Utilizing Chaotic Logistic Keys for LSB1 and LSB2 Message Steganography

Ahmad A. Sharadqh
Electrical Engineering Department, Faculty of Technology Engineering, Al-Balqa Applied University, Amman, Jordan
dr.ahmed.sharadqah@bau.edu.jo

Jawdat S. Alkasassbeh
Electrical Engineering Department, Faculty of Technology Engineering, Al-Balqa Applied University, Amman, Jordan
Jawdat1983@bau.edu.jo (corresponding author)

Tareq A. Alawneh
Electrical Engineering Department, Faculty of Technology Engineering, Al-Balqa Applied University, Amman, Jordan
Tareq.alawneh@bau.edu.jo

Aws Al-Qaisi
College of Engineering and Technology, American University of the Middle East, Eqaila 54200, Kuwait
Aws.Al-Qaisi@aum.edu.kw

Yahia F. Makableh
College of Engineering and Technology, American University of the Middle East, Eqaila 54200, Kuwait
yahia.makableh@aum.edu.kw

Safaa Al-Adwan
Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt, Jordan
safaa.aladwan@bau.edu.jo

Received: 15 July 2024 | Revised: 7 August 2024 and 8 August 2024 | Accepted: 22 August 2024

ABSTRACT

This paper introduces a novel hybrid data steganography method that combines the new techniques of LSB1 and LSB2. The proposed method simplifies data-hiding and extraction operations by utilizing a patch method. A unique Private Key (PK) divides the message into two parts. The first part is processed using the LSB1 method, while the second one is treated with the LSB2 method. The PK information is utilized to create secret keys, namely key1 and key2. The keys are generated by converting two Chaotic Logistic Keys (CLKs) and establishing the sequence of cover Stego bytes for concealing and revealing data. The secret message is protected within a secure key area by utilizing the PK, which improves security by preventing unwanted access. The secret message's effective extraction depends significantly on the PK's content. Any alterations to the key during the extraction step will be deemed unlawful, possibly leading to a compromized secret key. Moreover, the suggested approach is followed and assessed by using different messages. The results are comprehensively studied, ensuring a robust evaluation of the quality, efficiency, and security improvements of the data steganography process. The experimental results confirm the data steganography's quality, efficiency, and security enhancements.

Keywords-steganography; LSB; secret key; private key

I. INTRODUCTION

Least Significant Bit (LSB) steganography is a technique for concealing information within digital content, such as photos, in an invisible to the human eye way [1]. This method involves altering the least significant bit of a pixel value in an image to hide data, maintaining good visual quality, and increasing the storage capacity of the steganographic image [2]. While altering a pixel's LSB has a negligible effect on color perception, researchers have developed advanced techniques like filtering-based algorithms that use the Most Significant Bits (MSB) to hide large amounts of data in bitmap images [3]. Additionally, methods like LSB2 have been introduced to enhance storage capacity by increasing the maximum length of the hidden message [4]. LSB steganography enhancements include simulated annealing to improve the hidden telemetry data capacity and the new LSB matching approaches to minimize pixel modification [5]. Furthermore, techniques that modify color palettes instead of individual pixels have been developed to enhance user perception and reduce random noise in the image, making data concealment and security more effective [6]. The process involves utilizing a digital color image as the cover media, resulting in the steganographic image. This image justifies its use due to its large file size, which allows for hiding lengthy communications [7].

In this context, the cover media usually appears as a digital Color Image (CI). The resulting steganography medium is known as the Steganographic Image (SI). Using a digital CI as the cover media in data steganography is justifiable because of its big file size. This enables the hiding of lengthy communications and increases the ability to conceal data [8]. Digital CIs are represented by three-dimensional matrices, with each primary color channel (blue, green, and red) represented by a two-dimensional matrix [9]. A matrix-based representation simplifies CI processing by converting image operations into matrix operations [10]. Digital CIs enable the independent processing of individual color channels by manipulating each color matrix separately [11]. It is also practical to adjust particular sections of the CI [12]. This type of flexibility allows for targeted adjustments or improvements to particular areas in the image, providing precise management of the data concealment process and reducing the effect on the cover image's overall visual appeal. The LSB approach entails altering the LSB of the CI by substituting them with secret data bits from the hidden message [13]. The conventional LSB approach is recognized for its simplicity and computational efficiency. Nevertheless, it is constrained by a limited data-hiding capacity, so the LSB inversion technique has been devised to overcome these restrictions [14]. This method enhances the SI's quality by decreasing the chances of finding concealed data, which means that the LSB inversion approach differs from the typical LSB method because it does not substitute the original data with the secret data [15]. The LSB inversion approach preserves the visual quality of the SI while hiding the secret data by flipping the LSBs instead of replacing them [16]. Data steganography involves concealing data before transmission and disclosing them upon reception, requiring that the data concealment and retrieval operations use the same public key, with the cover media typically being a digital CI and the steganography media produced referred to as the SI. The data-hiding operation can be efficiently carried out by ensuring that the pixel values and message characters are within a compatible numerical range. Thus, the integrity and coherence of the cover image when modifying the LSBs, LSB1 or LSB2, of the pixel values in digital CI are maintained. However, there will be a slight impact on the pixel color, with changes in the latter resulting from LSB1 modifications typically ranging from -1 to +1 and LSB2 modifications varying from -3 to +3, certifying that these changes are not noticeable to the human eye and maintaining the visual coherence and integrity of the image, making it challenging for humans to discern any differences between the SI and CI [17-22]. Numerous techniques have been developed for data steganography, with many of them being based on the LSB1 and LSB2 methods. The LSB1 method utilizes the LSBs of consecutive bytes in the CI to store the message bits character by character in groups of 8 bytes within the cover image. It is capable of hiding data up to one-eighth the size of the CI, but it is not considered secure. The LSB2 approach overcomes this constraint by using the least significant bits of consecutive bytes in the cover picture to encode the message bits, enhancing the data-hiding capacity to one-fourth of the size of the cover image and providing increased security compared to the LSB1 method, making it more challenging to identify and extract the concealed message [23-26]. An innovative method uses modulus arithmetic instead of straight substitution, functioning in the spatial domain by depicting pixels as decimal values between 0 and 255, allowing for greater capacity without compromising the SI quality.

This study suggests an enhanced iteration of the LSB2 method, known for its simplicity and ability to conceal extensive messages, but often criticized for its lack of security. The proposed method creates a confidential PK with eight components to rearrange hidden bits in the cover image, reorganizing the bits of individual characters to improve security and allowing the primary key to be easily substituted without altering the method. Experiments utilizing various messages and cover graphics demonstrate the strategy's efficacy, with the results being analyzed to evaluate the SI's quality and increased data transfer rate. This paper introduces a steganography technique that involves modifying color palettes inside the color space. This technique emphasizes altering the image's color palette rather than manipulating individual pixels. The objective is to improve user perception by minimizing random noise in the image. Modifying the color palette transforms pixels of the same hue into a uniform new color, maintaining the integrity of areas with constant colors. This method improves data concealment and security by embedding messages into visuals, making the detection of the location and method of message concealing difficult. The main contributions of this work are:

- Hybrid Data Steganography Method: A novel hybrid data steganography method, combining the new techniques of LSB1 and LSB2, is introduced. It simplifies data-hiding and extraction operations deploying a patch method and a unique PK that divides the message into two parts, processed separately by LSB1 and LSB2.

- Improved Security Mechanism: The proposed method improves security by using PK information to create secret keys, key1 and key2, generated from chaotic logistic keys, establishing the sequence of cover Stego bytes for concealing and revealing data, and protecting the secret message within a secure key area to prevent unauthorized access.
- Comprehensive Evaluation: The research ensures a robust evaluation of the data steganography process's quality, efficiency, and security by using and assessing the suggested approach with different messages and studying the results comprehensively, confirming the enhancements in data steganography.

II. BACKGROUND

A. Patch Hiding and Extracting

LSB1 and LSB2 techniques are commonly followed for concealing and retrieving messages at a character level. Implementing the data hider and the extractor using these methods may incur added complications and necessitate sophisticated programming logic [14, 19, 24-28]. This research introduces a new method that utilizes data patching to hide and retrieve messages efficiently in a burst-like manner. The technique is outlined in Algorithm 1 and shown in Figure 1.

```
Algorithm 1: Patch hiding and extracting
algorithm
1. Get_Cover_Image_and_Extract_Dimensions()
1.1.   Get_Cover_Image()
1.2.   Extract_Cover_Image_Dimensions(CI)
1.3.   Width=Get_Width_of_Cover_Image(CI)
1.4.   Height=Get_Height_of_Cover_Image(CI)
2. Transform_Picture_Matrix_into_One-
Dimensional_Row_Matrix()
2.1. Transform_Picture_Matrix_into_Row_Matrix
(CI)
3. Obtain_Message_and_Calculate_Length(L)
3.1. Get_message()
3.2. Calculate_Message_Length(L)
4. Translate_Message_into_Decimal_
Representation()
4.1. Translate_Message_into_Decimal()
5. Convert_Decimal_Message_into_Binary_
Message()
5.1. Convert_Decimal_Message_into_Binary()
6. Transform_Binary_Message_into_Single_Column_
Matrix()
7. Ensure_Cover_Bytes_Equal_to_Message_Length
_Times_8()
8. Convert_Cover_Bytes_into_Binary_
Representation()
8.1. Convert_Cover_Bytes_into_Binary()
9. Modify_LSBs_of_Cover_Bytes_to_Match_Binary_
Message()
10. Convert_Modified_Cover_Bytes_into_Decimal
_Format()
10.1. Convert_Modified_Cover_Bytes_into_Decimal
()
11. Restore_Modified_Cover_Bytes_to_Original
_Positions()
12. Reshape_Row_Matrix_into_3D_Matrix_to_Obtain
_Stego_Image()
```

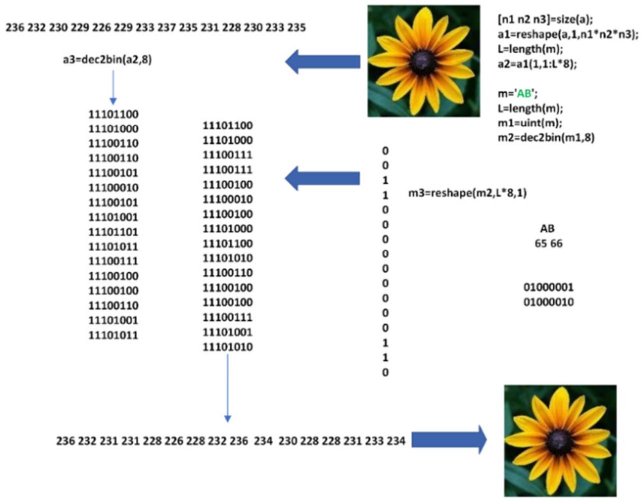

Fig. 1. LSB2 method of patch data hiding.

The implementation of the LSB method for data extraction using patching is displayed in Algorithm 2 and Figure 2.

```
Algorithm 2: LSB method extracting algorithm
1:Obtain_Stego_Image_and_Retrieve_Size_Informat
ion()
1.1:   Obtain_Stego_Image()
1.2:Retrieve_Stego_Image_Size_Information(SI)
1.3:   Width = Get_Width_of_Stego_Image(SI)
1.4:   Height = Get_Height_of_Stego_Image(SI)
2:Reconstruct_Image_Matrix_into_Single_Row_Matr
ix()
3:Retrieve_Length_of_Hidden_Message(L)
4:Extract_Stego_Bytes_from_Image_Row_Matrix()
5:Convert_Stego_Bytes_into_Binary_Representatio
n()
6:Extract_LSBs_from_Binary_Representation_of_St
ego_Bytes()
7:Reshape_LSBs_into_8_Column_Matrix()
8:Convert_Binary_Message_into_Decimal_Represent
ation()
9:Retrieve_Hidden_Message_by_Converting_Decimal
_Results_into_Characters()
```

The LSB2 data-hiding (see Algorithm 1) and the extracting method employing patching (see Algorithm 2) can be implemented by using the same scenario but two LSBs, as portrayed in Figures 3 and 4.

B. Private Key

The proposed method combines the LSB1 and LSB2 methods for message hiding and extraction, incorporating a patching process. It introduces using a PK to generate two secret keys, key1 and key2, which will be utilized for LSB1 and LSB2 steganography, respectively [29].

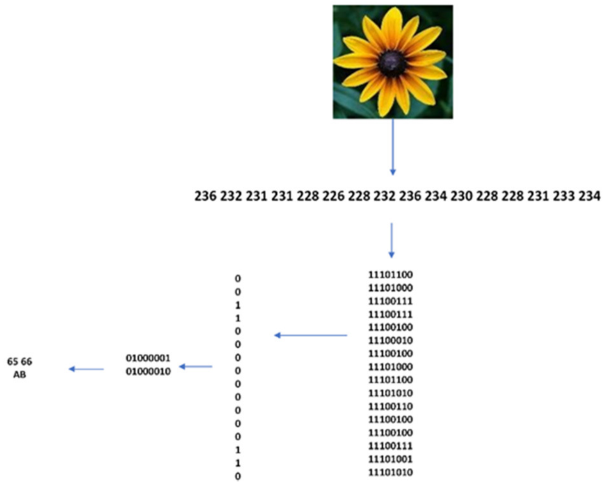

Fig. 2. LSB method of patch data extraction.

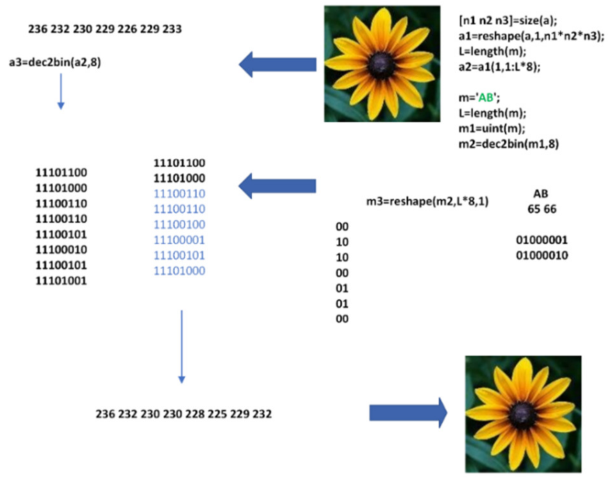

Fig. 3. LSB2 data-hiding using patching.

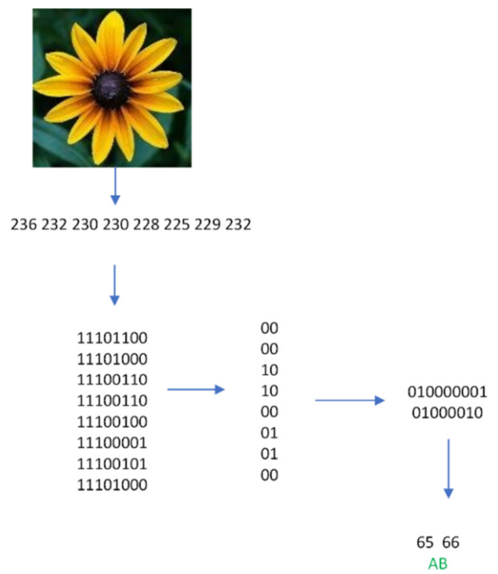

Fig. 4. LSB2 data extracting using patching.

The PK has a complex structure, as illustrated in Table I. It consists of the following components:

- L: Represents the length of the secret message to be hidden.
- P : Symbolizes the fraction parameter associated with message 1 and is used in the hiding process. Depending on the implementation details, this parameter's specific role may vary.
- r_1, x_1, r_2, x_2: These parameters are associated with Chaotic Logistic Map Models (CLMMs), which are variations or applications of the logistic map in the context of modeling complex systems or generating chaotic sequences. The logistic map itself is a mathematical model describing population growth. In the CLMM, the logistic map's iterative equation $x_{n+1} = r_n x_n (1 - x_n)$ is often employed as a tool for generating chaotic sequences or studying chaotic dynamics in different systems, and it is necessary to create two sets of CLKs. CLMMs are utilized as mathematical tools to produce sequences with chaotic behavior. The parameters r_1, x_1, r_2, x_2 serve as inputs to the CLMMs and impact the properties of the produced chaotic sequences.
- CLKs: key1 and key2 are the two CLKs created by the CLMMs. The keys are derived using a sorting algorithm on the chaotic sequences produced. key1 defines the sequence of cover bytes for data concealment, whereas key2 determines the sequence of cover bytes for data extraction. Non-sequential bytes for concealing and retrieving information are utilized so the keys may not adhere to a consecutive order.

TABLE I. PK STRUCTURE

PK					
P	L	r_1	x_1	r_2	x_2
Example					
0.35	100	3.77	0.12	3.91	0.2

Using the same PK in both stages is essential to maintain integrity and consistency in the message concealment and extraction procedure. Any changes to the primary key during extraction are unauthorized and may lead to the extraction of a corrupted or destroyed secret message. The CLKs produced are greatly influenced by the PK content, emphasizing the need to preserve the latter's integrity.

Figure 5 provides an example of the above statements manifesting the generation of key1 and key2.

III. THE PROPOSED METHOD

The proposed method leverages a PK to facilitate various operations. Initially, the confidential message is divided into two distinct components: message 1 and message 2. Message 1 undergoes scrutiny utilizing an enhanced LSB1 technique, whereas message 2 is subjected to an updated LSB2 approach. To ensure secure processing, two secret keys, key1 and key2, are generated by executing two CLMM. key1 is designated as the secret key governing the LSB section, while key2 assumes responsibility for the LSB2 section. This strategic division and encryption scheme aims to enhance the security and efficacy of the proposed method in concealing confidential information within cover images. Algorithms 3 and 4 explain how the sequential flow works.

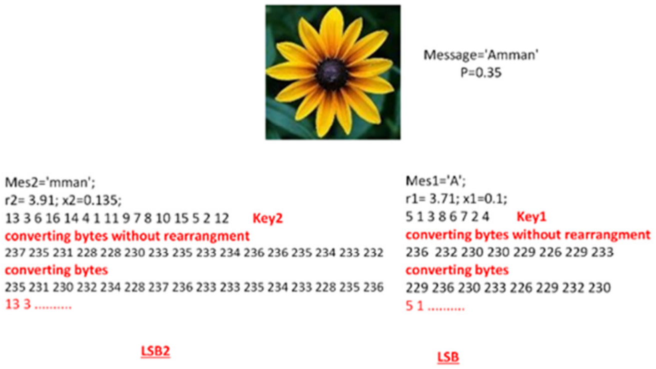

Fig. 5. An example of key1 and key2 generation.

```
Algorithm 3: Execution of the concealment phase
1. Acquiring the cover image
1.1:Obtain_Primary_Key(PK)
1.2:Obtain_Cover_Image()
1.3:Ascertain_Cover_Image_Dimensions()
1.4:Transform_Picture_Matrix_to_Single_Row_
Matrix
2: Preparation Message
2.1:Retrieve_Message_and_Calculate_Length(L)
2.2:Split_Message_Using_Private_Key(P)
2.3:Determine_Length_of_Each_Message(L1, L2)
2.4:Obtain_Cover_Bytes_for_Each_Message()
3:Generate the secret key
3.1:Extract_Disordered_Parameters_from_Private_
Key(PK)
3.2:Run_CLMM_to_Produce_Key1()
3.3:Run_CLMM_to_Produce_Key2()
4: Embedding message in the LSB
4.1:Use_Key1_to_Acquire_Cover_Bytes_for_Message
1()
4.2:Convert_Message1_to_Binary_Format()
4.3:Transform_Binary_Message1_into_Single_
Column_Matrix()
4.4:Translate_Cover_Byte_into_Binary_
Representation()
4.5:Assign_LSBs_of_BC1_to_BM1C()
4.6: Convert_BC1_Back_to_Decimal_Representation
()
4.7Reposition_Cover_Bytes_Using_Key()
5:Embedding message in the LSB2
5.1:Use_Key2_to_Acquire_Cover_Bytes_for_Message
2()
5.2:Convert_Message2_to_Binary_Format()
5.3:Transform_Binary_Message2_into_Two_Column_
Matrix()
5.4:Transform_Cover_Byte_into_Binary_
Representation()
5.5:Set_LSBs_of_BC2_to_BM2C()
5.6:Convert_BC2_to_Decimal_Representation()
5.7:Reposition_Cover_Bytes_Using_Key()
6:Obtaining a Steganographic Image
6.1:Regenerate_Initial_Bytes_of_Cover_Image_Row
_Matrix
6.2:Reinstate_Second_Cover_Bytes_into_Picture_
Row_Matrix()
6.3:Transform_Row_Matrix_into_3D_Matrix_to_
Create_Stego_Image()
```

```
Algorithm 4: Synopsis of the proposed
extraction method
1:Get the Stego image
1.1:Obtain_Private_Key(PK)
1.2:Retrieve_Stego_Image()
1.3:Ascertain_Stego_Image_Size(SI_size)
1.4:Transform_Picture_Matrix_to_Row_Matrix()
2:Generate a secret key
2.1:Extract_Disordered_Parameters(PK)
2.2:Run_CLMM_to_Produce_Key1()
2.3:Run_CLMM_to_Produce_Key2()
3: Prepare the stega byte
3.1:Find_Length_of_Message1(L1)
3.2:Find_Length_of_Message2(L2)
3.3:Retrieve_Stego_Bytes_for_Message1()
3.4:Retrieve_Stego_Bytes_for_Message2()
4: Extracting LSB1 data
4.1:Use_Key1_to_Retrieve_Steganographic_Bytes_
for_Message1()
4.2:Translate_Steganographic_Bytes_to_Binary_
Format()
4.3:Extract_LSBs_from_Binary_Output()
4.4:Reassemble_LSBs_into_Matrix()
4.5:Convert_Outcomes_to_Decimal_Form_for_
Message1()
5:Extracting data from LSB2
5.1:Use_Key2_to_Retrieve_Steganographic_Bytes_
for_Message2()
5.2:Translate_Steganographic_Bytes_to_Binary_
Format()
5.3:Extract_LSBs_from_Binary_Output()
5.4:Reassemble_LSBs_into_Matrix()
5.5:Convert_Outcomes_to_Decimal_Form_for_
Message2()
6:Combine messages and transform into
characters
6.1:Combine_Messages_to_Create_Hidden_Message()
6.2:Translate_Hidden_Message_to_Characters()
```

IV. RESULT ANALYSIS

This study uses a system that combines short and long messages along with different cover graphics to attain the best results.

A. *Visual Analysis*

To retain a message's secrecy, small alterations must be made to the SI while preserving its visual resemblance to the original cover image. The changes should be undetectable to the naked eye. The study's method was used to process a message of 1000 characters. Figures 6 and 7 display the outcomes obtained from this method. Figures 6 and 7 demonstrate the similarity between the SI and the cover image. Additionally, the color histograms of the cover image closely resemble those of the SI, which showcases the latter's quality.

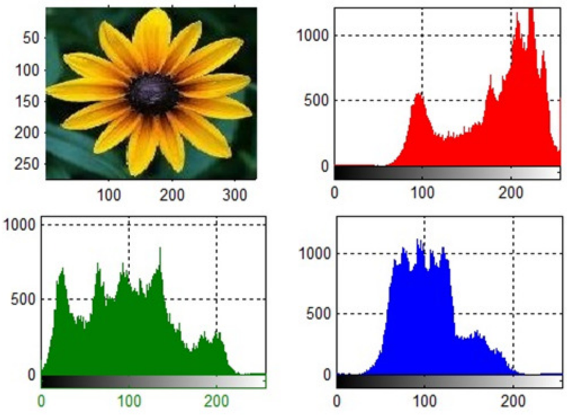

Fig. 6. Cover image (example).

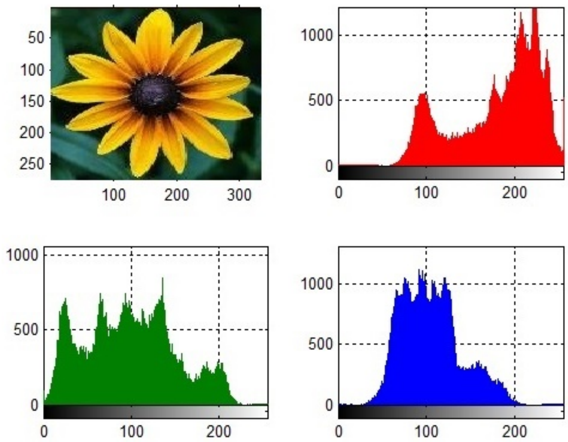

Fig. 7. Stego image (example).

B. Quality Analysis

Various measurements, such as the Mean Square Error (MSE) [30], Peak Signal-To-Noise Ratio (PSNR) [31], Correlation Coefficient (CC) [32], and the Number of Sample Change Ratio (NSCR) can assess the quality of a picture [33-34]. An effective data steganography technique should strive for a low MSE, a high PSNR, a CC close to 1, and a low Normalized Steganographic Capacity Rate value. The study's proposed strategy involved using and implementing several messages with the selected cover image shown in Figure 7. Quality parameters were computed for both the original and SIs, and the findings are displayed in Table II. The results demonstrate that the proposed method has effectively fulfilled the quality standards. The MSE rose as the message length increased, the PSNR declined, and the NSCR grew, as depicted in Figure 8. The CCs were calculated and continuously exhibited values near 1, suggesting a high association between the cover and the Stego images.

For better-quality parameter values, a larger cover image should be utilized. Enlarging the cover image can enhance the overall quality of the SI. The efficiency of the proposed method is not compromised even with a greater image size.

TABLE II. QUALITY PARAMETER RESULTS

Message length (bytes)	MSE	PSNR	NSCR
100	0.0029	169.4116	0.1214
200	0.0056	162.7618	0.2424
300	0.0090	157.9216	0.3670
500	0.0140	153.5340	0.6098
750	0.0217	149.1257	0.9255
1000	0.0290	146.2306	1.2155
2000	0.0580	139.3049	2.4512
3000	0.0865	135.3027	3.6995
4000	0.1159	132.3747	4.9290
5000	0.1465	130.0304	6.2072
Remarks	**Low**	**High**	**Low**

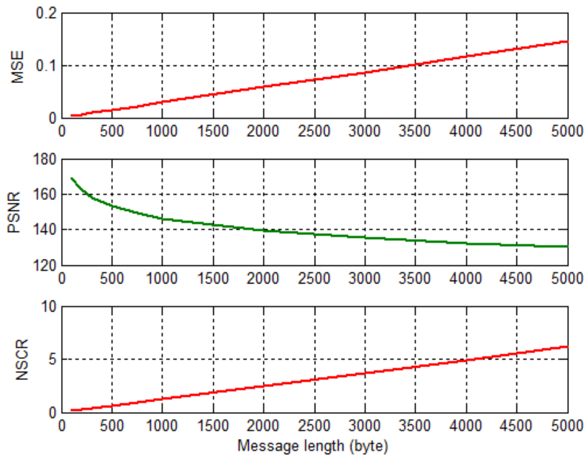

Fig. 8. Quality parameters vs message length.

C. Sensitivity Analysis

It is crucial for the proposed method to utilize the same PK during both the hiding and extraction phases. Any modifications or changes made to the private key during the extraction phase will be considered an unauthorized attempt to extract a potentially damaged message. To make a demonstration, PK1 was employed during the data-hiding phase to process the message "Improving data steganography." Subsequently, the remaining PKs were utilized during the data extraction phase, as outlined in Table V. The extracted messages resulting from this process are listed in Table V. The results presented in Table III indicate that the extraction phase of the proposed method is susceptible to even minor alterations in the contents of the PK. Any modifications made to the PK during the extraction phase can lead to corruption or loss of the secret message.

TABLE III. USED PKS IN THE EXTRACTION PHASE

PK1: $P1$=0.35; L=28; r_1=3.71; x_1=0.1; r_2=3.91; x_2=0.135;	**PK4**: $P1$=0.35; L=28; r_1=3.71; x_1=0.1; $\mathbf{r_2}$**=3.65**; x_2=0.135
PK2: $P1$=0.35; L=28; $\mathbf{r_1}$**=3.95**; x_1=0.1; r_2= 3.91; $\mathbf{x_2}$**=0.19**;	**PK5**: $P1$=0.75; L=28; r_1=3.71; x_1=0.1; r_2=3.91; x_2=0.135;
PK3: $P1$=0.35; L=28; $\mathbf{r_1}$**=3.95**; x_1=0.1; r_2=3.91; x_2=0.135;	**PK6**: $P1$=0.35; $\mathbf{L}$**=18**; r_1= 3.71; x_1=0.1; r_2=3.91; x_2=0.135;

TABLE IV. QUALITY PAREMETER RESULTS

PK in extraction phase	Extracted message	Remarks
PK1	Improving data steganography	Correct
PK2	<xï¿DDj_@uncÍv-tả ÑDàn 3ARDåi	Damaged
PK3	<¾Ÿ¿j_@ data steganography	Damaged
PK4	Improving@1£60`Ò³ ×"tAÅÉ#´ÊÒ	Damaged
PK5	h□ Azb#ÞV; 410c Ub #@08 ic"ØTal	Damaged
PK6	jtqboDgÝ:TFcåpJG¢	Damaged

Comparing the results of PSNR, MSE, and NSCR with the findings of previous studies can provide an insight into the proposed method's performance and applicability, as evidenced in Table V. It can be seen that the proposed method surpasses the others within the border of this paper’s technique.

TABLE V. QUALITY PARAMETER COMPARISON

Ref	PSNR	MSE	NSCR	Conclusion
[35]	High	Low	Moderate	Effective for preserving image quality
[36]	Moderate	Moderate	High	Strong correlation, suitable for detection
[37]	Low	High	Moderate	Challenges in preserving image quality
[38]	Moderate	Moderate	High	Balanced performance, suitable for various applications
[39]	High	Low	Moderate	High fidelity, suitable for imperceptible steganography
Proposed	High	Low	High	Superior quality, efficiency, security, and throughput

D. Speed Analysis

This study applied the proposed method to process the previous mentioned messages, measuring the Hiding Time (HT) and Extraction Time (ET). Hiding (HTP) and Extraction (ETP) Throughputs were also calculated to assess the method's efficiency. The obtained results are presented in Table VI.

TABLE VI. SPEED RESULTS

Message length (byte)	HT (s)	ET (s)	HTP (kB/s)	ETP (kB/s)
100	0.0184	0.0041	5.3076	23.7370
200	0.0216	0.0060	9.0440	32.7744
300	0.0239	0.0069	12.2530	42.2255
500	0.0312	0.0099	15.6273	49.5169
750	0.0407	0.0148	18.0054	49.3955
1000	0.0510	0.0209	19.1601	46.8059
2000	0.1026	0.0542	19.0426	36.0374
3000	0.1704	0.1042	17.1946	28.1110
4000	0.2533	0.1749	15.4232	22.3335
5000	0.3510	0.2529	13.9117	19.3050
Average				
1685	0.1064	0.0649	14.4970	35.0242

Table VI demonstrates that the proposed method offers acceptable data regarding the HTP and ETP. On average, the HTP is measured at 14.4970 kB/s, while the ETP is calculated at 35.0242 kB/s. The results also reveal that increasing the message length produces proportional increases in both HT and ET. Notably, using longer messages (exceeding 500 bytes) will decrease the throughput, as illustrated in Figure 9. To mitigate this issue, it is recommended to divide the message into smaller blocks, each with a size of less than or equal to 500 bytes. These blocks can be then treated as separate messages, allowing for more efficient processing and higher throughput.

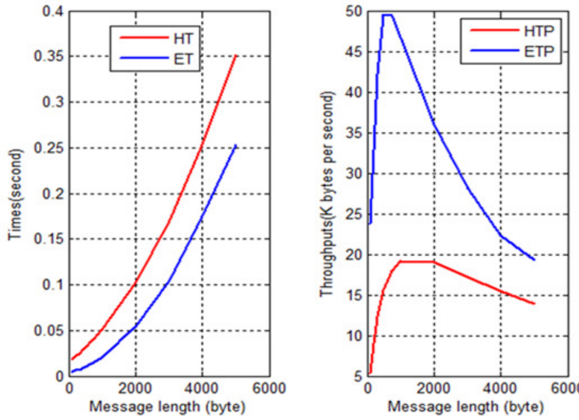

Fig. 9. Speed parameters vs message length.

E. Security Analysis

The PK in the proposed method consists of six components, each represented by a double data type. Consequently, the resulting key space can be presented as $2^{64} \times 6$ combinations, which is a vast key space, which significantly enhances the resistance against hacking attacks. The large number of possible combinations makes it computationally impossible to exhaustively search for or guess the correct PK, thereby ensuring the security and robustness of the method. To demonstrate the superiority of the proposed method, the latter is compared with several existing techniques, each evaluated based on specific performance criteria. Table VII summarizes the methodologies and performance metrics of these techniques.

TABLE VII. DIFFERENT TECHNIQUE COMPARISON

Ref	Methodology	Performance Criteria
[36]	PSNR measurement	Reliability and quality metrics using PSNR
[37]	CC for cover selection	Improved selection of cover images
[38]	Cryptographic techniques in modern CI processing	Security and computational performance analysis
[39]	Histogram features of MFCCs for emotion classification	Emotion classification accuracy
[40]	NTRU-LSB algorithm for cryptography and steganography	Enhanced security metrics
[41]	Separable reversible data hiding for 3D mesh models	Efficiency in data hiding and recovery
[42]	Pixel value differencing and LSB replacement	Adaptive steganographic performance
Proposed	Hybrid Data Steganography: Combination of LSB1 and LSB2 techniques using a patch method and PK with large key-space due to complex PK	Quality (MSE, PSNR), efficiency, security (CC, NSCR), and throughput

The proposed method integrates multiple LSB techniques, LSB1 and LSB2, with a patch method and utilizes a PK with a large key-space, providing significant improvements in several key performance areas:

- Quality: The method demonstrates superior MSE and PSNR values, indicating the higher fidelity of the steganographic process.
- Efficiency: The hybrid approach ensures efficient data embedding and extraction processes.
- Security: Using a complex PK enhances the security metrics, as evidenced by the improved correlation coefficients and NSCR values.
- Throughput: The method supports high throughput, which renders it suitable for practical applications.

Several existing methods primarily focus on specific aspects, such as PSNR, CCs, or cryptographic security, often at the expense of other critical performance criteria. The proposed method, in contrast, provides a balanced and comprehensive improvement across all evaluated metrics, constituting the superior choice for steganographic applications.

V. CONCLUSION

This research introduces a new hybrid data steganography method that enhances message hiding by splitting the message into two sections. The first section uses an enhanced LSB1 technique, while the second section employs an improved LSB2 technique for data steganography. The suggested method streamlines the data-hiding and extraction processes in LSB1 and LSB2 steganography by implementing a patching mechanism. Data-hiding and extraction are performed using a sophisticated Private Key (PK) that holds essential information for message splitting and secret key generation (key1 and key2). The keys are used to establish the sequence of cover and Stego bytes, aiding in the embedding and extraction procedures. Multiple messages were utilized during the execution of the proposed strategy, and the experimental outcomes were examined. The method's performance was evaluated by analyzing quality indicators, including Mean Square Error (MSE), Correlation Coefficient (CC), Peak Signal-To-Noise Ratio (PSNR), and the Number of Sample Changes Ratio (NSCR). The results showed that the proposed method meets the quality standards determined by these measures. The introduced method is fast and provides a satisfactory throughput, ensuring effective data hiding and extraction processes. The former also guarantees the confidentiality of the secret communication, which is important. The PK is essential for message security due to its complexity, which creates a large key space that makes hacking attempts difficult. Any alterations to the PK content during extraction may result in the retrieval of a corrupted message. Therefore, these alterations are deemed unlawful and jeopardize the integrity of the confidential message.

REFERENCES

[1] D. Nashat and L. Mamdouh, "An efficient steganographic technique for hiding data," *Journal of the Egyptian Mathematical Society*, vol. 27, no. 1, Dec. 2019, Art. no. 57, https://doi.org/10.1186/s42787-019-0061-6.

[2] I. F. Jafar, K. A. Darabkh, R. T. Al-Zubi, and R. R. Saifan, "An efficient reversible data hiding algorithm using two steganographic images," *Signal Processing*, vol. 128, pp. 98–109, Nov. 2016, https://doi.org/10.1016/j.sigpro.2016.03.023.

[3] Md. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal, and Md. D. Hossain, "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography," in *International Conference on Informatics, Electronics & Vision*, Dhaka, Bangladesh, Dec. 2014, pp. 1–6, https://doi.org/10.1109/ICIEV.2014.6850714.

[4] M.-L. Cruz, "Full image reconstruction with reduced speckle noise, from a partially illuminated Fresnel hologram, using a structured random phase," *Applied Optics*, vol. 58, no. 8, pp. 1917–1923, Mar. 2019, https://doi.org/10.1364/AO.58.001917.

[5] M. Bazyar and R. Sudirman, "A New Method to Increase the Capacity of Audio Steganography Based on the LSB Algorithm," *Jurnal Teknologi (Sciences & Engineering)*, vol. 74, no. 6, pp. 49–53, May 2015, https://doi.org/10.11113/jt.v74.4667.

[6] Z. Mi, H. Zhou, Y. Zheng, and M. Wang, "Single image dehazing via multi-scale gradient domain contrast enhancement," *IET Image Processing*, vol. 10, no. 3, pp. 206–214, 2016, https://doi.org/10.1049/iet-ipr.2015.0112.

[7] X. Yang, T. Mei, Y.-Q. Xu, Y. Rui, and S. Li, "Automatic Generation of Visual-Textual Presentation Layout," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 12, no. 2, Oct. 2016, Art. no. 33, https://doi.org/10.1145/2818709.

[8] G. Swain, *Advanced Digital Image Steganography Using LSB, PVD, and EMD: Emerging Research and Opportunities: Emerging Research and Opportunities*. Hershey, PA, USA: IGI Global, 2019.

[9] I. Zeger, S. Grgic, J. Vukovic, and G. Sisul, "Grayscale Image Colorization Methods: Overview and Evaluation," *IEEE Access*, vol. 9, pp. 113326–113346, Jan. 2021, https://doi.org/10.1109/ACCESS.2021.3104515.

[10] A. Y. Al-Rawashdeh and Z. Al-Qadi, "Using Wave Equation to Extract Digital Signal Features," *Engineering, Technology & Applied Science Research*, vol. 8, no. 4, pp. 3153–3156, Aug. 2018, https://doi.org/10.48084/etasr.2088.

[11] M. Aqel, Z. Al Qadi, and A. Abdullah, "RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication," *International Journal of Engineering & Technology*, vol. 7, no. 3, pp. 104–107, Jul. 2018, https://doi.org/10.14419/ijet.v7i3.13.16334.

[12] B. Zahran, Z. Al Qadi, J. Nader, and A. Abu-Ein, "A Comparison Between Parallel and Segmentation Methods Used for Image Encryption-Decryption," *International Journal of Computer Science and Information Technology*, vol. 8, no. 5, pp. 125–131, Nov. 2016, https://doi.org/10.5121/ijcsit.2016.8509.

[13] M. H. Mohamed, M. A. Mofaddel, and T. Y. Abd El-Naser, "Comparison Study Between Simple LSB and Optimal LSB Image Steganography," *Sohag Journal of Sciences*, vol. 8, no. 1, pp. 29–33, Jan. 2023, https://doi.org/10.21608/sjsci.2022.165686.1036.

[14] D. N. Tran, H.-J. Zepernick, and T. M. C. Chu, "LSB Data Hiding in Digital Media: A Survey," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 9, no. 30, Apr. 2022, Art. no. e3, https://doi.org/10.4108/eai.5-4-2022.173783.

[15] R. Shanthakumari and S. Malliga, "Retraction Note: Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," *Multimedia Tools and Applications*, vol. 82, no. 20, pp. 31865–31865, Aug. 2023, https://doi.org/10.1007/s11042-023-16005-5.

[16] U. Jayasankar, V. Thirumal, and D. Ponnurangam, "A survey on data compression techniques: From the perspective of data quality, coding schemes, data type and applications," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 2, pp. 119–140, Feb. 2021, https://doi.org/10.1016/j.jksuci.2018.05.006.

[17] K. Gupta, D. Gupta, S. K. Prasad, and P. Johri, "A Review on Cryptography based Data Security Techniques for the Cloud Computing," in *International Conference on Advance Computing and Innovative Technologies in Engineering*, Greater Noida, India, Mar. 2021, pp. 1039–1044, https://doi.org/10.1109/ICACITE51222.2021.9404568.

[18] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Information Security Journal: A Global*

Perspective, vol. 30, no. 2, pp. 63–87, Mar. 2021, https://doi.org/10.1080/19393555.2020.1801911.

[19] M. Jose, "Hiding Image in Image Using LSB Insertion Method with Improved Security and Quality," *International Journal of Science and Research*, vol. 3, no. 9, pp. 2281–2284, 2014.

[20] N. Mohamed, T. Rabie, and I. Kamel, "A Review of Color Image Steganalysis in the Transform Domain," in *14th International Conference on Innovations in Information Technology*, Al Ain, United Arab Emirates, Nov. 2020, pp. 45–50, https://doi.org/10.1109/IIT50501.2020.9299075.

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

[22] K. S. Minz and P. S. Yadav, "A Review on Secure Communication Method Based on Encryption and Steganography," *International Research Journal of Engineering and Technology*, vol. 6, no. 1, pp. 608–612, 2019.

[23] G. Mustafa, R. Ashraf, I. U. Haq, Y. Khalid, and R. U. Islam, "A Review of Combined Effect of Cryptography & Steganography Techniques to Secure the Information," in *5th International Conference on Computing Engineering and Design*, Singapore, Singapore, Apr. 2019, pp. 1–6, https://doi.org/10.1109/ICCED46541.2019.9161128.

[24] A. Singh, M. Rawat, A. K. Shukla, A. Kumar, and B. Singh, "An Overview of Pixel Value Differencing Based Data Hiding Techniques," in *Eleventh International Conference on Contemporary Computing*, Noida, India, Aug. 2018, pp. 1–3, https://doi.org/10.1109/IC3.2018.8530673.

[25] H. D. Najeeb, "Hiding voice message using both cryptography and steganography," *Al-Qadisiyah Journal Of Pure Science*, vol. 25, no. 1, pp. 10–17, 2020.

[26] R. H. Ali, B. N. Dhannoon, and M. I. Hamel, "Arabic text steganography using lunar and solar diacritics," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1559–1567, Sep. 2023, https://doi.org/10.11591/ijeecs.v31.i3.pp1559-1567.

[27] S. Malalla and F. R. Shareef, "A Novel Approach for Arabic Text Steganography Based on the 'BloodGroup' Text Hiding Method," *Engineering, Technology & Applied Science Research*, vol. 7, no. 2, pp. 1482–1485, Apr. 2017, https://doi.org/10.48084/etasr.1090.

[28] O. F. A. Wahab, A. A. M. Khalaf, A. I. Hussein, and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques," *IEEE Access*, vol. 9, pp. 31805–31815, Jan. 2021, https://doi.org/10.1109/ACCESS.2021.3060317.

[29] R. Das and I. Das, "Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques," in *Second International Conference on Research in Computational Intelligence and Communication Networks*, Kolkata, India, Sep. 2016, pp. 296–301, https://doi.org/10.1109/ICRCICN.2016.7813674.

[30] H. Kiya, A. P. M. Maung, Y. Kinoshita, S. Imaizumi, and S. Shiota, "An Overview of Compressible and Learnable Image Transformation with Secret Key and its Applications," *APSIPA Transactions on Signal and Information Processing*, vol. 11, 2022, Art. no. e11, https://doi.org/10.1561/116.00000048.

[31] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in Electric Power and Energy Systems," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 847–870, Apr. 2018, https://doi.org/10.1109/JIOT.2018.2802704.

[32] J. Vilkamo and T. Backstrom, "Time–Frequency Processing: Methods and Tools," in *Parametric Time-Frequency Domain Spatial Audio*, New York, NY, USA: John Wiley & Sons, 2017, pp. 1–24.

[33] A. H. K. MK and P. S. Aithal, "Voice Biometric Systems for User Identification and Authentication – A Literature Review," *International Journal of Applied Engineering and Management Letters*, vol. 6, no. 1, pp. 198–209, Apr. 2022, https://doi.org/10.47992/IJAEML.2581.7000.0131.

[34] L. Jiao, Y. Hao, and D. Feng, "Stream cipher designs: a review," *Science China Information Sciences*, vol. 63, no. 3, Feb. 2020, Art. no. 131101, https://doi.org/10.1007/s11432-018-9929-x.

[35] H. S. H. AlDerai and B. Kumar, "A Study of Image Encryption / Decryption by Using Elliptic Curve Cryptography 'ECC,'" *International Journal of Future Generation Communication and Networking*, vol. 13, no. 3, pp. 1148–1157, 2020.

[36] R. Kaur, J. Bhatia, H. Saini, and R. Kumar, "Multilevel Technique to Improve PSNR and MSE in Audio Steganography," *International Journal of Computer Applications*, vol. 103, no. 5, pp. 1–4, Oct. 2014, https://doi.org/10.5120/18067-9008.

[37] A. Almohammad and G. Ghinea, "Stego image quality and the reliability of PSNR," in *2nd International Conference on Image Processing Theory, Tools and Applications*, Paris, France, Jul. 2010, pp. 215–220, https://doi.org/10.1109/IPTA.2010.5586786.

[38] Y. Sun and F. Liu, "Selecting Cover for Image Steganography by Correlation Coefficient," in *Second International Workshop on Education Technology and Computer Science*, Wuhan, China, Mar. 2010, vol. 2, pp. 159–162, https://doi.org/10.1109/ETCS.2010.33.

[39] M. Samiullah *et al.*, "Rating of Modern Color Image Cryptography: A Next-Generation Computing Perspective," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, 2022, Art. no. 7277992, https://doi.org/10.1155/2022/7277992.

[40] M. Pakyurek, M. Atmis, S. Kulac, and U. Uludag, "Extraction of Novel Features Based on Histograms of MFCCs Used in Emotion Classification from Generated Original Speech Dataset," *Elektronika ir Elektrotechnika*, vol. 26, no. 1, pp. 46–51, Feb. 2020, https://doi.org/10.5755/j01.eie.26.1.25309.

[41] 41 S. Boukari and J. Bobbo, "An Improved Cybersecurity Model using Cryptography and Steganography with NTRU-LSB Algorithm," *SAR Journal - Science and Research*, vol. 3, no. 2, pp. 71–78, 2020, https://doi.org/10.18421/SAR32-04.

[42] R. Bhardwaj, "Efficient separable reversible data hiding algorithm for compressed 3D mesh models," *Biomedical Signal Processing and Control*, vol. 73, Mar. 2022, Art. no. 103265, https://doi.org/10.1016/j.bspc.2021.103265.

AUTHORS PROFILE

Ahmad A. Sharadqh received a B.Sc. in Computer Engineering and his MSc in Computing Systems and Networks from Kharkiv National University of Radio Electronics, Ukraine, in 2003 and 2004, respectively. Additionally, he obtained a Ph.D. in Computing Systems and Networks from the National Technical University of Ukraine, "Igor Sikorsky Kyiv Polytechnic Institute," Ukraine, in 2007. He is an Associate Professor at the Computer Engineering Department, Faculty of Engineering Technology, Al-Balqa Applied University. His research interests include network performance, quality of services, network security, IoT, and image processing.

Jawdat S. Alkasassbeh was born in 1983 in Jordan. He received a B.Sc. in communications engineering from the Department of Electrical Engineering, Faculty of Engineering, Mutah University, Al-Karak, Jordan, in 2006 and a master's degree in communications engineering from the University of Jordan, Amman, Jordan, in 2011. Alkasassbeh earned his PhD degree from the School of Mechanical Engineering and Electronic Information, China University of Geosciences, Wuhan, China, in 2021. He is an Assistant Professor at the Electrical Engineering Department at Al-Balqa Applied University, Amman, Jordan. His current research interests include applications of evolutionary algorithms, applied AI, power reduction of mobile communication mechanisms, digital wireless communication systems, radio link design, and digital image processing.

Tareq A. Alawneh was born in Irbid, Jordan, in 1984. He received the B.S. and M.S. degrees in computer engineering from the Jordan University of Science and Technology (JUST), Irbid, in 2006 and 2009, respectively, and the Ph.D. degree in computer engineering from the University of Hertfordshire, U.K., in 2021. From 2010 to 2013, he was a full-time Lecturer at the Electrical and Computer Engineering Department at Tafila Technical University (TTU), Al-Tafila, Jordan. In 2021, he was an Assistant Professor at Fahad Bin Sultan University (FBSU), Saudi Arabia. He is an Assistant Professor at the Electrical Engineering Department at Al-Balqa Applied University. His research interests include cache partitioning algorithms, low-power and high-performance designs, Dynamic Random-Access Memory (DRAM), cache memory, multicore systems, IoT, deep and machine learning, Chip Multiprocessors (CMPs) systems, image processing, algorithms, network security, computer networks, and embedded systems.

Aws Al-Qaisi is a professor at the Electrical Engineering Department, College of Engineering and Technology, American University of the Middle East, Kuwait. Prof. Al-Qaisi received his PhD and MSc in communication and signal processing from Newcastle University in 2006 and 2010, respectively. He is a member of the IEEE executive committee in Jordan, responsible for the industrial section. His research interests include feature extraction, artificial intelligence algorithms and transformations, and digital communication. He has been a reviewer for many international journals and has published more than 25 scientific papers in communication and signal processing.

Yahia Makableh earned a Bachelor's degree in Mechatronics Engineering from the University of Jordan, Jordan, in January 2009. He earned a master's degree in Applied Engineering and Mechatronics Systems from Georgia Southern University in May 2011. He earned a PhD in Electrical Engineering from the University of Arkansas, USA. He was awarded a research assistantship funded by NASA, the US Air Force, and the NSF to study high-efficiency photovoltaic devices, nanostructures, and nanomaterials. This research involves studying anti-reflection coatings, plasmonic effects, and hydrophobicity. He has several papers published in peer-reviewed journals, such as APL, SOLMAT, and Solar Energy. He served as the Material Research Society local chapter president at the University of Arkansas from 2011 to 2015. Now, he is an associate professor at The American University of the Middle East.

Safaa Y. Al Adwan is a researcher specializing in Artificial Intelligence (AI). Her current research focuses on Data Science at Universiti Kebangsaan Malaysia (UKM), where she is doing her Ph.D. (Expected in 2024). She is a computer engineer at the Innovation, Creativity, and Entrepreneurship Center (ICEC) at Al-Balqa Applied University, where she has been working since 2009. She received a B.S. from Al-Balqa Applied University in 2009 and an M.S. in computer science from the same university. Eng. Safaa is currently responsible for the innovative and entrepreneurial projects at the center.