Using Electrical Square Wave Form as an Efficient Carrying Media

Sara Al-Omari
Electrical Engineering Department, Faculty of Engineering Technology, Al-Balqa Applied University, Jordan
sara.omari@bau.edu.jo (corresponding author)

Received: 26 February 2025 | Revised: 9 April 2025 | Accepted: 19 April 2025

 DOI: https://doi.org/10.48084/etasr.10732

ABSTRACT

This paper proposes an efficient and simplified method of secret message steganography. The proposed method is characterized by its simplicity, efficiency, and security, which are achieved by utilizing a Square Wave (SW) signal as a carrying media. This signal can be readily generated, and its size can be controlled by the generation time and the sampling frequency. The SW signal can be efficiently processed; the samples can be readily converted from decimal fractions to binary, and from binary to decimal fractions. The 64-bit binary representation is employed to represent the sample values. This allows for the utilization of more Least Significant Bits (LSBs) for message hiding. The proposed method utilizes a set of LSBs for message hiding, with the length of this set ranging from 1 to 32 LSBs. The Private Key (PK) is used to determine the length of the set of LSBs and the sequence of LSBs employed for message hiding-extracting. The proposed method exhibits a high degree of sensitivity to the selected values of the PK. To ensure the efficacy of the hiding and extracting processes, it is imperative that these processes utilize precisely the same PK. The proposed method is implemented through the utilization of a variety of messages and PKs, and its efficacy in preserving the integrity of the stego SW is demonstrated. Furthermore, the sensitivity and the speed of the method are assessed to ensure that the proposed method meets the requirements of a effective stego method.

Keywords-carrying square wave; noise; stego square wave; secret message; Private Key (PK); Least Significant Bits (LSBs)

I. INTRODUCTION

Square Waves (SWs) are non-sinusoidal waveforms [1-4], distinguished by sudden transitions between minimum and maximum voltage levels, resulting in a series of square pulses. They find extensive use in digital systems, telecommunications, and switching power supplies due to their simplicity and suitability for digital applications. However, SWs can generate higher harmonic content, which may lead to issues such as Electromagnetic Interference (EMI) and distortion in sensitive analog circuits [3,4].

The SW samples have double data type values, and these values are fixed for a period of time, so we can add a noise to the SW to make the values different, as shown in Figures 1 and 2.

The generation of SW is a relatively straightforward process. The wave frequency (F), sampling frequency (SF), generation time (GT) and duty cycle (DC) can be selected to produce the desired SW. Figure 3 provides an example of generating a SW, and Figures 4 and 5 illustrate the plots of the generated SWs [3].

The number of generated samples can be controlled by adjusting the values of GT and SF. Increasing GT results in a longer SW, whereas increasing SF increases the total number of samples [5-9]. Each sample value is represented as a 64-bit binary number. Figure 6 illustrates an example of a SW sample representation [10-14].

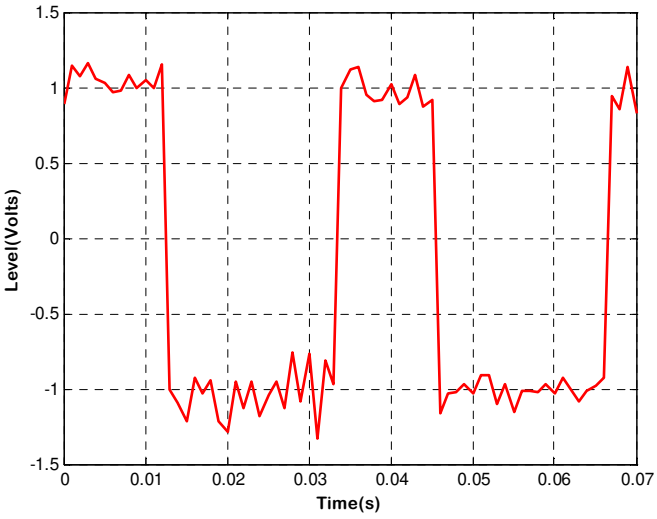

Fig. 1. SW with added noise.

SW samples (first 10)	SW with noise first 10 samples
1.0000	0.8750
1.0000	0.9593
1.0000	0.9327
1.0000	1.1547
1.0000	1.0198
1.0000	0.8815
1.0000	1.0224
1.0000	0.9678
1.0000	0.8847
1.0000	1.1041

Fig. 2. First 10 samples of the SW.

```
%Generate a 30 Hz square wave sampled at 1 kHz for 70 ms.
% Specify a duty cycle of 37%.
%Add white Gaussian noise with a variance of 1/100
t = 0:1/1e3:0.07;
y = square(2*pi*30*t,37)+randn(size(t))/10;
y1=square(2*pi*30*t,37);
subplot(1,2,1),plot(t,y1),grid on
subplot(1,2,2),plot(t,y),grid on
```

Fig. 3. An example of generating a SW.

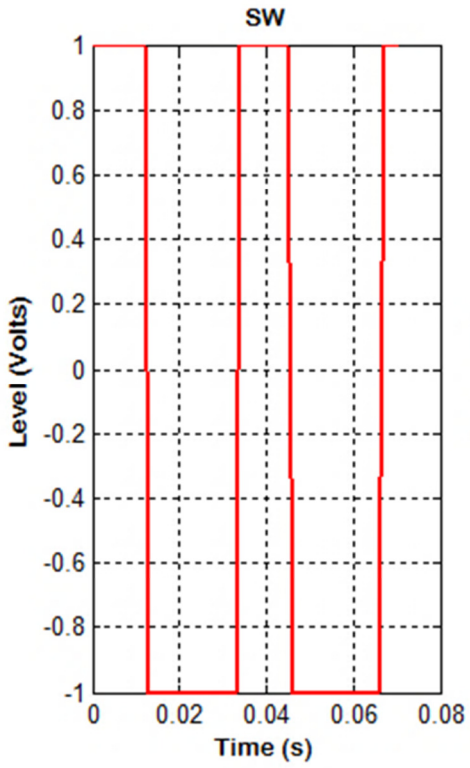

Fig. 4. The generated SW example.

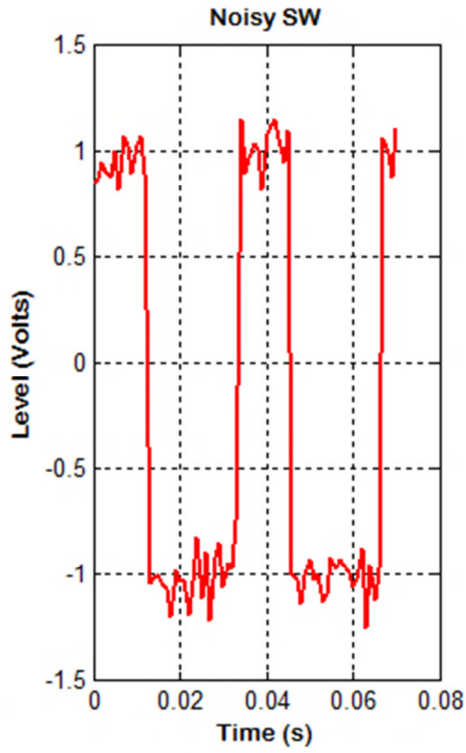

Fig. 5. The noisy generated SW example.

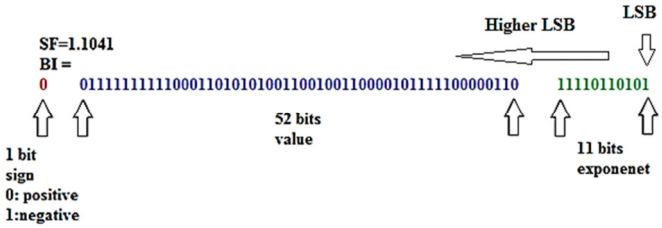

Fig. 6. Binary representation of a SW sample.

The 64-bit representation [15-18] of the SW sample is an excellent media for the utilization of the Least Significant Bits (LSBs) of the sample values to store the bits of other secret data, such as secret messages [19-23]. Changing one or more LSBs does not affect the sample value significantly, and the modified value must be close to the old value. The Mean Square Error (MSE) [24-26] between the two values must be low, whereas the Peak Signal to Noise Ratio (PSNR) must be high [27-34]. Based on this, we need to study the effect of changing any LSB of the sample value. To achieve this, the sample value shown in Figure 7 was selected and various LSBs of the binary version were changed from 0 to 1 or from 1 to 0. Table I shows the obtained new values of the sample [35-38].

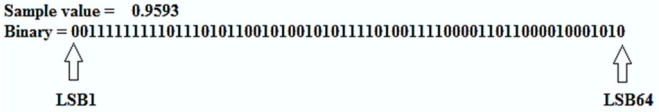

Fig. 7. Selected sample value.

TABLE I. EFFECTS OF CHANGING LSBS

LSB to be changed	New sample value	MSE	PSNR	Remarks
10	0.0600	0.8088	1.2908	Not close
11	0.2398	0.5176	5.7536	Not close
12	1.9186	0.9203	13.8629	Not close
13	0.7093	0.0625	26.8949	Not close
14	0.8343	0.0156	40.7578	Not close
15	0.8968	0.0039	54.6207	Not close
16	0.9906	9.7656e-004	69.1248	Not close
17	0.9437	2.4414e-004	82.3466	Close
18	0.9671	6.1035e-005	96.3718	Close
19	0.9554	1.5259e-005	110.0725	Close
20	0.9573	3.8147e-006	123.9355	Close
25	0.9592	3.7253e-009	193.2502	Close
33	0.9593	5.6843e-014	304.1537	Very close

As indicated in Table I, by changing LSB33, the new value of the sample will be close to the old one, the value of MSE between them will be very low, whereas the value of PSNR will be high [39-43]. Increasing the position of the used LSB will decrease the value of MSE and will increase the value of PSNR, so the set of LSBs between LSB33 and LSB64 can be used to hold the bits of other secret data without significant effect on the values of the SW samples. Numerous methods are used for data steganography by hiding the secret message in a covering media such as SW to create a stego media, which must be close to the covering media. A lot of the existing methods of data steganography are based on LSB and LSB2 methods [44-50]. These methods share certain characteristics that can be regarded as vulnerabilities. The novelty of the proposed method is to address these vulnerabilities as follows [51-60]:

- Existing methods provide insufficient security. Knowing that the stego media contains a message and with good programming experience it is possible to hack the message. The proposed method addresses this vulnerability by using a Private Key (PK). The PK contains information about the LSBs used for data hiding, such as how many LSBs are used, and what is the sequence of these LSBs. The proposed method is able to use 1 LSB, 2 LSBs, 4 LSBs, 8 LSBs, 16 LSBs, and 32 LSBs for message hiding.
- Existing methods mostly utilize digital color images as a covering media. The proposed method uses a SW with noise, as this signal can be easily generated and saved. The size of this signal can be easily controlled by the GT and SF values.
- The capacity hiding (the maximum message length that can be hidden) of the LSB based-method is equal to the covering media size divided by 8, whereas the capacity hiding of the LSB2-based method is equal to the covering media size divided by 4. The capacity hiding of the proposed method depends on the selected number of LSBs, and it ranges from the SW size divided by 8 to the SW size multiplied by 4.
- LSB-based method provides a moderate speed of data hiding and data extracting. The proposed method has the ability to increase the speed by using more LSBs for data hiding.
- LSB based methods hide the message characters in consecutive cover bytes, thus some arithmetic and logical operation are required. The proposed method applies data hiding/extracting by using simple replacement operation based on the reshaped required binary matrices; the characters are hidden in different inconsecutive samples.

II. PROPOSED METHOD

The proposed method uses a SW signal, which is generated with a size capable of holding the required secret message to be hidden. The SW size is controlled by the GT and the SF of the signal. The generated samples are converted to binary using 64_binary representation and the LSBs from LSB33 to LSB64 can be used for message hiding. Furthermore, a PK is utilized, that indicates the number of LSBs used for message hiding and the sequence of the LSBs used. Table II shows the PK structure and Table III shows some PK samples.

TABLE II. PK STRUCTURE

PK		
Number of used LSBs	**Sequence of LSBs**	
	Starting LSB	Last LSB

TABLE III. PK SAMPLES

PK sample	Meaning
1 64:64	1 LSB used, LSB64 is to be used
1 35:35	1 LSB used, LSB35 is to be used
2 63:64	2 LSBs used , LSB63 and LSB64 are to be used
4 33:36	4 LSBs used, LSBs from 33 to 36 are to be used
32 33:64	32 LSBs used, LSBs from 33 to 64 are to be used
32 64:33	32 LSBs used, LSBs from 64 to 33 are to be used
8 40:47	8 LSBs used, LSBs from 40 to 47 are to be used

The proposed method allows the user to select the required LSBs and their sequence; the following are the user's choices:

- 1 LSB, which can be any bit from LSB33 to LSB64. Here, the SW capacity hiding is equal to the SW size divided by 8.
- 2 LSBs from the range LSB33 to LSB64 Here, the SW capacity hiding is equal to the SW divided by 4.
- 4 LSBs from the range LSB33 to LSB64 Here, the capacity hiding of the SW is equal to the SW size divided by 2.
- 8 LSBs from the range LSB33 to LSB64. Here, the capacity hiding of the SW is equal to the SW size.
- 16 LSBs from the range LSB33 to LSB64. Here, the capacity hiding of the SW is equal to the SW size multiplied by 2.
- 32 LSBs from the range LSB33 to LSB64. Here, the capacity hiding of the SW is equal to the SW size multiplied by 4.

Both LSB and LSB2 based methods provide a stego media with good quality, the MSE between the covering media and the stego media is low, whereas the PSNR is high. The proposed method will decrease the value of MSE and will increase the value of PSNR. The selected number of LSBs for

message hiding will affect the quality of the stego SW and the speed of message hiding/extraction. Decreasing the number of LSBs will enhance the quality of the stego SW, whereas increasing the number of LSBs will increase the speed of message steganography by decreasing both the hiding and extracting times.

III. HIDING ALGORITHM

Hiding algorithm is implemented by applying the following steps:

- Step 1: Covering SW preparations:
  1. Get the GT, the SF.
  2. Generate the signal of SW.
  3. Add Gaussian noise to the generated SW.
- Step 2: PK preparation:
  1. Select the number of LSBs to be used for message hiding.
  2. Select the sequence of the LSBs.
- Step 3: Message preparation:
  1. Get the message.
  2. Get the message length (L).
  3. Convert the message to binary.
- Step 4: Message hiding:
  1. Get the cover samples from the covering SW based on the number of used LSBs.
  2. Convert the cover samples to binary using 64-bit binary representation.
  3. Reshape the message binary matrix to the number of columns to match the selected number of LSBs.
  4. Let the selected sequence of binary samples equal to the reshaped message binary matrix.
  5. Convert the cover samples back to decimal.
  6. Return the cover samples back to SW to get the stego SW.
  7. Save the stego SW.
  8. Save the message length L.

IV. EXTRACTING ALGORITHM

Extracting algorithm is implemented by applying the following steps:

- Step 1: Stego SW preparation:
  1. Load the stego SW.
  2. Load the message length L.
- Step 2: PK preparation:
  1. Select the number of LSBs used for message hiding.
  2. Select the sequence of the LSBs.
- Step 3: Message extraction:
  1. Get the stego samples based on the number of selected LSBs.
  2. Convert the stego sample to binary.
  3. Get the columns from stego binary values based on the selected sequence of LSBs.
  4. Reshape the results into an 8-column matrix to get the message binary matrix.
  5. Convert the message binary matrix to decimal and then to characters to get the secret message.

V. IMPLEMENTATION AND RESULTS DISCUSSION

A message of 1,500 characters was selected and implemented using the proposed method Variant PKs were used, and the MSE and PSNR values were calculated between each of the covering SW and the associated stego SW. Table IV presents the obtained quality results.

TABLE IV. QUALITY RESULTS

No of used LSBs	Used LSBs	MSE	PSNR
1	64	9.2076e-033	743.4428
1	40	2.5468e-018	411.8457
1	33	4.2957e-014	313.8111
2	63:64	2.3354e-032	734.2927
2	40:41	1.6298e-018	416.2234
2	33:34	2.5710e-014	319.6490
4	61:64	2.1491e-031	712.3769
4	40:43	8.3558e-019	422.1088
4	33:36	1.3973e-014	325.2118
8	57:64	2.4566e-029	664.9445
8	40:47	4.0462e-019	429.5867
8	33:40	6.7331e-015	332.4974
16	49:64	7.8536e-025	561.1285
16	40:55	2.1675e-019	436.3069
16	33:48	3.2467e-015	339.8422
32	33:64	1.6492e-015	347.7325

From Table IV, it can be observed that using any PK, the stego SW is always close to the covering SW. The MSE remains low in all cases, whereas PSNR remains high. Increasing the number of LSBs used decreases the PSNR, but the quality of the stego SW remains excellent. Figure 8 shows the covering and stego SW, holding 1500 characters and using 32 LSBs for message hiding. The proposed method is very sensitive to the selected values of the PK; the extracting processes must use the same PK that was used in the hiding process. Any minor changes in the PK in the extracting process will be considered as a hacking attempt by producing a corrupted extracted message. To demonstrate this fact, the message "Using square wave as an efficient carrying media" was hidden using PK1, the hidden message was extracted by each of the following PKs shown in Figure 9, and the obtained results shown in Table V prove the sensitivity of the proposed method.

TABLE V. PROPOSED METHOD SENSITIVITY

Used PK in the extracting process	Extracted message
PK1	Using square wave as an efficient carrying media
PK2	□□J□r©rT□□□#p¤□B□\W□1□□L@□□□□Ré□□U□□□ à□Ÿf□t□□à
PK3	]a@□□Y□Y_=%'"□«¾!□□Jx□i6³□©Y□□1:□1□%□□□¨J°~□□6D
PK4	□¢àm□□□□□y□□□¢□□□□□□□°BŸ`G□´³□□µg`³□¦z¬¦ëj□N□
PK5	□□□g□□□#□"□□□ézèj8n□□=p□¸□□¢X□C□□ªr□□ □□□□□\2□□
PK6	□□□□□¢□G»vë□$V¶□□ù1□□□□š□□□ç□ï§□×w□%□ô m£□b÷G¾□

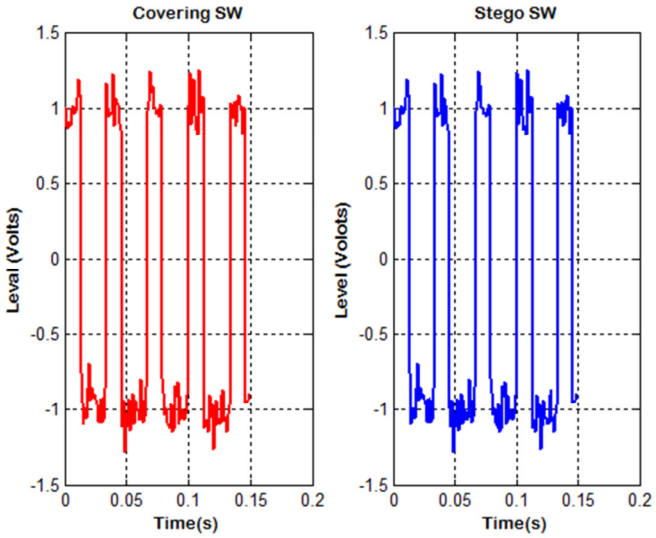

Fig. 8. Stego SW holding 1500 characters.

PK1:
1 33:33
PK2:
1 64:64
PK3:
2 50:51
PK4:
4 40:43
PK5:
1 32:32
PK6:
1 34:34

Fig. 9. The set of PKs used to extract the hidden message.

The speed of the proposed method was also examined and it was found that the selected PK affects the speed. Furthermore, increasing the number of LSBs used for message hiding decreases both the hiding and extracting times, thus increasing the speed of message steganography. To demonstrate this, a message of 1500 characters was hidden in a covering SW using various PKs, and Table VI shows the obtained speed results.

The proposed method provided satisfactory speed results. The average hiding throughput was equal to 6.6 KB/s, whereas the average extracting throughput was equal to 20.01 KB/s. The speed of the proposed method can be increased by increasing the number of LSBs used for message hiding; when 32 LSBs are used for message hiding the speed increases to 20.6316 KB/s, whereas the extracting speed increases to 45.7764 KB/s.

TABLE VI. SPEED RESULTS

No of used LSBs	PK	Hiding time (s)	Extracting time (s)
1	1 40:40	0.5340	0.1600
2	2 63:64	0.3440	0.1000
4	4 61:64	0.1750	0.0640
8	8 57:64	0.1170	0.0450
16	16 49:64	0.0870	0.0380
32	32 33:64	0.0710	0.0320
Average		0.2213	0.0732
Average throughput (KB/s)		6.6193	20.0115

VI. CONCLUSION

In this study, a method is proposed for the utilization of a Square Wave (SW) signal as a carrying media. This media can be readily generated, saved and loaded, and its size can be readily controlled by adjusting the generation time and the sampling frequency. A simple noise was incorporated into the SW signal to vary the samples values, and the samples values were represented using 64-bits binary representation. It was demonstrated that changing the bits from LSB33 to LSB64 had a negligible impact on the sample values. The proposed method utilizes a set of Least Significant Bits (LSBs) to contain the secret message bits, with the set length and the sequence of used LSBs determined by a secret Private Key (PK). This PK provides a satisfactory level of message security. The hiding and extracting processes use the same PK as the method is highly sensitive to the selected values of the PK. Furthermore, the proposed method provides variable hiding capacity. The SW signal has the capacity to contain a message of any length, ranging from the SW signal size divided by 8 to signal the size multiplied by 4, depending on the selected PK.

The proposed method has the potential to effectively replace the LSB and LSB2 methods of message steganography. Additionally, it can be expanded to utilize any set of LSBs for message hiding, while maintaining a high signal quality and a high speed for both message hiding and extraction.

The proposed method yielded satisfactory results in terms of speed. The average hiding throughput was equal to 6.6 KB/s, whereas the average extraction throughput was equal to 20.01 KB/s. Moreover, the speed of the proposed method can be increased by increasing the number of LSBs utilized for message bits hiding. When utilizing 32 LSBs for message hiding the speed of message hiding increases to 20.6316 KB/s, whereas the extraction speed increases to 45.7764 KB/s.

The proposed method was tested and implemented using various messages and various PKs and it was shown that the method was efficient when using any PK, satisfying the quality, speed, and security requirements of an effective stego method.

REFERENCES

[1] M. A. F. Al-Husainy, "Comparison Study Between Classic-LSB, SLSB and DSLSB Image Steganography," in *6th International Conference on Information Technology (Cloud Computing)*, Amman , Jordan, 2013.

[2] Z. A. A. Alqadi, M. K. Abu Zalata, and G. M. Qaryouti, "Comparative Analysis of Color Image Steganography," *International Journal of Computer Science and Mobile Computing*, vol. 5, no. 11, pp. 37–43, Nov. 2016.

[3] J. R. Rodriguez, J. W. Dixon, J. R. Espinoza, J. Pontt, and P. Lezana, "PWM regenerative rectifiers: state of the art," *IEEE Transactions on Industrial Electronics*, vol. 52, no. 1, pp. 5–22, Feb. 2005, https://doi.org/10.1109/TIE.2004.841149.

[4] M. Abuzalata, Z. Alqadi, J. Al-Azzeh, and Q. Jaber, "Modified Inverse LSB Method for Highly Secure Message Hiding," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 2, pp. 93–103, Feb. 2019.

[5] R. J. Rasras, Z. A. AlQadi, and M. R. A. Sara, "A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages," *Engineering, Technology & Applied Science Research*, vol. 9, no. 1, pp. 3681–3684, Feb. 2019, https://doi.org/10.48084/etasr.2380.

[6] X. Zhou, W. Gong, W. Fu, and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science*, Okayama, Japan, 2016, pp. 1–4, https://doi.org/10.1109/ICIS.2016.7550955.

[7] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9, pp. 1613–1626, Jun. 2003, https://doi.org/10.1016/S0167-8655(02)00402-6.

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

[9] R. J. Rasras, M. R. A. Sara, Z. A. AlQadi, and R. A. Zneit, "Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 8, no. 3, pp. 748–754, Jun. 2019, https://doi.org/10.30534/ijatcse/2019/64832019.

[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] K. Matrouk, A. Al-Hasanat, H. Alasha'ary, Z. Al-Qadi, and H. Al-Shalabi, "Speech Fingerprint to Identify Isolated Word-Person," *World Applied Sciences Journal*, vol. 31, no. 11, pp. 1767–1771, 2014.

[12] S. Khawatreh, B. Ayyoub, A. Abu-Ein, and Z. Alqadi, "A Novel Methodology to Extract Voice Signal Features," *International Journal of Computer Applications*, vol. 179, no. 9, pp. 40–43, Jan. 2018.

[13] Z. Alqadi, B. Zahran, Q. Jaber, B. Ayyoub, and J. Al-Azzeh, "Enhancing the Capacity of LSB Method by Introducing LSB2Z Method," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 3, pp. 76–90, Mar. 2019.

[14] M. O. Al-Dwairi, Z. A. Alqadi, A. A. AbuJazar, and R. A. Zneit, "Optimized True-Color Image Processing," *World Applied Sciences Journal*, vol. 8, no. 10, pp. 1175–1182, 2010.

[15] W. A. Ulbeh, A. Moustafa, and Z. A. Alqadi, "Gray image reconstruction," *European Journal of Scientific Research*, vol. 27, no. 2, pp. 167–173, Jan. 2009.

[16] A. A. Moustafa and Z. A. Alqadi, "Color Image Reconstruction Using A New R'G'I Model," *Journal of Computer Science*, vol. 5, no. 4, pp. 250–254, Apr. 2009, https://doi.org/10.3844/jcssp.2009.250.254.

[17] H. A. Alasha'ary, K. M. Matrouk, A. I. Al-Hasanat, Z. A. Alqadi, and H. M. Al-Shalabi, "Improving Matrix Multiplication Using Parallel Computing," *International Journal on Information Technology*, vol. 1, no. 6, pp. 346–349, Nov. 2013, https://doi.org/10.15866/ireit.v1i6.6427.

[18] B. Zahran, Z. Alqadi, J. Nader, and A. A. 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. 127–133, Oct. 2016, https://doi.org/10.5121/ijcsit.2016.8509.

[19] K. Matrouk, A. Al-Hasana, H. Alasha'ary, Z. Al-Qadi, and H. Al-Shalabi, "Analysis of Matrix Multiplication Computational Methods," *European Journal of Scientific Research*, vol. 121, no. 3, pp. 258–266, 2014.

[20] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, and M. Mesleh, "A Novel Based On Image Blocking Method To Encrypt-Decrypt Color," *JOIV : International Journal on Informatics Visualization*, vol. 3, no. 1, pp. 86–93, Jan. 2019, https://doi.org/10.30630/joiv.3.1.210.

[21] J. Al-Azzeh, B. Zahran, Z. Alqadi, B. Ayyoub, and M. Abu-Zaher, "A Novel Zero-Error Method to Create a Secret Tag for an Image," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 13, pp. 4081–4091, Jul. 2018.

[22] J. Al-Azzeh, Z. Alqadi, and Q. M. Jabber, "Statistical Analysis of Methods used to Enhance RGB Color Image Histogram," in *XX International Scientific and Technical Conference*, Kursk, Russia, 2017, pp. 8–15.

[23] J. Al-Azzeh, H. Alhatamleh, Z. A. Alqadi, and M. K. Abuzalata, "Creating a Color Map to be used to Convert a Gray Image to Color Image," *International Journal of Computer Applications*, vol. 153, no. 2, pp. 31–34, Nov. 2016, https://doi.org/10.5120/ijca2016911975.

[24] R. J. Rasras, M. Abuzalata, Z. Alqadi, J. Al-Azzeh, and Q. Jaber, "Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation," *International Journal of Computer Science and Mobile Computing*, vol. 18, no. 3, pp. 14–26, Mar. 2019.

[25] A. AlQaisi, M. AlTarawneh, Z. A. Alqadi, and A. A. Sharadqah, "Analysis of color image features extraction using texture methods," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 3, pp. 1220–1225, Jun. 2019, https://doi.org/10.12928/telkomnika.v17i3.9922.

[26] B. Zahran, J. Al-Azzeh, Z. Alqadi, A. Al, M.-A. Al-Zoghoul, and S. Khawatreh, "A Modified LBP Method to Extract Features from Color Images," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 10, pp. 3014–3024, May 2018.

[27] J. Al-Azzeh, B. Zahran, and Z. Alqadi, "Salt and Pepper Noise: Effects and Removal," *JOIV : International Journal on Informatics Visualization*, vol. 2, no. 4, pp. 252–256, Jul. 2018, https://doi.org/10.30630/joiv.2.4.151.

[28] J. Nader, Z. A. A. Alqadi, and B. Zahran, "Analysis of Color Image Filtering Methods," *International Journal of Computer Applications*, vol. 174, no. 8, pp. 12–17, Sep. 2017.

[29] Z. Alqadi, B. Zahran, and J. Nader, "Estimation and Tuning of FIR Lowpass Digital Filter Parameters," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 7, no. 2, pp. 18–23, Mar. 2017, https://doi.org/10.23956/ijarcsse/V7I2/01209.

[30] M. M. Abu-Faraj, Z. A. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods," *Journal of Hunan University Natural Sciences*, vol. 48, no. 12, pp. 177–182, Dec. 2021.

[31] M. T. Barakat and Z. A. Alqadi, "Highly Secure Method for Secret Data Transmission," *International Journal of Scientific Engineering and Science*, vol. 6, no. 1, pp. 49–55, Jan. 2022.

[32] M. M. Abu-Faraj and Z. A. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," *International Journal of Computer Science and Network Security*, vol. 21, no. 12, pp. 648–656, Dec. 2021, https://doi.org/10.22937/IJCSNS.2021.21.12.89.

[33] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Deep Machine Learning to Enhance ANN Performance: Fingerprint Classifier Case Study," *Journal of Southwest Jiaotong University*, vol. 56, no. 6, pp. 685–694, Dec. 2021.

[34] M. M. Abu-Faraj and Z. A. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," *International Journal of Computer Science and Network Security*, vol. 21, no. 12, pp. 451–458, Dec. 2021, https://doi.org/10.22937/IJCSNS.2021.21.12.61.

[35] M. M. Abu-Faraj and Z. A. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," *International Journal of Computer Science and Network Security*, vol. 21, no. 12, pp. 53–60, Dec. 2021, https://doi.org/10.22937/IJCSNS.2021.21.12.8.

[36] A. Hindi, M. O. Dwairi, and Z. Alqadi, "Procedures for Speech Recognition using LPC And ANN," *International Journal of Engineering Technology Research & Management*, vol. 4, no. 2, pp. 48–55, Feb. 2020.

[37] Z. A. Alqadi and M. T. Barakat, "A Case Study to Improve the Quality of Median Filter," *International Journal of Computer Science and Mobile Computing*, vol. 10, no. 11, pp. 19–28, Nov. 2021, https://doi.org/10.47760/ijcsmc.2021.v10i11.004.

[38] H. Zaini and Z. Alqadi, "High Salt and Pepper Noise Ratio Reduction," *International Journal of Computer Science and Mobile Computing*, vol. 10, no. 9, pp. 88–97, Sep. 2021, https://doi.org/10.47760/ijcsmc.2021.v10i09.009.

[39] M. K. Abu Zalata, H. N. Hatamleh, and Z. A. Alqadi, "Detailed Study of Low Density Salt and Pepper Noise Removal from Digital Color Images," *International Journal of Computer Science and Mobile Computing*, vol. 11, no. 2, pp. 56–67, Feb. 2022, https://doi.org/10.47760/ijcsmc.2022.v11i02.007.

[40] M. Abu-Faraj, A. Al-Hyari, K. Aldebei, Z. A. Alqadi, and B. Al-Ahmad, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," *IEEE Access*, vol. 10, pp. 69388–69397, 2022, https://doi.org/10.1109/ACCESS.2022.3187317.

[41] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Experimental Analysis of Methods Used to Solve Linear Regression Models," *Computers, Materials & Continua*, vol. 72, no. 3, pp. 5699–5712, Apr. 2022, https://doi.org/10.32604/cmc.2022.027364.

[42] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," *Symmetry*, vol. 14, no. 4, Apr. 2022, Art. no. 664, https://doi.org/10.3390/sym14040664.

[43] M. M. Abu-Faraj, K. Aldebei, and Z. A. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," *Traitement du Signal*, vol. 39, no. 1, pp. 173–178, Feb. 2022, https://doi.org/10.18280/ts.390117.

[44] M. M. Abu-Faraj and M. Zubi, "Analysis and implementation of kidney stones detection by applying segmentation techniques on computerized tomography scans," *Italian Journal of Pure and Applied Mathematics*, no. 43, pp. 590–602, Feb. 2020.

[45] Z. Alqadi, "Bits Substitution to Secure LSB Method of Data Steganography," *International Journal of Computer Science and Mobile Computing*, vol. 11, no. 8, pp. 9–21, Aug. 2022, https://doi.org/10.47760/ijcsmc.2022.v11i08.002.

[46] M. S. Khrisat and Z. A. Alqadi, "Enhancing LSB Method Performance Using Secret Message Segmentation," *International Journal of Computer Science & Network Security*, vol. 22, no. 7, pp. 383–388, Jul. 2022, https://doi.org/10.22937/IJCSNS.2022.22.7.47.

[47] M. S. Khrisat, A. Manasreh, H. G. Zaini, and Z. A. Alqadi, "Cover Image Rearrangement to Secure LSB Method of Data Steganography," *ARPN Journal of Engineering and Applied Sciences*, vol. 17, no. 3, pp. 295–302, Feb. 2022.

[48] M. K. A. Zalata, M. T. Barakat, and Z. A. Alqadi, "Carrier Image Rearrangement to Enhance the Security Level of LSB Method of Data Steganography," *International Journal of Computer Science and Mobile Computing*, vol. 11, no. 1, pp. 182–193, Jan. 2022, https://doi.org/10.47760/ijcsmc.2022.v11i01.024.

[49] M. T. Barakat and Z. A. Alqadi, "Image Transformation to Increase the Security Level of LBS Method of Data Steganography," *International Journal of Engineering Technology Research & Management*, vol. 6, no. 1, pp. 42–53, Jan. 2022.

[50] N. Asad, I. Shayeb, Q. Jaber, B. Ayyoub, Z. Alqadi, and A. Sharadqh, "Creating a Stable and Fixed Features Array for Digital Color Image," *International Journal of Computer Science and Mobile Computing*, vol. 8, no. 8, pp. 50–62, Aug. 2019.

[51] M. O. Al-Dwairi, A. Y. Hendi, M. S. Soliman, and Z. A. A. AlQadi, "A new method for voice signal features creation," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 5, pp. 4092–4098, Oct. 2019, https://doi.org/10.11591/ijece.v9i5.pp4092-4098.

[52] A. A. Moustafa and Z. A. Alqadi, "A Practical Approach of Selecting the Edge Detector Parameters to Achieve a Good Edge Map of the Gray Image," *Journal of Computer Science*, vol. 5, no. 5, pp. 355–362, May 2009, https://doi.org/10.3844/jcssp.2009.355.362.

[53] Z. A. A. Alqadi, M. Aqel, and I. M. M. El Emary, "Performance Analysis and Evaluation of Parallel Matrix Multiplication Algorithms," *World Applied Sciences Journal*, vol. 5, no. 2, pp. 211–214, 2008.

[54] I. Shayeb, N. Asad, Z. Alqadi, and Q. Jaber, "Evaluation of speech signal features extraction methods," *Journal of Applied Science, Engineering, Technology, and Education*, vol. 2, no. 1, pp. 69–78, May 2020, https://doi.org/10.35877/454RI.asci2151.

[55] A. Kaur, R. Dhir, and G. Sikka, "A New Image Steganography Based On First Component Alteration Technique." arXiv, Jan. 12, 2010, https://doi.org/10.48550/arXiv.1001.1972.

[56] A. Martin, G. Sapiro, and G. Seroussi, "Is image steganography natural?," *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2040–2050, Dec. 2005, https://doi.org/10.1109/TIP.2005.859370.

[57] D. Bhattacharyya, A. Roy, P. Roy, and T. Kim, "Receiver Compatible Data Hiding in Color Image," *International Journal of Advanced Science and Technology*, vol. 6, pp. 15–24, May 2009.

[58] N. A. Aletawi, M. A. A. Sameha, and Z. Alqadi, "Modified LSB2 Steganography Method to Secure the Embedded Secret Message," *International Journal of Computer Science and Mobile Computing*, vol. 11, no. 8, pp. 22–44, Aug. 2022, https://doi.org/10.47760/ijcsmc.2022.v11i08.003.

[59] D. Pleacher. "Calculating Password Entropy." Pleacher. https://www.pleacher.com/mp/mlessons/algebra/entropy.html.

[60] H. G. Zaini, "Image Segmentation to Secure LSB2 Data Steganography," *Engineering, Technology & Applied Science Research*, vol. 11, no. 1, pp. 6632–6636, Feb. 2021, https://doi.org/10.48084/etasr.3859.