Enhancing LSB Method Performance Using Secret Message Segmentation

Mohammad S. Khrisat[1†] and Ziad A. Alqadi[2††],
mkhrisat@bau.edu.jo dr.ziad.alqadi@bau.edu.jo
Balqa Applied university, Faculty of engineering Technology, Amman Jordan

Summary
Many methods used for secret data steganography are based on least significant bit method, which is suffering from security and the embedded message can be easily hacked. In this paper research a proposed method of adding security issues will be introduced, a complex private key will be constructed, the contents of this key will depend on the results of secrete message segmentation. The proposed method will be implemented and the obtained experimental results will be compared with least significant method results to prove that the proposed method raises the image quality parameters.

Keywords:
Steganography, PK, MSE, PSNR, quality, LSB, efficiency.

1. Introduction

The digital color image[1], [2] is a huge data collector that can be used to hide confidential data and messages[3]; in addition to that the digital image can be easily obtained and processed in easy and simplified ways[4], [5].
The colored digital image is represented by a three-dimensional matrix, where the first dimension is assigned to the red color, the second dimension to the green color, and the third dimension to the blue color. It is easy to separate these colors and deal with each two-dimensional matrix (color matrix) separately, just as it is dealt with a gray image [6]. And for the previous reasons, the digital color image is used as an excellent environment to hide confidential data [7]. [8] to protect it from intruders, and the process is called data steganography as shown in figure 1.

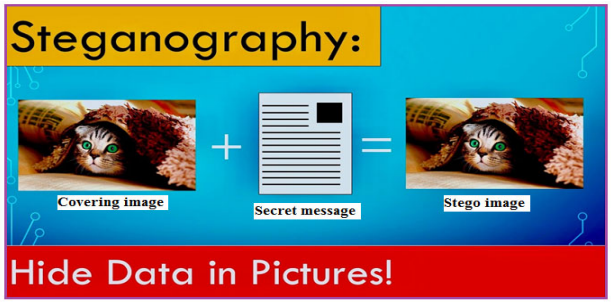


Figure 1: Data steganography

The process of data steganography requires the generation a stego image carrying confidential data that does not differ from the original image [21] and the differences cannot be noticed with the naked eye. Therefore, the method of hiding must fulfill the following conditions [9[, [10], [11]:

- Small value of mean square error (MSE)[19] between the original and the stego images [14], [15], [16].
- High value of the peak signal to noise ratio (PSNR) [20] between the original and the stego images (see equations 1 to 3[17], [18].
- Small times for data hiding and data extraction.

Securing the data by preventing intruders and people who are not authorized to view confidential data by not enabling them to retrieve the data properly [12], [13].

MSE of x channel

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

Total MSE

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

$$PSNR = 10 * \log_{10}\frac{(MAX_I)^2}{MSE_t} \tag{3}$$

Many methods are used to hide data, and many of them are based on the least significant (LSB) method.
LSB method of data steganography is a very simple method of data steganography and it has good features by providing good values for MSE and PSNR, but it is not secure and it can be easily hacked.
LSB can be implemented by applying the following sequence of operation:

Manuscript received July 5, 2022
Manuscript revised July 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.7.47

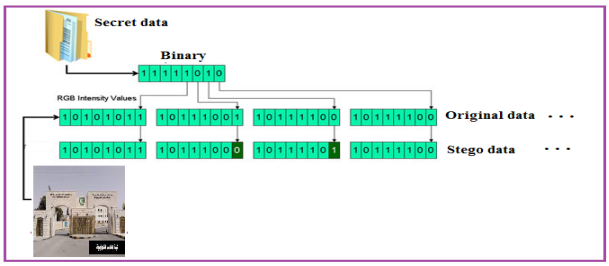


Figure 2: LSB operations

- Converting the secrete message to binary and reshaping the binary result to 1D array.
- Converting the covering image to binary and reshaping the resulting image to 1D array.
- Reserving 8 bytes from the image (starting from the first position) to hide 1 byte from the message.
- Using the LSB in each byte of the set of 8 bytes to store one it of the message byte (see figure 2), this step must be repeated for each byte of the secret message.
- Converting the obtained stego image to decimal and reshaping it back to 3D matrix.

Figures 3 and 4 show an example of hiding a message of 100 characters in a color image using LSB method:

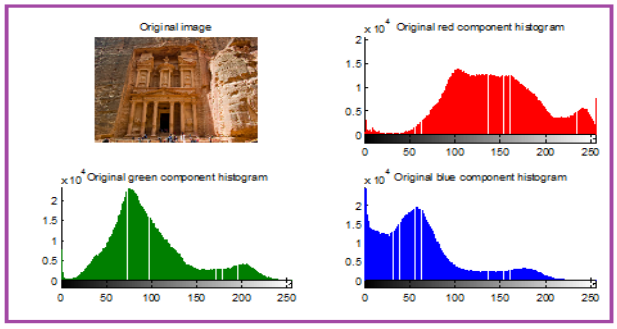


Figure 3: Original image

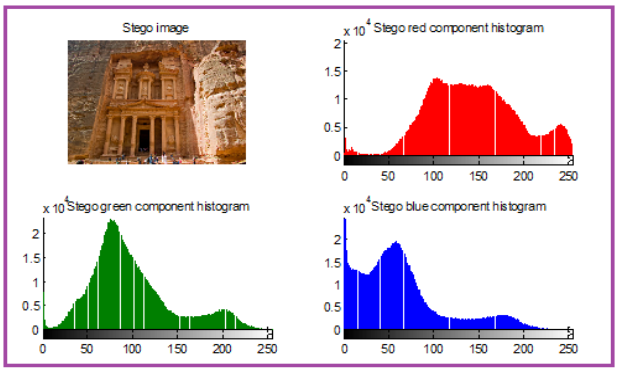


Figure 4: Stego image (Using LSB method)

2. The Proposed Method

The security of the proposed method can be achieved by introducing a private key (PK) which is to be used in the process of secrete message steganography. The secrete message must be divided into 3 segments with various length , each segment must be hidden in a color channel, so we have to select the color sequence(red=1, green=2, blue=3), then the bit plan number must be defined, figure 5 shows the structure of the PK, while figure 6 shows an example of PK.

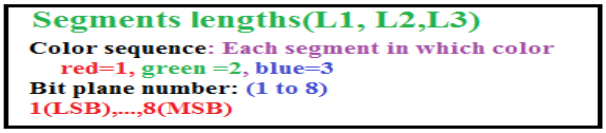


Figure 5: PK structure

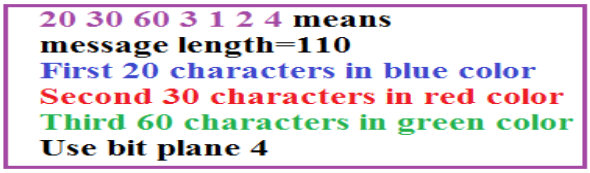


Figure 6: PK example

The defined PK can be used in the hiding and extracting process as show in the following steps on the proposed method implementation (See figure 7):

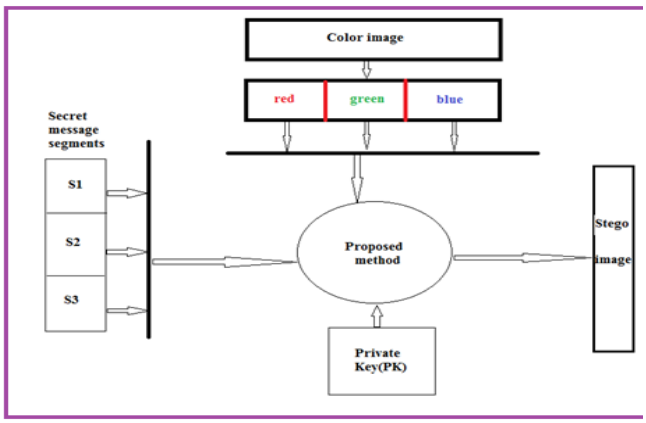


Figure 7: Proposed method implementation

For each message segment get the color channel and bit plane and apply the following
Step 1: Converting the required reshaped covering image ID matrix to a stream of binary bits (B1).
Step 2: Converting the ASCII value of the message segment to a stream of binary bits (B2).
Step 4: for each character reserve 7 pixels form B1.
Step 5: Reset all the bits in each set (the selected bit number =bit plane).
Step 6: Find the indexes of all bits which are equal 1 in B2.
Step 7: Adjust the associative to indexes bits in B1 to 1.
Step 8: Convert the resulting image to decimal, and reshape it back to 2D matrix.
After hiding the three segments, reshape back the three colors to one 3D matrix to get the stego image.

3. Implementation and experimental results

Figure 8 shows the images which were used in the implementation process of LSB and the proposed method.

Figure 8: Used images

Figure 9 shows the covering image to hide 75 characters (PK=25 30 20 1 2 3 1), while figure 10 shows the stego image.

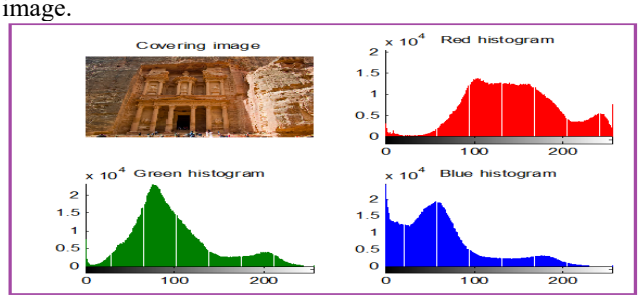


Figure 9: Covering image

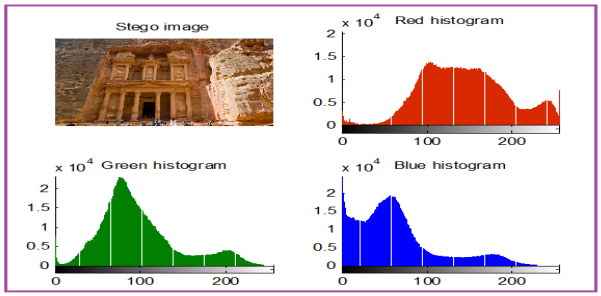


Figure 10: Stego image using proposed method

The above shown images where used to hide and extract message with length equal 75 characters using LSB and proposed methods (PK=25 30 20 1 2 3 1) tables 1 and 2 show the obtained experimental results:

Table 1: Results of quality parameters (MSE and PSNR) (message length=75 characters)

Image number	Size(byte)	LSB		Proposed	
		MSE	PSNR	MSE	PSNR
1	150849	0.0115	155.4550	0.0019	173.4708
2	77976	0.0251	147.6803	0.0034	167.7073
3	518400	0.0012	178.2430	5.1505e-004	186.5378
4	5140800	3.9177e-004	189.2737	5.1548e-005	209.5552
5	4326210	3.8787e-004	189.3737	6.1486e-005	207.7923
6	122265	0.0117	155.3314	0.0022	172.2052
7	518400	0.0012	178.2430	5.6134e-004	185.6771
8	150975	0.0060	162.0500	0.0019	173.4444
9	150975	0.0119	155.1241	0.0018	174.1269
10	151353	0.0122	154.8966	0.0018	174.1519
Average	1.1308e+006	0.0082	166.5671	0.0014	182.4669

Table 2: Results of efficiency parameters (hiding and extracting times) (message length=75 characters)

Image number	Size(byte)	LSB		Proposed	
		Hiding time(second)	Extraction time(second)	Hiding time(second)	Extraction time(second)
1	150849	0.0840	0.0350	0.0070	0.0530
2	77976	0.0450	0.0350	0.0020	0.0200
3	518400	0.0560	0.0370	0.0060	0.0210
4	5140800	0.2110	0.0790	0.0030	0.0200
5	4326210	0.1970	0.0710	0.0020	0.0200
6	122265	0.0460	0.0350	0.001	0.0200
7	518400	0.0570	0.0390	0.0020	0.0210
8	150975	0.0480	0.0340	0.0030	0.0200
9	150975	0.0470	0.0350	0.0020	0.0200
10	151353	0.0470	0.0350	0.0010	0.0200
Average	1.1308e+006	0.0838	0.0435	0.0029	0.0235

From tables 1 and 2 we can see that the proposed method enhanced the values of quality parameters, and the efficiency parameters values were closed to LSB method values.

The same implementations were taken using a message of 150 characters; the obtained results are shown in tables 3 and 4:

Table 3: Results of quality parameters (MSE and PSNR) (message length=150 characters)

Image number	Size(byte)	LSB		Proposed	
		MSE	PSNR	MSE	PSNR
1	150849	0.0237	148.2316	0.0036	167.0394
2	77976	0.0506	140.6623	0.0069	160.6255
3	518400	0.0024	171.3115	0.0010	179.5317
4	5140800	7.9015e-004	182.2582	1.0854e-004	202.1089
5	4326210	7.7920e-004	182.3976	1.2343e-004	200.8233
6	122265	0.0231	148.4986	0.0043	165.3689
7	518400	0.0024	171.3115	0.0011	179.0067
8	150975	0.0117	155.2810	0.0036	167.0295
9.	150975	0.0244	147.9673	0.0035	167.3830
10	151353	0.0248	147.8145	0.0036	167.1833
Average	1.1308e+006	0.0165	159.5734	0.0028	175.6100

Table 4: Results of efficiency parameters (hiding and extracting times) (message length=150 characters)

Image number	Size(byte)	LSB		Proposed	
		Hiding time(second)	Extraction time(second)	Hiding time(second)	Extraction time(second)
1	150849	0.0470	0.0340	0.0050	0.0690
2	77976	0.0440	0.0350	0.0020	0.0340
3	518400	0.0740	0.0380	0.0040	0.0670
4	5140800	0.2110	0.0860	0.0040	0.0330
5	4326210	0.1910	0.0760	0.0020	0.0350
6	122265	0.0460	0.0340	0.0050	0.0340
7	518400	0.0560	0.0390	0.0030	0.0350
8	150975	0.0550	0.0340	0.0010	0.0440
9	150975	0.0520	0.0340	0.0030	0.0370
10	151353	0.0470	0.0350	0.0020	0.0370
Average	1.1308e+006	0.0823	0.0445	0.0031	0.0425

From table 3 and 4 we can see that the results prove the achieved enhancement using the proposed method.

The proposed method was implemented using various values of bit plane number, and it was shown that if we use the higher number (8=MSB) the quality parameters remain acceptable as shown in figures 11 and 12 and table 5.

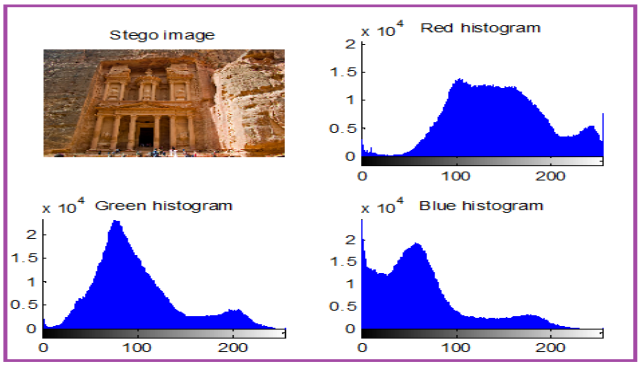


Figure 11: Stego image for bit plane=1 (100 characters)

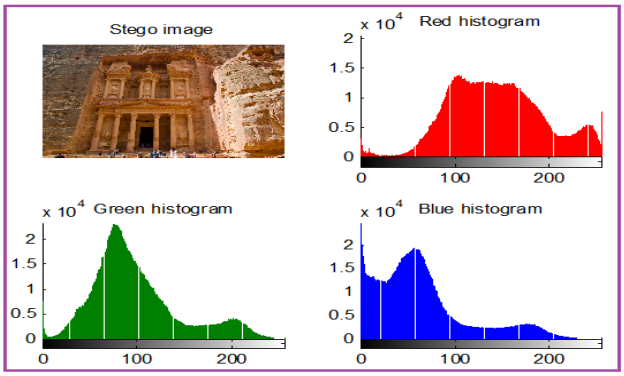


Figure 11: Stego image for bit plane=8 (100 characters)

Table 5: Quality parameters using various numbers of bit plane

Bit plane	MSE	PSNR
1	4.8631e-005	210.1379
2	2.0230e-004	195.8827
3	8.4656e-004	181.5686
4	0.0030	168.7920
5	0.0130	154.2555
6	0.0580	139.3045
7	0.1825	127.8376
8	0.9625	111.2076

4. Conclusion

A secure method of secret data steganography was proposed and implemented; the method was compared with LSB method. The proposed method require a private key for hiding and extracting data, this key is sophisticated making the hacking process very difficult. The proposed method is very simple and it is easy to implement, the obtained results showed that the proposed method provides good quality and efficiency parameters, and they are better than those for LSB method.

References

[1] Brown AS, Brown RJ, Coleman PJ, Conolly C, Sweetman AJ, Jones KC, et al, Twenty years of measurement of polycyclic aromatic hydrocarbons (PAHs) in UK ambient air by nationwide air quality networks. Environ Sci Process Impacts. 2013; 15(6):1199–215.

[2] Jia, Y.K., Ding, R.T., Ren, W., Shu, J.F., Jin, A.X. (2021). Gesture recognition of somatosensory interactive acupoint massage based on image feature deep learning model. Traitement du Signal, Vol. 38, No. 3, pp. 565-572. https://doi.org/10.18280/ts.380304

[3] F. Anctil, C. Perin, V. Andreassian, Impact of the length of observed records on the performance of ANN and of conceptual parsimonious rainfall-runoff forecasting models, Environ. Model. Softw. 19 (2004) 357–368.

[4] Chu, W., Hung, WC., Tsai, YH. *et al.* Learning to Caricature via Semantic Shape Transform. *Int J Comput Vis* **129,** 2663–2679 (2021). https://doi.org/10.1007/s11263-021-01489-1

[5] Ebrahim Ahmadlooa, Sadra Azizib, Prediction of thermal conductivity of various nanofluids using artificial neural network, International Communications in Heat and Mass Transfer, Volume 74, May 2016, Pages 69-75 https://doi.org/10.1016/j.icheatmasstransfer.2016.03.008

[6] Agay-Shay K, Friger M, Linn S, Peled A, Amitai Y, Peretz C. Air pollution and congenital heart defects. Environ Res. 2013; 124:28–34.

[7] M. Taghi Sattari, Kadri Yurekli, Mahesh Pal, Performance evaluation of artificial neural network approaches in forecasting reservoir inflow, Applied Mathematical Modelling, Volume 36, Issue 6,2012,Pages 2649-2657,ISSN0307-904X, https://doi.org/10.1016/j.apm.2011.09.048.

[8] Al Jallad F, Al Katheeri E, Al Omar M. Concentrations of particulate matter and their relationships with meteorological variables. Sustain Environ Res. 2013; 23(3):191–8.

[9] P.A.W. Lewis, B.K. Ray, Nonlinear modeling of periodic threshold auto regressions using TSMARS, J. Time Ser. Anal. 23 (4) (2002) 459–471

[10] S.K. Jain, Development of integrated sediment rating curves using ANNs, J. Hydraul. Eng. 127 (2001) 30–37.

[11] Khrisat, M.S., Zneit, R.S.A., Zaini, H.G., Alqadi, Z.A. (2021). Analysis methods used to extract fingerprints features. Traitement du Signal, Vol. 38, No. 3, pp. 711-717. https://doi.org/10.18280/ts.380318

[12] H.K. Cigizoglu, Suspended sediment estimation for rivers using artificial neural networks and sediment rating curves, Turkish J. Eng. Environ.Sci. 26(2002) 27–36.

[13] X.K. Wang, W.Z. Lu, S.Y. Cao, D. Fang, Using time-delay neural network combined with genetic algorithms to predict runoff level of Linshan Watershed,Sichuan, China, J. Hydrol. Eng. 12 (2) (2007) 231–236.

[14] Muammer Ozgoren, Mehmet Bilgili, Besir Sahin, Estimation of global solar radiation using ANN over Turkey, Expert Systems with Applications, Volume 39, Issue 5,2012, Pages 5043-5051, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2011.11.036.

[15] Muammer Ozgoren, Mehmet Bilgili, Besir Sahin, Estimation of global solar radiation using ANN over Turkey, Expert Systems with Applications, Volume 39, Issue 5, 2012, Pages 5043-5051, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2011.11.036.

[16] Harish Kumar Ghritlahre, Purvi Chandrakar, Ashfaque Ahmad, Application of ANN model to predict the performance of solar air heater using relevant input parameters, Sustainable Energy Technologies and Assessments, Volume 40, 2020, 100764, ISSN 2213-1388, https://doi.org/10.1016/j.seta.2020.100764.

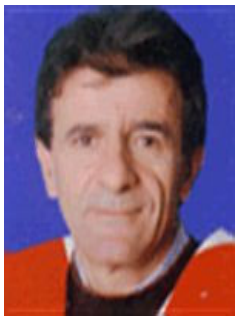
[17] Tadic, V. and S. Stankovic (2000). Learning in neural net-works by normalized stochastic gradient algorithm: Lo-cal convergence. In: Proc. 5th Seminar Neural Netw. Appl. Electr. Eng. (Yugoslavia, Sept. 2000), pp. 11–17.

[18] de Faria, V.A.D., de Queiroz, A.R., Lima, L.M. et al. An assessment of multi-layer perceptron networks for streamflow forecasting in large-scale interconnected hydro systems. Int. J. Environ. Sci. Technol. (2021). https://doi.org/10.1007/s13762-021-03565-y

[19] Lau, E.T., Sun, L. & Yang, Q. Modelling, prediction and classification of student academic performance using artificial neural

networks. SN Appl. Sci. 1, 982 (2019). https://doi.org/10.1007/s42452-019-0884-7
[20] Ravindra Nath Yadav, Vinod Yadava. (2021) Multi-response optimization for sequential application of erosion–abrasion in face grinding configuration. International Journal for Computational Methods in Engineering Science and Mechanics 22:5, pages 345-357.
[21] Amal Al-Rasheed, identification of important features and data mining classification techniques in predicting employee absenteeism at work, International Journal of Electrical and Computer Engineering (IJECE)Vol.11, No.5, October2021, pp. 4587~4596
[22] Sun, H., Wang, L., Yang, Z. et al. Research on Construction Engineering Quality Management Based on Building Information Model and Computer Big Data Mining. Arab J Sci Eng (2021). https://doi.org/10.1007/s13369-021-05601-y
[23] Gong Weidong, Guo Deyong1, Liang Yueqiang, Prediction Model of Coal and Gas Outburst Based on Rough Set-Unascertained Measure Theory, J. Eng. Technol. Sci., Vol. 50, No. 6, 2018, 758-777
[24] Muhammad Ali Musarat, Wesam Salah Alaloul, M.S. Liew, Ahsen Maqsoom, Abdul Hannan Qureshi, Investigating the impact of inflation on building materials prices in construction industry, Journal of Building Engineering, Volume 32, 2020, 101485, ISSN 2352-7102, https://doi.org/10.1016/j.jobe.2020.101485.
[25] Mohd Hairi Mohd Zaman, M.Marzuki Mustafa, M.A.Hannan, Aini Hussain , Neural Network Based Prediction of Stable Equivalent Series Resistance in Voltage Regulator Characterization, Bulletin of Electrical Engineering and InformaticsVol.7, No.1, March2018, pp. 134~142ISSN: 2302-9285, DOI: 10.11591/eei.v7i1.857
[26] Khrisat, M.S., Zaini, H.G., Alqadi, Z.A. (2021). Simple, flexible method to extract digital image features. Traitement du Signal, Vol. 38, No. 5, pp. 1509-1514. https://doi.org/10.18280/ts.380527
[27] Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Ahmad Sharadqh, Proposed Implementation Method to Improve LSB Efficiency, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 306-319, 2019.

Mohammad S. Khrisat assistances professor in faculty of engineering technology Balqa applied university Amman Jordan received the Ph.D. in the mechatronics engineering from People friendship university of Russia in 2017 and get the master's degree in computer engineering from NYIT and B.Sc. in electronic Engineering from Yarmouk university Irbid Jordan. He can be contacted at email: mkhrisat@bau.edu.jo.



Ziad A. Alqadi professor in Balqa applied university faculty of engineering technology electrical engineering department, received the Ph.D. in computer engineering from Igor Sikorsky Kyiv Polytechnic Institute 1986 and frim the same university get the master and the B.sc in the computer engineering, He can be contacted at email: dr.ziad.alqadi@bau.edu.jo.