Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography

MUAAD ABU-FARAJ1, ABEER AL-HYARI2, KHALED ALDEBEI3, ZIAD ALQADI4, and BILAL AL-AHMAD5

1Department of Computer Information Systems, The University of Jordan, Aqaba 77110, Jordan (e-mail: m.abufaraj@ju.edu.jo)
2Electrical Engineering Department, Al-Balqa Applied University, As Salt 19117, Jordan (e-mail: abeer.hyari@bau.edu.jo)
3Department of Information Systems, The University of Jordan, Aqaba 77110, Jordan(e-mail: k.debei@ju.edu.jo)
4Computers and Networks Engineering Department, Al-Balqa Applied University, Amman 15008, Jordan(e-mail:dr.ziad.alqadi@bau.edu.jo)
5Department of Computer Information Systems, The University of Jordan, Aqaba 77110, Jordan (e-mail: b.alahmad@ju.edu.jo)

Corresponding author: Bilal Al-Ahmad (e-mail: b.alahmad@ju.edu.jo).

ABSTRACT Due to the availability of several social media platforms and their use in sending text messages, it is necessary to provide an easy and safe way to protect messages from being hacked especially in the presence of intruders and data thieves, and taking into consideration that most of those messages are confidential and personal, it is necessary to provide an easy and safe way to protect messages from being hacked. In this research paper, a simple and easy method of message cryptography will be proposed. The method divides a message into blocks with fixed sizes. The block size ranges from 2 to 60. The method uses a secret color image to generate an array with a size equal to the number of resulted blocks. The array will then be used as a private key. Each element of the private key will be used to calculate the number of rotation digits for the associated block in order to apply block rotation left operation. The proposed method will be examined using the parameter’s Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Correlation Coefficient (CC), and throughput. The proposed method will be compared with other standard methods of message cryptography, such as Data Encryption Standard (DES), Triple-DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF). Experimental results show that the proposed method is secured enough based on using secret image, block size, and calculated Rotation Left Digits (RLD) for each block.

INDEX TERMS Block, BRV, CC, cryptography, MSE, PSNR, RLD, secret message, speedup, throughput.

I. INTRODUCTION

WHEN information or data is shared over the Internet, it transmits through a series of network devices around the world. Through the transmission, there is a possibility that the data is hacked or stolen by hackers. In order to prevent that, users need to install certain software or hardware to ensure secure transmission of data or information. This process in network security is called Encryption [1]–[6].

The encryption process involves converting plain text that is readable to humans into unintelligible text, which is known as ciphertext. This generally means changing the readable data into a format that it appears randomly. The encryption process uses an encryption key that is a set of mathematical values agreed upon by both the sender and the receiver. The recipient uses the key to decrypt the ciphertext and convert it back to readable plain text [7], [8]. The more complex the encryption key, the more secure the encryption as third parties are less likely to be able to decrypt data through brute force attacks (i.e. trying random keys until the right one is found) [3]. The Encryption is also used for protecting passwords. It hashes a password to become unreadable for hackers [9].

One of the most important methods for protecting text messages (i.e., short and long messages) is Data Cryptography. It encrypts the data before sending and decrypts it after receiving [10]–[13]. Data Encryption-Decryption process is usually applied by using a secret private key (PK) that is only known by the sender and receiver. In our research paper, we will focus on symmetric cryptography while the encryption and decryption processes [14] use the same PK as shown in
The encryption process destroys the original data so that it becomes incomprehensible and useless. The decryption process converts the encrypted data into the original data without any error by using the PK and specific methods. Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient (CC) are used to compare the quality of two messages (i.e., the sent message and received message). The equations 1, 2 and 3 represent the MSE, PSNR and CC respectively [15]. The value between the source message and the encrypted message must be very low in PSNR and CC and must be very high in MSE, and vice versa in the decryption process [16], [17].

According to the studies [16]–[18], the selected method of data cryptography must meet the following requirements: Simple and easy to implement, optimal values of quality parameters during the encryption and decryption phases, efficient by maximizing the throughput (i.e., processed bytes per second), and thus minimizing the encryption-decryption times, and highly secure by preventing message hacking.

The equations show the CC computation.

\[
MSE_x = \frac{1}{N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [S(i, j) - R(i, j)]^2 \tag{1}
\]

where \(N = m \times n\).

\[
PSNR = 10 \log_{10} \left( \frac{MAX_x}{MSE_t} \right)^2 \tag{2}
\]

\[
CC = \frac{\sum (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum (x_i - \bar{x})^2(y_i - \bar{y})^2}} \tag{3}
\]

where CC represents correlation coefficient, \(x_i\) denotes values for first message, \(y_i\) represents values of second message, and \(\bar{x}\) and \(\bar{y}\) indicate means for \(x\) and \(y\).

The digital color image [13], [18]–[22] has a huge amount of data that is organized in a three-dimensional matrix. Therefore, a two-dimensional matrix is allocated to each of the three colors (i.e., red, green and black), as shown in the Figure 2.

The matrix of a digital color image can be employed to carry out many processing operations that are necessary for many vital applications for many reasons. The most important of these reasons are:

1) Ease of obtaining a digital image with no extra cost due to the availability of multiple sources through which a digital color image can be generated [13], [23]–[25]
2) Ease of storing a digital image for reference at any time and when needed.
3) Possibility of dealing with a two-dimensional matrix separately for each of the three colors.
4) Ease of applying all arithmetic and logical operations on the colored graph.
5) Possibility of using parts of three color matrices.
6) Possibility of using a colored digital image to generate special secret keys and lengths on demand by implementing the process of resizing the image using the required dimensions.

In this research paper, the color image will be used as an image_key in order to generate a private key (PK) that will be used in the message block rotation operation. The length of the private key will be equal to the number of blocks in the secret message. Each value in PK will be used as a block rotation value (BRV) in order to calculate the number of rotation left digits (RLD) what are required to rotate the message block.

For the purpose of this work, we need to notice the following points: changing a block length will change the size and the values of PK, and replacing the image_key with another image will change the values of PK element, as shown in Figure 3, Figure 4, and Figure 5.

Figure 6 shows all the images that will be used in this research paper as a source images in order to generate needed PKs. Table 1 shows basic information about these images.

The organization of this paper is as follows. Section 2 presents related work. Section 3 demonstrates the proposed approach. Experiments are conducted in Section 4, followed by the conclusion in Section 5.

II. RELATED WORK

Information security is defined as a set of processes and practices that aim to protect and preserve information from external threats, such as destruction, theft, and sabotage. It mainly depends on the protection of all kind of information wherever it is found in a way that is largely determined by the policy of the company or the individual owning it [7].

Many Internet users suffer from data penetration problems,
FIGURE 3: Using 2D matrix to generate various PKs

TABLE 1: Information about the images used for the proposed approach

| Image number | Dimension   | Size(byte) |
|--------------|-------------|------------|
| 1            | 151x333x3   | 150849     |
| 2            | 152x171x3   | 77976      |
| 3            | 360x480x3   | 518400     |
| 4            | 1071x1600x3 | 5140800    |
| 5            | 981x1470x3  | 4326210    |
| 6            | 165x247x3   | 122265     |
| 7            | 360x480x3   | 518400     |
| 8            | 183x275x3   | 150975     |
| 9            | 183x275x3   | 150975     |
| 10           | 201x251x3   | 151353     |
| 11           | 600x1050x3  | 1890000    |
| 12           | 1144x1783x3 | 6119256    |

which have become a real threat to the security of the Internet and to the devices and electronics that are associated with it. In order to deal with this threat and enhance data privacy and protect it from espionage, some users and business owners resort to depend on closed Internet networks that are protected by special codes and ciphers. Some of other users and business owners prefer to dispense with the transfer of important or confidential data over the Internet. Therefore, they use external storage cards or disks to transfer data between devices [8], [9]. Other users and business owners are concerned in anti-virus programs and electronic piracy and they seek to obtain the programs from reliable companies that are more careful in adopting new and updated programs for detecting new viruses and malware. Various text messages are widely circulated through various and disparate social media. This imposes on us a responsibility to protect these messages, which are confidential and highly personal nature, from stealing, viewing and understanding by intruders or data thieves [23], [25].

Encryption algorithms are used to convert data into ciphertext. They use encryption keys to change the data in a predictable way, so it can be converted back to plain text by using the decryption key. According to the literature, there are several different types of encryption algorithms that are designed to suit different purposes. Furthermore, new encryption algorithms are also developed when old algorithms are unsafe. Some of the most popular encryption algorithms are a follows [26]–[30].

1) Encryption according to the Data Encryption Standard

The Data Encryption Standard (DES) is an obsolete symmetric encryption algorithm that is not suitable for today’s use. Therefore, other new encryption algo-
2) Encryption according to the triple Data Encryption Standard The triple Data Encryption Standard (3DES) is a symmetric key algorithm. It is called "triple" because the data is passed through the original DES algorithm three times during the encryption process. It is being phased out from the use of the triple standard for data encryption. However, it can still create a reliable encryption solution for the financial services and other industries [1]–[3].

3) Encryption according to the Advanced Encryption Standard The Advanced Encryption Standard (AES) is developed to update the original DES algorithm. Some of the most popular applications of the AES include messaging applications, such as Signal or Whatsapp and WinZip [27]–[30].

4) Encryption with the Rivest, Shamir, and Adelman algorithm The Rivest, Shamir, and Adelman algorithm (RSA) is the first available asymmetric cipher algorithm that uses a pair of keys. It is popular and widely used for secure data transmission because of its key length. The algorithm has this name according to the
family surnames of the three mathematicians who first described it, i.e., Ronald Rivest, Adi Shamir, and Leonard Adleman [31], [32].

5) Blowfish Encryption: The Blowfish algorithm is used in both hardware and software. It is considered one of the fastest of its kind. Blowfish is not patented, and this makes its encryption freely available to anyone who wants to use it. As a result, the Blowfish algorithm is built into a different encryption software like Photo Encrypt, GPG, and the popular open-source program TrueCrypt [23].

Many methods are used for message cryptography. Many of these methods are based on the standards (i.e., DES, 3DES, AES and Blowfish). Many of these methods have some disadvantages which are to be solved. However, these methods provide good values of the quality parameters (i.e., MSE, PSNR and CC), and have many advantages. The advantages are as follows [26]–[29]:

1) Block size: The block size is fixed for each of the standard methods of data cryptography and it differs from method to another with a minimum size equal to 8 bytes (64 bits) for the DES method.
2) PK: The standard methods use a fixed length of a private key, and sometimes it can be hacked.
3) Other keys: The PK is used to generate other needed keys for the encryption-decryption phases.
4) Round: Each standard method uses a number of round in order to apply the process of cryptography.
5) Throughput: Most of the standard methods provide a low throughput, especially if the data to be encrypted has a big size.
6) Flexibility: The standard methods require a sequence of arithmetic and logic operations in order to maintain the data cryptography, and it is very difficult to do any modifications to these operations.
7) Security: Some standard methods provide a low level of security. Therefore, new methods should be adopted in order to protect messages and to make the hacking process more difficult.
8) Structure: All the standard methods have a Feistel structure using Feistel sub functions in order to perform various logical operation and to make methods not simple and difficult to modify.

In this article, we take these advantages into consideration and introduce a new method of message cryptography to achieve the following points: [31]–[37]:

1) Increase the size of the message block that be encrypted and make the size variable and be selected by the user.
2) Select a PK from a secret message and must be kept in secret in order to protect it from being hacked. The PK can be of any length and its size depends on the message block size. The PK can be changed from block size to another and from selected image_key to another.
3) Increase the efficiency of cryptography by increasing the throughput. Therefore, the method must decrease both the encryption ET and decryption times.
4) Get an acceptable values of quality parameters (i.e., MSE, PSNR and CC). Process all data, messages and images regardless the data length. Ability to modify the PK and the block size with no need to modify the process of cryptography.

Many techniques were introduced for message cryptography. In [38] a method base on chaotic map model was introduced and the throughput was improved and reached 0.1691 M byte per second, while in [39] the introduced method gave a throughput equal 0.71 M byte per second. The benefits of our study is to solve the disadvantage of mostly introduced methods of data steganography by increasing the throughput, increasing the level of security, allowing using variable length blocks and variable length acting secret keys.

III. THE PROPOSED METHOD

The proposed method is based on implementing two basic operations. The two operations are PK generation and message block rotation. A secret color image will be selected to be used as an image_key. The image must be resized to get a PK with a size equal to a message block size. The generated PK contains a set of elements. A value of each element will be used as a block rotation value (BRV). Furthermore, it will be used to calculate rotation left digits (RLD) which is needed as a number of rotation left digits required to rotate the associated message block. The second operation is rotating left the message block RLD times. The rotation left is implemented as shown in Figure 7.

The value of RLD used in the encryption phase must be less than 500 because MATLAB cannot apply rotation left for a digit greater than 500. The retaliation left digits of the decryption process will be equal to a message length
multiplied by 8 (message length in bits). Then, we have to subtract RLD from the resulted value. The resulted RLD must be less than 55. We have to notice an important fact that is obtained experimentally. The fact is that the RLD value must be greater than the block size (in byte) to avoid the occurrence of message characters in the encrypted message as shown in Table 2.

The proposed algorithm of the encryption and decryption process is shown as in algorithm 1.

Figures 8 and 9 show a calculated example of the rotation process in the encryption and decryption phases.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed method is implemented using i5 processor, with 8 GB RAM using MATLAB. The proposed method will increase the security level of data cryptography based on (1) The image_key must be kept in secret, (2) The generated PK size depends on the block size, if the block size equal 50 elements, the number of combinations required to hack the key is equal \((2^8)^{50} = 2^{400}\), this satisfies the requirement for good key security.

### Algorithm 1 Proposed Algorithm

#### Encryption phase

**Input:** Secret message, image_key, block length (L)

**Output:** Encrypted message

1. Get the inputs
2. Resize image_key to get PK
3. Divide the secret message into N blocks
4. for all message block do
   a. Calculate RLD (RLD=L+PK(I)+1)
   b. Convert the message block to decimal
   c. Convert the decimal block to binary
   d. Reshape the binary version into one row matrix
   e. Rotate the row matrix to the left RLD times
   f. Reshape back to 8 columns matrix
   g. Convert the resulting matrix to decimal
   h. Pad to the encrypted message
5. end for

#### Decryption phase

**Input:** Encrypted message, block length (L), image_key

**Output:** Decrypted message

1. Get the inputs
2. Resize image_key to get PK
3. Divide the secret message into N blocks
4. for all message block do
   a. Calculate RLD1 (RLD1=L*8-RLD)
   b. Convert the message block to decimal
   c. Convert the decimal block to binary
   d. Reshape the binary version into one row matrix
   e. Rotate the row matrix to the left RLD1 times
   f. Reshape back to 8 columns matrix
   g. Convert the resulting matrix to decimal
   h. Pad to the decrypted message
5. end for

#### TABLE 2: Message block: Ziad Alqadi, length=11

| RLD | Encrypted message | MSE       | PSNR    | CC    |
|-----|-------------------|-----------|---------|-------|
| 1   | 02 'Ziad Al      | 1.2545e+003 | 32.5139 | 0.3016 |
| 2   | ad Alqadi        | 2853      | 27.3809 | 0.0526 |
| 3   | d Alqadi         | 3740      | 24.6737 | 0.0712 |
| 4   | Alqadi           | 4.1665e+003 | 23.5937 | 0.3132 |
| 5   | Alqadi           | 3.8915e+003 | 24.2768 | 0.3475 |
| 6   | lqadi            | 4.4034e+003 | 23.0409 | 0.1704 |
| 7   | qadi             | 6621      | 19.5256 | -0.2046|
| 8   | adi              | 8.6285e+003 | 17.7824 | -0.3588|
| 9   | di               | 9431      | 16.8931 | 0.1380 |
| 10  | i               | 9.2068e+003 | 17.1337 | 0.2383 |
| 11  | l                | 8.9682e+003 | 17.3963 | 1     |
| 12  |                 | 9.9841e+003 | 16.3232 | 0.1380 |

RLD=Block size (byte) + block key value +1
Several messages and image keys are used in the proposed approach. The following message block is implemented using various values of RLD. The images 1-12 (see Figure 6) are used to generate the needed BRV. Table 3 shows the obtained experimental result of a message block: ‘Amman is the capital city of Jordan’.

As shown in Table 3, the proposed method provides excellent values of the quality parameters, i.e., MSE, PSNR, and CC. Furthermore, the proposed approach gives a high and acceptable throughput value. The Average estimated time
TABLE 3: Results of encrypting the message block: 'Amman is the capital city of Jordan’. Block size is 35 characters

| Image.no | RLD  | MSE            | PSNR      | CC         | Estimated time |
|----------|------|----------------|-----------|------------|----------------|
| 1        | 132  | 5.6203e+003    | 23.7652   | 0.1957     | 0.006000       |
| 2        | 137  | 7343           | 21.0916   | -0.0277    | 0.006000       |
| 3        | 67   | 8.0044e+003    | 18.7970   | -0.1128    | 0.006000       |
| 4        | 158  | 7.6574e+003    | 20.6724   | -0.1486    | 0.000800       |
| 5        | 206  | 6.0975e+003    | 20.7163   | -0.0606    | 0.007000       |
| 6        | 139  | 8.0925e+003    | 20.1197   | -0.2176    | 0.006000       |
| 7        | 185  | 7.0943e+003    | 20.0040   | -0.1393    | 0.006000       |
| 8        | 72   | 7.6473e+003    | 21.3416   | -0.1669    | 0.006000       |
| 9        | 184  | 5.7517e+003    | 19.6915   | -0.0678    | 0.007000       |
| 10       | 99   | 7.5511e+003    | 20.8122   | -0.0898    | 0.007500       |
| 11       | 138  | 5.4613e+003    | 23.3068   | 0.0928     | 0.008000       |
| 12       | 179  |                |           |            |                |

Average 0.0060
Average throughput (byte per second) 5833.3

TABLE 4: Results of implementing messages blocks with various sizes

| Block size (byte) | Calculated RLD | Between the original and encrypted messages | Key generation time (second) | Encryption time (second) |
|-------------------|----------------|---------------------------------------------|-----------------------------|-------------------------|
|                   |                | MSE                                        | PSNR                        | CC                      |
| 5                 | 242            | 1.5194e+004                                | 12.6481                     | -0.2869                 | 0.001000      | 0.009000 |
| 10                | 254            | 8.3701e+003                                | 18.4374                     | -0.1406                 | 0.002000      | 0.009000 |
| 12                | 240            | 9075                                       | 19.5350                     | 0.4027                  | 0.002100      | 0.009000 |
| 15                | 144            | 8.1629e+003                                | 20.5150                     | 0.1996                  | 0.002200      | 0.009000 |
| 20                | 132            | 1.3923e+004                                | 15.1759                     | -0.3652                 | 0.002300      | 0.009000 |
| 25                | 115            | 7.9985e+003                                | 20.9552                     | 0.1262                  | 0.006000      | 0.009000 |
| 30                | 132            | 8.3216e+003                                | 20.3225                     | 0.0833                  | 0.007000      | 0.009000 |
| 35                | 137            | 1.2115e+004                                | 16.4867                     | -0.0437                 | 0.007300      | 0.009000 |
| 40                | 142            | 12849                                      | 16.1365                     | -0.0720                 | 0.008000      | 0.009000 |
| 50                | 255            | 1.0414e+004                                | 17.5979                     | -0.0155                 | 0.009000      | 0.009000 |
| 60                | 255            | 7.6702e+003                                | 21.2168                     | 0.2447                  | 0.010000      | 0.009000 |

Average 0.0052
Average throughput (byte per second) 5279.7

is 0.0060, and the average throughput is 5833.3 (byte per second).

Different random message blocks was used as an image_key. Table 4 shows the experimental results when image 2 is used as an image_key. The results of PSNR, MSE and CC listed in the table are between the original message and the encrypted one, but these value between the original message and the decrypted one were MSE=0, PSNR = infinite, and CC=1.

Furthermore, Table 4 shows that the proposed method provides excellent values of the quality parameters, i.e., MSE, PSNR and CC. Table 4 also reports that the proposed method gives a high and acceptable throughput value. The Average estimated time is 0.0052 and the Average throughput is 5279.7.

Considering the results shown in Tables 3 and 4, we notice the following important facts:

1) The block size of an image can range from 1 to 60. In our experiments, the limitation of the block size of an image is due to the MATLAB.

2) In general, increasing the size of an image_key will increase the encryption/decryption time. In the proposed method, the encryption time for the large images is still acceptable and the method remain efficient. Therefore, it is safe to select an image with any size and get a high value of throughput.

3) According to the results shown in Figures 10 and 11, there is a best block size selection that the method achieves best throughput value. That size is 20 bytes.

The standard methods of message cryptography are also implemented using various methods or algorithms. Table 5 summarizes the results of different algorithms compared to the proposed method:

The Speedup of the proposed method is the ratio of TP of the proposed method and TP of other methods. Table 5 shows that the proposed method is more efficient and has a significant speedup comparing to the other standard methods of data cryptography. The image shown in figure 12 was selected as an image_key, several messages were encrypted-decrypted using block size=50, table 6 shows the obtained results:

Clearly, the obtained average throughput and speedup were like (1856.4) and (1.8129 M byte per second) for encryption and decryption processes respectively. The average speedup The obtained throughput also better than those obtained in the studies [38], [39]. Here we must select a block size with
TABLE 5: Efficiency comparisons

| Method  | Average throughput (TP) | Speedup of the proposed method |
|---------|-------------------------|-------------------------------|
| DES     | 1336.3                  | 3.8927                        |
| 3DES    | 1179.7                  | 4.4755                        |
| AES     | 1465.4                  | 3.6029                        |
| BF      | 2453.7                  | 2.1517                        |
| Proposed method | 5279.7                  | 1.0000                        |

Speedup of the proposed method = TP of the proposed method / TP of other method

TABLE 6: Results of various messages cryptography

| Text file size(KB) | Encryption time(second) | Decryption time (second) | ETP (KB/second) | DTP (KB/second) |
|--------------------|-------------------------|--------------------------|----------------|-----------------|
| 1                  | 0.0090                  | 0.0090                   | 111.1111        | 111.1111        |
| 20                 | 0.0150                  | 0.0150                   | 1333.3          | 1333.3          |
| 100                | 0.0310                  | 0.0310                   | 3225.8          | 3225.8          |
| 200                | 0.0700                  | 0.0700                   | 2857.1          | 2857.1          |
| 300                | 0.1340                  | 0.1340                   | 2238.8          | 2238.8          |
| 400                | 0.2310                  | 0.2310                   | 1731.6          | 1731.6          |
| 500                | 0.3340                  | 0.3340                   | 1497.0          | 1497.0          |

Average throughput 1856.4 1856.4
Average throughput 1.8129 M byte per second 1.8129 M byte per second

FIGURE 10: Block size vs encryption time

FIGURE 11: Block size vs throughput

FIGURE 12: Selected image_key

bigger size to process an image with huge size.

V. CONCLUSION

In this article, we have proposed a method for secret message cryptography. It has been shown that the method is very secure and provides a high degree of protection in a way that making the process of hacking secret messages is very difficult. The method uses a secret image_key to generate a PK that is needed to extract BRV. The extracted BRV will then be used to calculate the RLD for each block. The key is changeable and depends on the size of a message block and on the selected image_key. The image_key must be kept in secret by the message sender and receiver. It can be replaced at any time when needed by another image without any method modification. The proposed method has no constraints on the selected image_key, i.e., the image...
key can be any image with any type and size. Although increasing the size of an image will increase the encryption time, the proposed method will remain efficient for large size of images. The message is divided into blocks. The size of blocks is varied between 1 to 60. In our experiments, each size has been examined and all the obtained results are acceptable. Furthermore, a maximum throughput value has been achieved when the block size is equal to 20 bytes. The obtained experiment results have shown that the proposed method provides excellent values of the quality parameters, i.e., MSE, PSN, and CC, and so it satisfies the requirements of good cryptography. The proposed method is very efficient and provides good values of encryption (decryption) time. The proposed method has been compared with standard methods of message cryptography. The experimental results have shown that the proposed method outperforms the standard methods and has a significant speedup.

REFERENCES

[1] W. H. Jeong, B.-G. Yeo, K.-H. Kim, S.-H. Park, S.-W. Yang, J.-S. Lim, and K.-S. Kim, “Performance analysis of the encryption algorithms in a satellite communication network based on h-arq.” The Journal of the Institute of Internet, Broadcasting and Communication, vol. 15, no. 1, pp. 45–52, 2015.

[2] Y. Zhang, D. Zheng, Q. Li, J. Li, and H. Li, “Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing,” Security and Communication Networks, vol. 9, no. 16, pp. 3688–3702, 2016.

[3] C.-K. Ke and Z.-H. Lin, “An optimal mobile service for telecare data synchronization using a role-based access control model and mobile peer-to-peer technology,” Journal of medical systems, vol. 39, no. 9, pp. 1–11, 2015.

[4] Z. Cai, Z. Xiong, H. Xu, P. Wang, W. Li, and Y. Pan, “Generative adversarial networks: A survey toward private and secure applications,” ACM Computing Surveys (CSUR), vol. 54, no. 6, pp. 1–38, 2021.

[5] B. A. Mahafzah and I. O. Al-Zoubi, “Broadcast communication operations for hyper hexa-cell interconnection network,” Telecommunication Systems, vol. 67, no. 1, pp. 73–93, 2018.

[6] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, “Vipi: visualization of parallel matrix multiplication algorithms,” Journal of Computing Sciences in Colleges, vol. 33, no. 1, pp. 24–31, 2017.

[7] A. M. Mandal, C. Parakash, and A. Tiwari, “Performance evaluation of cryptographic algorithms: Des and aes,” in 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science. IEEE, 2012, pp. 1–5.

[8] R. Singh, S. Singh, and K. Chandra, “A secure cryptographic scheme for audio signals,” in 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science. IEEE, 2012, pp. 1–5.

[9] S. K. Apoorva, “Comparative study of different symmetric key cryptography algorithms: Des and aes,” in 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science. IEEE, 2012, pp. 1–5.

[10] B. A. Mahafzah and I. O. Al-Zoubi, “Broadcast communication operations for hyper hexa-cell interconnection network,” Telecommunication Systems, vol. 67, no. 1, pp. 73–93, 2018.

[11] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, “Vipi: visualization of parallel matrix multiplication algorithms,” Journal of Computing Sciences in Colleges, vol. 33, no. 1, pp. 24–31, 2017.

[12] A. M. Mandal, C. Parakash, and A. Tiwari, “Performance evaluation of symmetric encryption algorithms,” IJCNS International Journal of Computer Science and Network Security, vol. 8, no. 12, pp. 280–286, 2008.

[13] S. S. Afzal, S. A. Shafique, and M. U. Rehman, “A proposed framework for secure data communication,” International Journal on Computer Science and Engineering & Management (IJAIEM), vol. 2, no. 7, pp. 10–15, 2013.

[14] Y. K. Apoorva, “Comparative study of different symmetric key cryptography algorithms,” International Journal of Application or Innovation in Engineering & Management (IJAEM), vol. 2, no. 7, pp. 10–15, 2013.

[15] H. Kader and M. Hadhoud, “Performance evaluation of symmetric encryption algorithms,” International journal of emerging technology and advanced engineering, vol. 1, no. 2, pp. 15–50, 2011.

[16] P. P. Santoso, E. Rilvani, A. B. Trisnawan, K. Adiyarta, D. Napitupulu, and T. Sutabri, “Systematic literature review: comparison study of symmetric key cryptographic algorithms on fpga,” in 2022 4th International Conference on Smart Systems and Inventive Technology (ICSIT). IEEE, 2022, pp. 293–300.

[17] R. Anusha, N. Shankari, V. S. Shetty, and S. Bhat, “Analysis and comparative study of different symmetric key cryptography algorithms,” in IOP Conference Series: Materials Science and Engineering, vol. 420, no. 1. IOP Publishing, 2018, p. 012111.

[18] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, “Comparative study of symmetric key and asymmetric key en-
encryption algorithms,” in 2017 international conference on engineering and technology (ICET). IEEE, 2017, pp. 1–7.

[38] R. A. Elmanfaloty and E. Abou-Bakr, “An image encryption scheme using a 1d chaotic double section skew tent map,” Complexity, vol. 2020, 2020.

[39] C. Vijayalakshmi, L. Lavanya, and C. Navya, “A hybrid encryption algorithm based on aes & rsa,” International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, no. 1, pp. 909–917, 2016.

MUAAD ABU-FARAJ received the B.Eng. degree in Computer Engineering from Mu’ta University, Mu’ta, 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, Associate Professor at The University of Jordan, Aqaba, Jordan. He is currently serving as 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).

ABEER AL-HYARI Abeer Al-Hayri is an assistant professor at the electrical engineering department at Al-Balqa Applied University, As Salt, Jordan. Abeer’s research involves cryptography, in addition to the application of machine learning, deep learning, recurrent neural networks to problems in FPGA CAD. Abeer received her Ph.D. degree in Computer Engineering from University of Guelph, Guelph, Canada.

KHALED ALDEBEI is an Assistant Professor at the Information Technology Department/The University of Jordan (Jordan). He received a Phd in computer science from the University of Technology Sydney, Australia. Aldebei has the higher degree by research publication award from the University of Technology Sydney. He has an Oracle Certified Associate (OCA) and Oracle Certified Professional (OCP). Aldebei worked in the computer centre at the University of Jordan as a computer programmer and system analysis. Then, Aldebei worked in the Faculty of Information Technology and Systems, University of Jordan, as a teaching assistant. Since 2018, Aldebei works in the same faculty as an assistant professor. Aldebei has many programming skills, e.g. Python, Oracle (Form and Report Builder), MATLAB and Database (SQL, PL-SQL). He has published many articles in high rank journals and international conferences. Currently he is the head of Information Technology and Computer Information Systems departments. His current research interests include machine learning, data mining, text processing and natural language processing.

BILAL AL-AHMAD received B.Sc. degree in computer information systems from Jordan University of Science Technology, Jordan, in 2006, M.Sc. degree in computer information systems from Yarmouk University, Jordan in 2009, PhD in software engineering from North Dakota State University, USA, in 2015. Currently, he is an assistant professor in Computer Information Systems department at The University of Jordan, Aqaba branch. His research interests include requirements engineering, software testing, software design, machine learning, and computer networks.

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 interests include signal processing, image processing, data security and parallel processing.