International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Fast and Secure Color Image Cryptography

Dr. Mohamad Tariq Barakat[1], Prof. Ziad A. Alqadi[2]
[1,2]Albalqa Applied University, Jordan
Faculty of Engineering Technology
Electrical Engineering Department
Amman, P.O.BOX 1008

Abstract— *Colored digital images are used in many vital and important applications. The digital image may be of a special nature or confidentiality, or it may be a medium that carries confidential and private data, which makes the process of protecting the image from intruders a very important process. The huge image size requires a lot of time to encrypt and decrypt it using classic and standards-based methods. In this paper research we will introduce a simple and easy to implement method of color image cryptography, the proposed method will be compared with other standard methods of data cryptography to show the improvements provided by this method. The proposed method will use a secret private key which will be extracted from a secret image_key, this image key will capable to encrypt decrypt any image with any size.*

Keywords— *Image_key, cryptography, encryption time, decryption time, MSE, PSNR, throughput, speedup.*

I. INTRODUCTION

The colored digital image [13-18] is one of the most widespread types of digital data and circulated through various social media, as it is used in many vital and important applications that sometimes require protection from intruders and data thieves for various reasons, the most important of which are:

- The digital photo may be confidential.
- The digital image may be personal.
- The digital image may be a medium containing confidential data.

Digital color image [19-25] as shown in figure 1 contains 3 2D matrices, one 2 D matrix for each color (red, green and blue), each matrix can be treated separately or with combination with other matrices, each color value ranges from 0 to 255, and the total pixel color is a mixed of the three colors values as shown in figure 2.

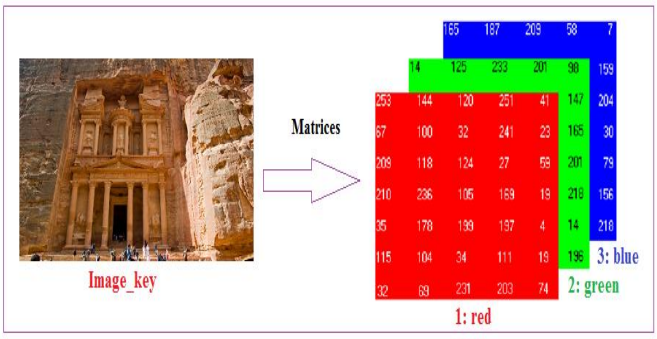

Fig. 1. Color image matrices

Color image can be represented by a histogram, which points to the repetition of each intensity in the image as show in figure 3. From the histogram we can see the huge repetition of each value, this mean that color image has a huge size which can be deployed in image encryption-decryption.

Color	Red Value	Green Value	Blue Value
True Black	0	0	0
True White	255	255	255
True Red	255	0	0
True Green	0	255	0
True Yellow	255	255	0

Fig. 2. Mixing colors to form the pixel color

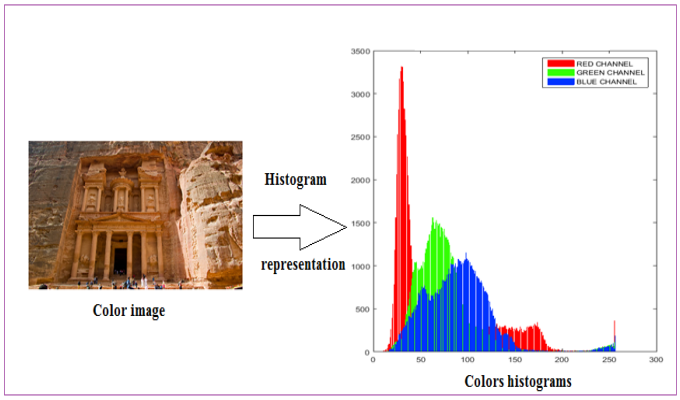

Fig. 3. Color image histograms

Many operations are implemented on the digital image, and what concerns us here is the possibility of modifying the image in order to fit it with another image. The re-size operation can be implemented either by reducing the dimensions of the image or expanding its dimensions, as shown in the figures 4 and 5 [26-33].

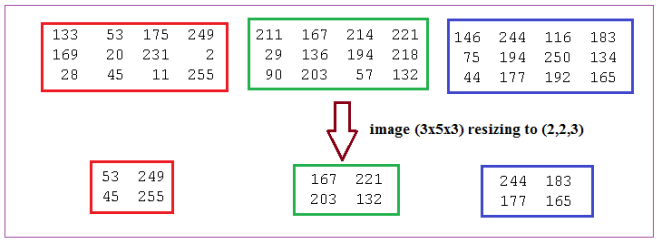

Fig. 4. Image resizing, reducing the image size

Dr. Mohamad Tariq Barakat and Prof. Ziad A. Alqadi, "Fast and Secure Color Image Cryptography," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 4, pp. 171-177, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

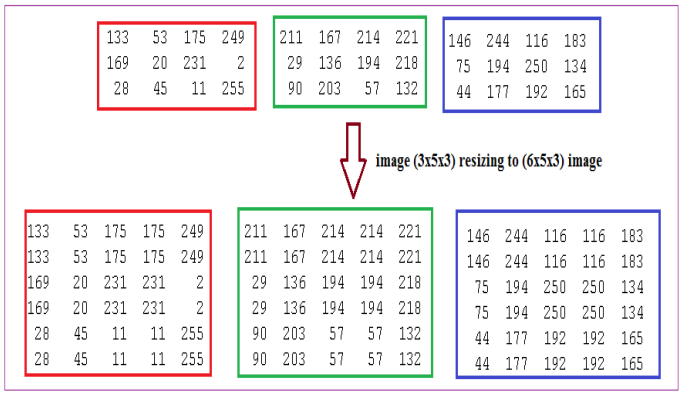

Fig. 5. Image resizing, expanding the image size

Many of the images circulating through various social media require protection due to the importance of the image, its privacy, or the fact that it bears confidential data. To protect the image one of the data cryptography method will be needed. The selected method must be secure, simple and efficient. Image symmetric cryptography (see figure 6) means image encryption and decryption using the same secret private key (PK). Encryption must destroy the original data and make it unuseful for any third party, while decryption means recovery of the original image without losing any piece of information, the degree of destruction can be measured by MSE (mean squire error) or PSNR (peak signal to noise ratio), here MSE must be very high and/or PSNR must be very low. Decryption phase must recover the original image, and here MSE between the original and decrypted image must be equal zero and PSNR value must equal infinite.

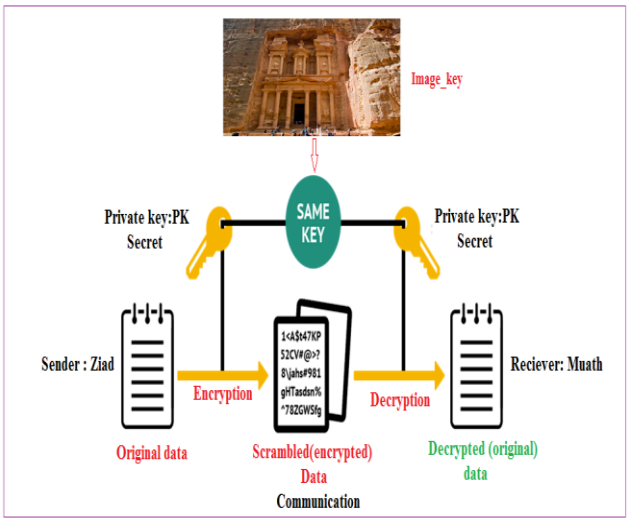

Fig. 6. Symmetric data cryptography

II. RELATED WORKS

Many methods of data cryptography were developed based on data cryptography standards such as DES [1-4] (data encryption standard, AES [5-8] (advance encryption standard), triple DES (3DES) and Blowfish (BF) [9-12], these methods provide good quality parameters but the efficiency will dropped down when the data size increases (so for image cryptography they require much time to apply encryption and decryption, the main characteristics of these methods are listed in table I.

TABLE I. Characteristics of data cryptography standard methods

Factor	DES	3DES	AES	BF
Image cryptography	Bad	Bad	Bad	Bad
Encryption quality	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR
Decryption quality	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR
Efficiency	Moderate	Slow	Moderate	High
Attack	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack
Structure	Feistel	Feistel	Substitution-Permutation	Feistel
Block cipher	Binary	Binary	Binary	Binary
PK length(bit)	56	112, 168	128, 192, 256	32-448
Block size(bit)	64	64	128	64
Rounds	16	48	10,12,14	16
Flexibility to modification	no	yes	yes	yes
Simplicity	no	no	no	no
Security level	Adequate	Adequate	Excellent	Excellent
Throughput	Low	low	Low	Moderate

Figures 7, 8, 9 and 10 summarize the operations of these methods:

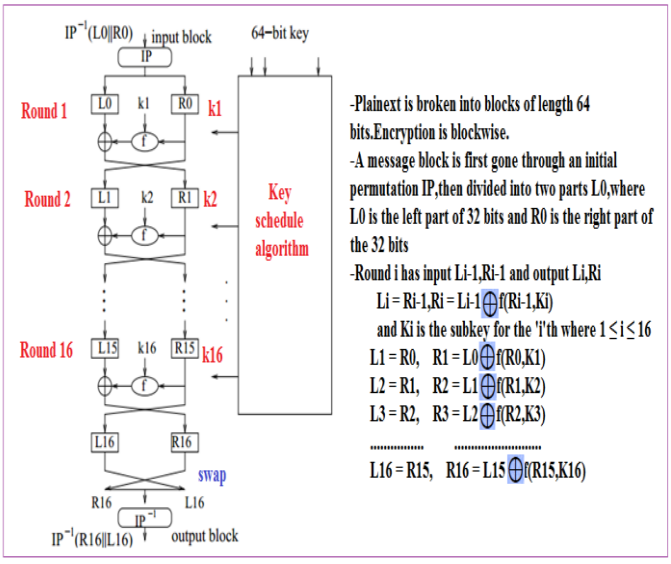

Fig. 7. DES data encryption

The 3DES is a triple DES method by expanding the private key to 3 keys as shown in figure 8.

Dr. Mohamad Tariq Barakat and Prof. Ziad A. Alqadi, "Fast and Secure Color Image Cryptography," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 4, pp. 171-177, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

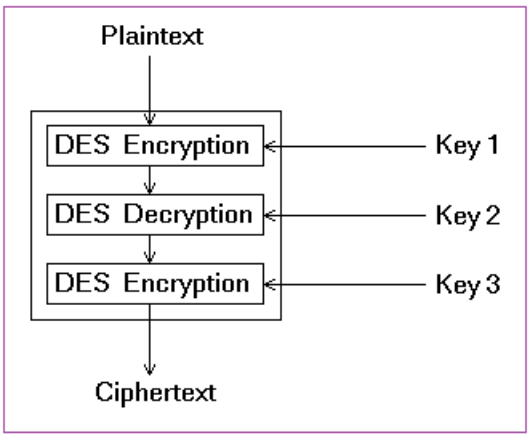

Fig. 8. 3DES data encryption

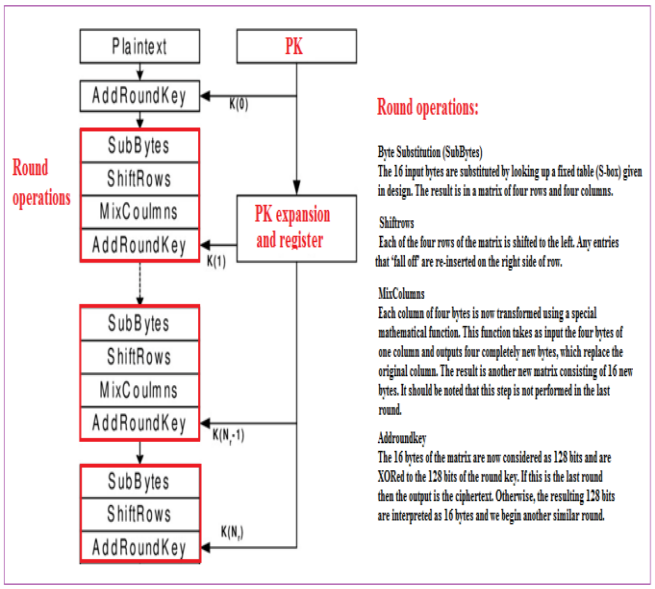

Fig. 9. AES data encryption

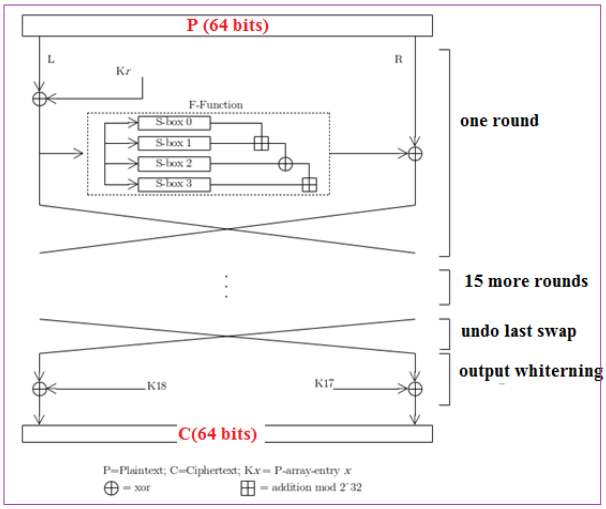

Fig. 10. B data encryption

III. The Proposed Method

The proposed method is based on the use of a colored image (image_key) that is used as a secret key to generate the required private key. The image used by the sender and receiver and is agreed upon, and both of them keep this image without the need to communicate with it with the possibility of changing it from time to time and if necessary. The color image is to be resized to match the PK size. The private key size depends on the image to be encrypted size.

The process of data encryption can be implemented apply the following steps (as shown in figure 11):

1) *Get the image_key.*
2) *Get the image to be encrypted.*
3) *Get the size of the image to be encrypted.*
4) *Resize the image_key to match the size of the image to be encrypted.*
5) *Apply XORing to get the encrypted image.*

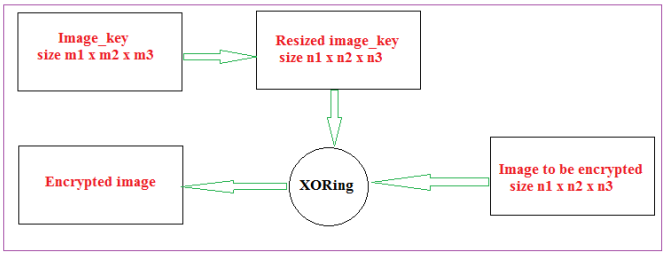

Fig. 11. Encryption phase

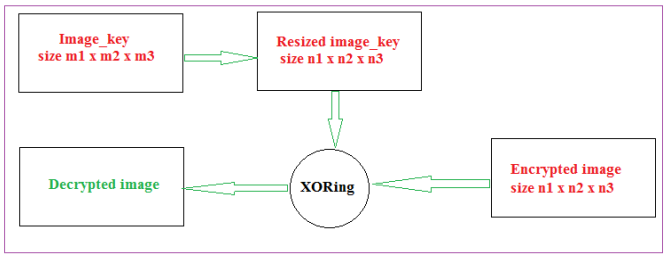

Fig. 12. Decryption phase

The decryption process can be implemented in using the same sequence as shown in figure 12.

IV. Implementation and Experimental Resulys

The selected image_key can be used to encrypt-decrypt any other color image with any size, the image to be encrypted may be too small or big, or even bigger than the image_key, figure 13 shows an encryption-decryption example using small image, while figure 14 shows the result of encryption decryption using bigger image.

A high resolution image with size equal 5140800 was selected as image_key various images were selected and encrypted-decrypted using this image_key, table II shows the obtained experimental results.

Dr. Mohamad Tariq Barakat and Prof. Ziad A. Alqadi, "Fast and Secure Color Image Cryptography," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 4, pp. 171-177, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

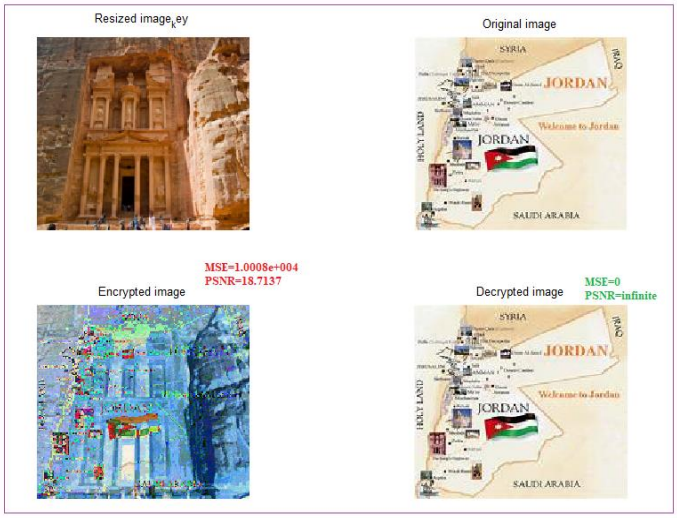

Fig. 13. Small image encryption-decryption

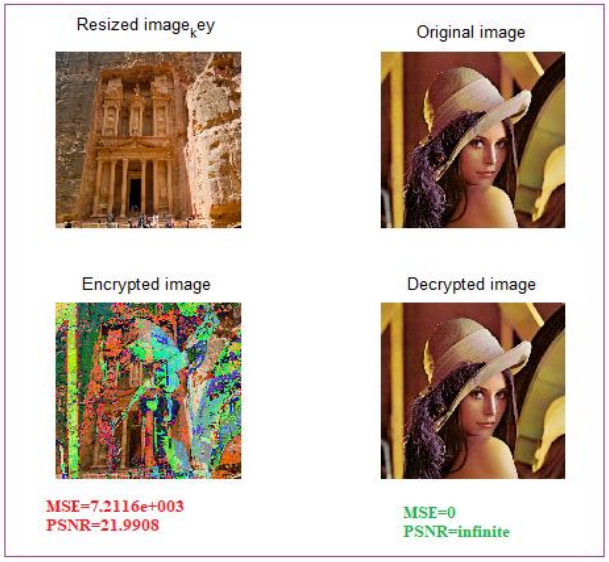

Fig. 14. Bigger image encryption-decryption

TABLE II. Results of using huge image as an image_key

Image #	Image size(byte)	Encryption time(second)	MSE	PSNR
1	77976	0.055973	1.0008e+004	18.7137
2	150849	0.099893	8.1247e+003	20.7986
3	518400	0.110946	8.0777e+003	20.8566
4	4326210	0.192905	7.1780e+003	22.0376
5	122265	0.092803	7.2320e+003	21.9626
6	518400	0.109314	8.3555e+003	20.5186
7	150975	0.099397	7.7658e+003	21.2504
8	150975	0.099315	6.4303e+003	23.1376
9	151353	0.097427	7.8722e+003	21.1143
10	1890000	0.165109	7.6080e+003	21.4557
11	6119256	0.206395	6.5885e+003	22.8944
12	786432	0.119257	7.2116e+003	21.9908
Average	1246900	0.1207		
Throughput (bytes per second)	1.0331e+007			
Throughput (K bytes per second)	10089			

A smaller image with size equal 122265 bytes was selected as an image_key, figures 15 and 16 show an examples of image cryptography using this image_key:

Fig. 15. Image cryptography using smaller image_key

Fig. 16. Image cryptography using the same image as image_key

The same selected images were encrypted-decrypted using the small in size image_key; table III shows the obtained experimental results.

A matlab codes were written to implement DES, 3DES, AES and BF methods of data cryptography, table IV shows the obtained experimental results:

Dr. Mohamad Tariq Barakat and Prof. Ziad A. Alqadi, "Fast and Secure Color Image Cryptography," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 4, pp. 171-177, 2021.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

TABLE III. Results of using small image as an image_key

Image #	Image size(byte)	Encryption time(second)	MSE	PSNR
1	77976	0.038574	8.7878e+003	20.0141
2	150849	0.040915	8.9071e+003	19.8793
3	518400	0.079122	7.7683e+003	21.2472
4	4326210	0.150762	7.7725e+003	21.2418
5	122265	0.025941	1.3296e+004	15.8734
6	518400	0.047414	9.1479e+003	19.6125
7	150975	0.039620	8.2761e+003	20.6139
8	150975	0.039382	7.8511e+003	21.1412
9	151353	0.039410	8.8615e+003	19.9306
10	1890000	0.063047	7.9658e+003	20.9961
11	6119256	0.130704	7.4175e+003	21.7093
12	786432	0.050957	7.9395e+003	21.0292
Average	1246900	0.0622		
Throughput(bytes per second)	2.0047e+007			
Throughput(K bytes per second)	19577			

TABLE IV. Standard methods results

Image #	Image size(byte)	Encryption time(second)			
		DES	3DES	AES	Blowfish
1	77976	0.394340	0.630944	0.299154	0.1306995
2	150849	0.762873	1.220597	0.578731	0.2528456
3	518400	2.621651	4.194642	1.988839	0.8689163
4	4326210	21.878503	35.005605	16.597485	7.2513786
5	122265	0.6183183	0.989309	0.469069	0.2049345
6	518400	2.6216517	4.19464	1.988839	0.86891636
7	150975	0.7635105	1.221616	0.579214	0.25305680
8	150975	0.76351056	1.221616	0.579214	0.2530568
9	151353	0.76542218	1.224675	0.580665	0.2536903
10	1890000	9.558105468	15.292968	7.250976	3.1679242
11	6119256	30.9462932	49.514069	23.476498	10.256793
12	786432	3.9771428	6.36342	3.017142	1.318178
Average	1246900	6.3059	10.0895	4.7838	2.0900
Throughput(bytes per second)		197740	123580	260650	596600
Throughput(K bytes per second)		193.1055	120.6836	254.5410	582.6172

V. RESULTS ANALYSIS

From the obtained results (table II and III) we can see that the proposed method satisfies the quality requirements by providing excellent values for MSE and PSNR. Using smaller image as an image_key will decrease the encryption-decryption times making the method more efficient by increasing the data cryptography process throughput. The proposed method provides a high security level and excellent protection of the secret message, because the PK is so huge and impossible to guess.

The proposed method efficiency can be compared with the results of standard methods of data cryptography, and from table IV we can see that the proposed method provide a significant big speedup, thus it will rapidly increases the method throughput as show in table V:

TABLE V. Speedup calculation

Method	DES	3DES	AES	BF	Proposed
DES	1.0000	1.6001	0.7586	0.3314	0.0099
3DES	0.6250	1.0000	0.4741	0.2071	0.0062
AES	1.3181	2.1092	1.0000	0.4369	0.0130
BF	3.0171	4.8276	2.2889	1.0000	0.0298
Proposed	**101.3798**	**162.2176**	**76.9110**	**33.6018**	1.0000

The proposed method adds a good improvement to the process of color image cryptography, these improvements are listed in table VI (green colored):

TABLE VI. Improvements provided by the proposed method

Factor	DES	3DES	AES	BF	Proposed
Image cryptography	Bad	Bad	Bad	Bad	Excellent
Encryption quality	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR	Excellent: High MSE and low PSNR
Decryption quality	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR	Excellent: Zero MSE and infinite PSNR
Efficiency	Moderate	Slow	Moderate	High	Excellent
Attack	Brute force attack	Brute force attack, Known plaintext, Chosen plaintext	Side channel attack	Dictionary attack	Impossible
Structure	Feistel	Feistel	Substitution-Permutation	Feistel	XORing

Dr. Mohamad Tariq Barakat and Prof. Ziad A. Alqadi, "Fast and Secure Color Image Cryptography," *International Research Journal of Advanced Engineering and Science*, Volume 6, Issue 4, pp. 171-177, 2021.

Block cipher	Binary	Binary	Binary	Binary	Decimal
PK length(bit)	56	112, 168	128, 192, 256	32-448	Variable
Block size(bit)	64	64	128	64	Image size
Rounds	16	48	10,12,14	16	1
Flexibility to modification	no	yes	yes	yes	yes
Simplicity	no	no	no	no	Yes
Security level	Adequate	Adequate	Very good	Very good	Excellent
Throughput	Low	low	Low	Moderate	Excellent

VI. CONCLUSION

A secure method of secret color image cryptography was introduced, implemented and investigated. The proposed method used a huge color image as complex PK key, this key will be kept in secret making the process of guessing or hacking impossible, thus making the secret image secure and protected. Other parameters of the method were studied and analyzed; it was shown that the proposed method provides a good quality of encryption-decryption by giving good values for MSE and PSNR. The proposed method is very efficient, it rapidly increases the throughput of cryptography and it has a significant big speedup comparing with other standard methods of data cryptography.

REFERENCES

[1] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", *IJCSNS International Journal of Computer Science and Network Security*, VOL.8 No.12, pp. 280-286, December 2008.

[2] W. Stallings, Cryptography and Network Security, 4th Edition, Pearson Prentice Hall, 2006.

[3] Singh S Preet, Mani Raman, "Comparison of Data Encryption Algorithms", *International Journal of Computer science and Communications*, Vol. 2, No.1, January-June 2011, pp. 125-127.

[4] Singh Gurjeevan, Kumar Ashwani, Sandha K.S. "A Study of New Trends in Blowfish Algorithm" *International Journal of Engineering Research and Applications (IJERA)*, Vol. 1, Issue 2, pp.321-326.

[5] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", *International Journal on Computer Science and Engineering (IJCSE)*, Vol. 4 No. 05 May 2012, pp. 877-882.

[6] Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", *International Journal of Computer Science and Technology*, vol. 2, Issue 2, June 2011, pp. 292-294.

[7] Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" *IJARCSSE*, volume 2, Issue 9, September 2012, pp. 196-201.

[8] Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", *IJAIEM*, vol. 2, Issue 7, July 2013, pp. 204-206.

[9] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", *Communications of the IBIMA*, Volume 8, 2009, pp. 58-64.

[10] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", *Communications of the IBIMA*, Volume 8, 2009, pp. 58-64.

[11] Thakur Jawahar, Kumar Nagesh. "DES, AES and Blowfish Symmetric Key Cryptography algorithm Simulation Based Performance Analysis", *IJETAE*, vol. 1, Issue 2, DEC. 2011, pp. 6-12.

[12] Marwaha Mohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, "Comparative Analysis of Cryptographic Algorithms", *International Journal of Advanced Engineering Technology*, IV/III/July-Sep, 2013/16-18.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] Jamil Al-azzeh Ahmad Sharadqh, Belal Ayyoub, Ziad Alqadi, "Experimental investigation of method used to remove salt and pepper noise from digital color image", *International Journal of Research in Advanced Engineering and Technology*, vol. 5, issue 1 pp. 23-31, 2019.

[18] Haitham Alasha'ary, Abdullah Al-Hasanat, Khaled Matrouk, Ziad Al-Qadi, Hasan Al-Shalabi, "A Novel Digital Filter for Enhancing Dark Gray Images", *European Journal of Scientific Research*, Vol.122 No.1, pp.99-106, 2014.

[19] Dr. Mohammad S. Khrisat Prof. Ziad Alqadi, "ZA special filter to eliminate salt and pepper noise from gray and color images", *International Journal of computer applications*, vol. 175, issue 11, pp. 36-42, 2020.

[21] Jamil Azzeh, Bilal Zahran, Ziad Alqadi, "Salt and Pepper Noise: Effects and Removal", *JOIV: International Journal on Informatics Visualization*, vol. 2, issue 4, pp. 252-256, 2018.

[21] Dr. Mohammad S. Khrisat Prof. Ziad Alqadi, "Simple, Qualities, Efficient and Secure Method to Encrypt Voice Signal", *International Journal of Computer Applications*, vol. 183, issue 7, pp. 25-29, 2021.

[22] Hatem Zaini Prof. Ziad Alqadi, "Color Image Cryptography Using Huge Random Private Key", *Word Journal of Engineering Research and Technology*, vol. 7, issue 3, pp. 42-52, 2021.

[23] Prof. Ziad Alqadi, "Efficient and highly secure method of message encryption", *IJETRM*, vol. 5, issue 2, pp. 58-64, 2021.

[24] A Waheeb, Ziad AlQadi, "Gray image reconstruction", *Eur. J. Sci. Res*, vol. 17, pp. 167-173, 2009.

[25] Jihad Nader, Ziad A. A. Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", *International Journal of Computer Applications*, vol. 174, issue 8, pp. 12-17, 2017.

[26] 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.

[27] 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.

[28] 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.

[29] Mohammad S. Khrisat, Rushdi. S. Abu Zneit, Hatim Ghazi Zaini, Ziad A. Alqadi, Analysis Methods Used to Extract Fingerprints Features, Traitement du Signal, vol. 38, issue 3, pp. 711-717, 2021.

[30] Dr. Mohammad S. Khrisat Prof. Ziad Alqadi, "Color Images Classifier Optimization", *International Journal of Engineering Technology Research & Management*, vol. 5, issue 5, pp. 6-14, 2021.

[31] 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.

[32] 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.
[33] Ziad A AlQadi, "Accurate Method for RGB Image Encryption", *IJCSMC*, vol. 9, issue 1, pp. 12-21, 2020.

PhD in Energy from POLITEHNICA University of Bucharest / Romania
Full-time lecturer in the Electrical Engineering Department / College of Technological Engineering at Al-Balqa Applied University Previously, worked as Assistant Dean for Planning and Training and Director of the National Institute for Training of Trainers also worked as an international procurement Advisor in the Ministry of Education.

Prof. Ziad Alqadi:
Professor in computer engineering, head of computer engineering, department, Faculty of engineering technology, Albalqa applied university. Jordan, Amman: Interest: Image and signal processing, parallel processing, computer applications.