IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 November 2022, accepted 29 November 2022, date of publication 1 December 2022,
date of current version 7 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3226319

RESEARCH ARTICLE

CASDC: A Cryptographically Secure Data System Based on Two Private Key Images

MUA'AD ABU-FARAJ[1], (Member, IEEE), ABEER AL-HYARI[2], (Member, IEEE), ISMAIL AL-TAHARWA[1], BILAL AL-AHMAD[1], AND ZIAD ALQADI[3]

[1]Department of Computer Information Systems, The University of Jordan, Aqaba 77110, Jordan
[2]Department of Electrical Engineering, Al-Balqa Applied University, As-Salt 19117, Jordan
[3]Department of Computers and Networks Engineering, Al-Balqa Applied University, Amman 15008, Jordan

Corresponding author: Mua'ad Abu-Faraj (m.abufaraj@ju.edu.jo)

ABSTRACT Colored digital images are one of the most important types of digital data to be used in many vital applications, which require a safe way to protect them from hacking operations and the danger of intruders and data thieves. This paper presents an effective and safe method for storing digitally colored images (CASDC). A high level of protection is provided through a complex secret key agreed upon between the sender and the receiver. The secret key consists of nine decimal digits (and can be increased as needed). These digits are processed to extract three values for each color of the three color channels. A left rotation process is performed for the value of each color to produce three new values, where an exclusion process is performed between them to obtain the encrypted value for the color. CASDC is evaluated against a wide range of images to calculate its throughput to show the extent to which this method fulfills encryption and decryption requirements. The Mean Square Error (MSE) values, Peak Signal Noise Ratio (PSNR), and Correlation Coefficient for the three primary channels of the RGB coloring system were analyzed. The practical results of the proposed method are compared with other standard methods such as Data Encryption Standard (DES), Tripple-DES (3DES), Advanced Encryption Standard (AES), and Blow Fish (BF). According to the obtained results, CASDC outperforms all standard methods in terms of efficiency by reducing the time of encryption and decryption and increasing the throughput of the corresponding process. Besides, CASDC is robust against breaks, as the attempts to break the private key will require hundreds of years in the best case.

INDEX TERMS Cryptography, PK, bit rotation, throughput, MSE, PSNR, CC, speedup.

I. INTRODUCTION

Colored digital images are one of the most widely used types of digital data through various social media platforms. This wide spread of digital images is due to several reasons, the most important reasons of which are [1], [2], [3], [4]:

- Ease of obtaining the digital image at a negligible cost due to the multiplicity of equipment through which images can be generated and the multiplicity of different sources available through the Internet.
- Ease of processing the digital image because the digital color image can be represented by a three-dimensional matrix (one dimension for each of the three color channels: red, green, and blue).
- The possibility of processing the matrix of each of the three colors separately.
- The use of digital color images in many critical vital applications.
- Ease of applying arithmetic and logical operations to digital color images and the matrix of each of the three colors. One of these operations is rotating to the left for a specified number of digits, as shown in Figure 1 [5], [6], [7], [8].

The colored digital image may be confidential or of a personal nature, or it may be carrying confidential data, which requires providing the necessary protection for it and preventing attempts to penetrate or eavesdrop on it, whether by

The associate editor coordinating the review of this manuscript and approving it for publication was Ramakrishnan Srinivasan.

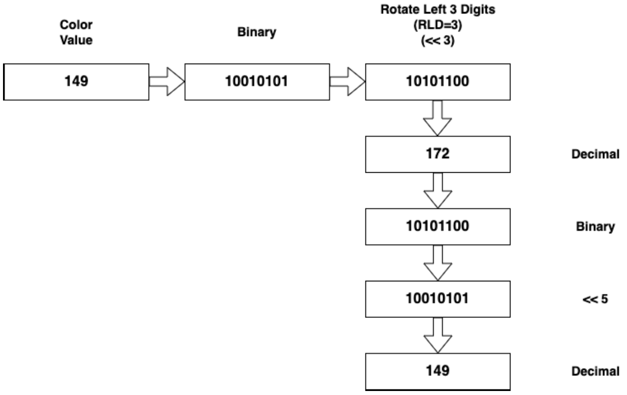


FIGURE 1. Rotation left operations.

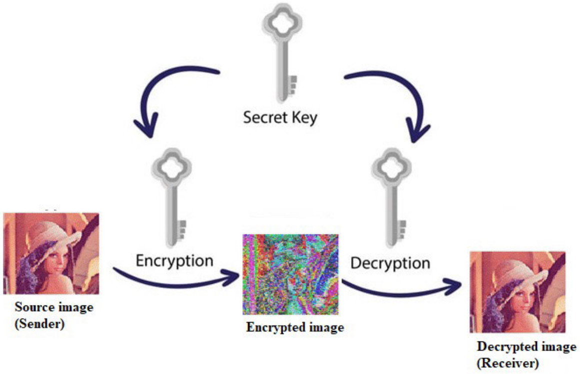


FIGURE 2. Process of image cryptography.

unauthorized parties or by data thieves [9], [10], [11], [12]. One of the essential methods used to protect the digital image is the data cryptography method, which means encrypting the image when sending and decrypting the image when it is received. As shown in Figure 2, data cryptography can be applied using a private secret key (PK) and performing operations to form encrypted and decrypted images. PK must be very complex in order to avoid hacking attempts. Also, it must be kept secret between the sender and receiver and should be updatable whenever a need arises [13], [14].

A good way of data encryption and decryption should destroy the data when the encryption becomes incomprehensible and useless, provided that the process of retrieval of the original data is done so that the decrypted data is precisely the same as the original data [15].

The quality of the data can be judged by using some recommended evaluation metrics, including Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Correlation Coefficient (CC) for the three color channels. These parameters can be calculated between two data sets using equations 1, 2, 3, and 4, as indicated in the studies [13], [15], [16]:

MSE of x channel:

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

where m is the number of rows in the cover image, n is the number of columns in the cover image, S_{ij} is the pixel value from the sent image, and R_{ij} is the pixel value from original image

Total MSE can be calculated as follows:

$$MSE_t = MSE_R + MSE_G + MSE_B \tag{2}$$

PSNR is calculated as follows:

$$PSNR = 10\log_{10}\frac{[MAX_I]^2}{MSE_t} \tag{3}$$

where MAX_I is the maximum signal value that exists in our original "known to be good" image

Correlation coefficient (CC) is calculated as follows:

$$CC = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{4}$$

where x_i is the value of the first message, $\bar{x}$ is the mean of x, y_i is the value of the second message, and $\bar{y}$ is the mean of y.

A positive correlation is measured on a 0.1 to 1.0 scale. The stronger the positive correlation, the more likely the two messages are very close. A weak positive correlation would be in the range of 0.1 to 0.3, a moderate positive correlation from 0.3 to 0.5, and a solid positive correlation from 0.5 to 1.0.

Here we have to remember the following:

- Decreasing PSNR will increase the distortion degree.
- Increasing MSE will increase the distortion degree.
- Decreasing correlations will increase the distortion degree.
- MSE between the source image and encrypted one must be very high.
- MSE between the source image and decrypted one must equal to zero.
- PSNR between the source image and encrypted one must be very Low.
- PSNR between the source image and decrypted one must equal to infinity.
- CC between the source image and encrypted one must be very low.
- CC between the source image and the decrypted one must equal one.

Colored digital images are considered one of the most widely used types of digital data due to their use in multiple vital applications. Therefore, the main objective of this research is to provide an easy-to-implement method to protect the digital image from the risk of penetration by using two secret keys that are difficult to penetrate. This method will be implemented using multiple images to prove its efficiency compared to the standard methods used in data encryption.

What is new in the proposed method is to raise the degree of protection for confidential digital images using a secret key that have the following characteristics:

- Ease of key generation.
- The generation process does not require large time or memory requirements.
- The PK will increase the key space, making the hacking attempt impossible.

The organization of this research paper is as follows: Section II presents related work. Section III demonstrates the proposed method. Implementation and experimental results are conducted in Section IV, followed by the conclusions in Section V.

II. RELATED WORKS

Image cryptology is the science that studies image cryptography and image cryptanalysis. Image cryptology conceptually resembles data cryptography. However, crucial differences exist due to the intrinsic characteristics of image format. While data is directly encrypted in either block or stream pattern, image encryption differs. Image is stored in a two-dimensional array in C_{ij} form, $1 \leq i \leq H$ and $1 \leq j \leq W$, such that H and W represent the height and the width of the image. C_{ij} represents the color intensity of the image pixel at position (i, j). Intensity depends on the coloring system in use. The grayscale coloring system uses 8 bits to encode an image's pixels, making cryptographic algorithms deal with $(8 \times H \times W)$ input. Similarly, the RGB coloring system uses three color channels (i.e., Red, green, and Blue) which make the cryptographic algorithm deal with $(3 \times 8 \times H \times W)$ input [17].

The nature of images is different from regular data (e.g., system files, text messages, input fields in web pages). Images preserve relationships in bulks alongside multi-directions (i.e., horizontal, vertical, and diagonal). Moreover, the coloring system deals with more values than conventional alphabet encoding systems. All these complications bring extra challenges to image cryptography. Any cryptographic image algorithm should scramble intrinsic characteristics in all directions to encounter well-known attacks such as statistical and differential attacks [17], [18]. Additionally, it should maintain a trade-off between robustness and efficiency as image size may grow due to the improvement in the capturing devices and the use of real-time applications [19], [20].

Initial attempts to encrypt images resort to conventional data encryption techniques as they were the only available options. Those techniques include standard block ciphering techniques (e.g, *DES*, *Triple-DES*, *AES*, *BlowFish*) [21], [22], [23], [24], [25]. Also, stream cryptographic techniques (e.g., *Vigenere*, *RC4*) are used to encrypt images [26], [27]. Besides the high computation complexity, almost all conventional data encryption standards are weak against one or more types of image encryption attacks [28], [29], [30], [31]. Data Encryption Standard (*DES*) uses quite small key space (2^{56}), which makes it vulnerable to brute force attacks and known-plaintext cryptanalysis attacks [32], [33], [34]. *Blowfish*, another symmetric block cryptographic algorithm, utilizes variable-length keys, enabling it to encounter brute force attempts [35], [36], [37], [38], [39]. *Blowfish* is constrained to a limited range of applications due to the complexities of updating keys [17]. Advanced encryption standard (*AES*), the most commonly used encryption method today for data in transit [40], [41], appears to be vulnerable to statistical attacks such that cryptanalysis of the histogram, which opens a window for breaks [42], [43].

All algorithms mentioned above are defined according to multiple characteristics as follows as in [44], [45], and [46]:

- **Block size**: the data to be encrypted must be divided into equal blocks; block size is fixed.
- **Private key**: these methods use a fixed-length private key, and this key is used to generate other subkeys needed in the encryption process.
- **Efficiency**: these methods are used to protect short-length data, and they are effective, but when used to encrypt digital images, they become inefficient.
- **Quality of cryptography**: these methods provide good values for the quality parameters (MSE, PSNR, and CC) in both phases: the encryption and decryption phases as declared in the studies [14], [47], [48], [49], [50]
- **Confusion and Diffusion**: these methods alternate between diffusion and confusion to thwart cryptanalysis efforts as proposed by Claude Shannon [51], [52].
- **Rounds**: Different operation rounds are conducted to perform data cryptography.
- **Used data**: these methods deal with binary numbers; thus, the data to be encrypted must be converted to binary.
- **Simplicity**: It is easy to implement and modify.
- **Symmetry**: These methods are symmetric and use the same key in the encryption and decryption phases.
- **Level of protection**: Some of these methods can be hacked easily.

RC4 stream cryptographic algorithm approved to be vulnerable to differential attacks exploiting 2^{44} chosen plaintext. This is due to the key repetition inherited in the pseudo-random number generator utilized to synchronize key generation between sender and receiver [17].

Chaos-based cryptography algorithms emerged as the trending approach for image encryption [53], [54]. A wide range of variations and hybrid schemes was proposed to enhance its performance [55], [56], [57]. However, many studies advocate the superiority of chaos-based cryptography techniques in terms of robustness [17], [18], [58], [59], [60], [61], [62]. Many other researchers question these claims, raising efficiency and robustness concerns. In many cases, the simplicity of chaotic maps resulted in security breaks [63], [64]. Choosing a chaotic map remains a crucial aspect of any chaos-based cryptography scheme. Simple representations such as logistic maps and tent maps result in less complex and relatively faster schemes. However, such efficiency comes at the expense of robustness. In contrast, sophisticated chaotic maps improve security at the expense of time efficiency [17]. Murillo-Escobar et al. [65] proposed an integral analysis

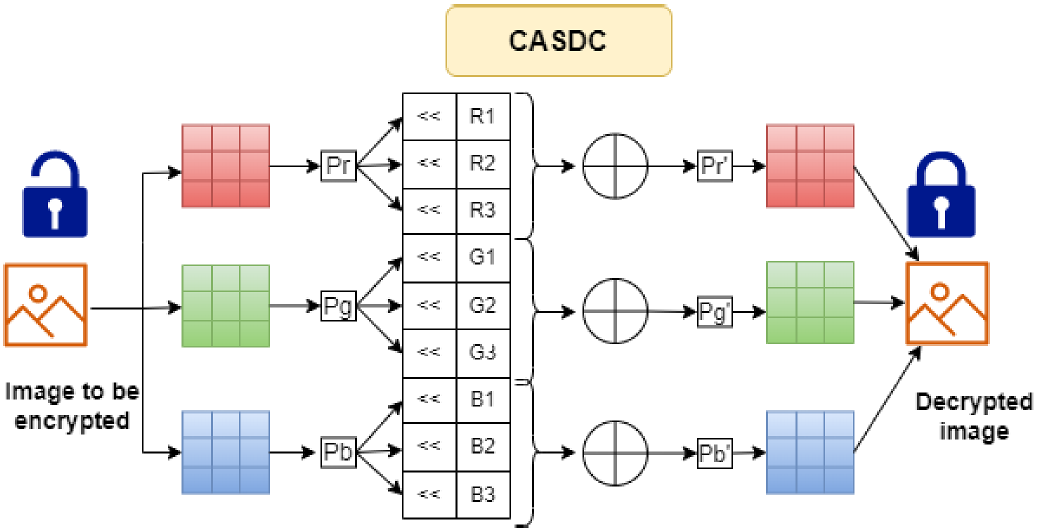


FIGURE 3. High-level Abstraction of CASDC cryptographic schema.

approach to analyze the robustness of chaos-based image cryptography approaches.

We are focusing only on the standard data cryptography methods, which is why we compare the results obtained by the proposed method, namely *CASDC*, with traditional methods' results. *CASDC* can encrypt-decrypt any colored image, including medical images; replacing the selected images for implementation with medical images is very easy and does not require any change in the proposed algorithm.

III. CASDC CRYPTOGRAPHIC SCHEME

CASDC is a novel, colored image encryption algorithm. It suits the RGB-coloring system. The key motive behind CASDC is to improve the efficiency of confidential colored image transmission among communication networks, e.g., social media, while maintaining the same levels of robustness similar to standard data encryption schemes. (i.e., DES, 3DES, AES, and BF). CASDC is based on rotation left and XORing operations. The encryption-decryption phases use two PKs to calculate the number of rotation left digits (RLD). RLDs are required to rotate the color value; this PK contains nine decimal digits, three digits for each color (R1, R2, and R3 for the red color, G1, G2, and G3 for the green color, and B1, B2, and B3 for the blue color), these parameters can be calculated from PK by applying remainder and modulus operations. The range of the PK is from (0 to 777777777) decimal, or from 0 to $2E5BF271$) hexadecimal, and this range will make the hacking process very difficult. The sequence of colors must be determined and agreed upon between the sender and the receiver. RGB coloring system has 6 different color combinations. Each combination will require 9 decimal digits to encrypt/decrypt the three coloring channels. The size of the key space will be calculated according to Equation 5.

$$Keyspace = 2^{(9\times 8\times 6)} = 2^{432} = 1.0 \times 10^{130} \tag{5}$$

The private key is agreed upon between the sender and the receiver. The PK is kept confidential, with the possibility of modifying it at any moment and when needed without modifying the proposed method. PK can be expanded to more than nine digits, adding extra time to the encryption-decryption processes. Figure 3 depicts a high-level abstraction of CASDC cryptographic schema. The colored image to be encrypted is split into three matrices, one for each color channel; red, green, and blue. Each pixel of these matrices then undergoes an RLD operation three times using three values of PK; the results of this operation are XORed to obtain a new value for the pixel, which will be padded to the color matrix in the decrypted image. Finally, the three new color matrices are combined to obtain the decrypted colored image.

As indicated in Figure 3, CASDC is a symmetric cryptographic schema, such that the same process can be used for both encryption and decryption phases. The only change is the used key. The agreed key is used in the encryption phase to encrypt the input image. However, in the decryption phase, the decryption key is derived at the recipient part according to Table 1. There are two approaches to implementing the calculation of the decryption key. Either by maintaining a lookup table matching values given Table 2. Alternatively, implement an inline process that calculates the decryption key on the fly. The process has to replace each digit in the key with the corresponding result of subtracting it out of eight. The newly resulted in nine digits number becomes the decryption key.

The key advantage of the symmetric design of CASDC schema is the simpler implementation, particularly for telecommunication devices. Both encryption and decryption phases may utilize the same process regardless of the implementation type (software vs. hardware). The same process used to encrypt images to be sent may be used for decrypting

TABLE 1. RLD for encryption-decryption.

Encryption RLD	Decryption RLD
1	7
2	6
3	5
4	4
5	3
6	2
7	1

TABLE 2. Calculated RLDs using PK = 345172463.

Color	Encryption		Decryption	
	RLD	PK_i	RLD	PK_i
Red	R1	3	R1	5
	R2	4	R2	4
	R3	5	R3	3
Green	G1	1	G1	7
	G2	7	G2	1
	G3	2	G3	6
Blue	B1	4	B1	4
	B2	6	B2	2
	B3	3	B3	5

```
Algorithm 1 Encryption Phase
Input: Source color image (S), PK
Output: Encrypted image (E)
  1. Get the image to be encrypted
  2. Extract each color matrix (R, G, and B)
  3. Get the PK
  4. Use PK to find the RLDs(R1, R2, R3, G1, G2, G3, B1, B2, and B3)
  for each pixel in each color matrix do
    i. Get A by rotating left the color byte value using the first associated RLD
    ii. Get B by rotating left the color byte value using the second associated RLD
    iii. Get C by rotating left the color byte value using the third associated RLD
    iv. Apply XORing of A, B, and C to get the encrypted color value
    5. Combine the obtained color matrices to form the encrypted color image (E).
  end for
```

received images. At the same time, such a character has a limited benefit for software implementation. It is greatly desirable when considering hardware implementation for limited resources devices such as devices utilized in the Internet of Things (IoT) and smart city applications. Encryption and decryption phases are best described in Algorithm 1 and Algorithm 2, respectively. Figure 4 and Figure 5 show the diagrams of encryption-decryption, while Figure 6 and Figure 7 illustrate an example of encrypting-decrypting a color value.

```
Algorithm 2 Decryption Phase
Input: Encrypted color image (E), PK
Output: Source color image (S)
  1. Get the encrypted image
  2. Extract each color matrix (R, G, and B)
  3. Get the PK
  4. Use PK to find the RLDs(R1, R2, R3, G1, G2, G3, B1, B2, and B3)
  for each pixel in each color matrix do
    i. Get A by rotating left the color byte value using the first associated (8-RLD)
    ii. Get B by rotating left the color byte value using the second associated( 8-RLD)
    iii. Get C by rotating left the color byte value using the third associated( 8-RLD)
    iv. Apply XORing of A, B, and C to get the encrypted color value
    5. Combine the obtained color matrices to form the decrypted color image.
  end for
```

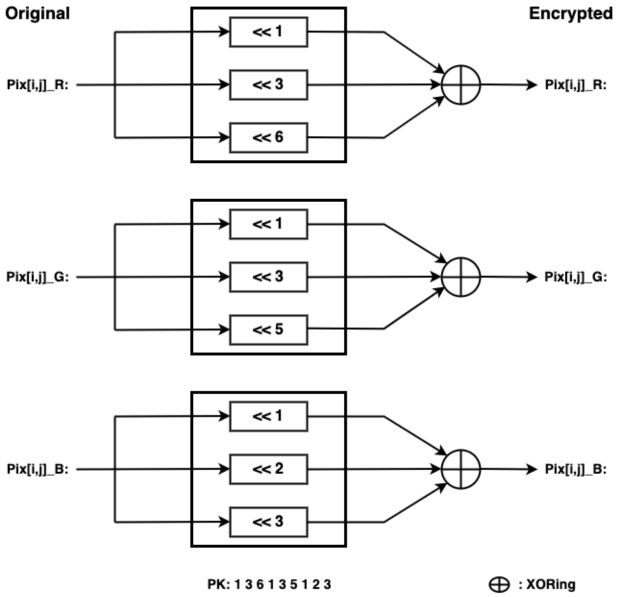


FIGURE 4. Encryption diagram.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The proposed method has been implemented using MATLAB on a computer with an i5 processor, a 2.4 GHz machine, and 8 G Bytes RAM. Multiple images of different sizes were used (up to 6 million bytes), and multiple keys were used to calculate all the values necessary to evaluate the performance and efficiency of the proposed method. Figure 8 depicts the image set used in the implementation, while Table 3 lists the basic information of the images.

As indicated in Table 3, the set of used images varies greatly in dimension and size. All images are colored,

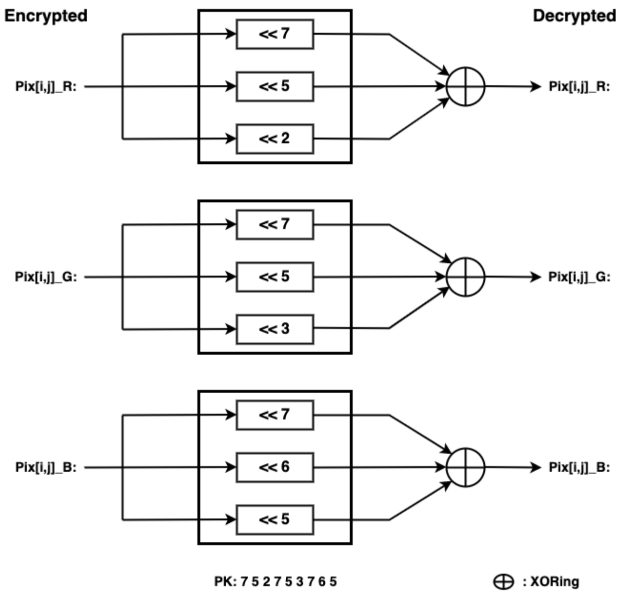


FIGURE 5. Decryption diagram.

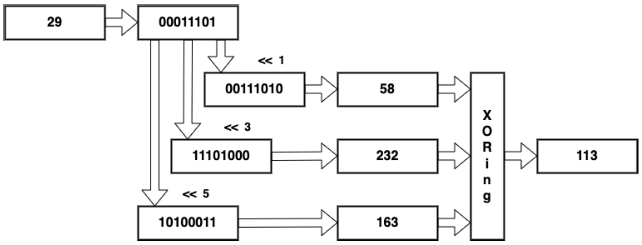


FIGURE 6. Encrypting the color value 29.

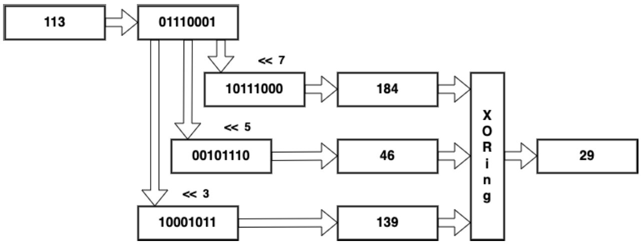


FIGURE 7. Decrypting the color value 113.

maintaining the same coloring system, which is the RGB-coloring system. The value 345172463 was selected as a PK. Encryption RLDs were calculated as illustrated in Table 2 ($R1 = 3$, $R2 = 4$, $R3 = 5$, $G1 = 1$, $G2 = 7$, $G3 = 2$, $B1 = 4$, $B2 = 6$, $B3 = 3$). Similarly, corresponding decryption RLDs were calculated ($R1 = 5$, $R2 = 4$, $R3 = 3$, $G1 = 7$, $G2 = 1$, $G3 = 6$, $B1 = 4$, $B2 = 2$, $B3 = 5$). Each image was encrypted-decrypted using this key; Figure 9 shows the characteristics of an input image. Figure 10 shows the result of the encryption phase. Plotted histograms provide concrete evidence that CASDC affects the three color channels equally.

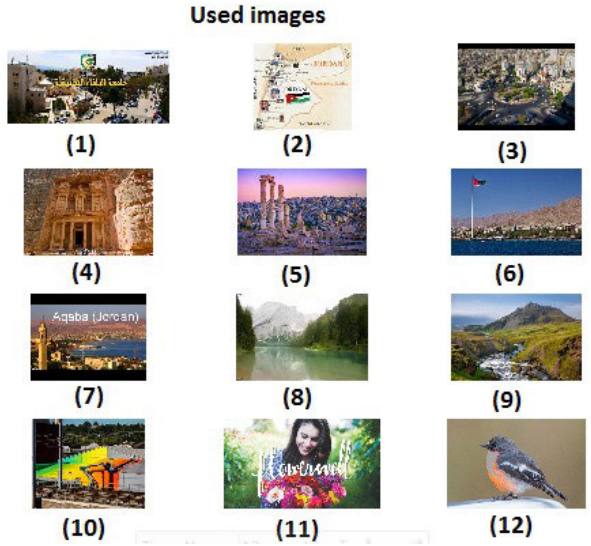


FIGURE 8. Set of used images.

TABLE 3. Selected used color images basic information.

Image #	Dimension	Size(byte)
1	151 × 333 × 3	150849
2	152 × 171 × 3	77976
3	360 × 480 × 3	518400
4	1071 × 1600 × 3	5140800
5	981 × 1470 × 3	4326210
6	165 × 247 × 3	122265
7	360 × 480 × 3	518400
8	183 × 275 × 3	150975
9	183 × 275 × 3	150975
10	201 × 251 × 3	151353
11	600 × 1050 × 3	1890000
12	1144 × 1783 × 3	6119256
Average size		1609800

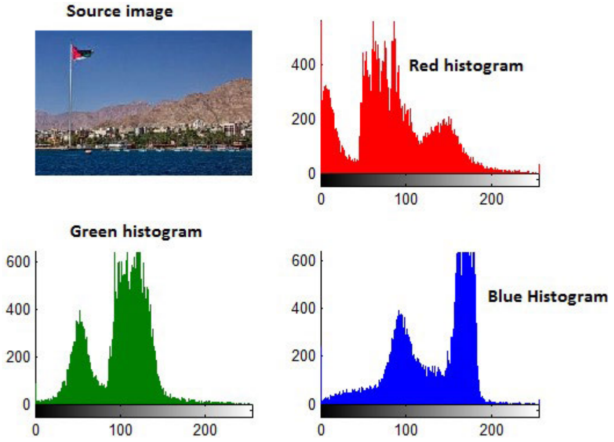


FIGURE 9. Sample output (image 6).

The key expected benefit of CASDC schema is to improve the efficiency of encryption-decryption operations.

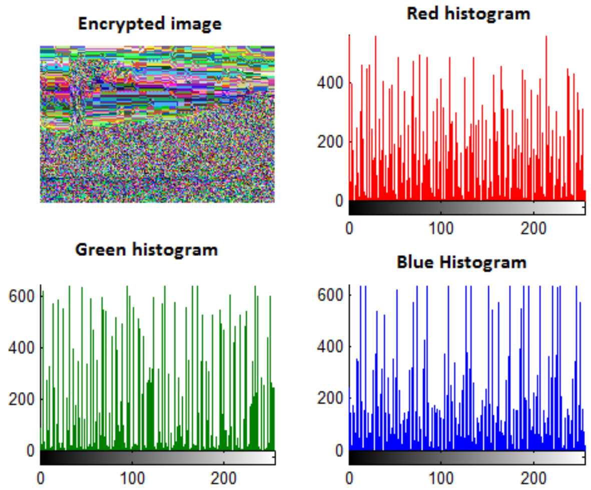


FIGURE 10. Encrypted image 6 using 345172463 as a PK.

TABLE 4. Efficiency parameters using 345172463 as a PK.

Image #	Encryption time (sec)	Throughput (bps)
1	46.1160	3271.1
2	24.0530	3241.8
3	158.8140	3264.2
4	1739.2	2955.9
5	1342.6	3222.4
6	36.7220	3329.5
7	159.7030	3246.0
8	45.7380	3300.9
9	46.2020	3267.7
10	46.4200	3260.5
11	582.4880	3244.7
12	1887.9	3241.3
Average	509.6630	3237.2
Hacking time	$\frac{509.6630\times 7^9}{(60\times 60\times 24\times 365.25)}$	$=$ 651.7207 years

The efficiency of the CASDC schema was studied in terms of encryption time and throughput. Encryption time is measured in seconds (sec), while throughput is measured in bytes per second (bps). Table 4 compares the set of used images, Figure 8, in terms of both metrics. Encryption time varies significantly, which is explainable due to the variation in image size. When considering the throughput metric, results are very close among all images, with average encryption throughput equivalent to 3237.2 bps.

Robustness remains the key requirement of any cryptographic schema. The robustness of the CASDC schema was investigated by studying its performance against *MSE*, *PSNR*, and *CC* metrics. *MSE*, *PSNR* were calculated to each image according to the equations 1, 2, and 3. *CC* was computed three times for each image, once for each color channel, according to the equation 4. Table 5 shows the obtained quality parameter results. All images attain extremely high values of *MSE* and *PSNR*, indicating irrelevance between plain and encrypted images. Similarly, *CC* values of the three color channels were too low for all images. This indicates no correlation between input images and corresponding encrypted images.

TABLE 5. Quality parameters using 345172463 as a PK.

Image #	MSE	PSNR	CCR	CCG	CCB
1	1.2491×10^4	16.4975	0.0420	−0.0893	0.1565
2	1.4158×10^4	15.2447	0.1136	0.0062	0.0518
3	8.9478×10^3	19.8337	0.2153	0.2155	0.1851
4	9.3165×10^3	19.4298	0.0067	0.0437	0.0583
5	9.5011×10^3	19.2337	−0.0090	0.0651	−0.0154
6	8.1434×10^3	20.7757	0.0640	0.0057	0.0518
7	6.9787×10^3	22.3190	0.4861	0.4571	0.4209
8	1.0074×10^4	18.6477	0.1809	−0.0354	0.1062
9	9.1269×10^3	19.6354	0.0100	−0.0065	0.0884
10	1.1056×10^4	17.7183	0.1010	0.0332	0.1431
11	1.0586×10^4	18.1527	0.0951	0.0955	0.1028
12	7.0456×10^3	22.2237	0.0351	0.0013	−0.0260

The MSE, PSNR, and CC values between the original images and the decrypted image were 0, infinite, and 1, respectively, which means that the original image was completely recovered and the decrypted image is identical to the source image.

From Tables 4 and 5 we can draw the following facts:

- The values of MSE were very high, meaning that the original image was fully destructed, and the proposed method meets the data encryption requirement.
- The values of PSNR were very low, meaning that the original image was fully destructed, and the proposed method meets the data encryption requirement.
- The values of CC were very low, meaning that the original image does not match the encrypted one, and it was fully destructed, and the proposed method meets the requirement of data encryption.
- The proposed method has good throughput, and the average throughput was equal to 3237.2 byte per second.
- The encryption time will increase when increasing the image size, and there is a linear relationship between the image size and the encryption (decryption) time; see Figure 11.
- A regression analysis was implemented between the image size and the encryption time, and equation 6 shows the relationship between them:

$$tt = -3.3933 + 0.0003 \times IS \tag{6}$$

where *tt* is the total time of the encryption process, and *IS* is the image size. From equation 6, we can see that the time complexity of the proposed method is $O(N)$, where N is the image size.

In addition to the facts mentioned above, it is challenging to hack the PK; below is the hacking time calculation in the best case:

Average penetration (hacking) time per attempt = 509.6630 sec.

Total number of attempts = 7^9 = 40353607.

Hacking time (best case) = (40353607 × 509.6630) sec.

= (40353607 × 509.6630)/(60 × 60 × 24 × 365.25) years.

= 651.7207 years.

Thus the proposed method provides a high level of image protection, making the hacking process impossible.

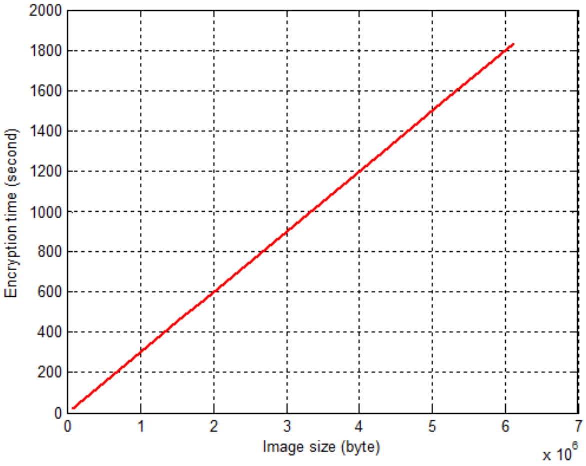


FIGURE 11. Image size vs encryption time.

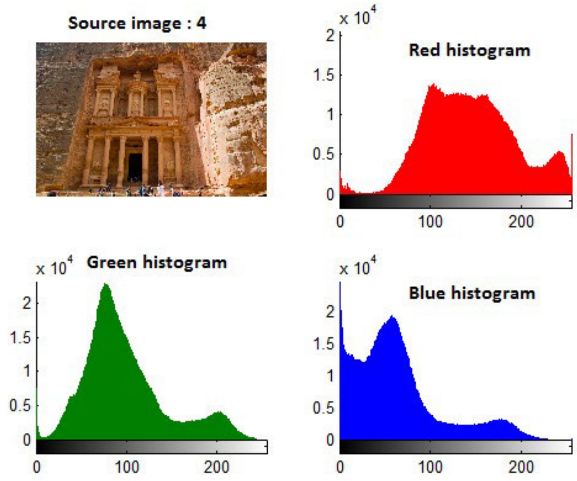


FIGURE 12. Source image 4.

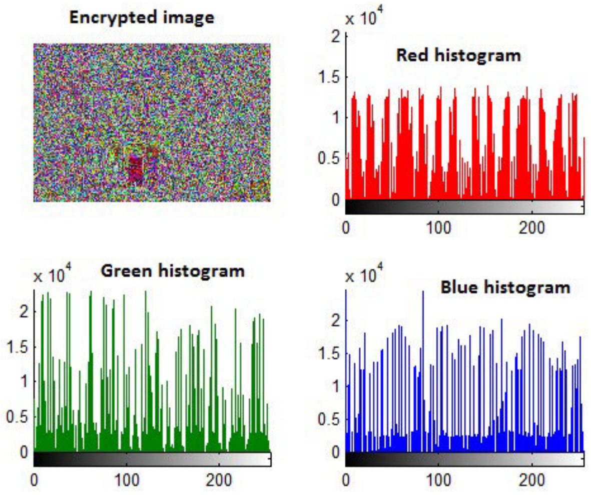


FIGURE 13. Encrypted image 4 using PK=725134264.

TABLE 6. Efficiency parameters using 725134264 as a PK.

Image #	Encryption time (sec)	Throughput (bps)
1	46.8530	3219.6
2	23.5840	3306.3
3	155.5200	3333.3
4	1667.2	3083.4
5	1353.3	3196.7
6	40.8430	2993.5
7	158.3920	3272.9
8	45.1660	3342.7
9	45.1340	3345.0
10	45.7800	3306.1
11	566.1710	3338.2
12	2002.5	3055.8
Average	512.5369	3232.792

TABLE 7. Quality parameters using 725134264 as a PK.

Image #	MSE	PSNR	CCR	CCG	CCB
1	1.2781×10^4	16.2679	0.0266	−0.0707	0.1359
2	1.5849×10^4	14.1164	0.0442	−0.0802	0.0375
3	8.9635×10^3	19.8161	0.2059	0.2167	0.1968
4	9.2483×10^3	19.5033	0.0083	0.0297	0.0593
5	9.3886×10^3	19.3528	0.0061	0.0542	−0.0089
6	8.4036×10^3	20.4612	0.0797	−0.0638	0.0113
7	6.9726×10^3	22.3279	0.4268	0.5265	0.3977
8	9.9814×10^3	18.7405	−0.0574	0.2703	0.1233
9	9.1895×10^3	19.5671	0.0035	0.0060	0.0548
10	1.1198×10^4	17.5906	0.0822	0.0865	0.1380
11	1.0647×10^4	18.0952	0.0603	0.0998	0.1083
12	6.7064×10^3	22.7171	0.0110	−0.0303	−0.0382

The same images were encrypted and decrypted using another PK with a value of 725134264. Figure 12 and Figure 13 show sample outputs, while Tables 6 and 7 show the obtained experimental results.

From the results shown in Tables 4, 5, 6, and 7, we can see that when using another PK, the proposed method keeps the efficiency and quality parameters excellent and acceptable.

For comparisons purposes, the standard methods of data cryptography methods (DES, 3DES, AES, and BF) were tested using the same images; Table 8 lists the encryption time for each image in the used dataset in addition to the throughput for each of the standard methods.

Table 9 summarizes the throughput for the standard and proposed methods. Here we can see that the proposed method drastically decreases the encryption time (thus increases the cryptography throughput significantly), and the proposed method has a significant speedup compared with other methods that reach up to 8.41, as shown in Table 10. Speedup is calculated by dividing the proposed method's throughput by any targeting method's throughput (e.g., DES, 3DES, AES, and BF). Equation 7 illustrates the computation of the speed up.

$$Speedup = \frac{Throughput_{technique_i}}{Throughput_{technique_j}} \tag{7}$$

where $technique_i$ refers to the considered technique, and $technique_j$ to the target technique to compare with.

TABLE 8. Standard methods of data cryptography encryption time and throughput.

	Encryption time (sec)			
Image #	DES	3DES	AES	BF
1	172.4	512	302	142.6
2	90.2	263	154	72.3
3	601.3	1772	1051	500.1
4	601.26	1750.5	10460	495.22
5	5051.9	14716	8801	4165.9
6	143.0	409	243	112.0
7	603.3	1765	1046	500.1
8	171.6	514	307	142.7
9	172.6	515	307	142.7
10	176.0	515	308	141.1
11	2208.5	6471	3839	1804.3
12	7147.0	20946	12453	5816.6
Average encryption time (sec)	1428.3	41790	3272.6	1169.6
Average throughput (bps)	1127.1	385	491.9	1376.4

TABLE 9. Throughput summary.

Method	Average Encryption Time (sec)	Average throughput
DES	1428.3	1127.1
3DES	41790	385
AES	3272.6	491.9
BF	1169.6	1376.4
Proposed	509.6630	3237.2

TABLE 10. Speedup calculations.

Method	DES	3DES	AES	BF	Proposed
DES	1.0000	2.9275	2.2913	0.8189	0.3482
3DES	0.3416	1.0000	0.7827	0.2797	0.1189
AES	0.4364	1.2777	1.0000	0.3574	0.1520
BF	1.2212	3.5751	2.7981	1.0000	0.4252
Proposed	2.8721	8.4083	6.5810	2.3519	1.0000

V. CONCLUSION

A secure method has been proposed to protect color digital images from unauthorized users, intruders, and data thieves. The high degree of digital image security was achieved through a special key that was used to generate three values for each of the three color channels. These values of the private key are used to determine the RLDs for each color and were used to produce three values that are the product of the left rotation process for the color value and a specified number of digits. The resulting three values were XORed to get the encrypted pixel.

The proposed method minimized the encryption and decryption time, the results of the proposed method were compared with the results of standard methods of data cryptography, and it was shown that the proposed method has a significant speedup. Thus it maximizes the cryptography process throughput.

Furthermore, it was shown that there is a linear relationship between the image size and the encryption time; the time complexity of the proposed method is $O(N)$. The proposed method was tested using various color images and PKs, and the obtained experimental results showed that the proposed method provided good MSE, PSNR, and CC; thus, it satisfied the requirements of robust and secure cryptography.

REFERENCES

[1] R. Tripathi and S. Agrawal, "Comparative study of symmetric and asymmetric cryptography techniques," *Int. J. Advance Found. Res. Comput.*, vol. 1, no. 6, pp. 68–76, 2014.

[2] A. Shetty, K. Shravya, and K. Krithika, "A review on asymmetric cryptography—RSA and ElGamal algorithm," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 2, no. 5, pp. 98–105, 2014.

[3] W. C. Alisawi, Z. C. Oleiwi, W. A. Alawsi, A. S. Alfoudi, and N. K. Hadi, "Improvement of classical cipher algorithm based on a new model of timed-released encryption," *Int. J. Appl. Eng. Res.*, vol. 14, no. 16, pp. 3531–3536, 2019.

[4] Q. Zhang, L. T. Yang, Z. Chen, and P. Li, "High-order possibilistic c-means algorithms based on tensor decompositions for big data in IoT," *Inf. Fusion*, vol. 39, pp. 72–80, Jan. 2018.

[5] P. Li, Z. Chen, L. T. Yang, L. Zhao, and Q. Zhang, "A privacy-preserving high-order neuro-fuzzy c-means algorithm with cloud computing," *Neurocomputing*, vol. 256, pp. 82–89, Sep. 2017.

[6] S. Yin and J. Liu, "A k-means approach for map-reduce model and social network privacy protection," *J. Inf. Hiding Multim. Signal Process.*, vol. 7, no. 6, pp. 1215–1221, 2016.

[7] L. Meng, S. Yin, C. Zhao, H. Li, and Y. Sun, "An improved image encryption algorithm based on chaotic mapping and discrete wavelet transform domain," *Int. J. Netw. Secur.*, vol. 22, no. 1, pp. 155–160, 2020.

[8] L. Teng, H. Li, J. Liu, and S. Yin, "An efficient and secure cipher-text retrieval scheme based on mixed homomorphic encryption and multi-attribute sorting method," *Int. J. Netw. Secur.*, vol. 20, no. 5, pp. 872–878, 2018.

[9] B. Karthikeyan, T. Sasikala, and S. B. Priya, "Key exchange techniques based on secured energy efficiency in mobile cloud computing," *Appl. Math. Inf. Sci.*, vol. 13, no. 6, pp. 1039–1045, 2019.

[10] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system," *Future Gener. Comput. Syst.*, vol. 108, pp. 1287–1296, Jul. 2020.

[11] K. Haseeb, A. Almogren, I. Ud Din, N. Islam, and A. Altameem, "SASC: Secure and authentication-based sensor cloud architecture for intelligent Internet of Things," *Sensors*, vol. 20, no. 9, p. 2468, 2020.

[12] Y. Qin, Z. Wang, H. Wang, Q. Gong, and N. Zhou, "Robust information encryption diffractive-imaging-based scheme with special phase retrieval algorithm for a customized data container," *Opt. Lasers Eng.*, vol. 105, pp. 118–124, Jun. 2018.

[13] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A complex matrix private key to enhance the security level of image cryptography," *Symmetry*, vol. 14, no. 4, p. 664, Mar. 2022.

[14] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. A. Alqadi, and B. Al-Ahmad, "Rotation left digits to enhance the security level of message blocks cryptography," *IEEE Access*, vol. 10, pp. 69388–69397, 2022.

[15] M. M. Abu-Faraj, K. Aldebei, and Z. A. Alqadi, "Simple, efficient, highly secure, and multiple purposed method on data cryptography," *Traitement du Signal*, vol. 39, no. 1, pp. 173–178, Feb. 2022.

[16] M. Abu-Faraj and Z. A. Alqadi, "Rounds reduction and blocks controlling to enhance the performance of standard method of data cryptography," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 12, pp. 648–656, 2021.

[17] M. Kumari, S. Gupta, and P. Sardana, "A survey of image encryption algorithms," *3D Res.*, vol. 8, no. 4, pp. 1–35, Dec. 2017.

[18] Q. H. Makki, A. M. Abdalla, and A. A. Tamimi, "A survey of image encryption algorithms," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 598–602.

[19] M. O. Al-Dwairi, A. Y. Hendi, and Z. A. AlQadi, "An efficient and highly secure technique to encrypt and decrypt color images," *Eng., Technol. Appl. Sci. Res.*, vol. 9, no. 3, pp. 4165–4168, Jun. 2019.

[20] M. Van Droogenbroeck, "Partial encryption of images for real-time applications," in *Proc. 4th IEEE Signal Process. Symp.*, Apr. 2004, pp. 11–15.

[21] D. S. A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Performance evaluation of symmetric encryption algorithms," *Int. J. Comput. Sci. Netw. Secur.*, vol. 8, no. 12, pp. 280–286, 2008.

[22] W. Stallings, *Cryptography and Network Security, 4/E*. London, U.K.: Pearson Education India, 2006.

[23] S. P. Singh and R. Maini, "Comparison of data encryption algorithms," *Int. J. Comput. Sci. Commun.*, vol. 2, no. 1, pp. 125–127, 2011.

[24] G. Singh, A. Kumar, and K. Sandha, "A study of new trends in blowfish algorithm," *Int. J. Eng. Res. Appl.*, vol. 1, no. 2, pp. 321–326, 2011.

[25] M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *Int. J. Comput. Sci. Eng.*, vol. 4, no. 5, p. 877, 2012.

[26] Q.-A. Kester, "A hybrid cryptosystem based on Vigenere cipher and columnar transposition cipher," 2013, *arXiv:1307.7786*.

[27] A. Mousa and A. Hamad, "Evaluation of the RC4 algorithm for data encryption," *Int. J. Comput. Sci. Appl.*, vol. 3, no. 2, pp. 44–56, 2006.

[28] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, pp. 749–761, Jul. 2004.

[29] P. P. Dang and P. M. Chau, "Image encryption for secure internet multimedia applications," *IEEE Trans. Consum. Electron.*, vol. 46, no. 3, pp. 395–403, Aug. 2000.

[30] M. Younes and A. Jantan, "Image encryption using block-based transformation algorithm," *Int. J. Comput. Sci.*, vol. 35, pp. 407–415, Jan. 2008.

[31] Z. Yun-Peng, L. Wei, C. Shui-Ping, Z. Zheng-Jun, N. Xuan, and D. Wei-Di, "Digital image encryption algorithm based on chaos and improved DES," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, Oct. 2009, pp. 474–479.

[32] M. Matsui, "The first experimental cryptanalysis of the data encryption standard," in *Advances in Cryptology—CRYPTO*, Y. G. Desmedt, Ed. Berlin, Germany: Springer, 1994, pp. 1–11.

[33] S. M. Seth and R. Mishra, "Comparative analysis of encryption algorithms for data communication," *Int. J. Comput. Sci. Technol.*, vol. 2, no. 2, pp. 1–3, Jul. 2011.

[34] P. C. Mandal, "Superiority of blowfish algorithm," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 2, no. 9, pp. 196–201, 2012.

[35] H. Dibas and K. E. Sabri, "A comprehensive performance empirical study of the symmetric algorithms: AES, 3DES, Blowfish and Twofish," in *Proc. Int. Conf. Inf. Technol. (ICIT)*, Jul. 2021, pp. 344–349.

[36] M. A. Muin, M. A. Muin, A. Setyanto, Sudarmawan, and K. I. Santoso, "Performance comparison between AES256-Blowfish and Blowfish-AES256 combinations," in *Proc. 5th Int. Conf. Inf. Technol., Comput., Electr. Eng. (ICITACEE)*, Sep. 2018, pp. 137–141.

[37] K. Patel, "Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files," *Int. J. Inf. Technol.*, vol. 11, no. 4, pp. 813–819, Dec. 2019.

[38] M. Mahendra and P. S. Prabha, "Classification of security levels to enhance the data sharing transmissions using blowfish algorithm in comparison with data encryption standard," in *Proc. Int. Conf. Sustain. Comput. Data Commun. Syst. (ICSCDS)*, Apr. 2022, pp. 1154–1160.

[39] K. Logunleko, O. Adeniji, and A. Logunleko, "A comparative study of symmetric cryptography mechanism on DES AES and EB64 for information security," *Int. J. Sci. Res. Comput. Sci. Eng.*, vol. 8, no. 1, pp. 45–51, 2020.

[40] P. P. Santoso, E. Rilvani, A. B. Trisnawan, K. Adiyarta, D. Napitupulu, T. Sutabri, and R. Rahim, "Systematic literature review: Comparison study of symmetric key and asymmetric key algorithm," in *Proc. IOP Conf. Mater. Sci. Eng.*, vol. 420, no. 1. Bristol, U.K.: IOP Publishing, 2018, Art. no. 012111.

[41] M. Abu-Faraj and Z. Alqadi, "Improving the efficiency and scalability of standard methods for data cryptography," *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 12, pp. 451–458, 2021.

[42] K. Anuradha and P. Naik, "Medical image cryptanalysis using histogram matching bitplane and adjoin mapping algorithms," *Int. J. Mag. Eng., Technol., Manage. Res.*, vol. 2, pp. 100–105, Sep. 2015.

[43] V. Karuvandan, S. Chellamuthu, and S. S. Periyasamy, "Cryptanalysis of AES-128 and AES-256 block ciphers using Lorenz information measure," *Int. Arab J. Inf. Technol.*, vol. 13, no. 3, pp. 306–312, 2016.

[44] M. Abu-Faraj, Z. Alqadi, and M. Zubi, "Creating color image features based on morphology image processing," *Traitement du Signal*, vol. 39, no. 3, pp. 797–803, Jun. 2022.

[45] A. S. Alshammari, "Comparison of a chaotic cryptosystem with other cryptography systems," *Eng., Technol. Appl. Sci. Res.*, vol. 10, no. 5, pp. 6187–6190, Oct. 2020.

[46] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric encryption algorithms: Review and evaluation study," *Int. J. Commun. Netw. Inf. Secur.*, vol. 12, no. 2, pp. 256–272, 2020.

[47] K. S. Varkuti and P. Benakop, "VLSI design flow for secure integrated circuits based on DES, TDES, AES and blowfish algorithms and their performance," *Int. J. Eng. Technol.*, vol. 7, nos. 2–16, pp. 94–97, 2018.

[48] J. Agarwal, M. Kumar, and A. K. Srivastava, "Estimation of various parameters for AES, DES, and RSA," in *Emerging Technologies in Data Mining and Information Security*. Singapore: Springer, 2021, pp. 275–283.

[49] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *Int. J. Sci. Res. Publications*, vol. 8, no. 7, pp. 495–516, Jul. 2018.

[50] R. Verma and A. K. Sharma, "Simulation-based comparative analysis of symmetric algorithms," *Int. J. Adv. Res. Comput. Sci.*, vol. 11, no. 5, pp. 64–69, Oct. 2020.

[51] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12452–12466, 2020.

[52] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[53] I. S. Sam, P. Devaraj, and R. Bhuvaneswaran, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 1995–2007, 2012.

[54] M. François, T. Grosges, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," *Signal Process., Image Commun.*, vol. 27, no. 3, pp. 249–259, Mar. 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0923596511001354

[55] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "A novel image cipher based on mixed transformed logistic maps," *Multimedia Tools Appl.*, vol. 56, no. 2, pp. 315–330, Jan. 2012.

[56] G. Hanchinamani and L. Kulkarni, "An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher," *3D Res.*, vol. 6, no. 3, pp. 1–15, Sep. 2015.

[57] R. Bansal, S. Gupta, and G. Sharma, "An innovative image encryption scheme based on chaotic map and Vigenère scheme," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16529–16562, Aug. 2017.

[58] P. Kumari and K. Jain, "A survey on image encryption schemes," *Int. J. Innov. Eng. Res. Technol.*, vol. 4, pp. 73–77, Dec. 2017.

[59] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of 'an improvement over an image encryption method based on total shuffling,'" *Opt. Commun.*, vol. 350, pp. 77–82, Sep. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0030401815002801

[60] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method," in *Proc. IEEE Int. Symp. Circuits Syst.*, vol. 2, May 2002, pp. 708–711.

[61] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006, doi: 10.1142/S0218127406015970.

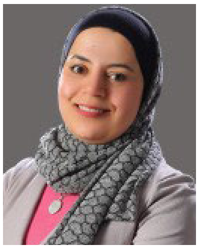
[62] E. Solak, C. Çokal, O. Yildiz, and T. Biyikoğlu, "Cryptanalysis of Fridrich's chaotic image encryption," *Int. J. Bifurcation Chaos*, vol. 20, no. 5, pp. 1405–1413, 2010, doi: 10.1142/S0218127410026563.

[63] D. Arroyo, G. Alvarez, and V. Fernandez, "On the inadequacy of the logistic map for cryptographic applications," 2008, *arXiv:0805.4355*.

[64] C. Li, "Cracking a hierarchical chaotic image encryption algorithm based on permutation," *Signal Process.*, vol. 118, pp. 203–210, Jan. 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0165168415002431

[65] M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutiérrez, and C. Cruz-Hernández, "Suggested integral analysis for chaos-based image cryptosystems," *Entropy*, vol. 21, no. 8, p. 815, Aug. 2019. [Online]. Available: https://www.mdpi.com/1099-4300/21/8/815

MUA'AD ABU-FARAJ (Member, IEEE) 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, U.K., in 2005, and the M.Sc. and Ph.D. degrees in computer science and engineering from the University of Connecticut, Storrs, CT, USA, in 2012. He is currently an Associate Professor with The University of Jordan, Aqaba, Jordan. His research interests include computer architecture, reconfigurable hardware, image processing, cryptography, and wireless networking. He is a member of the Jordan Engineers Association (JEA).



ABEER AL-HYARI (Member, IEEE) received the Ph.D. degree in computer engineering from the University of Guelph, Guelph, Canada. She is currently an Assistant Professor with the Department of Electrical Engineering, Al-Balqa Applied University, As-Salt, Jordan. Her research interests include cryptography, in addition to the application of machine learning, deep learning, and recurrent neural networks to problems in FPGA CAD. She is a member of the Jordan Engineers Association (JEA).

ISMAIL AL-TAHARWA received the B.Sc. degree in computer science and its applications from The Hashemite University, Jordan, in 2005, the M.Sc. degree in computer science (emphasizes in AI techniques especially computational intelligence and evolutionary computations) from Al-Balqa Applied University, Jordan, in 2008, and the Ph.D. degree in computer science and information engineering (emphasized in machine learning techniques and information security) from the National Taiwan University of Science and Technology, Taiwan, in 2014. He is currently an Associate Professor with the Department of Computer Information Systems, The University of Jordan, Aqaba Campus.

BILAL AL-AHMAD received the B.Sc. degree in computer information systems from the Jordan University of Science Technology, Jordan, in 2006, the M.Sc. degree in computer information systems from Yarmouk University, Jordan, in 2009, and the Ph.D. degree in software engineering from North Dakota State University, USA, in 2015. He is currently an Assistant Professor with the Department of Computer Information Systems, The University of Jordan, Aqaba Branch. His research interests include requirements engineering, software testing, software design, machine learning, and computer networks.

ZIAD ALQADI received the B.E., M.E., and Dr.Eng. degrees from the Kiev Polytechnic Institute, in 1980, 1983, and 1986, respectively. Since 1986, he has been a Researcher with the Department of Electrical Engineering, Amman Applied College, where he has been an Assistant Professor, since 1991. He has been an Associate Professor at the Faculty of Engineering Technology, since 1996. He has been a Professor at Al-Balqa Applied University, since 2010. His research interests include signal processing, image processing, data security, and parallel processing.