Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 14, Issue. 2, February 2025, pg.14 – 22

A Highly Secure Method to Hide DCI in SPWS

Naseem Masoud Asad; Ismail Ghazi Shayeb; Taha Sami Othman

Albalqa Applied University, Jordan Amman

DOI: https://doi.org/10.47760/ijcsmc.2025.v14i02.002

Abstract: A simple and efficient method of digital color image steganography will be introduced, the method will replace the popular color image used as a covering method in most recently existing method by a simple saw tooth periodic wave signal, this signal can be easily generated, and the size in samples of this signal can be easily controlled by the selected values of the generation time and the sampling frequency. The covering SPWS samples will be presented using 64_bits binary presentation, while the unsigned decimal values of the secret image to be hidden will be presented using 8_bits binary presentation. Changing the 32 LSBs of the covering samples will not much affect the sample value, so each sample will be used to hold 4 bytes from the secret image, thus the capacity hiding will increased and it will equal the size of SPWS in samples multiplied by 4. The proposed method will use a batch operation to replace-extract the 32 LSBs of the covering samples using only one operation based on the reshaping process of the binary matrices. The proposed method will be tested using various images, the obtained results will be used to prove the enhancements provided by the proposed method in the quality and speed of image steganography.

Keywords: Steganography, SPWS, DCI, Covering samples, stego samples, IBM, RIBM, SBM.

Introduction

Digital color image (DCI) [1-10] is one of the most popular digital data type, it is now used in many computer vital applications, and it may secret, private or it may contains confidential data, so it requires protection to prevent any hacking attacks. One of the easiest way to protect DCI is image steganography, which means hiding DCI in another covering media without affecting much the covering media, the holding media (stego) media will be transmitted and the receiver will use this media to extract the source hidden DCI [11-16].

A good stego method must meet the following requirements [17-22]:

- The extracted DCI must be the same as the hidden DCI; the mean square error (MSE) [23-29] between them must be zero, while the peak signal to noise ratio (PSNR) between them must be infinite [30-35].
- The stego media must have a high quality, it must be closed to the covering media to eliminate any doubts that the media is holding a secret data; here the MSE between the covering media and the stego media must be very low, while the PSNR must be very high.
- The method must minimize both the hiding and extracting times and it must maximize the speed of image steganography [36-40].
- Easy to program and easy to implement, the method must use simple hiding and extracting function, the process of image hiding-extracting must be simplified.

DCI as a secret data type can be easily processed [41-46], it is usually represented by a 3D matrix (one 2D matrix for each color: red, green and blue) as shown in figure 1, the following DCI processing operations can be easily implemented [47-53]:

- Reshaping the 3D matrix to one row matrix and vise versa.
- Converting the decimal values of the image colors to binary to obtain the image binary matrix (IBM), see figure 1 [54-60].
- Easy to reshape IBM to 32 columns to get the reshaped IBM (RIBM).

In this paper research we will use a generated saw tooth periodic wave signal (SPWS) as a covering media for the following reasons:

- Easy to generate the SPWS with any size, depending on the selected generation time (t) and the sampling frequency (fs) we can generate a SPWS with a required size, this size in samples will equal t multiplied by fs.
- The samples values are double data type, each sample has a fractional value within the range -1 to +1, the decimal values of the samples can be easily converted to binary to get the saw tooth signal binary matrix (STBM) as shown in figure 2.
- The 64_bits binary representation of the sample value gives us the ability to use the 32 least significant bits to hide the DCI bits, each sample will hold 4 bytes from the image, and thus the capacity hiding in bytes will equal the SPWS size in samples multiplied by 5.
-

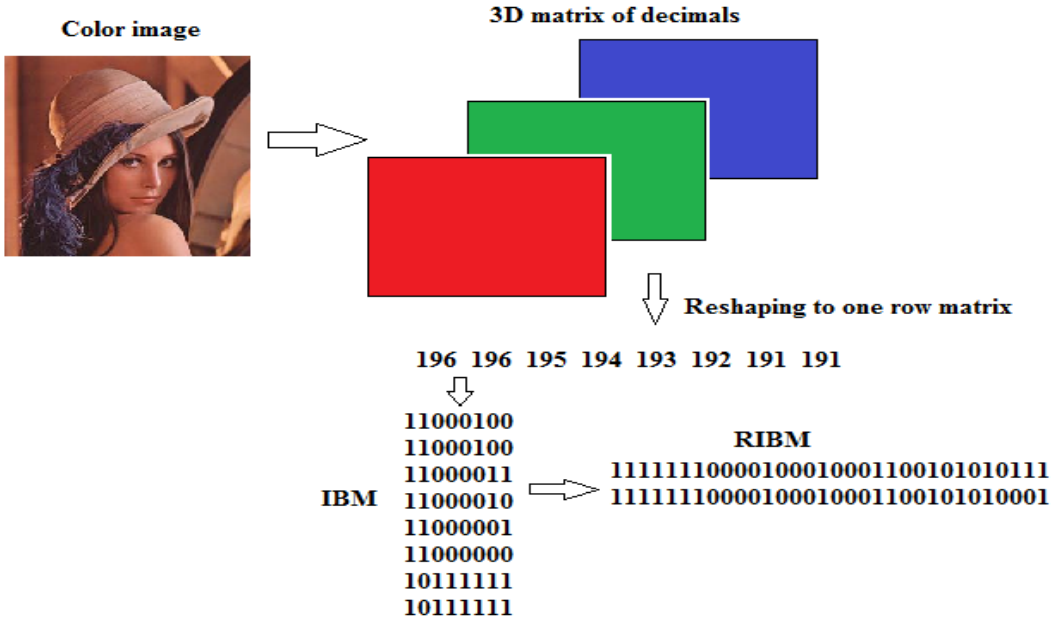

Figure 1: DCI presentation

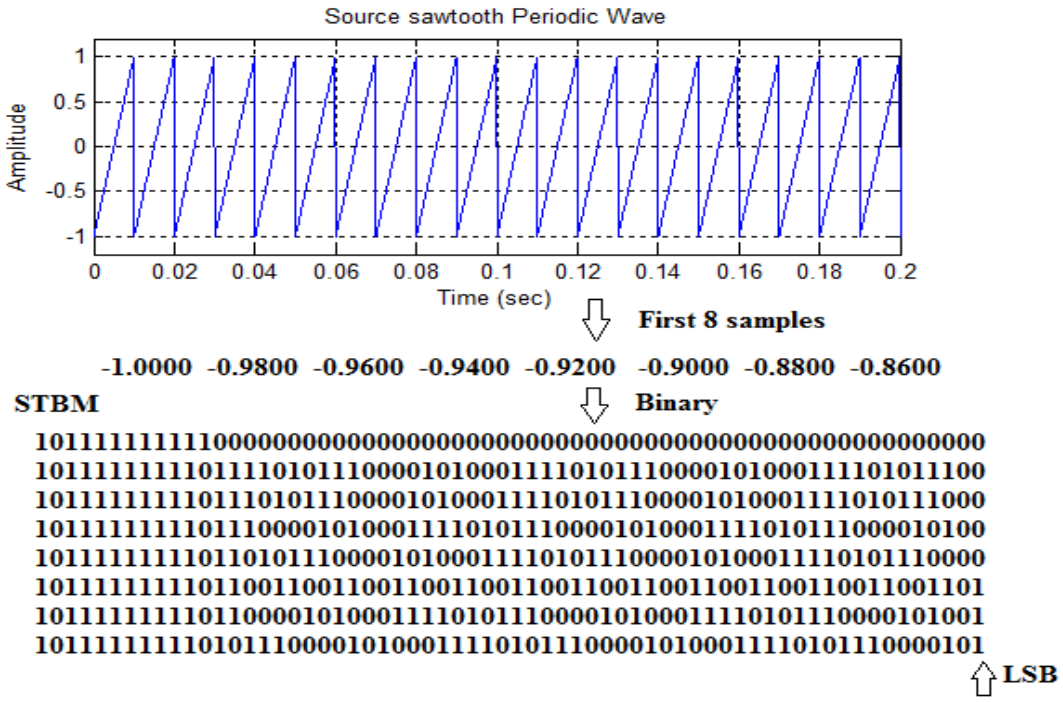

Figure 2: SPWS presentation

- Changing the 32 LSBs of the sample will not much affect the sample value, the stego sample will be closed to the covering sample, the MSE between them will be low, while the PSNR will be high as shown in the example illustrated in figure 3:

-

sample=0.1379;
binary:
00111111110000011010011010110101000010110000111100100111101111011
DCI bytes: 85 100 97 105
Binary:
01010101
01100100
01100001
01101001
Reshaped to 32 columns:
00001111011110000001110000001011
Hide message in the 32 LSBs of the sample:
00111111110000011010011010110101000011110111100000011100000001011
New sample value: 0.13790000205356
MSE between old and new values:
4.217092211954765e-018 **Low value**
PSNR between old and new values:
3.604493287406580e+002 **High value**

Figure 3: Effectes of replacing the 32 LSBs of the sample value

Many methods for DCI steganography were introduced, a lot of these methods were based on classical least significant bit (CLSB) method such as SLSB and DSLSB, these methods shared the following features, and some of these features require enhancement, these features include [61-69]:

- Mostly they use a digital color image as a covering media, this image can too big and some parts of the covering image may be not used, the proposed method will use a required genertaed SPWS with the required size, the size is cotrolled by the user by selecting the required values for generation time and sampling frequency [1-10].
- The LSBs of the covering bytes are used to hold the secret image, thus each secret byte reures 8 covering bytes, and the hiding capacity will be limited to the covering image size divided by 8. The proposed method will use the 32 LSBs from the SPWS samples, thus each sample will hold 4 bytes from the secret image, thus the hiding capacity of the proposed method will be invreased and it will equal the size of SPWS multiplied by 4.
- The MSE and PSNR values will get worst when increasing the secret image size, the quality of the stego image will be negatively affected when increasing the secret image size. The proposed method will keep the quality of stego SPWS good and the values of MSE and PSNR will good and acceptale even if the size of the secret image is big.
- Theses method provid a low speed, the fastest method (CLSB) [1-3] provides an average speed equal 12 K bytes per second, the proposed method will increase this speed and it will provide a good speed up.
- These methods use consicutive covering bytes to hide the image, thus some logical opearions will be required, The proposed method will apply image hiding in batch way by replacing all the 32 LSBs of the covering samples using one operation.

The Proposed Method

The hiding process of the proposed wmethod will be implemented applying the following algorithm:

Step 1: Secret image preparation:

a) Get the secret image to be hidden.
b) Get the image size.
c) Resize (if needed) the number of rows or the number of columns to be multiple of 4.
d) Reshape the image into one row matrix.
e) Convert the image decimal values to binary to get the image binary matrix (IBM).

Step 2: Stego media preparation:

a) Select the values of generation time and sampling frequency.
b) Generat the SPWS.
c) Get the covering samples with length equal image size divided by 4.

Step 3: DCI hiding:

a) Convert the covering samples to binary (64 bits each) to get samples binary matrix (SBM).
b) Reshape IBM to 32 columns matrix to get reshaped IBM (RIBM).
c) Let all the 32 LSBS in SBM equal RIBM.
d) Convert back the samples to decimals.
e) Return back the stego samples to the source covering SPWS to get the stego SPWS.
f) Save SPWS to be used by the reciever.
g) Save the DCI dimensions.

The extracting algorith will be implemented applying the following steps:

Step 1: Stego SPWS preparation:

a) Load the stego SPWS.
b) Load the image dinenstion.
c) Calculate the hidden image size.

Step 2: DCI extraction:

a) Get the stego samples from SPWS with size equal image size divided by 4.
b) Convert the stego samples to binary to get SBM.
c) Extract the 32 LSBs from SBM to get RIBM.

d) Reshape RIBM to 8 colums matrix to get IBM.
e) Convert IBM to decimal to get the image row matrix.
f) Reshape the image row matrix to 3D matrix to get the secret image.

Implementation and Results Discusion

The proposed method was impleemented using various images, the extracted image was always identical to the source hiddn image, the MSE between the two images was always zero, while the PSNR value between the two images was always infinte, figure 4 shows sample images:

Figure 4: Sample images

The quality of the stego SPWS was tested, several images were selcted and each of them was hidden in a SPWS with 2000001 samples, the MSE and PSNR between the covering and the stego SPWSs were calculated and table 1 shows the obtained quality results:

Table 1: Quality parameters

DCI size (Byte)	MSE	PSNR
76608	3.708125974158181e-016	3.552683115227314e+002
150396	5.068831523574200e-016	3.521424745056274e+002
172800	4.351447992190292e-016	3.536684899728178e+002
518400	1.848951361220892e-015	3.392015397582618e+002
1886400	5.521992253687518e-015	3.282603395402969e+002
Remarks	Very low	High

From table 1 the following can be seen:

- MSE value was always low, while PSNR value was always high, this prove the fact that the proposed method satisfied the quality requirements of good stego method.
- Incearsing the image size will keep the stego SPWS in high quality, the MSE value remaned low, while the PSNR value remained high, the stego SPWS shown in figure 5 is very closed to the source SPWS, this stego SPWS is holding a big image with size equal 1886400 bytes.

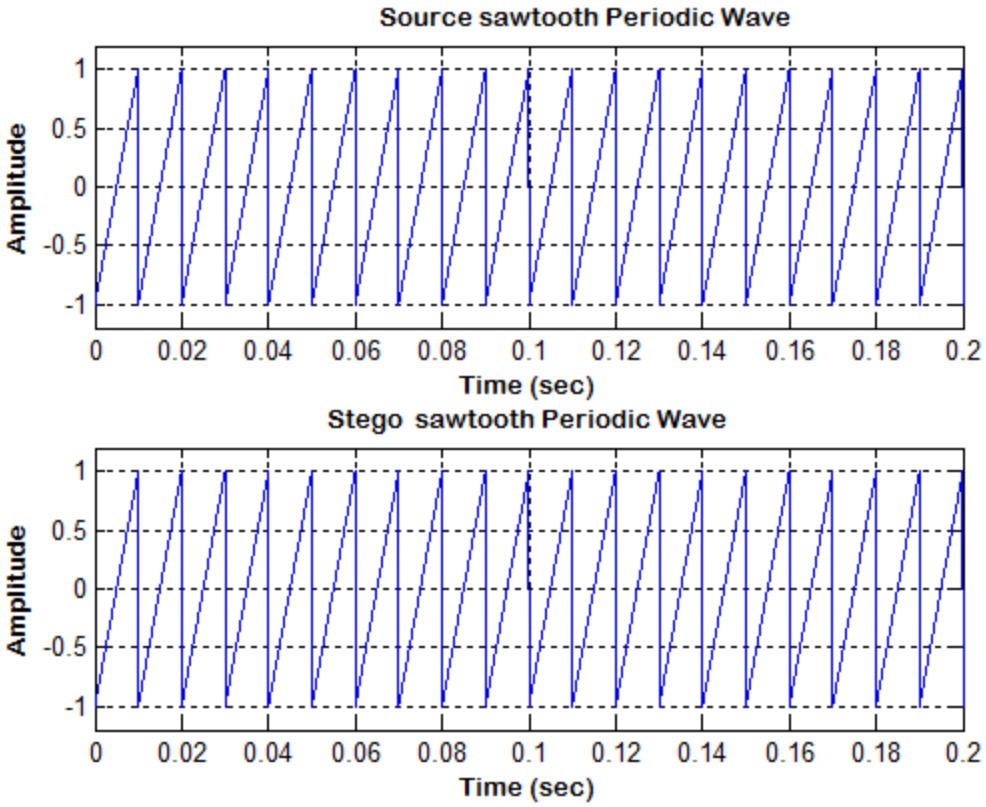

Figure 5: Stego SPWS holding 1886400 bytes of a DCI

The speed of the proposed method was examned, the previous experiment was repeated, the hiding and extarcyting times were calculated, and using the values of these times and the images sizes the hidding and the extracting thoughputs (speeds) were calculated and table 2 shows the obtained speed results:

Table 2: Proposed method speed reults

DCI size (Byte)	Hiding time (second)	Extracting time(Second)	Hiding throughput (K bytes per second)	Extracting throughput (K bytes per second)
76608	0.894	0.535	83.68	139.83
150396	1.683	1.129	87.26	130.08
172800	1.871	1.175	90.19	143.61
518400	5.569	3.67	90.90	137.94
1886400	20.978	12.952	87.81	142.23
Average				
560920.8	6.199	3.8922	87.967	138.73

The propsed method provided a good speed parametrers, the average hiding speed was equal 87.9 K bytes per second, while the average extracting speed was equal 138.7 K bytes per second, these results are better than the results provided by CLSB, the proposed method provided a good speed up comparing with the existing methods CLSB, SLSB and DSLSB.

Conclusion

A simple and easy to implement method of digital color image steganography was proposed, the method used a saw tooth periodic wave singnal as a covering media, this signal was created and generated easily, the size of this signal

was easily cotrolled by the selcted values of the generation time and the sampling freauency. The SPWS samples were easily represnted by 64_bits binary numbers, and the 32 LSBs of the covering samples were used to hide the bits of the secret color image. The proposed method used each sample from the covering SPWS to hold 4 bytes from the secret image, thus the proposed method increased the hiding capacity of the covering media to reach the covering media size multiplied by 4. Chamging the 32 LSBs of the covering samples will not much affect the samples values, the MSE value calculted betwee the source and stego SPWS was always low, even if the image size is big, while the PSNR value calculated between the covering and stego SPWSs was lways high.

The proposed method was implemented using various images, the obtained results proved that the proposed method satisfied the quality requirements of good stego method, the speed of image steganography was enhanced, and the proposed method provided a speed up comparing with other existing methods of image steganography.

References

[1]. Dr. Mohammed Abbas Fadhil Al-Husainy, COMPARISON STUDY BETWEEN CLASSIC-LSB, SLSB AND DSLSB IMAGE STEGANOGRAPHY, ICIT 2013 The 6th International Conference on Information Technology.

[2]. Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.

[3]. 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.

[4]. Emam, M. M., Aly, A. A., & Omara, F. A. An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. International Journal of Advanced Computer Science & Applications,1(7), pp. 361-366, (2016). https://doi.org/10.14569/IJACSA.2016.070350.

[5]. Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Modified Inverse LSB Method for Highly Secure Message Hiding, IJCSMC, Vol. 8, Issue. 2, February 2019, pg.93 – 103.

[6]. Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Engineering, A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages Engineering Technology & Applied Science Research, Vol.9 Issue 1, Pages 3681-3684, 2019.

[7]. Zhou X, Gong W, Fu W, Jin L. 2016An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15th Int. Conf. on Computer and Information Science (ICIS), Okayama, Japan, pp. 1–4 . https://doi.org/10.1109/ICIS.2016.7550955.

[8]. Wu D-C, Tsai W-H. A steganographic method for images by pixel value differencing. Pattern Recognition. Lett. 24, 1613–1626. 2003 https://doi.org/10.1016/S0167-8655(02)00402-6.

[9]. Das R, Das I. Secure data transfer in IoT environment: adopting both cryptography and steganography techniques. In Proc. 2nd Int. Conf. on Research in Computational Intelligence and Communication Networks, Kolkata, India, pp. 296–301, 2016. https://doi.org/10.1109/ICRCICN.2016.7813674.

[10]. Rashad J. Rasras, Mutaz Rasmi Abu Sara, Ziad A. AlQadi, Rushdi Abu zneit, Comparative Analysis of LSB, LSB2, PVD Methods of Data Steganography, International Journal of Advanced Trends in Computer Science and Engineering, vol. 8, issue 3, pp.748-754, 2019, http://www.warse.org/IJATCSE/static/pdf/file/ijatcse64832019.pdf

[11]. Ayman Al-Rawashdeh, Ziad Al-Qadi, using wave equation to extract digital signal features, Engineering, Technology & Applied Science Research, vol. 8, issue 4, pp. 1356-1359, 2018.

[12]. K Matrouk, A Al-Hasanat, H Alasha'ary, Z. Al-Qadi Al-Shalabi, "Speech fingerprint to identify isolated word person", World Applied Sciences Journal, Vol. 31, No. 10, pp. 1767-1771, 2014.

[13]. Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi , A Novel Methodology to Extract Voice Signal Features , International Journal of Computer Applications, Volume 179 – No.9, January 2018.

[14]. Ziad Alqadi, Bilal Zahran, Qazem Jaber, Belal Ayyoub, Jamil Al-Azzeh, Enhancing the Capacity of LSB Method by Introducing LSB2Z Method, International Journal of Computer Science and Mobile Computing, vol. 8, issue 3, pp. 76-90, 2019.

[15]. Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, Optimized True-RGB color Image Processing, World Applied Sciences Journal 8 (10): 1175-1182, ISSN 1818-4952, 2010.

[16]. Waheeb, A. and Ziad AlQadi, Gray image reconstruction. Eur. J. Sci. Res., 27: 167-173, 2009.

[17]. A. A. Moustafa, Z. A. Alqadi, "Color Image Reconstruction Using a New R'G'I Model", Journal of Computer Science, Vol.5, No. 4, pp. 250-254, 2009.

[18]. Prof. Ziad A.A. Alqadi, Prof. Mohammed K. Abu Zalata, Ghazi M. Qaryouti, Comparative Analysis of Color Image Steganography, JCSMC, Vol.5, Issue. 11, November 2016, pg.37–43.

[19]. H. Alasha'ary, K. Matrouk, A. Al-Hasanat, Z. A alqadi, H. Al-Shalabi (2013), Improving Matrix Multiplication Using Parallel Computing, International Journal on Information Technology (I.RE.I.T.) Vol.1, N. 6 ISSN 2281-2911.

[20]. Bilal Zahran, Ziad Alqadi, Jihad Nader, Ashraf Abu Ein A COMPARISON BETWEEN PARALLEL AND SEGMENTATION METHODS USED FOR IMAGE ENCRYPTION-DECRYPTION, International Journal of Computer Science & Information Technology (IJCSIT) Vol 8, No 5, October 2016.

[21]. Z.A. Alqadi, A. Abu-Jazar (2005), Analysis of Program Methods Used for Optimizing Matrix Multiplication, Journal of Engineering, vol. 15 n. 1, pp. 73-78.

[22]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh: A Novel Based On Image Blocking Method to Encrypt-Decrypt Color JOIV: International Journal on Informatics Visualization, 2019.

[23]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub and Mazen Abu-Zaher: A Novel Zero-Error Method to Create a Secret Tag for an Image; Journal of Theoretical and Applied Information Technology 15th July 2018.

[24]. Jamil Al Azzeh, Ziad Alqadi Qazem, M. Jabber: Statistical Analysis of Methods Used to Enhanced Color Image Histogram; XX International Scientific and Technical Conference; Russia May 24-26, 2017.

[25]. Jamil Al Azzeh, Hussein Alhatamleh, Ziad A. Alqadi, Mohammad Khalil Abuzalata: Creating a Color Map to be used to Convert a Gray Image to Color Image; International Journal of Computer Applications (0975– 8887). Volume 153 – No2, November 2016.

[26]. Khaled Matrouk, Abdullah Al- Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi Analysis of Matrix Ziad Alqadi et al, International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 76-90.

[27]. Mohammed Abuzalata; Ziad Alqadi, Jamil Al-Azzeh; Qazem Jaber Modified Inverse LSB Method for Highly Secure Message Hiding: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, February- 2019, pg. 93-103.

[28]. Qazem Jaber Rashad J. Rasras, Mohammed Abuzalata, Ziad Alqadi, Jamil Al-Azzeh; Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation: International Journal of Computer Science and Mobile Computing, Vol.8 Issue.2, 2019/3.

[29]. Rashad J. Rasras, Mohammed Abuzalata; Ziad Alqadi; Jamil Al-Azzeh; Qazem Jaber, Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation International Journal of Computer Science and Mobile Computing, Vol.8 Issue.3, March- 2019, pg. 14-26.

[30]. AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad , Analysis of Color Image Features Extraction using Texture Methods , TELKOMNIKA, vol. 17, issue 3, 2018.

[31]. B. Zahran, J. AL-Azzeh, Z. Al Qadi, M. Al Zoghoul and S. Khawatreh, "A MODIFIED LBP METHOD TO EXTRACT FEATURES FROM COLOR IMAGES", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 10, 2018.

[32]. J. AL-AZZEH, B. ZAHRAN, Z. ALQADI, B. AYYOUB, M. ABU-ZAHER, "A novel Zero-error Method to Create a Secret Tag for an Image", Journal of Theoretical and Applied Information Technology(JATIT), Vol.96. No 13, 2018.pp: 4081-4091.

[33]. J. AL-AZZEH, B. ZAHRAN, Z. ALQADI," Salt and Pepper Noise: Effects and Removal", International Journal on Informatics Visualization, Vol.2. No 4, 2018.pp: 252-256.

[34]. Jihad Nader, Ziad Alqadi, Bilal Zahran, "Analysis of Color Image Filtering Methods", International Journal of Computer Applications (IJCA), Volume 174, issue 8, 2017, pp:12-17.

[35]. Ziad Alqadi, Bilal Zahran, Jihad Nader, " Estimation and Tuning of FIR Low pass Digital Filter Parameters", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 2, 2017, pp:18-23.

[36]. Khaled Aldebei, Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Comparative Analysis of Fingerprint Features Extraction Methods, Journal of Hunan University Natural Sciences, vol. 48, issue 12, pp. 177-182, 2022.

[37]. Dr. Mohamad Barakat Prof. Ziad Alqadi, Highly Secure Method for Secret Data Transmission, International Journal of Scientific Engineering and Science, vol. 6, issue 1, pp. 49-55, 2022.

[38]. Ziad A. Alqadi Mua'ad M. Abu-Faraj, 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, issue 12, pp. 648-656, 2021.

[39]. Ziad Alqadi Mua'ad Abu-Faraj , Khaled Aldebei, DEEP MACHINE LEARNING TO ENHANCE ANN PERFORMANCE: FINGERPRINT CLASSIFIER CASE STUDY, JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY, vol. 56, issue 6, pp. 686-694, 2021.

[40]. Ziad A. Alqadi Mua'ad M. Abu-Faraj, Improving the Efficiency and Scalability of Standard Methods for Data Cryptography, International Journal of Computer Science and Network Security, vol. 21, issue 12, pp.451-458, 2021

[41]. Mua'ad M. Abu-Faraj Prof. Ziad Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, International Journal of Computer Science and Network Security, vol. 20, issue 11, pp. 53-60, 2021.

[42]. AlQaisi Aws, AlTarawneh Mokhled, A Alqadi Ziad, A Sharadqah Ahmad, Analysis of Color Image Features Extraction using Texture Methods, TELKOMNIKA, vol. 17, issue 3, 2018.

[43]. Ziad A AlQadi Amjad Y Hindi, O Dwairi Majed, PROCEDURES FOR SPEECH RECOGNITION USING LPC AND ANN, International Journal of Engineering Technology Research & Management, vol. 4, issue 2, pp. 48-55, 2020.

[44]. Ziad A Alqadi, Mohamad Tariq Barakat, A Case Study to Improve the Quality of Median Filter, International Journal of Computer Science and Mobile Computing, vol. 10, issue 11, pp. 19 – 28, 2021.

[45]. Dr. Hatim Ghazi Zaini Prof. Ziad Alqadi, High Salt and Pepper Noise Ratio Reduction, International Journal of Computer Science and Mobile Computing, vol. 10, issue 9, pp. 88 – 97, 2021.

[46]. Prof. Mohamad K. Abu Zalata, Hussein N. Hatamleh, Prof. Ziad A. Alqadi, Detailed Study of Low Density Salt and Pepper Noise Removal from Digital Color Images, IJCSMC, Vol. 11, Issue. 2, PP. 56 – 67, February 2022.
[47]. M. Abu-Faraj, A. Al-Hyari, K. Aldebei, B. Al-Ahmad, and Z. Alqadi, "Rotation Left Digits to Enhance the Security Level of Message Blocks Cryptography," IEEE Access, vol. 10, pp. 69388- 69397, 2022, doi:10.1109/ACCESS.2022.3187317.
[48]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Experimental Analysis of Methods Used to Solve Linear Regression Models," CMC-Computers, Materials & Continua, vol. 72, no. 3, pp. 5699-5712, 2022, doi:10.32604/cmc.2022.027364. (Web of Science Indexed, Scopus Indexed).
[49]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," Symmetry, vol. 14, Iss. 4, pp. 664-678, 2022, doi:10.3390/sym0664. (Web of Science Indexed, Scopus Indexed)
[50]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," Traitement du Signal, vol. 39, no. 1, pp. 173-178, 2022, doi:10.18280/ts.390117. (Web of Science Indexed, Scopus Indexed)
[51]. M. Abu-Faraj, and Z. Alqadi, "Rounds Reduction and Blocks Controlling to Enhance the Performance of Standard Method of Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no. 12, pp. 648-656, 2021, doi: 10.22937/IJCSNS.2021.21.12.89. (Web of Science Indexed)
[52]. M. Abu-Faraj, and Z. Alqadi, "Improving the Efficiency and Scalability of Standard Methods for Data Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 451-458, 2021, doi:10.22937/IJCSNS.2021.21.12.61. (Web of Science Indexed)
[53]. M. Abu-Faraj, and Z. Alqadi, "Using Highly Secure Data Encryption Method for Text File Cryptography," International Journal of Computer Science and Network Security (IJCSNS), vol. 21, no.12, pp. 53-60, 2021, doi:10.22937/IJCSNS.2021.21.12.8. (Web of Science Indexed)
[54]. 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, iss. 43, pp. 590-602, 2020. (Scopus Indexed)
[55]. Prof. Ziad Alqadi, Bits Substitution to Secure LSB Method of Data Steganography, International Journal of Computer Science and Mobile Computing, vol. 11, issue 8, pp. 9 – 21, 2022.
[56]. Mohammad S. Khrisat Prof. Ziad Alqadi, Enhancing LSB Method Performance Using Secret Message Segmentation, International Journal of Computer Science and Network Security, vol. 22, issue 7, pp. 1-6, 2022.
[57]. Hatim Ghazi Zaini and Ziad A. Alqadi Mohammad S. Khrisat, Adnan Manasreh, COVER IMAGE REARRANGEMENT TO SECURE LSB METHOD OF DATA STEGANOGRAPHY, Journal of Engineering and Applied Sciences, vol. 17, issue 3, pp. 294-302, 2022.
[58]. Mohamad K Abu Zalata, Mohamad T Barakat, Ziad 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, issue 1, pp. 182 – 193, 2022.
[59]. Dr. Mohamad barakat Prof. Ziad Alqadi, IMAGE TRANSFORMATION TO INCREASE THE SECURITY LEVEL OF LBS METHOD OF DATA STEGANOGRAPHY, International Journal of Engineering Technology Research & Management, vol. 6, issue 1, pp. 42-53, 2022.
[60]. Naseem Asad, Ismail Shayeb, Qazem Jaber, Belal Ayyoub, Ziad Alqadi, Ahmad Sharadqh, creating a Stable and Fixed Features Array for Digital Color Image, IJCSMC, Vol. 8, Issue. 8, August 2019, pg.50 –62.
[61]. Majed O. Al-Dwairi, Amjad Y. Hendi, Mohamed S. Soliman, Ziad A.A. Alqadi, A new method for voice signal features creation, International Journal of Electrical and Computer Engineering (IJECE), vol. 9, issue 5, pp. 4092-4098, 2018.
[62]. Akram A. Moustafa and Ziad 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 5 (5): 355-362, 2009.
[63]. ZA Alqadi, Musbah Aqel, Ibrahiem MM El Emary, Performance analysis and evaluation of parallel matrix multiplication algorithms, World Applied Sciences Journal, vol. 5, issue 2, pp. 211-214, 2008.
[64]. Ismail Shayeb, Naseem Asad, Ziad Alqadi, Qazem Jaber, Evaluation of speech signal features extraction methods, Journal of Applied Science, Engineering, Technology, and Education is licensed under an Attribution-Non Commercial-Share Alike 4.0 International (CC BY-NC-SA 4.0)
[65]. Kaur, R. Dhir, & G. Sikka,"A new image steganography based on first component alteration technique", International Journal of Computer Science and Information Security (IJCSIS), 6, pp.53-56, 2009.http://arxiv.org/ftp/arxiv/papers/1001/1001.1972.pdf.
[66]. Alvaro Martin, Guillermo Sapiro, &Gadiel Seroussi,"Is Steganography Natural", IEEE Transactions on Image Processing, 14(12), pp.2040-2050, 2005.doi: 10.1109/TIP.2005.859370 .
[67]. Bhattacharyya, A. Roy, P. Roy, & T. Kim, "Receiver compatible data hiding in color image", International Journal of Advanced Science and Technology, 6, pp.15-24, 2009.http://www.sersc.org/journals/IJAST/vol6/2.pdf .
[68]. Namer Ali Aletawi; Mansour A. Abu Sameha; Prof. Ziad Alqadi, Modified LSB2 Steganography Method to Secure the Embedded Secret Message, IJCSMC, Vol. 11, Issue. 8, August 2022, pg.22 – 44.
[69]. Pleacher, D. (n.d.), Calculating password entropy. Retrieved February 16, 2023, from https://www.pleacher.com/mp/mlessons/algebra/entropy.htmlPotter

