World Journal of Engineering Research and Technology
WJERT
www.wjert.org
Impact Factor Value: 5.924

SIMPLE, EFFICIENT AND HIGHLY SECURE METHOD FOR TEXT FILES CRYPTOGRAPHY

***Dr. Hatim Zaini and Prof. Ziad A. Alqadi**

[1]Taif University, KSA.

[2]Albalqa Applied University, Jordan.

Article Received on 26/08/2021 **Article Revised on 16/09/2021** **Article Accepted on 06/10/2021**

***Corresponding Author**
Dr. Hatim Zaini
Taif University, KSA.

ABSTRACT

The process of protecting text files and secret messages is a very important process to protect this data from the risk of penetration and protect it from intruders and data thieves. Therefore, it is necessary to provide an easy-to-implement, fast and secure way to protect confidential data. In this research article, an easy, secure and highly efficient method will be presented. This method will depend on the use of the digital image as a data store from which all the keys necessary to perform the encryption and decryption process can be extracted. The proposed method will be implemented to obtain the experimental results needed to make comparisons with other methods used to protect data to prove the efficiency of the proposed method.

KEYWORDS: Digital image, cryptography, PSNR, MSE, DES, AES, PK, throughput, speedup.

INTRODUCTION

A digital color image[1-6] is a huge data complex that can be used or parts of it for different important applications for data processing. This huge volume of data is circulated on a large scale daily and can be obtained from various sources. It can also be easily generated due to the availability of advanced equipment spread among people, including cellular devices.[7-11]

The digital image, as shown in the figure 1, is represented by a three-dimensional matrix, where each dimension is assigned to represent a color from the three colors red, green and blue.[12-15]

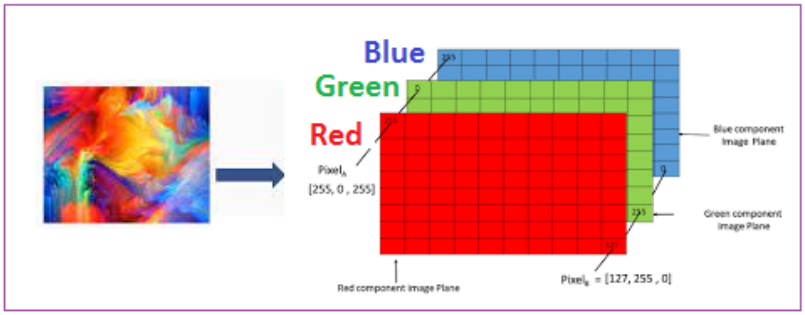

Figure 1: Digital color image matrices.

The process of dealing with the digital image as a matrix facilitates the various processing operations of the image, as it is possible to deal with the image completely or to deal with parts of it extracted from the image.[36-42]

The digital color image has a specific size of values, which is confined between zero and 255, and this size can be changed to suit the required application by enlarging or reducing its size or by converting it to a linear or vertical matrix by implementing a resizing operation illustrated in figure 2.

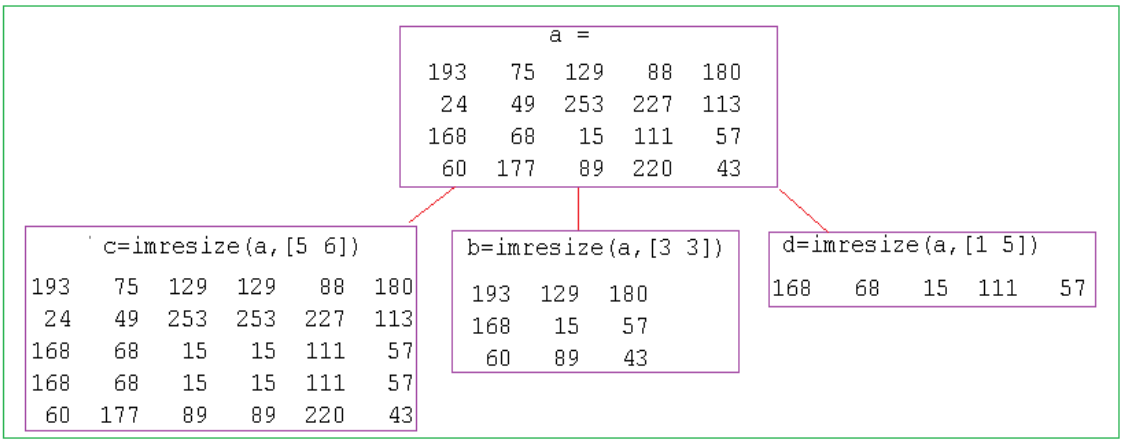

Figure 2: Image resizing.

Data cryptography as shown in figure 3 is a process of completely destroying the data so that it is not understood or illegible by intruders or who are not authorized to view confidential data, this can be done during the encryption phase, while the decryption phase must return a data completely identical to the secret one without losing any piece of information.[17-20]

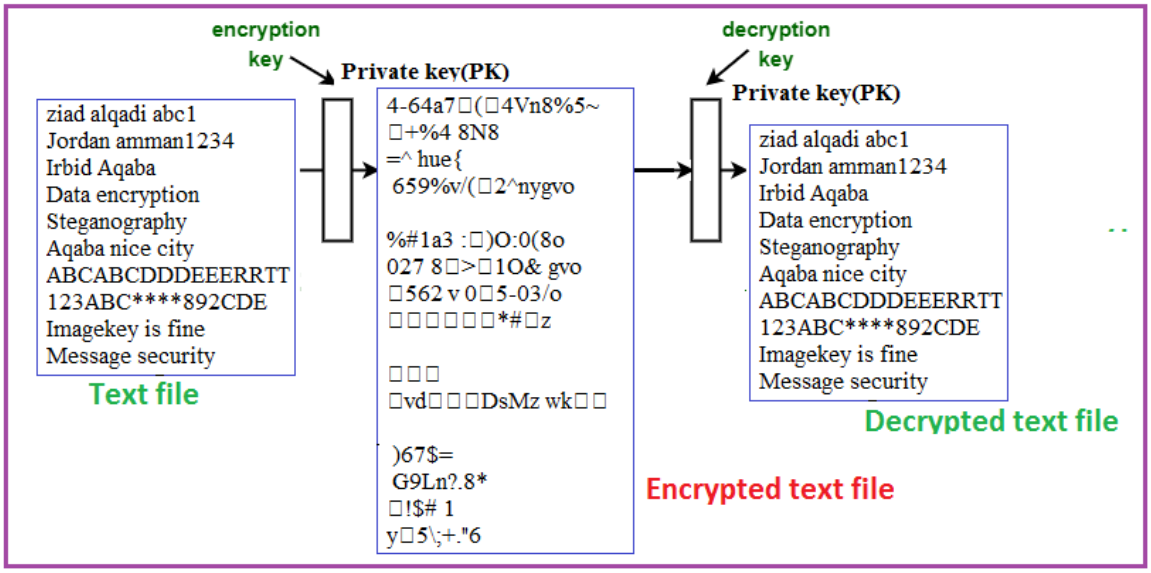

Figure 3: Data cryptography.

The quality of cryptography method measures by mean square error (MSE) and/or peak signal to noise ratio (PSNR), these quality parameters are calculated using equations (1) 1nd (2)[30-35]:

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

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

Where: f and g are the files to be compared for quality.[28]

Therefore, the good data cryptography method must satisfy the following important things[21-30]

- Easy to use and implement.
- High efficiency, by minimizing the encryption and decryption times, and thus increasing the method throughput (number of bytes encrypted or decrypted in a second).
- Provides a high level of data communication security by increasing the degree of data protection and making the process of data penetration difficult or even impossible.
- Provide a high quality by providing zero MSE value and infinite PSNR value between the original text file and the decrypted text file.
- Providing a fully destruction of the encrypted file by providing big value for MSE and small value of PSNR between the original and the encrypted files.

Related works

Many methods[33],[34] are used to protect data and many of these methods are based on standards DES (data encryption standard) and AES (advanced encryption standard).[25],[26]

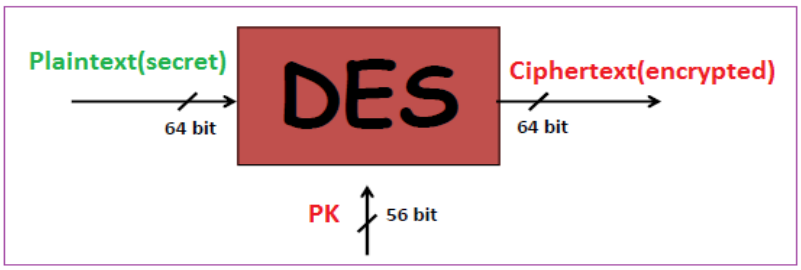

Figure 4: DES encryption.

DES cryptography divides the text file into equal blocks (see figure 4), each block will be encrypted using a private key and some logical and mathematical operations, the decrypted blocks will be gathered to form the encrypted text file. Using DES based methods require generating key, key scheduling and work keys calculation; this will increase the encryption, decryption times and thus negatively affects the method efficiency. The encryption decryption processes are implemented using a fixed number (16) of rounds based on the private key which can be hacked making the method not highly secure.[28],[29]

AES expands the security level by using longer PK (see figure 5), also this methods uses 14 rounds to accomplish the cryptography, each round is implemented using the work and sub leys generated from the PK. DES and AES are suffering from the times required to generate and calculate various keys used in various rounds, and this will slow the process of cryptography and thus resulting in inefficient method of data encryption/decryption.

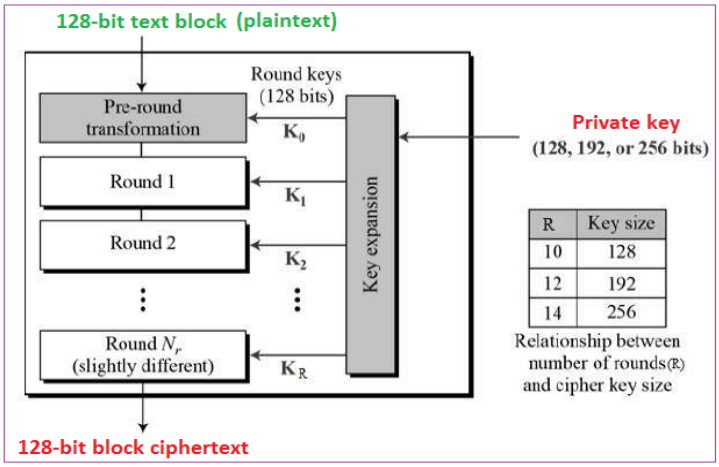

Figure 5: AES encryption.

The proposed method

The proposed method uses the digital color image as a data collector to obtain the secret key or keys needed for the encryption and decryption process. This image provides a high degree of protection for the following reasons:

- ✓ The huge image size, which is difficult to guess.
- ✓ The image is kept confidential and agreed upon by the sender and receiver.
- ✓ The image is not sent via various social media.
- ✓ Possibility to change the image at any time.
- ✓ The possibility of using parts of the image and from specific locations to extract the keys necessary for the encryption process.

The proposed method allows the possibility of encrypting the secret text files in a block by block and the block size can be variable or the possibility of encrypting the text file in burst way.

The process of encrypting the secret text file is carried out by block by block, as shown in the figure 6 according to the following steps:

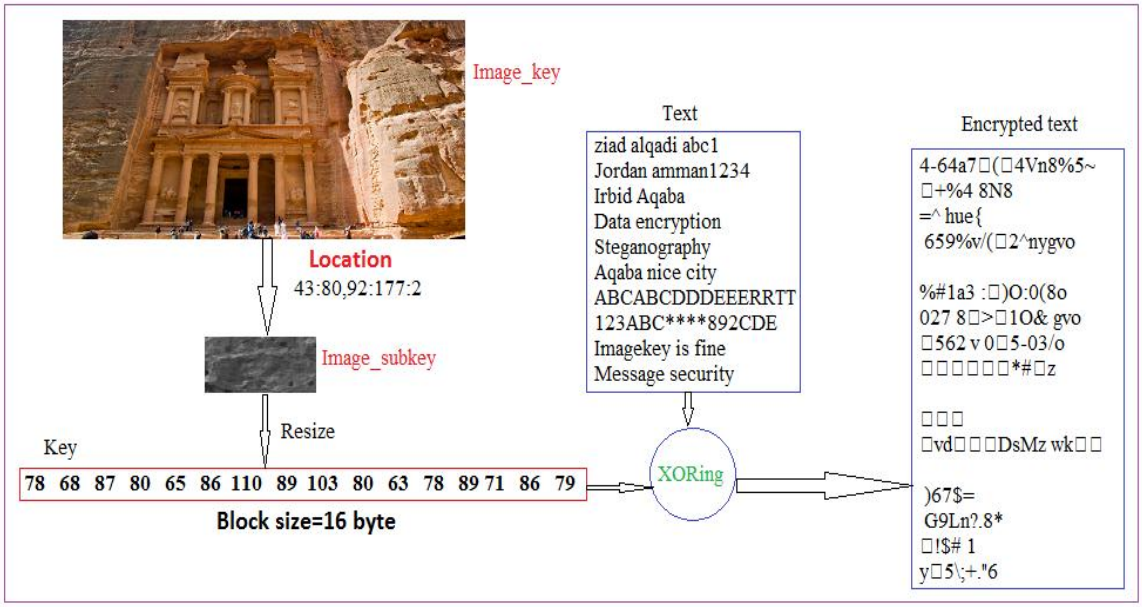

Figure 6: Encrypting text file block by block.

Step 1: Select the secret image.

Step 2: Select the image_subkey, extract it from the image depending on the selected locations.

Step 3: Divide the text file into blocks with equal sizes.

Step 4: Get the private key (PK) by resizing the image_subkey.

Step 5: For each block: apply XORing of the PK and the text block to get the encrypted block.

Step 6: Merge the encrypted blocks to get the encrypted text file.

The decryption process can be implemented applying the following steps (see figure 7):

Step 1: Get the secret image.

Step 2: Get the image_subkey, extract it from the image depending on the selected locations.

Step 3: Divide the encrypted text file into blocks with equal sizes.

Step 4: Get the private key (PK) by resizing the image_subkey.

Step 5: For each block: apply XORing of the PK and the encrypted text block to get the decrypted block.

Step 6: Merge the decrypted blocks to get the decrypted text file.

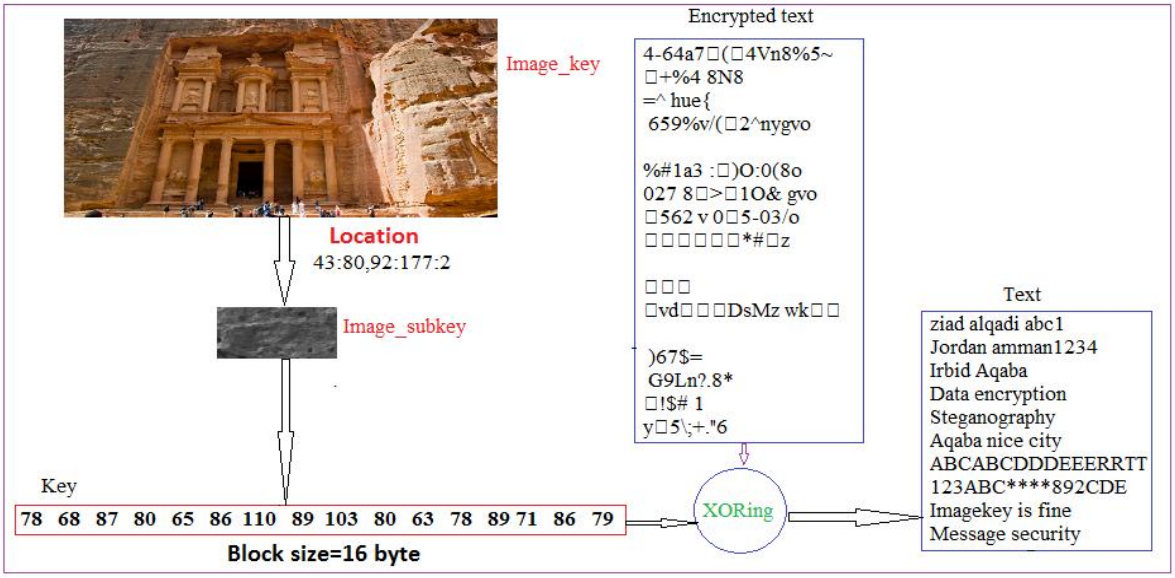

Figure 7: Blocks decryption.

The second way is to encrypt decrypt the text file in burst way, here the encryption process will be implemented applying the following steps (see figure 8)

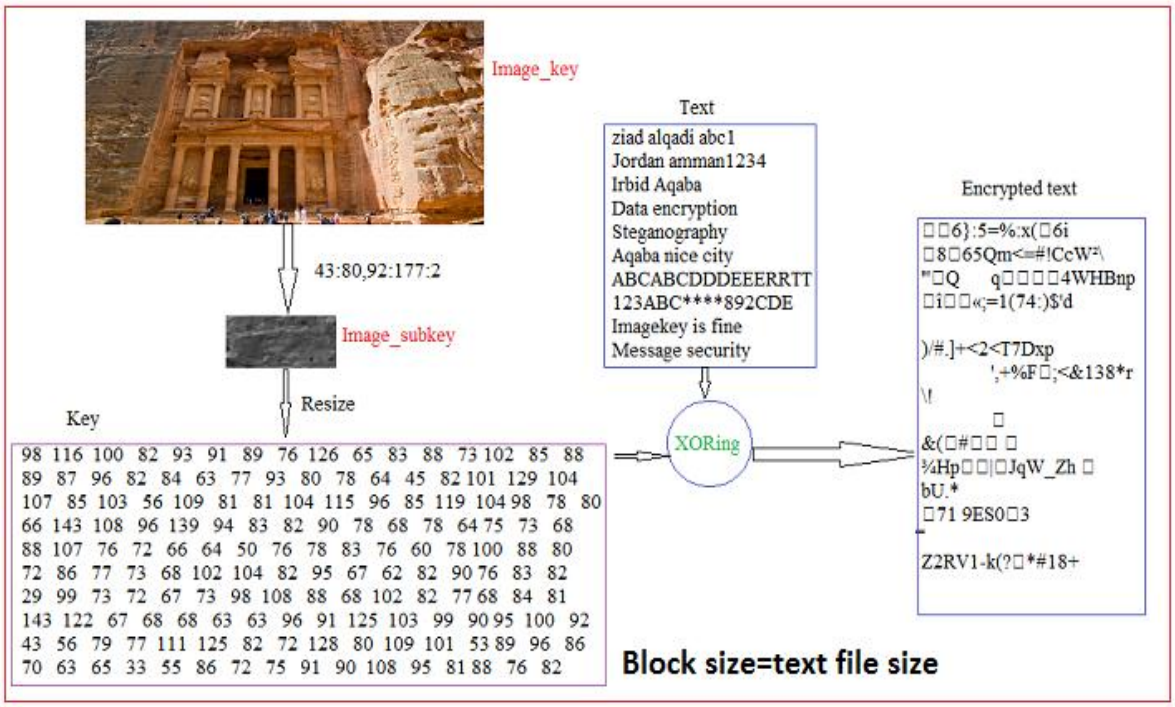

Figure 8: Encrypting text file in burst way.

Step 1: Select the secret image.

Step 2: Select the image_subkey, extract it from the image depending on the selected locations.

Step 3: Get the private key (PK) by resizing the image_subkey.

Step 5: Apply XORing of the PK and the text file to get the encrypted file.

The decryption process can be implemented applying the following steps (see figure 9)

Step 1: Get the secret image.

Step 2: Select the image_subkey, extract it from the image depending on the selected locations.

Step 3: Get the private key (PK) by resizing the image_subkey.

Step 5: Apply XORing of the PK and the encrypted text file to get the decrypted file.

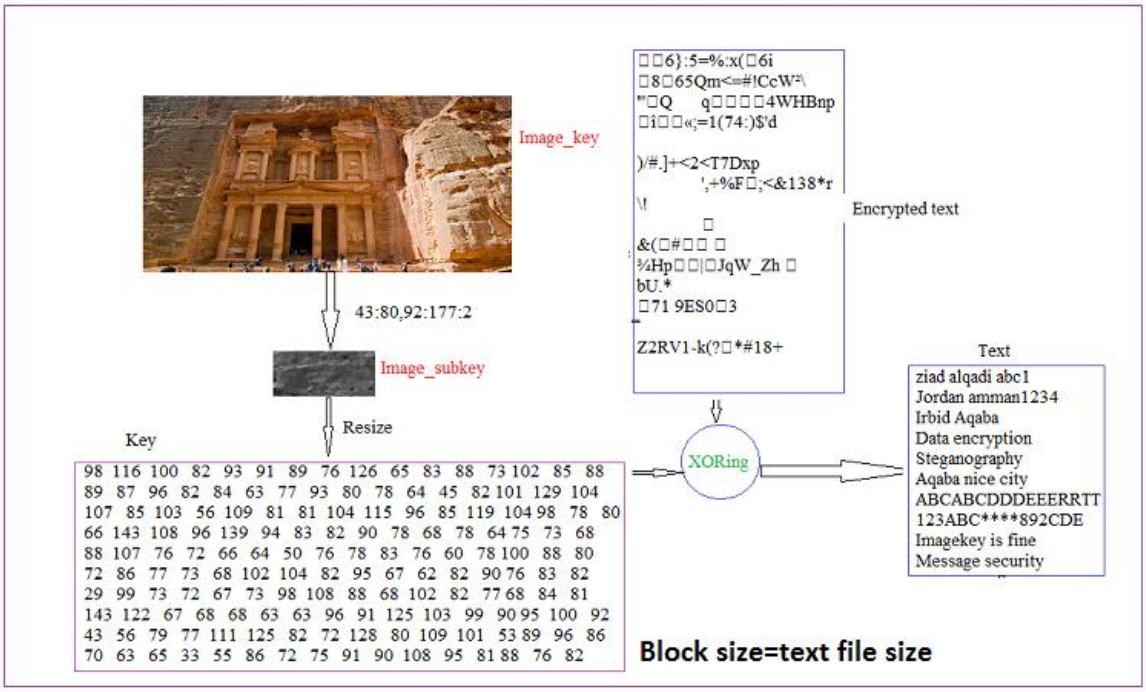

Figure 9: Decryption using burst way.

Implementation and experimental results

Before analyzing the obtained experimental results, let us summarize the main features of the proposed method comparing with DES and AES methods, table 1 show the comparisons:

Table 1: Methods features comparison.

Feature	DES	AES	Proposed
Data block size	64	128	Any size, Text size
PK length	56	128, 192, or 256	Size of selected block or text file size
Principle	Feistel Cipher	substitution and permutation	Image selecting, resizing
Rounds	14	16	No rounds
Operation	Expansion Permutation, Xor, S-box, P-box, Xor and Swap	Sub bytes, Shift rows, Mix columns, Add round keys	resizing, XORing
Security	Low	High	Very high
Speed	slow	slow	Very fast
Image encryption	Difficult	Difficult	Very easy
Simplicity	Not simple	Not simple	Very simple

Various messages with various lengths were treated using the proposed, DES and AES methods; table 2 shows the obtained experimental results:

Table 2: DES, AES and proposed methods efficiency results.

Message size	DES encryption time(seconds)	AES encryption time(seconds)	Proposed encryption time(seconds)
20527	2	4	0.043000
36002	4	6	0.044000
45911	5	8	0.044300
59852	7	11	0.045300
69545	9	13	0.045400
137325	17	26	0.047000
158959	20	30	0.047900
166364	21	31	0.048300
191383	24	36	0.050700
232398	30	44	0.051000
Average Time	14	21	0.0467
Throughput (Bytes/sec)= Average size/average time	7987.9	5325.2	2394600

From table 2 we can see that the proposed method is more efficient and it increases the process of cryptography throughput rapidly, table 3 shows the speedup provides by the proposed method, while figure 10 shows a comparison of encryption times for the three methods.

The quality parameters (MSE and PSNR) were calculated and the proposed method gave excellent values for these parameters during the encryption and decryption phases, thus the proposed method satisfy the requirements of good method of cryptography.

Table 2: Speedup calculation (speedup1=time2/time1).

Method	DES	AES	Proposed
DES	1	1.5000	0.0033
AES	0.6667	1	0.0022
Proposed	299.7859	449.6788	1

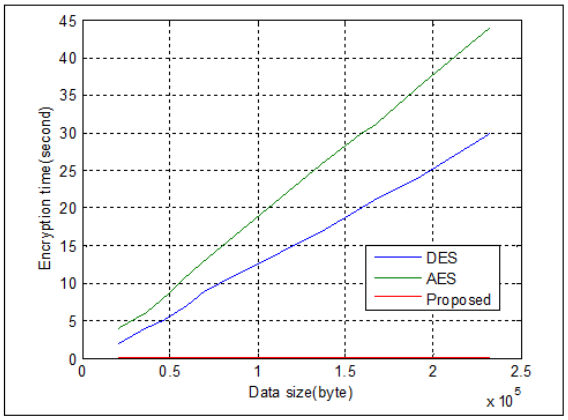

Figure 10: Encryption times comparisons.

The proposed method was implemented using various text file using various private key (private key length=text file length), table 4 shows the obtained results:

Table 4: Various file encryption-decryptions proposed method results.

Text size(byte)	Encryption time(seconds)	Decryption time(seconds)	Throughput (K bytes per second)
160	0.004548	0.004548	34.3558
240	0.049947	0.049947	4.6925
320	0.052635	0.052635	5.9371
400	0.053271	0.053271	7.3328
480	0.053913	0.053913	8.6946
560	0.054575	0.054575	10.0206
640	0.054602	0.054602	11.4465
720	0.054809	0.054809	12.8286
800	0.054884	0.054884	14.2346
880	0.054951	0.054951	15.6389
960	0.054467	0.054467	17.2123
8000	0.059866	0.059866	130.4998
16000	0.063176	0.063176	247.3249
24000	0.063575	0.063575	368.6591

The obtained results shown in table 4 also prove the efficiency of the proposed method providing a high value of the cryptography throughput, figures 11 and 12 show the relationship between the text file size and the encryption time and the throughput.

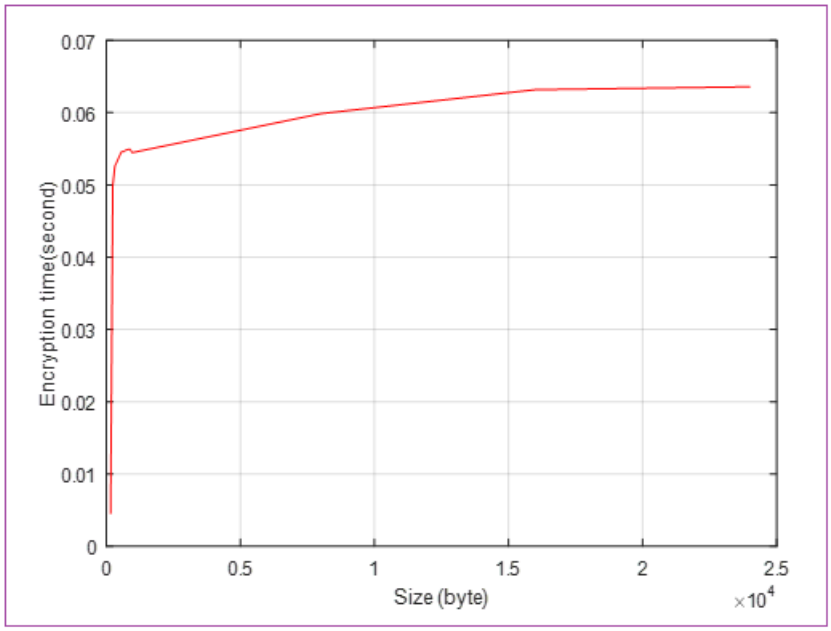

Figure 11: Relationship between text file size and encryption time.

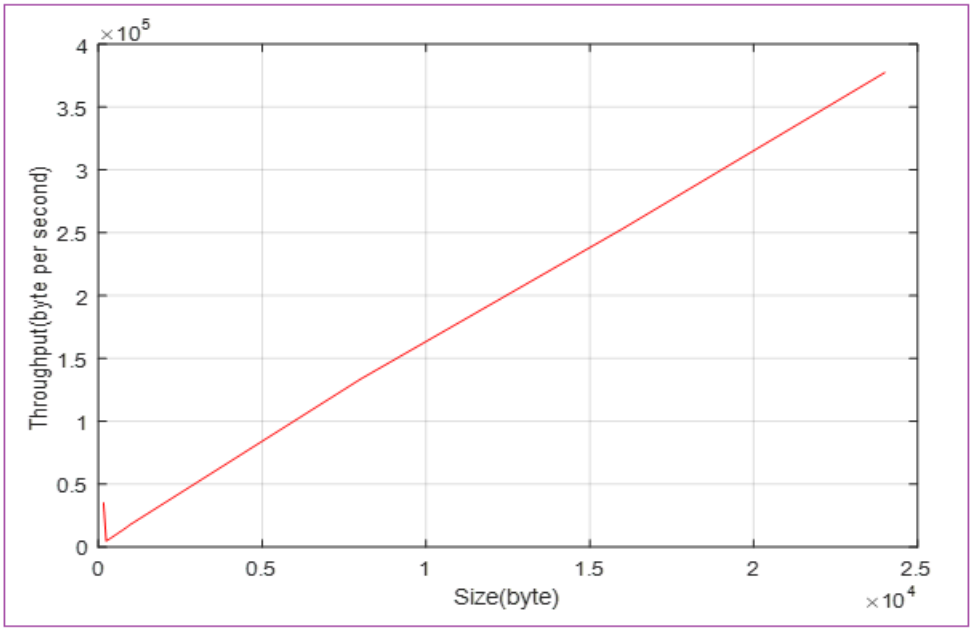

Figure 12: Relationship between text file size and throughput.

CONCLUSION

A simple, easy to implement, accurate, highly secure and efficient method of text file cryptopograpghy was proposed and implemented. The proposed method used a huge color image as an image_key, this key is impossible to hack and it can be used to generate the cryptography private key. The proposed method results were compared with other cryptography stanadard method and the proposed method increased the effiiency by significantly deacreasing both the encryption and decryption times, thus rapidly increased the cryptography process throughput. The proposed method satisfied the requirements of good method of cryptography by giving excellent values for the quality parameters MSE and PSNR in the encryption and decryption phases.

ACKNOWLEDGMENT

This work was supported by the Research Groups Program Funded by Deanship of Scientific Research, Taif University, Ministry of Education. Saudi Arabia, under Grant (TURSP-2020/345).

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 Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad 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.

Dr. Hatim Zaini, associate professor, Computer Engineering-Taif University, KSA.

Interests: Image processing, algorithms, combinational optimization, computer applications and programming.

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.