Simplified and Effective Dual-Round Image Encryption Robust Technique

Mohamad Al-Laham
Department of Management Information Systems, Al-Balqa Applied University, Jordan
dr_laham@bau.edu.jo

Bilal Bataineh
Department of Computer Science
Jadara University, Jordan
b.bataineh@jadara.edu.jo

Ziad Alqadi
Department of Computer and Engineering
Al-Balqa Applied University, Jordan
dr.ziad.alqadi@bau.edu.jo

Abstract: *A simplified and efficient technique of cryptography of an image will be developed. The technique will utilize two simple rounds to apply image encryption and decryption, each round will be implemented by performing a simple rows shuffling and columns shuffling, eliminating the need for computational logical and arithmetic operations required for other techniques of image encryption. Our approach, while simplifying computational demands by eliminating complex arithmetic and logical operations, maintains robust security through the integration of dual Chaotic Logistic Map Models (CLMM) to generate highly sensitive indices keys. These indices keys control row and column shuffling, which provides a high degree of permutation and resists known-plaintext and cipher text-only attacks. The technique will require two secret indices keys, these keys will be variable in the length and the contents and they will depend on the image to be encrypted-decrypted, generation of these keys will be very easy and simple. The shuffling operations will be implemented using two secret indices keys, and by implementing couple of chaotic logistic map these keys will be produced using selected chaotic parameters values included in the private key. The technique uses a 256-bit private key, chaotic logistic maps, and high sensitivity to parameter variations to achieve "Very strong" key space entropy, with encryption throughput of 19,540 KB/s and robust performance across diverse image sizes. The generated decrypted image may become so sensitive to chosen of private key values, and any little variation in the private key through the decryption task, it will be showed as a hacking try. The proposed technique will be flexible, it will be used to process every image with any size (gray and/or color), and image changing will not require any updating in the decryption and encryption processes. The developed technique will be efficient; it will decrease both the encryption and decryption times, and lead to accelerate the image encryption process comparing with other techniques. The study systematically utilizes specific evaluation metrics to substantiate claims regarding the quality, security, and velocity of the proposed cryptographic technique. Quality is assessed by Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) metrics.*

Keywords: *Cryptography, plain image, cipher image, decrypted image, PK, indices key, CK, CLMM, rows shuffling, columns shuffling.*

Received September 01, 2024; accepted November 29, 2024
https://doi.org/10.34028/iajit/22/2/9

1. Introduction

Digital images are composed of pixels arranged in a 2D matrix for grayscale or 3D for color images, with grayscale values stored in a single byte and color images utilizing three bytes (red, green, and blue). These images are highly susceptible to unauthorized access, as they often contain confidential, private, or hidden data. Given the potential vulnerabilities in communication channels, robust protection mechanisms, such as image encryption, are necessary.

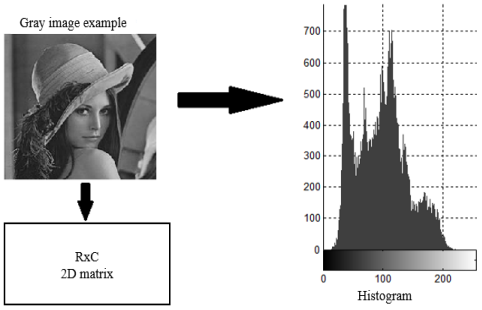


Figure 1. Presentation of gray image.

Digital image can be presented by the image itself, the decimal matrix and the histograms. The histogram is a 1D matrix with 256 elements, and each element value points to the count of repetition of each gray value (from 0 to 255). Figures 1, 2, and 3 show how digital images are presented [8]:

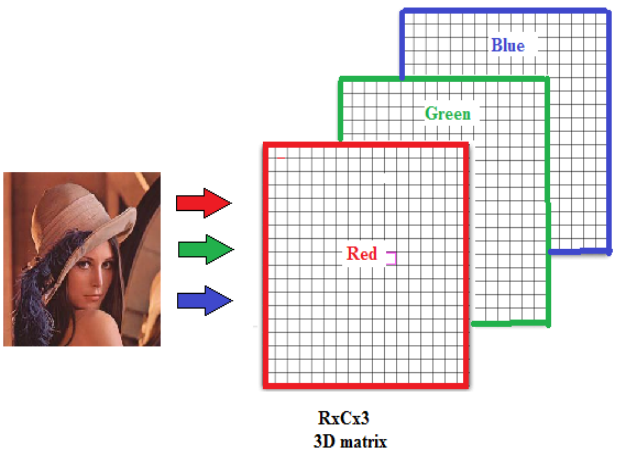


Figure 2. 3D matrix representation of color image.

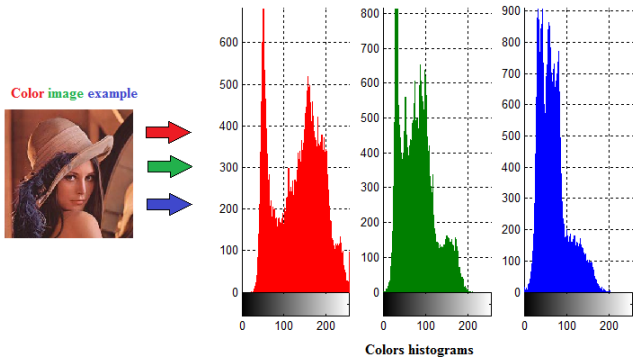


Figure 3. Colors image histograms presentation.

Digital images are utilized and circulated through communication environments widely, thus a protection is required by it to prevent hacking attacks for the following reasons [6]:

1) The image perhaps secret.
2) The image perhaps used as a hidden image and contain confidential information.
3) The image perhaps private.
4) The communication environments perhaps unsafe.

Image encryption transforms the source image into an encrypted version using a private key and encryption function, allowing secure transmission. Decryption reverses this process using the same key, recovering the original image. Effective cryptosystems for image encryption must meet several key requirements:

1) Encryption quality: the encrypted image should be significantly distorted, with high Mean Square Error (MSE) and low Peak Signal-to-Noise Ratio (PSNR) relative to the original.
2) Decryption quality: the decrypted image must match the source precisely, yielding an MSE of zero and an infinite PSNR.
3) Security: a strong encryption key with a large key space (over 128 bits of entropy) is essential.
4) Efficiency: minimizing encryption and decryption times, as well as maximizing throughput, is crucial for practical applications.
5) Simplicity and flexibility: simplified processes and compatibility with varied data types further enhance the system's applicability.

Various cryptographic techniques have been developed, including DES and AES, each with distinct attributes. However, these methods also exhibit limitations when applied to image data. Emerging approaches address these shortcomings through innovative mechanisms like chaotic maps, shuffling, and DNA encryption, achieving enhanced speed and security. Table 1 provides a comparative overview of standard encryption methods and improvements offered by recent innovations.

Table 1. Standard techniques, features and expected proposed enhancements.

Basis for comparison	**DES**	**AES**	**Proposed**
Data blocking	Yes	Yes	No
Block size	Fixed and equal 64 bits	Fixed and equal 128 or 192 or 256 bits	Image size
PK size	56 bits	128, or 192 or 256 bits	256 bits
Rounds	16	10, or 12 or 14	2
Principle	It works on Feistel Cipher structure	The substitution and permutation principles are used	Image rows and columns shuffling
Number of secret keys	16	10, 12, 14	2
Secret key length	Fixed	Fixed	Variable
Needs for computation: arithmetic and logic operations	Needs	Needs	No needs
Speed	Low	Moderate	High
Security	Not secure	Secure	Secure
Simplicity	Not simple	Not simple	Simple

Table 2. Introduced technique performance comparisons [4, 5, 12, 14, 26, 30].

Source reference technique	**Throughput (K bytes per second)**
Proposed by Kumara *et al*. [14] non-chaotic approach	170.3906
Proposed by Kumara *et al*. [14] Chaotic approach	141.2305
Proposed by Kumara *et al*. [14] Hyper Chaotic approach	636.3379
Proposed by Yepdia *et al*. [26]	888.8867
Proposed by Hua *et al*. [12]	638.4082
Proposed by Asgari-Chenaghlu *et al*. [4]	911.0352
Proposed by Chu and Zhang [5]	360.4102
Proposed by Zhenjun *et al*. [30]	384.9609

Many other techniques of image encryption were introduced, for instance, Yepdia *et al*. [26] developed a very fast and robust image encryption framework which based on the shuffling technique. Hua *et al*. [12] proposed a chaotic scheme based on cosine transform for image encryption, while Asgari-chenaghlu *et al*. [4] designed a new image encryption technique which based on dynamic function generation and polynomial combination of chaotic maps. In addition, Chu and Zhang [5] proposed a multi-image encryption algorithm which based on chaotic system and DNA encryption, whereas Zhenjun *et al*. [30] suggested multi-image encryption combined with bit-level decomposition in addition to chaotic maps. These techniques included high quality and different and extended data encryption speeds (see Table 2):

2. Literature Review

Image encryption techniques and techniques have subsequently evolved to reflect the essential need for secure data transmission and storage in the digital environment. This work presents several image encryption techniques focusing on chaotic frameworks, neural networks, and mathematical sciences.

Chaotic techniques in image encryption have received much attention due to their sensitivity to the underlying environment and pseudo-random behavior. Many research studies have presented chaotic techniques for image encryption. For example, [4] presented an improved 2D hyper-chaotic logistic sine map, in order to improve the results of existing 2D chaotic maps. Also, Wang *et al*. [24] presented a novel 2D absolute sine-cosine coupling technique in order to include more complex and better pseudo-random properties.

In addition, Fei *et al*. [9] proposed to couple a discrete sinusoidal memory resistor to a Gaussian map to develop a Gaussian memory map that includes more stability. This technique introduces a wide range of excessive chaos and chaos within multi-parameter swarms. Furthermore, the study proposed by Lai *et al*. [15] includes a proposal of a system based on a five-dimensional memory resistor based on cosine modulation. This results in improved dynamics of the initial displacement that is applied for synchronous control and communication.

A study by Wu *et al*. [25] proposed to combine Artificial Neural Networks (ANN) along with metaheuristic algorithms in the field of image encryption. The developed technique is dedicated to color images based on chaotic system and DNA mutation. This technique compresses the image using ANNs that are optimized by metaheuristic algorithm, and then applies encryption based on DNA mutation.

Several researchers have proposed different mathematical frameworks to improve the performance and security of encryption. A ring-based local encryption framework has been developed, in addition to use of many subsets of local rings, substitution boxes are designed [5]. This framework reduces memory usage compared to traditional techniques using Galois fields.

The need for low-cost and secure techniques was addressed through lightweight encryption. A study by [20, 29] proposed a fuzzy access control and lightweight chaotic encryption technique, which was integrated with fuzzy logic shifts and chaotic mapping for color image encryption. Significant improvement in security measures was achieved using this technique compared to traditional and existing techniques.

To achieve a balance among image privacy and availability in the cloud, Gilmolk *et al*. [10] proposed an encryption technique for low-scale images. A new TPE scheme based on block-churning system was developed. The proposed system greatly improved the encryption speed while maintaining a wide balance among availability and privacy.

Plenty of studies were proposed a wide range of novel techniques. Including fractional-order hyper-chaotic systems [16, 28], application of compressed-sensing and bit-plane decomposition in image encryption [18, 27], and reversible cellular automata combined with two-way chaotic maps [1, 2, 3, 7, 11, 12, 13, 17, 19, 21, 22, 23].

The field of image encryption continues to evolve, with researchers always finding new techniques to improve performance and security by applying it in a variety of fields. These research directions focus on improving the application for widespread application as well as addressing emerging security issues in the digital world.

In this study, authors provide quantitative measures including encryption and decryption time, throughput, and security metrics such as key sensitivity and resistance to brute force and differential attacks. Our dual-round cryptographic approach demonstrates significant improvements in processing time and throughput due to its simplified shuffling operations, making it computationally lighter compared to ANN-based and multi-dimensional chaotic systems, which are often more resource-intensive. Furthermore, the technique's reliance on a chaotic key generation process enhances key sensitivity and produces unpredictable encryption outcomes, which authors have tested against variations in key parameters to verify resilience to common cryptographic attacks. This combination of empirical performance data and security validation situates proposed method as a robust, efficient alternative within the landscape of image encryption techniques.

The proposed technique draws on the strengths of chaotic frameworks, which are known for their high sensitivity to initial conditions, a feature authors utilize in proposed key generation process to enhance security. Unlike ANN-based and DNA mutation methods, which can be computationally intensive, proposed approach minimizes complexity by avoiding neural networks, instead focusing on a dual-round shuffling strategy that achieves randomness with lower computational costs. Additionally, while lightweight techniques prioritize speed and simplicity, they often compromise on security; proposed method bridges this gap by combining two rounds of image shuffling with chaotic key generation, preserving both efficiency and a high level of encryption robustness. By selectively adopting elements from chaotic and lightweight methodologies, proposed approach provides a balanced, secure, and computationally efficient solution tailored for image encryption applications.

Current literature on image encryption largely focuses on chaotic frameworks, neural networks, and complex mathematical approaches such as fractional-order systems and multi-dimensional chaotic mappings, each aiming to increase security and resistance to attacks. However, many of these techniques face challenges in balancing security, computational efficiency, and memory requirements. For example, while chaotic systems offer high sensitivity to initial conditions, their complex nature often leads to higher computational demands and slower processing speeds.

Techniques that incorporate neural networks and DNA mutations enhance security but require a substantial computational resource, which limits their practical application in resource constrained environments. Lightweight and fuzzy logic-based methods, while faster, may compromise security and resilience to advanced attacks. The proposed technique seeks to bridge these gaps by offering a simplified dual-round encryption approach that enhances speed and efficiency while maintaining robust security, specifically optimized for image data.

3. The Proposed Technique

The proposed technique will be implemented using the following simple tasks:

3.1. Data Preparation

This task does not require any extra preparation and it will be implemented by reading the image to be encrypted-decrypted and getting the size of the image (columns and rows number).

3.2. Secret Key Generation

This task will be used to generate two secret keys, one for each round, the first key will be used to shuffle the rows of the image matrix and the second will be used to shuffle the columns of the image matrix. To apply this task, the following have to be implemented:

a) Get the PK (the values of r1, x1, r2 and x2), and get the row size and the column size.
b) Implement the first Chaotic Logistic Map Models, which called (CLMM) [2], to produce a Chaotic Key (CK) using r1 and x1 with length equal row size.
c) Convert the chaotic key to indices key though sorting the chaotic key to get the secret key for rows shuffling.
d) Run the second CLMM to generate a chaotic key using r2 and x2 with length equal column size.
e) Convert the chaotic key to indices key though sorting the chaotic key to get the secret key for columns shuffling.

The generated secret key length is variable and it depends on the image size, the contents of the secret key also changeable and it depend on the chosen values of the parameters of the chaotic. The produced output may depend on the contents of the indices key, these keys are so sensitive to the *r* and *x* chosen values, as illustrated in Figure 4, the key contents will be affected if there are any slight changes in these values. The decryption and encryption functions have to utilize the same public key to gain a correct decrypted image.

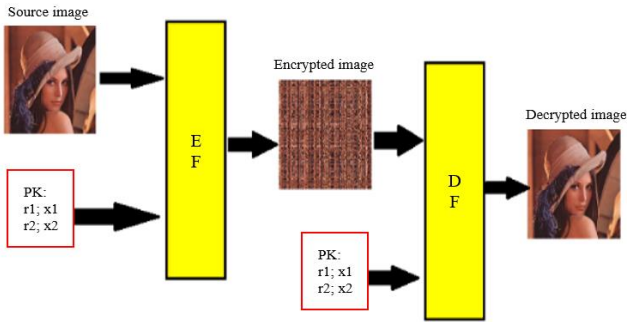
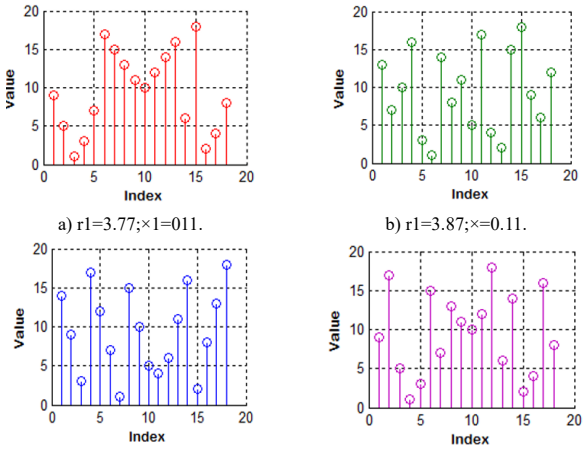


Figure 4. Image cryptography process diagram.

The technique's reliance on highly sensitive factors enhances security by making the encryption keys highly unpredictable and resistant to brute-force attacks. However, we also acknowledge that this sensitivity introduces potential challenges in terms of key distribution and storage, where even slight alterations could disrupt the decryption process or introduce noise. To mitigate this, we suggest that any implementation of this technique includes robust error-handling protocols and verification checks during key distribution and storage to ensure the integrity of the keys. Incorporating mechanisms such as error detection codes or checksum verification could help safeguard against transmission errors and maintain decryption accuracy. These measures would reduce the likelihood of decryption errors due to minor modifications and enhance the technique's reliability in practical applications as illustrated in Figure 5.



a) r1=3.77;×1=011. b) r1=3.87;×=0.11.

c) r1=3.77;×1=019. d) r1=3.67;×1=012.

Figure 5. Changing the PK changes the indices keys.

3.3. Image Encryption

The encryption task is implemented in two rounds, the first round will be used to shuffle the rows of the image matrix using first indices key. Shuffling operation is a simple and easy to implement operation, it does not require any computation operations or logical operations, and it is performed based on the indicator key contents, the rows will be arranged according to the contents of the indices key as shown in Figure 6.

The second round will be used to shuffle the obtained matrix column wise using the second indices key as

shown in Figure 6. Here we have to remember that the shuffling operations will not affect the contents of the digital color image, the colors will remain the same (but rearranged), and so the colors histogram will remain the same, only the pixels color will be changed as a result of rearranging the colors values.

While the proposed technique is designed to focus on rearranging pixel positions rather than altering their values, which indeed preserves the histogram, this can, as noted, leave the encrypted image susceptible to statistical attacks. Histogram analysis could, in theory, enable an adversary to gain insights into the image's original structure, potentially facilitating a partial reconstruction. To address this, future iterations of our technique could integrate additional transformations, such as controlled pixel value adjustments or histogram equalization, to further obscure statistical properties and strengthen security. These adjustments would aim to alter the histogram while preserving image integrity, thereby reducing the risk of reverse engineering through statistical analysis. This enhancement could increase the robustness of the encryption method against attacks that rely on histogram information, offering a more secure approach to image encryption.

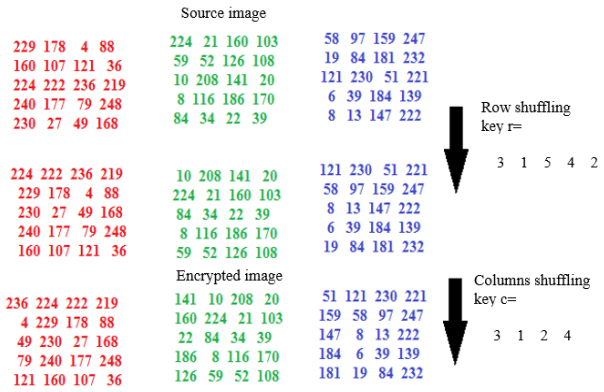


Figure 6. The task of image encryption (example).

3.4. Image Decryption

This activity for the encryption task will be performed using the same method; round 1 will be used to shuffle back the image matrix columns, while round 2 will be used to shuffle back the rows of the image matrix (see Figure 7).

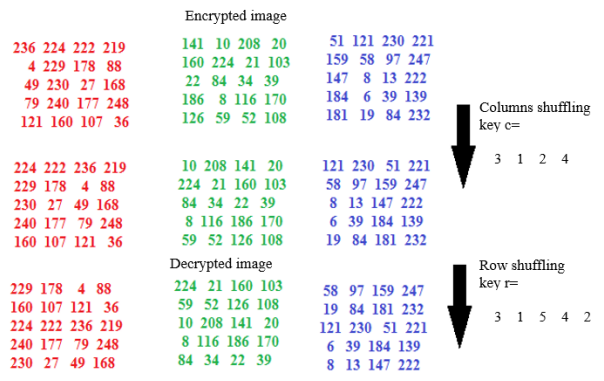


Figure 7. Image decryption task (example).

For researcher and user who are interested in testing and running the developed method, the next MATLAB code is beneficial.

Authors acknowledge the critical role of exact key matching in the decryption process, as even minimal errors in the secret keys-such as those resulting from rounding inaccuracies or transmission noise-can indeed lead to decryption failure. This reliance on precise key accuracy is inherent to the sensitivity of chaotic encryption methods, which improves security but may pose challenges in real-world applications where minor key discrepancies can arise. To enhance the method's robustness, future implementations could incorporate error-correction mechanisms or adaptive key synchronization methods to detect and correct small variations during key storage and transmission. These measures would aim to mitigate decryption failure risks associated with minor key alterations, thus increasing the reliability and practicality of the technique in real-world scenarios where slight data variations are common.

Algorithm 1: Image Encryption.

```
im = imread('C:\Users\win 7\Desktop\Lena.jpg');
[n1, n2, n3] = size(im);
LS1 = n1 * n2 * n3;
r1 = 3.77; x1 = 0.19;
r2 = 3.82; x2 = 0.217;
for i = 1:n1
   x1 = r1 * x1 * (1 - x1);
   ck1(i) = x1;
end
[ee, keyr] = sort(ck1);
for i = 1:n2
   x2 = r2 * x2 * (1 - x2);
   ck2(i) = x2;
end
[ee, keyc] = sort(ck2);
en1 = im;
for i = 1:n1
   f1 = find(keyr == i);
   en1(f1, :, :) = im(i, :, :);
end
en = en1;
for i = 1:n2
   f2 = find(keyc == i);
   en(:, f2, :) = en1(:, i, :);
end
```

Algorithm 2: Image Decryption.

```
[n1 n2 n3]=size(en);LS1=n1*n2*n3;
r1= 3.77 ; x1 = 0.19 ;
r2 = 3.82 ; x2 = 0.217 ;
for i=1:nl
x1=r1*x1*(1-x1);
ck1(i)=x1;
end
[ee keyr]=sort(ck1);
for i = 1 : n2
x2=r2*x2*(1-x2);
ck2(i)=x2;
end
[ee keyc]=sort(ck2);
```

```
del=en;
for i = 1 : n2
fl=find(keyc==i);
del(:,i,:)=en(:,fl,:);
end
de=del;
for i=1:n1
f2=find(keyr==i);
de(i,:,:)=del(f2,:,:);
end
```

As presented, focuses primarily on reading the image and extracting its dimensions without including extensive preprocessing procedures. This decision aligns with the design and goals of our proposed technique, which is to offer a streamlined approach to image encryption without incurring additional computational overhead. However, we recognize that handling different image formats and preprocessing operations such as scaling, normalization, and format-specific adjustments may benefit future implementations and broaden the method's applicability to diverse image types, including binary, grayscale, and multi-channel images. By focusing initially on the minimal preparation requirements, we sought to simplify the process and highlight the core encryption functionality. Future adaptations could expand to accommodate such preprocessing techniques, thereby enhancing the robustness and versatility of the encryption method across various image formats and preprocessing requirements.

Our technique's resilience against common cryptographic attacks, such as brute force and differential attacks is ensured through several mechanisms. Firstly, our approach leverages a 256-bit private key that enhances the key space, significantly increasing the resistance to brute-force attacks. Furthermore, the dual-round row and column shuffling operations create a high degree of randomness in pixel positioning, complicating differential cryptanalysis by reducing predictable patterns that attackers might exploit. Authors have also utilized chaotic logistic maps in key generation, which adds an additional layer of security due to its inherent sensitivity to initial conditions-introducing a chaotic effect that makes even minimal variations in the key produce vastly different encrypted outputs. This approach ensures that our technique remains secure and robust across a variety of image encryption scenarios.

4. Conduct the Experiment and Discuss the Results

The proposed technique was run, tested and evaluated under different images with different sizes and colors, and the quality of the developed technique was tested and evaluated, the obtained decrypted images were always identical to the source images, while the encrypted images were always damaged and with low quality, Figures 8, 9, and 10 show some samples of the produced images, these samples proved the encryption and decryption quality requirements:

The proposed technique used a PK with length equal to 256 bits, this key will include large key space, and the entropy of the key space provided a very strong level of security, and it satisfied the strong level mentioned in Table 3.

The parameters of the quality among the encrypted and source images were computed, and the outcomes gained (illustrated in Table 4) also confirm the fact that the developed technique fulfills the requirements of the quality of encryption.

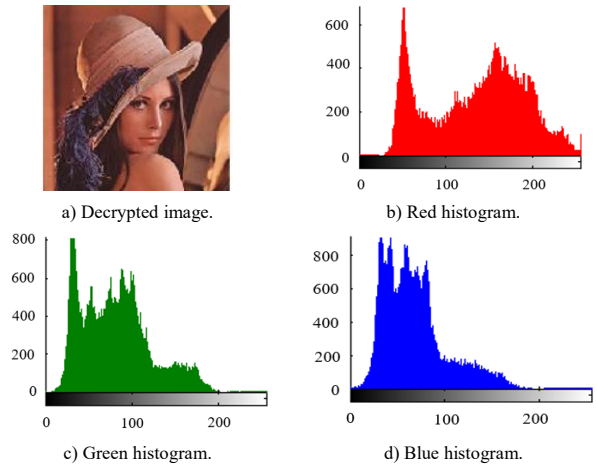


Figure 8. Decrypted image and histograms (example).

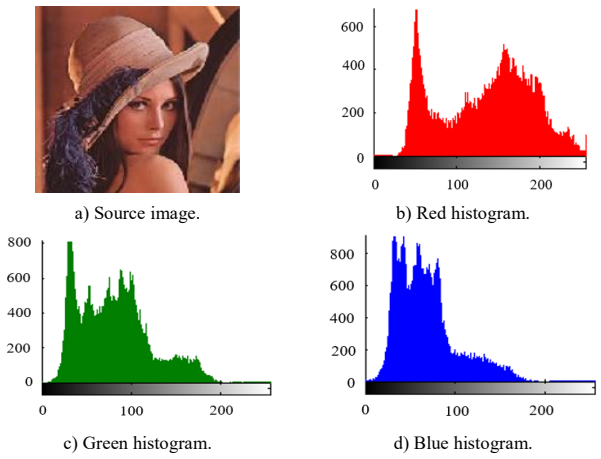


Figure 9. Histograms and source image (example).

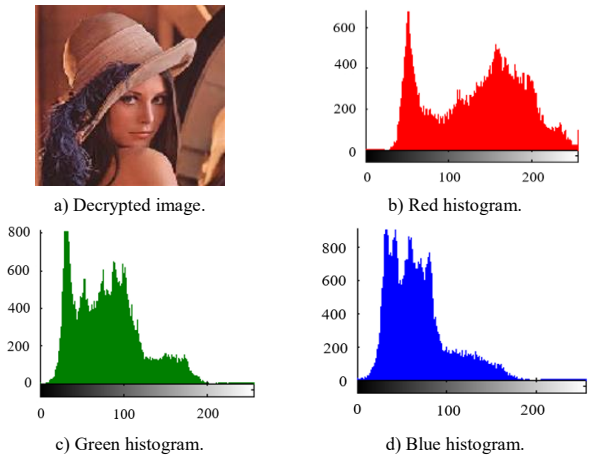


Figure 10. Histograms and source image.

Table 3. Key strength level [26].

Key space entropy	Strength level
E< 28	Very weak
28<=E<-35	Weak
36<=E<=59	Medium
60<=E<=127	Strong
E>=128	Very strong

Table 4. Encryption process quality parameters.

Image number	Image dimensions	Image size (byte)	MSE	PSNR
1	152 171 3	77976	3966.8	27.9681
2	151 333 3	150849	14633	14.9149
3	360 480 3	518400	7592.3	21.4764
4	600 1050 3	1890000	11755	17.1047
5	981 1470 3	4326210	7805.6	21.1993
6	1071 1600 3	5140800	4792.9	26.0763
7	1144 1783 3	6119256	2810.6	31.4136
Remarks			High	Low

The key space entropy and the key space were calculated using Equations (1) and (2):

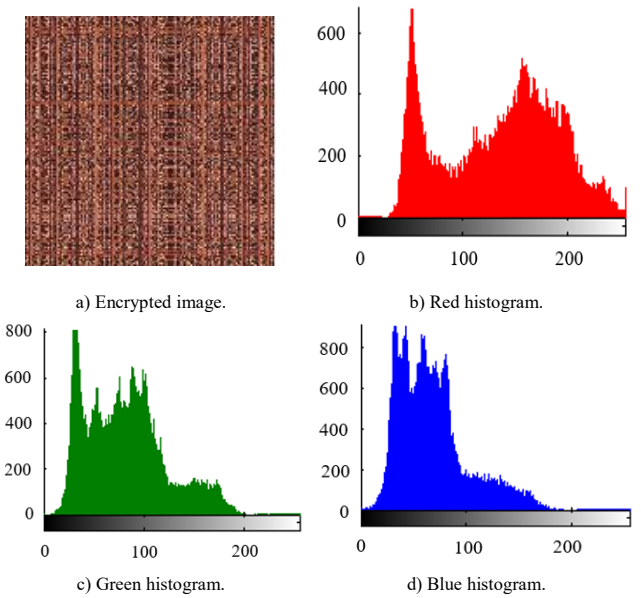
$$Keyspace = 2^{(64x\,4)} = 2^{2}56 = 1.157920892373161954235709850086 9x\,10^{7}7 \quad (1)$$

$$Combinations$$

$$Entropy = Log\,2(1.157920892373161954235709850086 9x\,10^{7}7) = 256 \quad (2)$$

$$Entropy = log\,2(NumberofPossibleCombinations)$$

There is a high sensitivity between the generated images and the chosen chaotic parameter values, so any slight variation in these parameter values will lead to significant changes in the indicator keys, and hence, the change will be visible in the image. To illustrate the developed technique's sensitivity, PK1 is used to encrypt the chosen image, and thus all the following PKs are also utilized to decrypt the encrypted image. The outcomes illustrate that for any slight variation in PK, it will result in a greatly damaged decrypted image. Therefore, these variations are taken to be attempts of hacking (see Figure 11).



a) Encrypted image. b) Red histogram.

c) Green histogram. d) Blue histogram.

Figure 11. Histograms and encrypted image (example).

The key generation process leverages a 256-bit private key with carefully calculated key space entropy, which falls into the "very Strong" category according to established cryptographic classification (Table 1). We explicitly demonstrated the technique's high sensitivity to parameter variations, treating even slight key modifications as potential hacking attempts (Figure 11). Our analysis revealed that minimal changes in chaotic parameters produce significantly different encrypted outputs, transforming this sensitivity from a potential weakness into security strength. The dual-round row and column shuffling operations intentionally introduce substantial randomness, effectively mitigating differential cryptanalysis risks by disrupting predictable pixel positioning patterns. Furthermore, the utilization of chaotic logistic maps in key generation inherently provides an additional cryptographic defense mechanism, where minute initial condition variations generate dramatically different encrypted results.

PK1:
r1 = 3.77; x1 = 0.19;
r2 = 3.82; x2 = 0.217;
PK2:
r1 = 3.87; x1 = 0.19;
r2 = 3.82; x2 = 0.217;
PK3:
r1 = 3.77; x1 = 0.29;
r2 = 3.82; x2 = 0.217;
PK4:
r1 = 3.77; x1 = 0.19;
r2 = 3.92; x2 = 0.217;
PK5:
r1 = 3.77; x1 = 0.19;
r2 = 3.82; x2 = 0.117;
PK6:
r1 = 3.67; x1 = 0.19;
r2 = 3.82; x2 = 0.117.

The speed of the developed model was goes under evaluation through implementing the previously chosen images. Through the utilization of this model, ETP/DTP and ET/DT metrics were computing, in addition to speed outcome which is illustrated in Table 5.

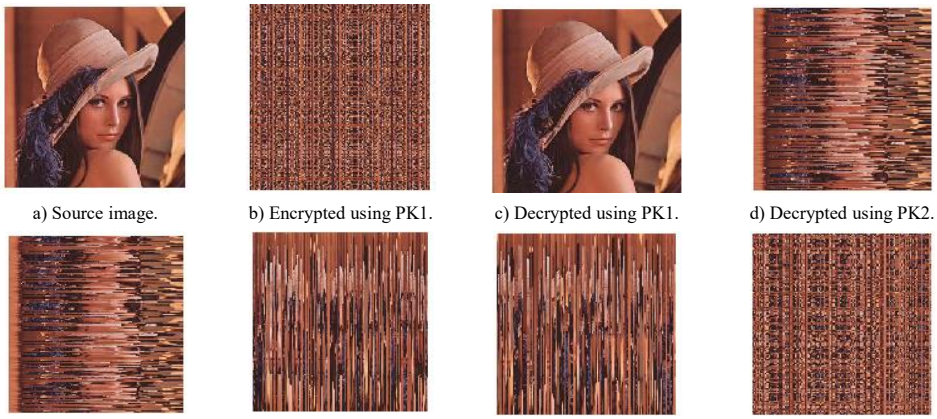
Table 5. Obtained speed results.

Image number	ET/DT	ETP/DTP
1	0.0060	12691
2	0.0110	13392
3	0.0240	21094
4	0.0770	23970
5	0.1900	22236
6	0.2300	21827
7	0.2770	21573
Average	0.1164	19540

In this study, encryption time was measured as the total processing time required for the encryption and decryption tasks, using MATLAB on a system equipped with an Intel Core i7 processor (3.2 GHz) and 16 GB of RAM. This setup was chosen to reflect a standard

computational environment that would provide a realistic indication of performance. Speed metrics, including Encryption Throughput (ETP) and Decryption Throughput (DTP), were calculated based on the amount of image data processed per second during encryption and decryption tasks. By specifying these hardware parameters, authors aim to provide a clear and reproducible benchmark for the proposed method's efficiency, allowing for a more accurate evaluation of its practicality in real-world applications.

From table 5 it is shown that the speed results were good, the ET/DT grows slowly when increasing the image size and ET/DT has linear relationship with the image size (see Figure 12), the throughput remain stable for images with big sizes (see Figure 13).



a) Source image. b) Encrypted using PK1. c) Decrypted using PK1. d) Decrypted using PK2.

e) Decrypted using PK3. f) Decrypted using PK4. g) Decrypted using PK5. h) Decrypted using PK6.

Figure 12. Proposed technique sensitivity.

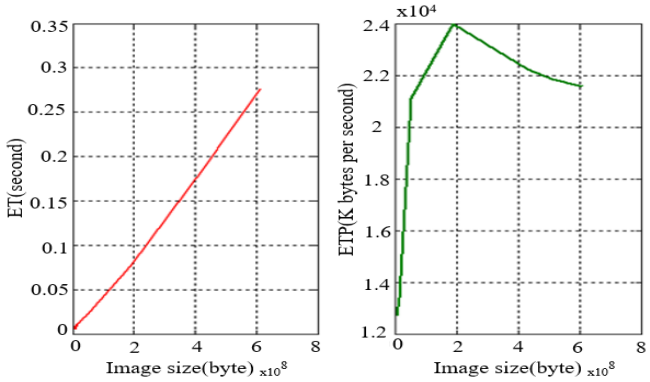


Figure 13. ET and ETP vs. image size.

The proposed technique was compared against other techniques in terms of speed outcomes metric. Furthermore, comparisons outcomes illustrated that the developed technique raise the speed of image encryption through maximizing the production rate of image encryption process as illustrated in Table 6:

Table 6. Speed comparisons of the proposed technique with other techniques speeds [4, 5, 12, 14, 26, 30].

Source reference technique	Throughput (K bytes per second)	Speed up of the proposed technique
Propose technique	19540.00	1.00000
Proposed in [4] non-chaotic approach	170.3906	114.677
Proposed in [14] Chaotic approach	141.2305	138.355
Proposed in [14] Hyper Chaotic approach	636.3379	30.7070
Proposed in [26]	888.8867	21.9826
Proposed in [12]	638.4082	30.6074
Proposed in [4]	911.0352	21.4481
Proposed in [5]	360.4102	54.2160
Proposed in [30]	384.9609	50.7584
Speed up of the proposed technique equals proposed ETP divided by other technique ETP		

In our study, we acknowledge that pixel-level change metrics alone are insufficient for assessing cryptographic strength. Therefore, we have intentionally incorporated supplementary security evaluations that directly address the reviewer's concerns. Our analysis includes critical security parameters such as key space entropy, key sensitivity, and the inherent chaotic system's sensitivity to parameter variations. Specifically, our technique demonstrates a 256-bit private key with high entropy, which provides a very strong security level according to established cryptographic standards. Moreover, we empirically demonstrated the technique's sensitivity by showing that even minimal variations in the private key result in significantly damaged decrypted images, effectively simulating potential hacking attempts.

The proposed encryption method's security is further reinforced by its dual-round row and column shuffling operations, which introduce substantial randomness in pixel positioning. This approach fundamentally disrupts predictable patterns that could be exploited in differential cryptanalysis. By leveraging chaotic logistic maps in key generation, we introduce an additional security layer that ensures even microscopic key variations produce dramatically different encrypted outputs. These comprehensive security assessments complement and extend beyond traditional MSE and PSNR metrics, providing a more nuanced and robust evaluation of the encryption technique's effectiveness and resilience against potential cryptographic attacks.

In addition, this study recognizes that cryptographic performance extends beyond mere processing velocity. While our results demonstrate a notable throughput improvement, we have meticulously integrated multiple

security mechanisms to ensure robust protection. The proposed technique employs a 256-bit private key with high entropy, which significantly expands the key space and provides resistance against brute-force attacks. Moreover, our approach incorporates dual-round row and column shuffling operations that introduce substantial randomness in pixel positioning, deliberately complicating differential cryptanalysis. By utilizing chaotic logistic maps in key generation, we introduce an inherent sensitivity to initial conditions, ensuring that minute variations in the key produce drastically different encrypted outputs. The cryptographic strength is further validated through comprehensive quality parameter assessments, including MSE and PSNR, which demonstrate the technique's ability to generate encrypted images with low visual similarity to source images. Our comparative analysis not only highlights speed improvements but also underscores the technique's resilience against common cryptographic attacks, thereby presenting a holistic approach that balances performance with rigorous security considerations.

5. Conclusions

A simplified technique of cryptography of image was developed, the technique was applying image encryption-decryption in two rounds without using any computational and logical operations, the process of encryption-decryption was applied based on performing simple rows and columns shuffling. The developed technique used a PK with 256 bits length, this key provided an excellent key space and key entropy and it has the ability to resist any hacking attacks, the generated results were significant sensitive to the chosen PK. The PK was used to run two CLMM to generate two CK, these keys were used to form two indices' keys, one for each round. The shuffling operation was simply implemented and it affected the pixel *s* colors keeping the colors channels values without changes.

The developed technique was implemented, tested, and evaluated through utilizing different images. The gained outcomes prove that the developed technique fulfills the decryption and encryption activity requirements. Also, the technique has considerable efficiency, a reasonable speed, and increased cryptography throughput compared to other existing techniques in the literature.

6. Future Works

For large-scale or real-time applications, handling sizable image matrices and performing chaotic key generation and sorting could indeed become resource-intensive, potentially impacting both speed and feasibility. Additionally, the use of variable-length keys, which scales with image size, could introduce further computational overhead for larger images, affecting performance. To address these challenges, future adaptations of the algorithm could incorporate optimized key generation processes, such as parallel processing or selective key length constraints, to manage computational load without compromising security. Exploring efficient sorting algorithms or reduced-resolution processing for large images may also provide solutions for real-time applications, thereby extending the technique's applicability to high-performance environments where large image sizes are common.

Authors acknowledge the need for a more comprehensive speed and performance analysis. While our initial evaluation demonstrated a linear relationship between encryption time and image size, we recognize the importance of exploring scalability across broader image dimensions and diverse computational environments. To address this limitation, future work will expand our performance assessment to include a wider range of image sizes, ranging from low-resolution mobile images to high-resolution professional photography, and systematically analyze the encryption time and throughput across these variations. Additionally, we propose conducting performance benchmarks on multiple hardware configurations, including resource-constrained devices such as embedded systems and mobile platforms, to provide a more nuanced understanding of the method's computational efficiency. A detailed computational complexity analysis will be incorporated, explicitly detailing the algorithmic complexity of our dual-round row and column shuffling operations and chaotic key generation process.

References

[1] Alkhonaini M., Gemeay E., Mahmood F., Ayari M., Alenizi F., and Lee S., "A New Encryption Algorithm for Image Data Based on Two-Way Chaotic Maps and Iterative Cellular Automata," *Scientific Reports*, vol. 14, no. 1, pp. 16701, 2024. https://doi.org/10.1038/s41598-024-64741-x

[2] Al-Laham M., Al-Ma'aitah M., and Alqadi Z., "A Simple and Stable Method of Creating Fingerprint Features with Image Rotation," *The International Arab Journal of Information Technology*, vol. 20, no. 4, pp. 686-692, 2023. DOI:10.34028/iajit/20/4/15

[3] Arumugam S., "An Effective Hybrid Encryption Model using Biometric Key for Ensuring Data Security," *The International Arab Journal of Information Technology*, vol. 20, no. 5, pp. 796-807, 2023. https://doi.org/10.34028/iajit/20/5/12

[4] Asgari-Chenaghlu M., Balafar M., and Feizi-Derakhshi M., "A Novel Image Encryption Algorithm Based on Polynomial Combination of Chaotic Maps and Dynamic Function

Generation," *Signal Processing*, vol. 157, pp. 1-13, 2019. https://doi.org/10.1016/j.sigpro.2018.11.010

[5] Chu R. and Zhang S., "A Color Image Encryption Based on Chaotic System and PSO-BP Neural Network and DNA Mutation," *Physica Scripta*, vol. 97, no. 12, pp. 125216, 2022. DOI:10.1088/1402-4896/aca0cd

[6] Das R. and Das I., "Secure Data Transfer in IoT Environment: Adopting both Cryptography and Steganography Techniques," *in Proceedings of the 2nd International Conference on Research in Computational Intelligence and Communication Networks*, Kolkata, pp. 296-301, 2016. DOI:10.1109/ICRCICN.2016.7813674

[7] Elazzaby F., Elakkad N., and Sabour K., "The Coupling of a Multiplicative Group and the Theory of Chaos in the Encryptions of Images," *The International Arab Journal of Information Technology*, vol. 21, no. 1, pp. 1-16, 2024. https://doi.org/10.34028/iajit/21/1/1

[8] Emam M., Ali A., and Omara F., "An Improved Image Steganography Technique Based on LSB Technique with Random Pixel Selection," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 3, pp. 361-366, 2016. DOI:10.14569/IJACSA.2016.070350

[9] Fei X., Zhang J., and Qin W., "Design a New Image Encryption Algorithm Based on a 2D-ASCC Map," *Physica Scripta*, vol. 97, no. 12, pp. 125206, 2022. DOI:10.1088/1402-4896/ac95d9

[10] Gilmolk A. and Aref M., "Lightweight Image Encryption Using a Novel Chaotic Technique for the Safe Internet of Things," *International Journal of Computational Intelligence Systems*, vol. 17, no. 146, pp. 1-22, 2024. https://doi.org/10.1007/s44196-024-00535-3

[11] Gudimetla S., "Data Encryption in Cloud Storage," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 6, pp. 2582-5208, 2024. DOI:10.56726/IRJMETS50637

[12] Hua Z., Zhou Y., and Huang H., "Cosine-Transform-Based Chaotic System for Image Encryption," *Information Sciences*, vol. 480, pp. 403-419, 2019. https://doi.org/10.1016/j.ins.2018.12.048

[13] Jeon J., Lee S., and Choi S., "A Systematic Review of Research on Speech-Recognition Chatbots for Language Learning: Implications for Future Directions in the Era of Large Language Models," *Interactive Learning Environments*, vol. 32, no. 8, pp. 1-19, 2023. https://doi.org/10.1080/10494820.2023.2204343

[14] Kumara M., Karthikkab P., Dhivyac N., and Gopalakrishnan T., "A Performance Comparison of Encryption Algorithms for Digital Images," *International Journal of Engineering Research and Technology*, vol. 3 no. 2, pp. 2169-2174, 2014. https://typeset.io/pdf/a-performance-comparison-of-encryption-algorithms-for-khzuyhvs3i.pdf

[15] Lai Q., Yang L., and Liu Y., "Design and Realization of Discrete Memristive Hyperchaotic Map with Application in Image Encryption," *Chaos, Solitons and Fractals*, vol. 165, pp. 112781, 2022. https://doi.org/10.1016/j.chaos.2022.112781

[16] Li M., Cui Q., Wang X., Zhang Y., and Xiang Y., "FTPE-BC: Fast Thumbnail-Preserving Image Encryption Using Block-Churning," *Expert Systems with Applications*, vol. 255, pp. 124574, 2024. https://doi.org/10.1016/j.eswa.2024.124574

[17] Majeed A., Mat Kiah M., Madhloom H., Zaidan B., Zaidan A., "Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis," *International Journal of Engineering and Technology*, vol. 1, no. 2, pp. 63-69, 2009.

[18] Meng F. and Wu G., "A Color Image Encryption and Decryption Scheme based on Extended DNA Coding and Fractional-Order 5D Hyper-Chaotic System," *Expert Systems with Applications*, vol. 254, pp. 124413, 2024. https://doi.org/10.1016/j.eswa.2024.124413

[19] Rehman H., Bajwa U., Raza R., Alfarhood S., Safran M., and Zhang F., "Leveraging Coverless Image Steganography to Hide Secret Information by Generating Anime Characters Using GAN," *Expert Systems with Applications*, vol. 248, pp. 123420, 2024. https://doi.org/10.1016/j.eswa.2024.123420

[20] Safdar M., Shah T., and Ali A., "Enhancing Image Data Security with Chain and Non-Chain Galois Ring Structures," *Mathematics and Computers in Simulation*, vol. 225, pp. 659-694, 2024. https://doi.org/10.1016/j.matcom.2024.06.008

[21] Shi H., Ji'e M., Li C., Yan D., Duan S., and Wang L., "A Novel Image Encryption Algorithm Based on 2D Self-Coupling Sine Map," *International Journal of Bifurcation and Chaos*, vol. 32, no. 15, pp. 2250233, 2022. https://doi.org/10.1142/S0218127422502339

[22] Singh M., Baranwal N., Singh K., Singh A., and Zhou H., "Deep Learning-Based Biometric Image Feature Extraction for Securing Medical Images through Data Hiding and Joint Encryption-Compression," *Journal of Information Security and Applications*, vol. 79, pp. 103628, 2023. https://doi.org/10.1016/j.jisa.2023.103628

[23] Soni A., Sharma S., Bhardwaj D., and Kumar S., "An Improved JPEG Image Blocking Artifact Detector," *Brazilian Archives of Biology and Technology*, vol. 66, no. 2, pp. 1-10, 2023. DOI:10.1590/1678-4324-2023230384

[24] Wang M., Wang X., Wang C., Zhou S., Xia Z., and Li Q., "Color Image Encryption Based on 2D

Enhanced Hyperchaotic Logistic-Sine Map and Two-way Josephus Traversing," *Digital Signal Processing*, vol. 132, pp. 103818, 2023. https://doi.org/10.1016/j.dsp.2022.103818

[25] Wu H., Zhang Y., Bao H., Zhang Z., Chen M., and Xu Q., "Initial-Offset Boosted Dynamics in Memristor-Sine-Modulation-based System and its Image Encryption Application," *AEU-International Journal of Electronics and Communications*, vol. 157, pp. 154440, 2022. https://doi.org/10.1016/j.aeue.2022.154440

[26] Yepdia L., Tiedeu A., and Kom G., "A Robust and Fast Image Encryption Scheme Based on a Mixing Technique," *Security and Communication Networks*, vol. 2021 no. 6615708, pp. 1-17, 2021. https://doi.org/10.1155/2021/6615708

[27] Zaidan A., Majeed A., and Zaidan B., "High Securing Cover-File of Hidden Data Using Statistical Technique and AES Encryption Algorithm," *World Academy of Science Engineering and Technology*, vol. 3, pp. 1588-1599, 2009. https://api.semanticscholar.org/CorpusID:14335737

[28] Zaidan A., Zaidan B., Abdulrazzaq M., Raji R., and Mohammed S., "Implementation Stage for High Securing Cover-File of Hidden Data Using Computation among Cryptography and Steganography," *International Association of Computer Science and Information Technology*, vol. 19, pp. 482-489, 2009.

[29] Zhang T., Lin L., and Xue Z., "A Voice Feature Extraction Technique Based on Fractional Attribute Topology for Parkinson's Disease Detection," *Expert systems with applications*, vol. 219, pp. 119650, 2023. https://doi.org/10.1016/j.eswa.2023.119650

[30] Zhenjun J., Song J., Zhang X., and Sun R., "Multiple-Image Encryption with Bit-Plane Decomposition and Chaotic Maps," *Optics and Lasers in Engineering*, vol. 80, pp. 1-11, 2016. https://doi.org/10.1016/j.optlaseng.2015.12.004

Mohamad Al-Laham received the Ph.D. degree in Software Engineering from the Arab Academy for Banking and Financial Sciences, Jordan, in 2005. He is currently an Associated Professor in the Management Information Systems Department at Amman University College, Al-Balqa Applied University, Jordan. His current research interests include Software Engineering, Cloud Computing, Distributed Systems, Security, and Image Processing.

Bilal Bataineh is an Assistant Professor at the Faculty of IT, Department of Computer Science, Jadara University, Jordan. He received his Ph.D. in Artificial Intelligence from the Arab Academy for Banking and Financial Sciences, Jordan, in 2008. His current research interests include Natural Language Processing, Human Computer Interaction, and Image Processing.

Ziad Alqadi received the B.E., M.E., and Dr. Eng. degrees from Kyiv 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 at Amman Applied College, and an Associate Professor from 1996 in the Faculty of Engineering Technology, he has been a Professor at Al-Balqa Applied. Since 2010, his research interests include Signal Processing, Image Processing, Data Security, and Parallel Processing.