Improving the Efficiency and Scalability of Standard Methods for Data Cryptography

Mua'ad M. Abu-Faraj[1†] **Ziad A. Alqadi** [2††]

The University of Jordan Albalaqa Applied University

Summary
Providing a secure and effective way to protect confidential and private data is an urgent process, and accordingly, we will present in this research paper a new method, which is called multiple rounds variable block method (MRVB) which depends on the use of a colored image that is kept secret to generate needed work and round keys. This method can be used to encrypt-decrypt data using various lengths private key and data blocks with various sizes. The number of rounds also will be variable starting from one round. MRVB will be implemented and compared with the encryption-decryption standards DES and AES to show the improvements provided by the proposed method in increasing the security level and in increasing the throughput of the process of data cryptography. The generated private key contents will depend on the used image_key and on the selected number of rounds and the selected number of bytes in each block of data.

Keywords: *MRVB, DES, AES, PK, WK, RK, throughput, MSE, PSNR.*

1. Introduction

The digital color image [1] is one of the most widely used types of data, and this is due to the following reasons:

- Ease of access and little cost due to the availability of various digital equipment used to generate the image.
- Ease of digital image processing.
- The huge image size, which provides a large data storage.
- The ability to keep the digital image secretly.
- The pixels values are the same as ASCII values.

Digital color image as shown in Figure 1 is represented by 3 2D matrices, one matrix for each color (Red, green and blue) [2].
The color matrices can be used separately, and from each matrix we can extract its contents to be used to form any key (or set of keys) with any length.
Color image matrix can be resized to one row matrix with a defined number of elements, Figure 2 shows and example of red color resizing:

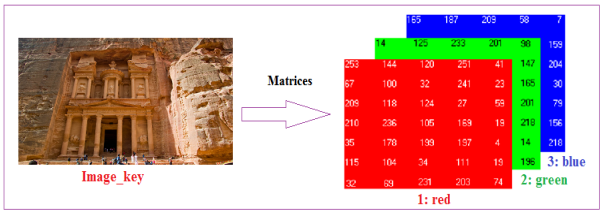


Figure 1: Color image matrices

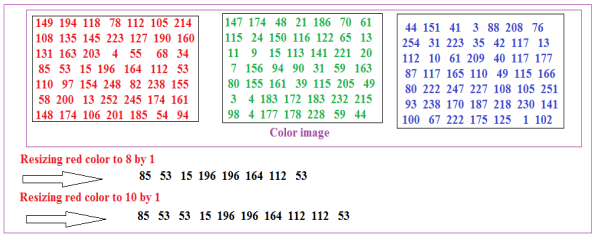


Figure 2: Red color matrix resizing example

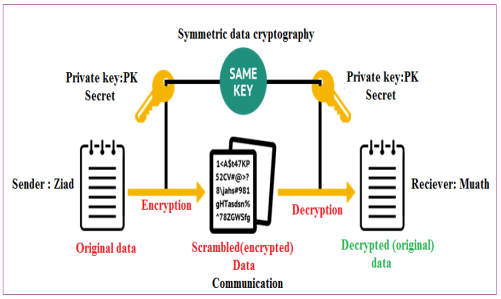


Figure 3: Data cryptography

Protecting secret data [3-7] from hackers can be done applying data cryptography (see Figure 3), which means data encryption before data transmission and data decryption after receiving the secret data, the security of data transmission can be obtained by using a secret private key (PK), which must be kept in secret, the security level depends on the PK length and here a high security level can be achieved by using a complex large PK.

Encryption means fully destruction of the original data to make it unreadable and unuseful [8-11], while decryption means fully recovery of the original data [12-17]. The quality of encrypted can be measured by mean

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.12.61

square error (MSE) and/or peak signal to noise ratio (PSNR), the higher the MSE value the higher level of destruction, and the lower the PSNR value the higher level of destruction. The MSE value between the original data and the decrypted data must equal zero, while PSNR must equal infinite, MSE and PSNR can be calculated using equations 1 and 2 [18-19].

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

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

f and j are text files

2. Related work

Many methods of data cryptography [20-23] were built and designed based on the standards DES (data encryption standard) [22-25] and AES (advance encryption standard), these methods are varies in the provided features specially the efficiency and the level of security [1], table 1 summarizes the main features of DES and AES methods:

Table 1: DES and AES main features

Factor	DES	AES
Block size(byte)	8	16
PK length(bit)	56	128, or 192 or 256
Rounds	16	10 or 12 or 14
Cipher type	Symmetric block	Symmetric block
Security level	Low	High
Throughput	Good	Moderate
Key generation and expansion	Yes	Yes
S-Box	Yes	Yes
Scalability	No	Yes
Key(s)	Single	Single
Encryption-decryption quality	Excellent	Excellent

DES and AES methods divided the data in blocks with fixed length, these blocks are then encrypted-decrypted using a PK and various rounds with specific operations are to be implemented. The PK is used to generate other keys needed in each round; the PK length will determine the level of security. Figure 4 shows how DES works, while Figure 5 shows how to implement AES method.

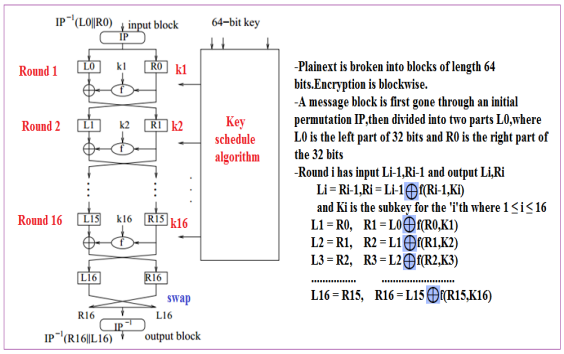


Figure 4: DES encryption

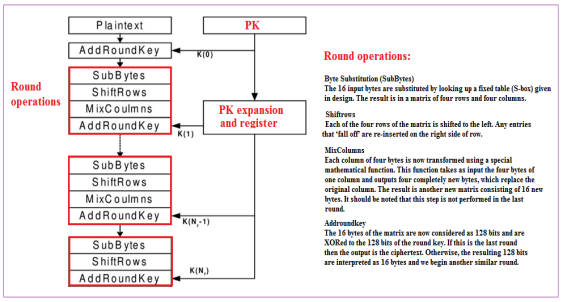


Figure 5: AES encryption

3. The proposed MRVB

The proposed method uses a multiple PK to complete the encryption-decryption phases. PK is to be extracted from a secret image key by resizing this image to a required one row array with a required length as shown in Figure 6.

Extracted PK contains the necessary number of working keys (WK) and the necessary number of round keys (RK), the number of WK depends on the block size and it will be equal the number of bytes in each block, half of them will be used in the initial state, while the other half will be used in the final state. The number of RK depends on the selected number of rounds (number of rounds will start from one to 32), each round requires a number of RK equal the block size in byte divided by 2.

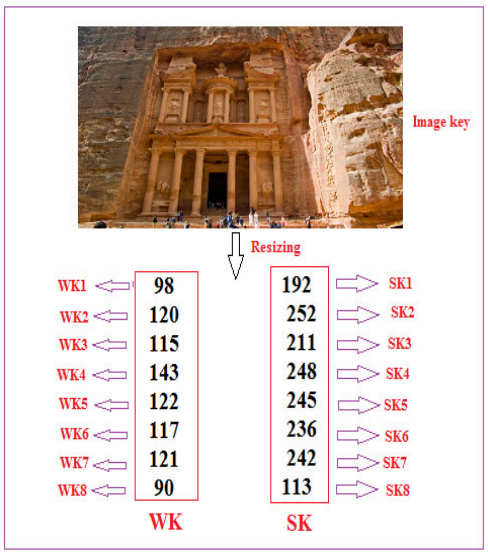


Figure 6: PK extraction

The data block (8 or 16 or 32 or 64 bytes) is to be divided into bytes, and the initial state is to be performed, this state uses WKs to implement modules 256 addition and XORing as shown in Figure 7:

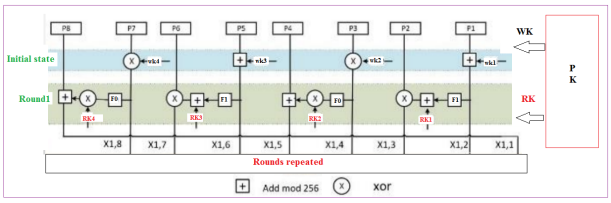


Figure 7: MRVB encryption

Each selected round performs the following operations:

- Applying the Feistel function F0 and F1.
- Modules 256 addition using RK (see Figure 7).
- XORing.
- Circular shift of the final results

The Feistel function performs a logical left right sifting with a defined number of digits, this number can be changed if needed, tables 2 and 3 show how these functions operate:

Table 2: Feistel function F0: 1, 2, 7

Data byte	Operation	Output	Converted byte
65	Convert to binary	bin =01000001	198
	Rotate left one digit	A1=10000010	
	Rotate left 2 digits	A2=00000101	
	Rotate left 7 digits	A3= 01000001	
	Binary to decimal A1, A2 and A3	A4=130, A5=5,A6= 65	
	Bitxor A4 and A5	A7=135	
	Bitxor A6 and A7	A8=39	

Table 3: Feistel function F1: 3, 4, 6

Data byte	Operation	Output	Converted byte
65	Convert to binary	bin =01000001	156
	Rotate left three digit	A1= 00010100	
	Rotate left 4 digits	A2= 00101000	
	Rotate left 6 digits	A3= 10100000	
	Binary to decimal A1, A2 and A3	A4= 20, A5= 0,A6=160	
	Bitxor A4 and A5	A7= 60	
	Bitxor A6 and A7	A8= 156	

The final state performs modules 256 addition and XORing using the second half of WK as shown in Figure 8

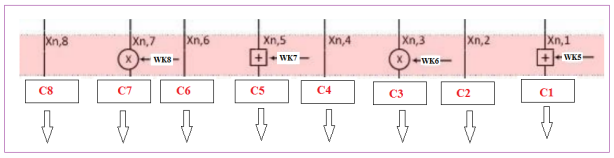


Figure 8: Final state

The decryption phase can be implemented in inverse way replacing the modules 256 addition to modules 256 subtraction.
The generated PK contains the work and the round keys; each key is a one byte; the number and the contents of the generated key will depend on the following:

- The selected image_key.
- The selected block size in bytes.
- The selected number of rounds.

Figure 9 shows the extracted PK using an image_key to implement MRVB method using a block of 16 bytes.

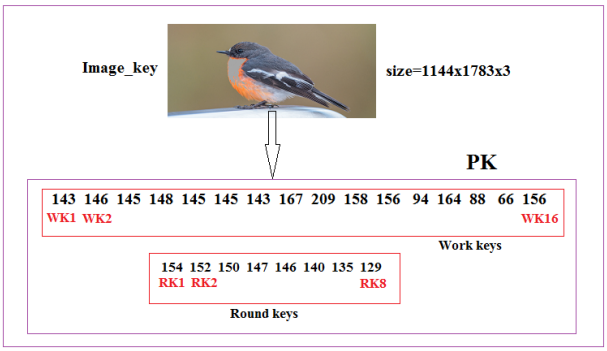


Figure 9: PK generation example (block size =16 bytes)

The private key will be changed if we adjust the block size to 8 bytes, even if use the same image_key as shown in Figure 10.

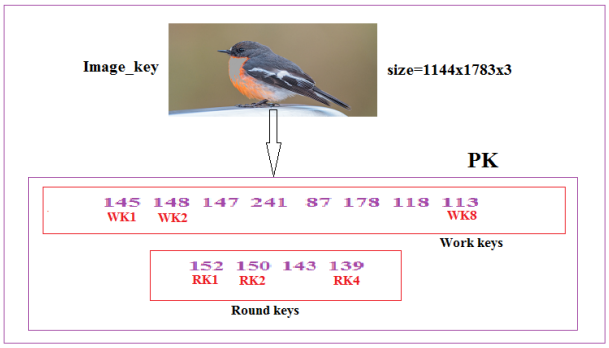


Figure 10: Using the same image_key to generate PK with block size=8 bytes

Changing the image_key keeping the same conditions will change the contents of the private key as shown in Figures 11 and 12:

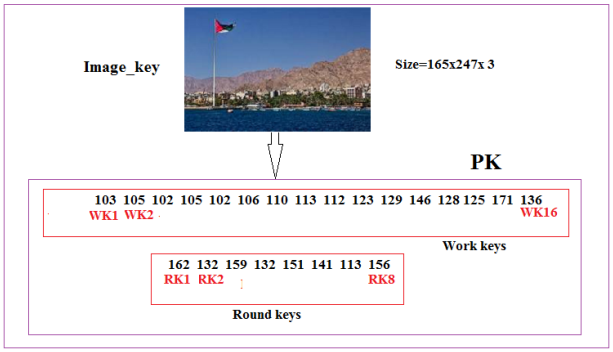


Figure 11: Using another image_key to generate PK with block size =16 bytes

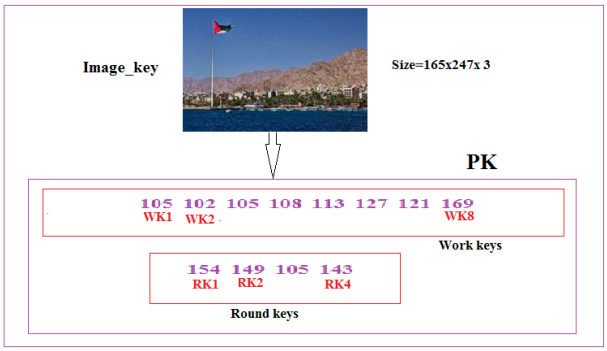


Figure 12: Using the same image_key (in Figure 11) to generate PK with block size=8 bytes

The process of generating private keys for encrypting text files in the proposed MRVB method depends on the use of a secret image that can be changed from moment to moment and when needed, which will make the possibility of hacking the private key a complex and almost impossible process for the following reasons:

1) The image_key used must be agreed upon between the sender and receiver, and it must be kept confidential and not to be sent.
2) The image_key can be changed from time to time if the need arises.
3) The number of keys used and their contents changes depending on the size of the selected data block, and the contents of the keys will change if the block size is changed even when the same image_key is used to generate the keys.
4) For the same data block size, the contents of the used keys will change if the image_key is changed.

4. Implementation and experimental results

DES, AES and the proposed MRVB methods were programmed using Matlab; the programs were executed using I5 processer with 2.4 G hertz and 8 G bytes RAM. The proposed MRVB method was implemented using various in size messages, MSE and PSNR between the original and encrypted messages were calculated, table 4 shows the obtained results:

Table 4: MSE and PSNR results

Message length (byte)	MSE	PSNR
8	2768	30.2705
16	4224	25.5354
32	4360	26.7863
64	4552	26.5135
128	4356	27.0322
256	4222	27.3446
512	4349	27.0471

1024	4353	27.0379
2048	4326	27.1001
4096	4372	26.9935

Increasing the number of rounds will increase the value of MSE and decrease the value of PSNR.
A message if 16 bytes length was taken and encrypted-decrypted applying various numbers of rounds, table 5 shows the obtained results:

Table 5: Encryption-decryption times using various number of rounds

Number of rounds	Encryption time(seconds)	Decryption time(seconds)
1	0.0220	0.0120
2	0.0277	0.0240
3	0.0281	0.0252
4	0.0289	0.0344
5	0.0297	0.0429
6	0.0301	0.0471
7	0.0367	0.0547
8	0.0382	0.0594
10	0.0390	0.0660
12	0.0430	0.0720
16	0.0480	0.0790

Several text files were encrypted-decrypted using DES, AES and MRVB methods; table 6 shows the obtained experimental results:

Table 6: Cryptography times for DES, AES and MRVB

Data size (Kbytes)	DES		AES		Proposed	
	Encryption time(second)	Decryption time(second)	Encryption time(second)	Decryption time(second)	Encryption time(second)	Decryption time(second)
1	6.8344	10.7772	47.6169	57.8563	6.1445	10.1129
2	12.6704	20.5557	95.2320	114.7127	11.2880	18.2243
3	21.5056	31.3329	142.8481	172.5682	17.4320	27.3362
4	29.3408	42.1105	190.4644	230.4249	23.5760	34.4485
5	33.1760	51.8883	238.0806	288.2805	29.7200	48.5609
6	40.0112	63.6657	285.6963	346.1364	35.8640	57.6727
7	44.8464	74.4434	333.3122	403.9929	43.0080	65.7846
8	52.6816	85.2209	380.9282	461.8483	47.1520	77.8963
9	60.5168	94.9986	428.5443	518.7044	53.2960	87.0089
10	66.3520	106.7762	476.1605	572.5608	59.4400	98.1207
Average	**36.7935**	**58.1769**	**261.8884**	**316.7085**	**32.6921**	**52.5166**
Byte cost(seconds)	**0.0065**	**0.0103**	**0.0465**	**0.0562**	**0.0058**	**0.0093**
Throughput (byte per second)	**153.8462**	**97.0874**	**21.5054**	**17.7936**	**172.4138**	**107.5269**

5. Results Analysis

From the obtained experimental results, we can see that the proposed MRVB method adds some improvements to the process of data cryptography, and these improvements can be summarized in the following points:

1) SED method provides a high level of security by using multiple and complex PK, these keys are generated from a color image, which is kept in secrete and can be changed from time to time when it is needed. The PK is a set of work and round keys, and the set of key will be complicated making the hacking process impossible.
2) SED satisfies the quality requirements by providing good values for MSE and PSNR (see table 4), these values can be enhanced by increasing the number of rounds.

3) The number of rounds is variable, the minimum number equal 1, and adding an extra rounds will not so much affect the method efficiency, as shown in Figure 12 (see table 5):

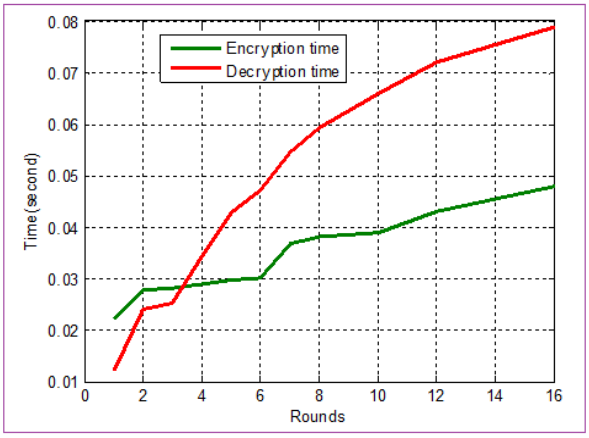


Figure 12: Times using various numbers of rounds

4) MRVB decreases the encryption-decryption times comparing with DES and AES methods, this is shown in Figure 13 and 14

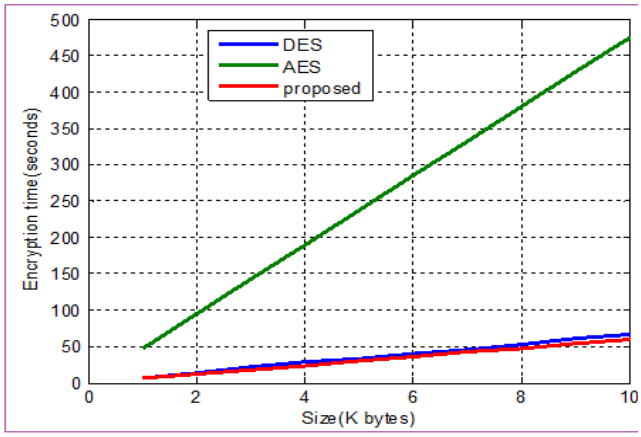


Figure 13: Encryption times comparisons

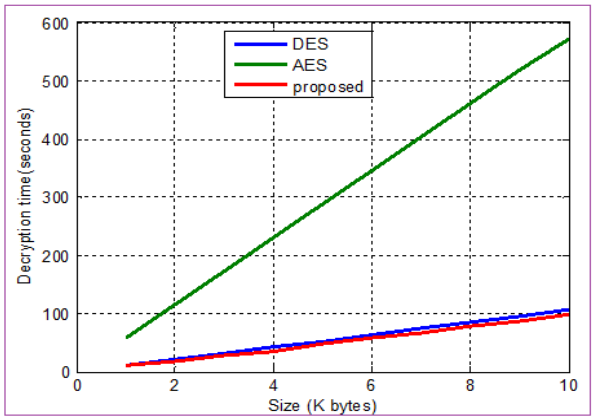


Figure 14: Decryption times comparisons

The proposed method increases the efficiency and the throughput of data cryptography and it speeds up the process of encryption decryption as shown in tables 7 and 8:

Table 7: MRVB encryption speedup

Method	DES	AES	Proposed
DES	1.0000	7.1538	0.8923
AES	0.1398	1.0000	0.1247
Proposed	**1.1207**	**8.0172**	1.0000

Table 8: MRVB decryption speedup

Method	DES	AES	Proposed
DES	1.0000	5.4563	0.9029
AES	0.1833	1.0000	0.1655
Proposed	**1.1075**	**6.0430**	1.0000

Table 9 summarizes the add improvements of MRVB method:

Table 9: MRVB improvements (green colors)

Factor	DES	AES	MRVB
Block size(byte)	8	16	**Variable**
PK length(bit)	56	128, or 192 or 256	Complex and variable
Rounds	16	10 or 12 or 14	Starting from 1
Cipher type	Symmetric block	Symmetric block	Symmetric block
Security level	Low	High	Very high
Throughput	Good	Moderate	Excellent
Key generation and expansion	Yes	Yes	No
S-Box	Yes	Yes	No
Scalability	No	Yes	Yes
Key(s)	Single	Single	Multiple
Encryption-decryption quality	Excellent	Excellent	Excellent

6. Conclusion

An efficient and highly secure MRVB was proposed. The proposed method was implemented using various messages, and it provided excellent quality parameters (MSE and PSNR) during the encryption and decryption phases. The proposed MRVB method used a secret color image to generate multiple PK which includes working and round keys, the number of executed rounds can be controlled by the user starting from one round. The PK is a complex combination of WK and RK , the number and contents of these key depends on the used secret image_key and the selected data block size, making the hacking process impossible. The Feistel functions can be created and updated when needed. The proposed method does not need s_box and other keys expansions and generation. The proposed MRVB method was compared with data cryptography standards DES and AES the obtained results showed that MRVB provides a significant speedup and in increases the throughput of the data cryptography process.

References

[1] Hindi, A., Dr. Dwairi, M., Alqadi, Z.: *Analysis of Procedures used to Build an Optimal Fingerprint Recognition System*. International Journal of Computer Science and Mobile Computing 9(2), 21-37 (2020)

[2] Zahran, B., Ayyoub, B., Nader, J., Al-Qadi, Z.: *Suggested Method to Create Color Image Features Victor*. Journal of Engineering and Applied Sciences 14(1), 2203-2207 (2019)

[3] Abdul Elminaam, D., Abdul Kader, H. and Hadhoud, M.: *Performance Evaluation of Symmetric Encryption Algorithms*. IJCSNS International Journal of Computer Science and Network Security 8(12), 280-286 (2008)

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

[5] Preet, S., Raman, M.: *Comparison of Data Encryption Algorithms*. International Journal of Computer science and Communications 2(1), pp. 125-127 (2011)

[6] Gurjeevan, S., Ashwani, K., Sandha, K.S.: *A Study of New Trends in Blowfish Algorithm*. International Journal of Engineering Research and Applications (IJERA) 1(2), pp.321-326 (2018)

[7] Monika, A., Pradeep, M.: *A Comparative Survey on Symmetric Key Encryption Techniques*. International Journal on Computer Science and Engineering (IJCSE) 4(5), pp. 877-882 (2012)

[8] Li, P., Chen, Z., Yang, L. T., Zhao, L. , and Zhang, Q.: *A Privacy-preserving High-order Neuro-fuzzy C-means Algorithm with Cloud Computing*. Neurocomputing 256, pp. 82–89 (2017)

[9] Yin, S., and Liu, J.: *A K-means Approach for Map-reduce Model and Social Network Privacy Protection*. Journal of Information Hiding and Multimedia Signal Processing 7(6), pp. 1215-1221 (2016)

[10] Teng, L., Li, H., Liu, J., and Yin, S.: *An Efficient and Secure Cipher-text Retrieval Scheme Based on Mixed Homomorphic Encryption and Multi-attribute Sorting Method.* International Journal of Network Security 20(5), pp. 872-878 (2018)

[11] Elgendy, I., Zhang, W., Liu, C., and Hsu, C.: An Efficient and Secured Framework for Mobile Cloud Computing. IEEE Transactions on Cloud Computing 9(1), pp. 79-87 (2018)

[12] Karthikeyan, B., Sasikala, T., and Priya, S. B.: *Key Exchange Techniques Based on Secured Energy Efficiency in Mobile Cloud Computing*. Applied Mathematics & Information Sciences 13(6), pp. 1039-1045 (2019)

[13] B. Karthikeyan, T. Sasikala, and S. B. Priya, "Key exchange techniques based on secured energy efficiency in mobile cloud computing," *Applied Mathematics & Information Sciences*, vol. 13, no. 6, pp. 1039–1045, 2019.

[24] Xu, J. Wei, L., Wu, W., Wang, A., Zhang, Y., and Zhou ,F.: *Privacy-preserving Data Integrity Verification by using Lightweight Streaming Authenticated Data Structures for Healthcare Cyber-physical System*. Future Generation Computer Systems 108, pp. 1287-1296 (2020)

[15] Haseeb, K., Almgren, A., Ud Din, I., Islam, N., and Altameem, A.: *SASC: Secure and Authentication-based Sensor Cloud architecture for intelligent Internet of Things*. Sensors 20(9), pp. 2468-2486 (2020)

[16] Zhu, H., Yuan, Y., Chen, Y., et al.: *A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature*. IEEE Access 7, pp.9003-90044 (2019)

[17] Zhang, Z., and Luo, J.: *A Data Value Classification and Encryption Mechanism Based on Metadata Attributes.* Journal of Northwest University 46(2) pp. 188-194 (2016)

[18] Mehrotra S., Rajan, M.: *Comparative Analysis of Encryption Algorithm for Data Communication*. International Journal of Computer Science and Technology 2(2), pp. 292-294 (2011)

[19] Chandra M.: *Superiority of Blowfish Algorithm*. IJARCSSE 2(9), pp. 196-201 (2012)

[20] Yogesh, K. A.: *Comparative Study of Different Symmetric Key Cryptography*. International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2(7), pp. 204-206 (2013)

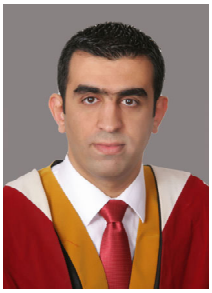
[21] Abdul, D.S., Kader, H.M., Abdul, Hadhoud, M.M.: *Performance Evaluation of Symmetric Encryption Algorithms*. Communications of the IBIMA 8, pp. 58-64 (2009)

[22] Jawahar, T., Nagesh, K.: *DES, AES and Blowfish Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis*. The International Journal of Emerging Technology and Advanced Engineering IJETAE 1(2), pp. 6-12 (2011)

[23] Mohit, M., Rajeev, B., Amritpal, S., Tejinder, S.: *Comparative Analysis of Cryptographic Algorithms*. International Journal of Advanced Engineering Technology, pp.16-18 (2018)

[24] Imran, A., Rafeek, K.: *Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography*. International Journal of Advanced Research in Computer Science and Software Engineering 3(10), pp.713-(2013)

[25] Riman, C., and Hallal, H.: *DES Based Educational Data Encryption System.* International Conference on Security and Management (WORLDCOMP'13) (2013)



Mua'ad Abu-Faraj received the B.Eng. degree in Computer Engineering from Mu'tah University, Mu'tah, Jordan, in 2004, the M.Sc. degree in Computer and Network Engineering from Sheffield Hallam University, Sheffield, UK, in 2005, and the M.Sc. and Ph.D. degrees in Computer Science and Engineering from the University of Connecticut, Storrs, Connecticut, USA, in 2012. He is, at present, an Associate Professor at The University of Jordan, Aqaba, Jordan. He is currently serving as a reviewer for the IEEE Micro, IEEE Transactions on Computers, Journal of Supercomputing, and International Journal of Computers and Their Applications (IJCA). His research interests include computer architecture, reconfigurable hardware, image processing, cryptography, and wireless networking. Dr. Abu-Faraj is a member of the IEEE, ISCA (International Society of Computers and their Applications), and JEA (Jordan Engineers Association).

Ziad A. Alqadi received the B.E., M. E., and Dr. Eng. degrees from Kiev Polytechnic Institute. in 1980, 1983, and 1986, respectively. After working as, a researcher from 1986, an assistant professor from 1991 in the department of Electrical Engineering, Amman Applied College, and an Associate Professor from 1996 in the Faculty of Engineering Technology, he has been a professor at Albalqa Applied. since 2010. His research interest includes signal processing, image processing, data security and parallel processing.