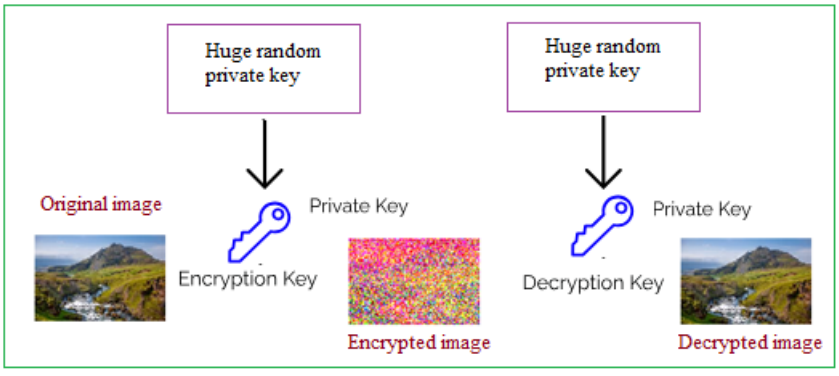

Figure 1: Image encryption-decryption process.

The encryption method is excellent if it fulfills the following characteristics.[29,30]

1. Ease of implementation and use.[31]
2. Provide a high degree of protection for the digital image, by using a secret key that is difficult to penetrate or knowing how to use it.

3. Providing a high degree of efficiency by reducing encryption time and increasing throughput by increasing the number of encrypted data per unit time.
4. Total destruction of data and that by maximizing the mean square error (MSE) between the original image and the encrypting one, or minimizing the peak signal to noise ratio (PSNR) between the original and the encrypted images.
5. Retrieving an image that is completely identical to the original image upon decryption, so that it MSE between the original image and decrypted one is equal to zero, or PSNR between the original and decrypted images is equal infint.[32-40]

Multiple methods are used for encrypting-decrypting digital images, some of which are based on world famous standards such as DES and AES, these methods are characterized by a moderate degree of protection in addition to their low effectiveness because they need to implement multiple processes to generate the secret key and generate encrypted data.

The proposed method of color image encryption-decryption

The proposed method provides a high level by using a huge random private key, this key can be generated once and saved by both the sender and reciever. The private key size must so big to suit any image needs encryption-decryption.

The encryption procces can as shown in figure 2 can be implemented applying the following steps:

Step1: Private key initialization: here we have to create a huge 3D matrix with random numbers, this key must be saved by the sender and reciever.

Step2: Image blocking, here we have to select the block size by selecting the number of rows and columns, these number must be kept also in secrete to increase the level of security.

Step3: Changing the obtained block from RGB to YIQ.

Step4: From the private key, get a subkey for each block.

Step5: Add each block to the associated subkey.

Step6: Combine the obtained by addition blocks to form the encrypted YIQ image.

Step7: Convert the encrypted YIQ image to RGB image to get the encrypted image.

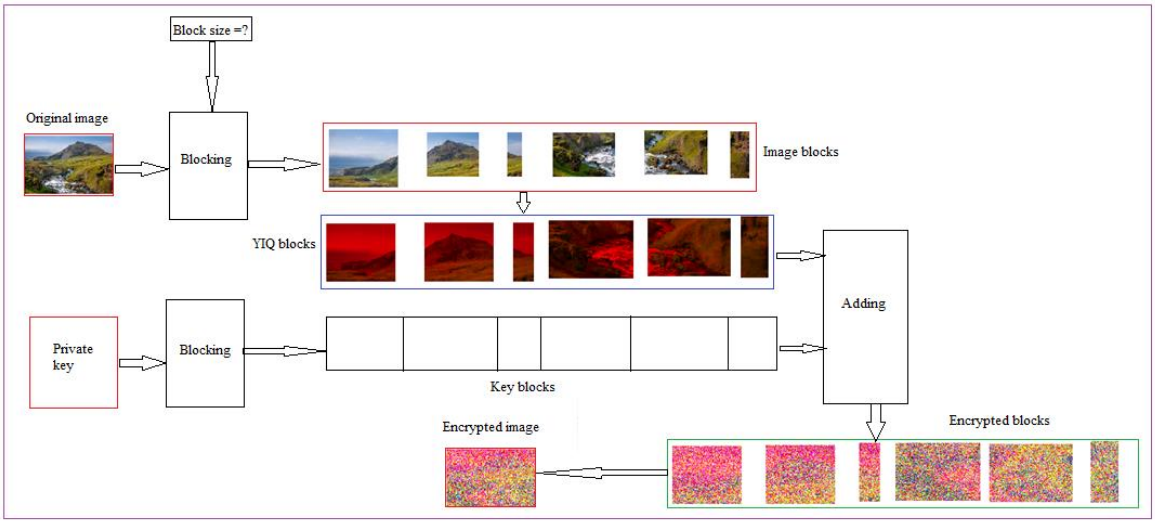

Figure 2: Encryption process.

The decryption process can be implemented applying the following steps:

Step1: Get the private key: here we have to load.

Step2: Image blocking, here we have to get the block size.

Step3: Changing the obtained block from RGB to YIQ.

Step4: From the private key, get a subkey for each block.

Step5: Subtract each subkey from the associated .

Step6: Combine the obtained by subtraction blocks to form the decrypted YIQ image.

Step7: Convert the decrypted YIQ image to RGB image to get the decrypted image.

Implementation and experimental results

For color image encryptiondecryption we created a random private key with size 2000x2000x3, this key was used to encrypt-decrypt the images used in our experiments.

Twelve color images with various sizes(small, mediume and large) were selected, then the encryption-decryption processes were applied using each of the selected images(block size was taken with the size 100x120x3), figure 3 shows the output obtained after blocking one image, figure 4 shows the resulting blocks after converting to YIQ, figure 5 shows the encrypted YIQ blocks, while figure 6 shows the original, encrypted and decrypted images:

Figure 3: Image blocking (example).

Figure 4: YIQ blocks.

Figure 5: Encrypted YIQ blocks.

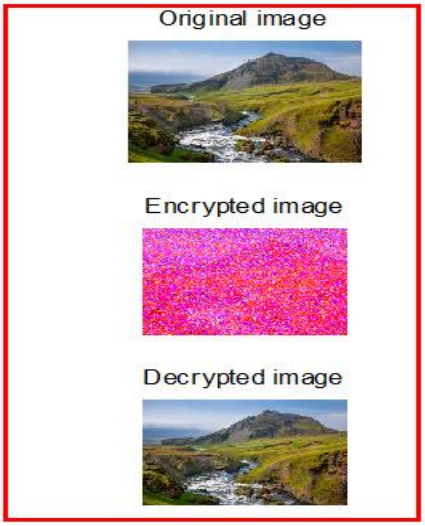

Figure 6: Original, encrypted and decrypted images.

Table 1 shows the obtained experimental results after encrypting each of the selected image:

Table 1: Encryption results.

Image number	Size(byte)	PSNR	MSE	Encryption time(seconds)
1	150975	15.6150	13644	0.0190
2	77976	20.8912	80499	0.0062
3	518400	14.4412	15343	0.0412
4	5140800	18.1608	10577	0.4086
5	4326210	18.3597	10369	0.3439
6	122265	18.1608	12837	0.0097
7	518400	14.3585	15470	0.0412
8	150975	16.1723	12904	0.0120
9	150975	16.7136	12224	0.0120
10	151353	14.6136	15081	0.0123
11	1890000	16.9553	11932	0.1502
12	6119256	20.2384	85929	0.4864
Average	1609800	17.0567	24734	0.1286
Throughput	1609800/0.1286= 12229 Kbytes per second			

Table 2 shows the experimental results after appllying decryption process:

Table 2: Decryption results.

Image number	Size(byte)	PSNR	MSE	Encryption time(seconds)
1	150975	Infinit	0	0.0190
2	77976	Infinit	0	0.0062
3	518400	Infinit	0	0.0412
4	5140800	Infinit	0	0.4086
5	4326210	Infinit	0	0.3439
6	122265	Infinit	0	0.0097
7	518400	Infinit	0	0.0412
8	150975	Infinit	0	0.0120

9	150975	Infinit	0	0.0120
10	151353	Infinit	0	0.0123
11	1890000	Infinit	0	0.1502
12	6119256	Infinit	0	0.4864
Average	1609800	Infinit	0	0.1286
Throughput	1609800/0.1286= 12229 Kbytes per second			

From the results shown in tables 1 and 2 we can raise the following facts:

1. The proposed method is very secure, becuese the used private key is very huge and it can not be guessed by any third party, this key will not be transmitted and it will be kept by the sender and reciever, also the block size is to be kept in secret, this will increase the level of security.
2. The proposed method totally destryed the original image when encrypting by maximizing MSE and minimizing PSNR.
3. The proposed method totally Recover the original image without lossing any information, here the MSE always zero and PSNR always infinit.
4. The proposed method provides a high level of effeciency needing a small time for encryption and decryption processes, here the average throughput will be high and it is better than DES and AES results as shown in table 3:

Table 3: Comparisons with DES and AES methods.

Color image size(KB)	**Encryption time(second)**		
	DES	**AES**	**Proposed**
15	3.8	5.07	0.0012
30	7.5	17.09	0.0025
45	8.5	19.96	0.0037
60	8.8	22.91	0.0049
75	9.33	29.99	0.0061
90	10.7	38.15	0.0074
Average time	**8.1050**	**22.1950**	**0.0043**
Throughput(KB./second)	52.500/8.105=**6.4775**	52.5000/22.195=**2.3654**	52.5000/**0.0043**=**12209**
Speedup of proposed	8.9210/**0.0043**=**20747**	**22.1950**/**0.0043**=**5161.6**	**1**

CONCLUSION

A simple and easy to implement method of color image cryptography was introduced, the method was implemented using various in sizes color images. The obtained experimental results showed that the proposed method provides a high level of secuurity to protect the image by using a huge private key with random numbers. The proposed mothod provides an efficient way of color image encryoption decryption and satisfies the requirement of good method of cryptography.

REFERENCES

1. Majed O Al-Dwairi, Ziad A Alqadi, Amjad A Abujazar, Rushdi Abu Zneit, Optimized true-color image processing, World Applied Sciences Journal, 2010; 8(10): 1175-1182.
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, 2016; 153(2): 31-34.
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, 2016; 5(11): 21-28.
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, 2016; 5(11): 29-36.
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, 2020; 9(2): 21 –37.
7. Aws AlQaisi, Mokhled AlTarawneh, Ziad A. Alqadi, Ahmad A. Sharadqah, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, 2019; 17(3): 1220-1225.
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, 2019; 8(8): 50-56.
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, 2020; 9(2): 2319.
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, 2017; 6(2): 60-66.
11. Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, 2019; 14(1): 2203-2207.

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, 2019; 8(8): 50-56.
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, 2020l 4(1): 66-75.
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, 2020; 4(2): 48-55.
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), 2019; 9(5): 4092-4098.
16. Ziad Alqadi, 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, 2019; 8(8): 30-48.
17. Ayman Al-Rawashdeh, Ziad Al-Qadi, Using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, 2018; 8(4): 1356-1359.
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, 2018; 8(5): 2780-2787.
19. Jihad Nader Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, 2019; 1(4): 49-55.
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, 2019; 8(3): 76-90.
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, 2019; 5(3): 82-87.
22. Musbah Aqel Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences, 2009; 6(1): 45-52.
23. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, International Journal of Computer and Information Technology, 2016; 5(5): 465-470.

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, 2018; 7(3): 104-107.
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, 2019; 8(6): 3228-3235.
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, 2019; 9(3): 4165-4168.
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, 2019; 11(1): 232-238.
28. Ziad A AlQadi, Accurate Method for RGB Image Encryption, International Journal of Computer Science and Mobile Computing, 2020; 9(1): 12-21.
29. Ziad Alqadi, 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, 2019; 8(9): 30-48.
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, 2019; 3(3): 262-265.
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), 2020; 6(5): 6-12.
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, 2019; 9(1): 3681-3684.
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), 2016; 8(5): 125-131.
34. Prof. Ziad a. Alqadi, a simple method to encrypt-decrypt speech signal, International Journal of Engineering Technology Research & Management, 2021; 5(2): 44-52.

35. Ziad ALQadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, 2007; 2(4): 288-298.
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, 2019; 8(3): 14-26.
37. Musbah Aqel, Ziad A. Alqadi, Performance analysis of parallel matrix multiplication algorithms used in image processing, World Applied Sciences Journal, 2009; 6(1): 45-52.
38. Amjad Y Hindi, Majed O Dwairi, Ziad A AlQadi, A Novel Technique for Data Steganography, Engineering, Technology & Applied Science Research, 2019; 9(6): 4942-4945.
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), 2019; 9(5): 4092-4098.
40. Bilal Zahran Belal Ayyoub, Jihad Nader, Ziad Al-Qadi, Suggested Method to Create Color Image Features Victor, Journal of Engineering and Applied Sciences, 2019; 14(1): 2203-2207.
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, 2009; 5(5): 355-362.
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, 2019; 8(6): 106-123.