

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. 13, Issue. 1, January 2024, pg.93 – 105

DSF Cryptography by Rotating Left the Samples Binary Values

Prof. Ziad Al Qadi; Prof. Qazem Jaber; Prof. Mohammad Abu Zalata

Albalqa Applied University, Faculty of Engineering Technology, Jordan-Amman

DOI: <https://doi.org/10.47760/ijcsmc.2024.v13i01.008>

Abstract:

A novel method of digital speech file cryptography will be proposed. The method will apply speech encryption-decryption at the bit level. The binary values of the speech samples will be shifted left to a defined number of rotating left digits. The private key will determine the length of the set of the bits to be rotated will be selected, the starting bit from where to start rotating and the number of rotating digits. The speech sample value will be represented in binary using 64_bits binary representation. Because of the fractional decimal value of the speech sample, changing the LSBs of the binary value may not affect the speech sample, so the starting bit for selecting the bits to be rotated will be investigated, and this bit will be used in the encryption-decryption process to get a damaged encrypted speech file. The private key will contains the starting bit; the bits set length and the number of rotating left digits, conditional selections of the private key value will be provided based on analyzing the quality of the encrypted speech files.

The encryption and decryption process of the proposed method will be implemented in one round using a simple rotate left operation. The proposed method will not need key generation process; the values included in the private key will be directly used to apply speech encryption-decryption.

The proposed method will be implemented using various speech files, the obtained results will be analyzed using quality, speed and sensitivity analysis to prove the efficiency of the proposed method.

Keywords: DSF, cryptography, PK, SB, BSL, NRLD, SBM, MSE, PSNR.

Introduction

Digital speech file (DSF) is a set of speech sample organized in one or two columns matrix. Speech sample has the following features [1-10]:

- Sample value is a double data type value.
- Sample value can be positive or negative (signed value).
- Sample value is a decimal fraction.
- The sample value is within the range -1 to +1.
- The decimal value of the sample can be converted to binary and vice versa using a 64_bits binary representation.
- The binary value of the speech sample as shown in figure 1 is divided into three parts (sign, value and exponent) [11-15].

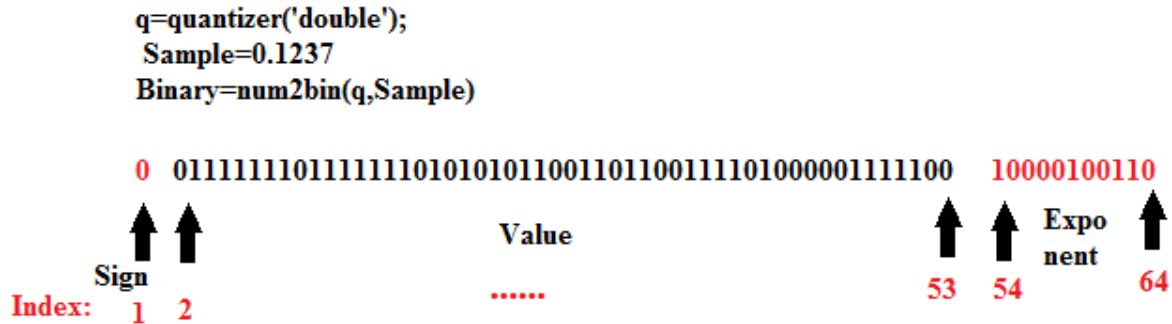


Figure 1: Speech sample binary value

- Changing any of the most significant bits (MSB) starting from 1 to 24 will much affect the sample value (see table 1).
- Changing the least significant bits (LSB) starting from bit 25 to 64 will not much affect the speech value (see table 1).
- To obtain a high degree of encrypted file destruction the bits from 1 to 24 must be affected.

Table 1: Effects of changing sample binary value bits

Initial sample value: 0.419			
Binary:			
001111111011010110100001110010101100000010000011000100100110111			
Changed bit index	New sample value	Changed bit index	New sample value
1	-0.4190	25	0.4190
2	7.5323e+307	26	0.4190
3	3.1250e-155	27	0.4190
4	3.6186e-078	28	0.4190
5	1.2313e-039	29	0.4190
6	2.2714e-020	30	0.4190
21	0.4195	61	0.4190
22	0.4192	62	0.4190
23	0.4191	63	0.4190
24	0.4191	64	0.4190

Based on the results shown in table 1 we can recommend using bits 1 to 24 for data cryptography [13-20], and using bits from 25 to 64 for data steganography [1-12].

DSF for analysis can be represented as shown in figure 2 by: speech wave plot, speech histogram, decimal matrix and speech binary matrix (SBM). The SBM can be easily obtained by converting the reshaped to one row matrix the speech decimal matrix using 64_bits binary representations, SBM can also be easily converted to decimal matrix using the same binary representation [16-23].

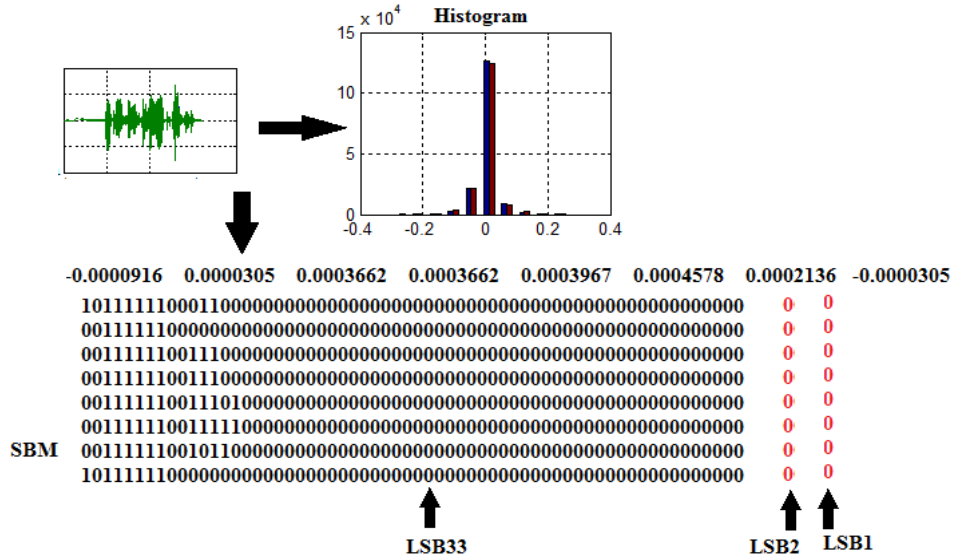


Figure 2: DSF presentation

DSF is one of the most circulated through the internet digital data type, it is used in many important computer applications, and most of these applications require securing the DSF from being hacked [24-31].

Data cryptography is one of the easiest ways to protect DSF. DSF cryptography as shown in figure 3 is implemented by the encryption and decryption functions. Encryption function (figure 3 (a)) manipulates the source DSF and the private key (PK) to produce a damaged encrypted DSF, while decryption function (figure 3 (b)) manipulates the encrypted DSF and the PK to produce a decrypted identical to the source file DSF [32-40].

The aim of this paper research is to introduce a new method of DSF cryptography to overcome some disadvantages of the standard methods of data cryptography such as DES and AES [1-10] methods by providing the following enhancements [41-50]:

- Encrypting and decrypting DSF, which are difficult to process using standard methods.
- Increasing the degree of encrypted DSF destruction by increasing the value of mean square error (MSE), measured between the source and encrypted DSFs [30-35], and at the same time decreasing the value of peak signal to noise ratio (PSNR) measured between the source and the encrypted DSFs [51-56].
- Recovering the source DSF by producing a decrypted DSF identical to the source one (MSE=0, PSNR=infinity) [57-63].
- Simple process of PK manipulation, there is no need to generate secret keys [64-70].
- Encryption and decryption processes will be implemented in one round.
- Replacing the complex sequence of logical and arithmetic operations used in standard method by a simple rotate left operation [6-10].
- Treating the whole DSF without the need to divide it into blocks as in standard methods.
- Simplicity of converting decimal values of the speech samples to binary and vice versa, and simplicity of treating any set of the bits of the binary values.
- Providing a good speed of DSF cryptography.
- Securing the DSF by using a simple PK.
- Sensitive using of the PK in the decryption process, this process must use the same PK used in the encryption process[40-36].

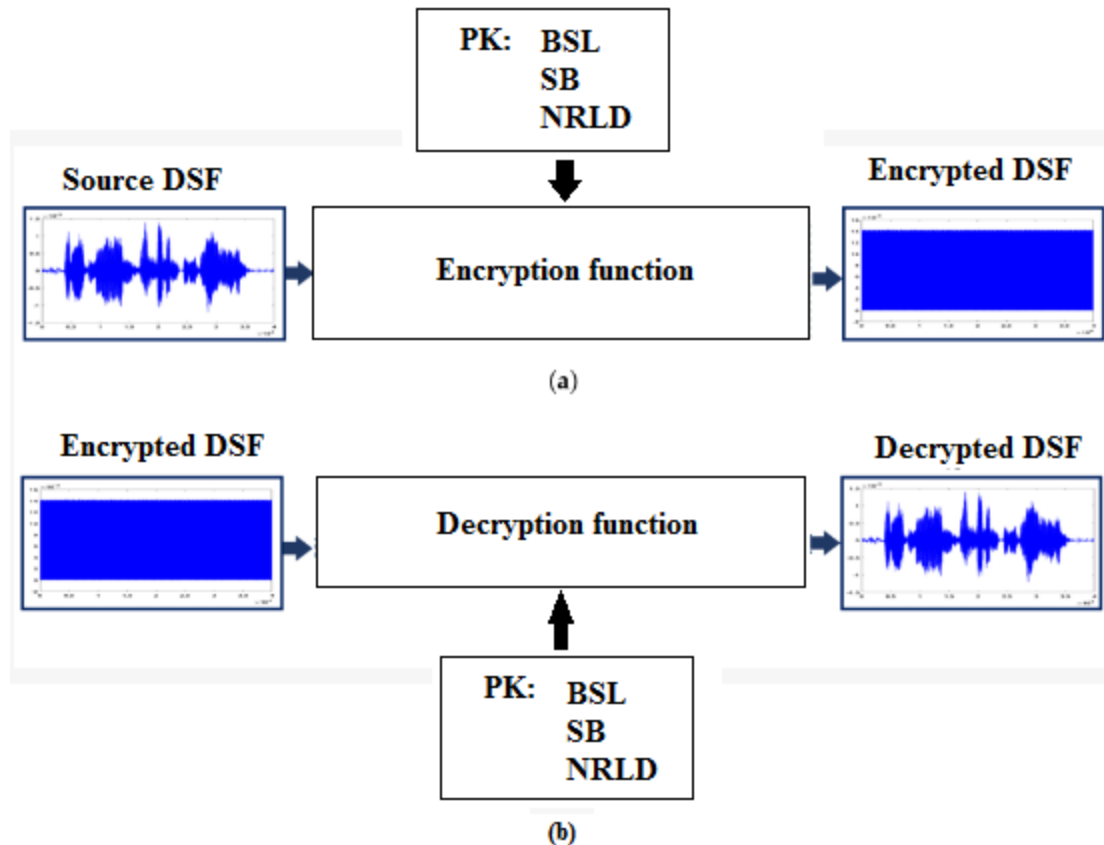


Figure 3: DSF cryptography process

The Proposed Method

Speech samples is a decimal fraction represented by a 64 bits binary number, this big number of bits give use the ability to change low LSB bits without affecting much the sample value, and at the same time allow us to change high order LSBs to apply minor changes in the speech sample value. To get an encrypted DSF with high degree of destruction the high order bits must be selected to add big changes in the encrypted sample value [5-12]. Table 2 shows the effects of changing various bits in the source speech sample value by applying rotate left operation:

Table 2: Effects of changing sample bits with various orders (source sample value 0.173)

Number of bits	Starting bits	Number of rotating left digits	Encrypted value	Decrypted value	MSE	PSNR
63	2	40	1.9125e-180	0.173	0.0299	0
30	5	11	6.4844e-072	0.173	0.0299	0
10	2	6	1.9818e+250	0.173	Infinity	0
15	30	9	0.1730	0.1730	1.4842e-014	283.3237
20	32	10	0.1730	0.1730	8.3989e-015	289.0174
20	40	7	0.1730	0.1730	9.3726e-021	426.0757

In the proposed method the high order bits (MSBs) will be used to achieve high values of MSE and low values of PSNR between the source and the encrypted DSFs, and based on the obtained results the following conditions must be applied when using the proposed method (see table 3):

- Starting bit (SB) must be less or equal 11.

- Bits set length (BSL) must be greater than 1 and less than 64.
- Number of rotating left digits (NRLD) must be less than BSL.

Table 3: The recommended selected order of the sample value

Starting bit	MSE	PSNR
1	5.8637e-004	29.8751
2	5.8637e-004	29.8751
3	5.8637e-004	29.8751
4	5.8637e-004	29.8751
5	5.8637e	29.8751
6	5.8637e	29.8751
7	5.8637e	29.8751
8	5.8637e	29.8751
9	5.8543e-004	29.8911
10	4.0089e-004	33.6778
11	3.9882e-004	33.7295
12	1.3478e-004	44.5785
15	5.4334e-006	76.6890
20	5.1817e-009	146.2410
30	0	Infinity
34	0	Infinity

The PK contains the values of three parameters:

- SB: starting bit and it is recommended to be from 1 to 11.
- BSL: bit set length; the value of this parameter is between 2 and 64.
- NRLD: number of rotating left digits and it must be less than BSL, for the decryption function NRLD must equal NRLD subtracted from BSL.

Figures (4 and 5) show how to apply encryption-decryption using rotate left operation:

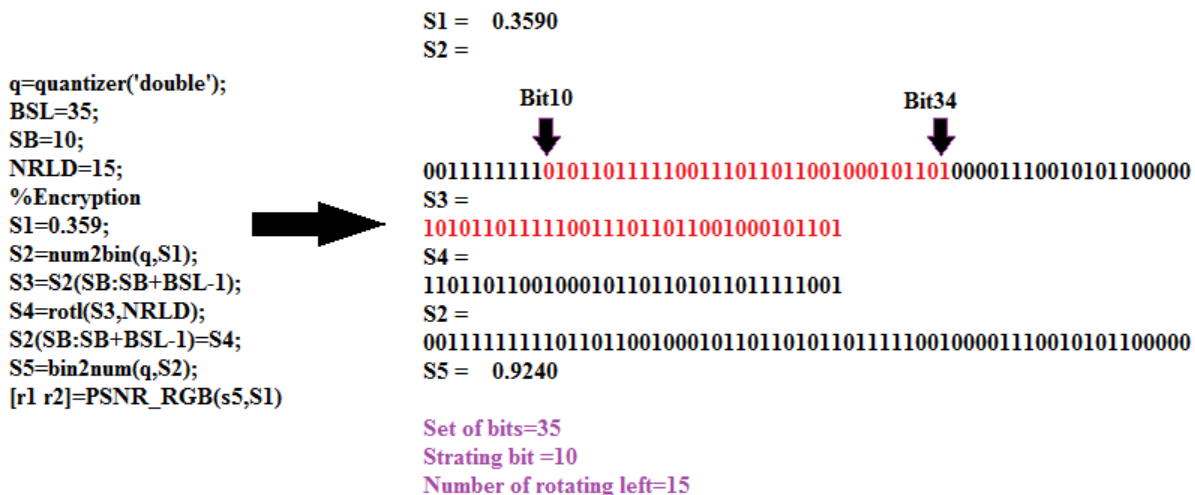


Figure 4: Encryption using rotate left operation

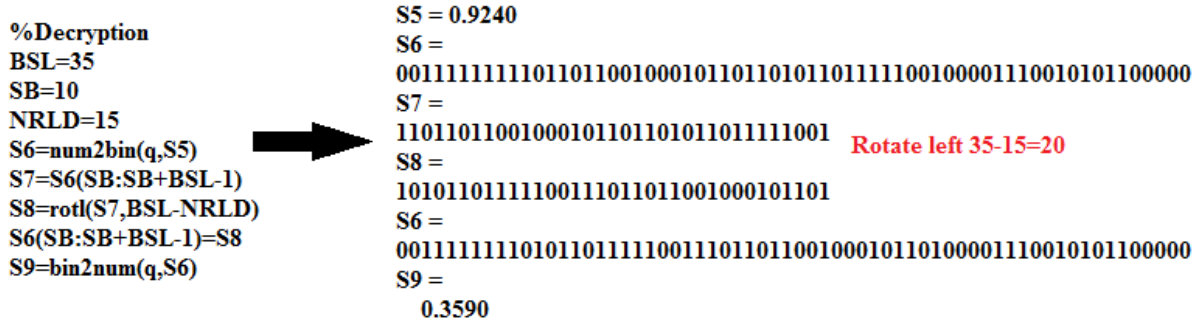


Figure 5: Decryption using rotate left operation

The proposed method encryption process will simply implemented applying the following steps:

Step 1:

Inputs preparation:

- 1) Get the DSF.
- 2) Get the file size.
- 3) Reshape the file to one row matrix.
- 4) Get the PK (get the values of SB, BSL and NRLD).

Step 2:

Encryption:

- 1) Convert the DSF row matrix to binary using 64_bits binary representation to get SBM.
- 2) For each sample rotate left the set of selected bits NRLD times.
- 3) Convert the resulting SBM to decimal.
- 4) Reshape back the matrix to the original size to get the encrypted DSF.

The process of decryption will be applied using the same steps as for encryption process, but the rotation will be applied by rotating left the bits number of times equal NRLD subtracted from BSL.

Below is a mat lab code, which can be easily used to run the proposed method:

```

;Encryption
[c1 fs1]=wavread('C:\Users\win 7\Desktop\voices\al.wav');
[nn1 nn2]=size(c1);L1=nn1*nn2;
c2=reshape(c1,1,L1);
q=quantizer('double');
c3=num2bin(q,c2);
BSL=30;
SB=2;
NRLD=23;
S1=c3;
for i=1:L1
    S1(i,SB:SB+BSL-1)=rotl(S1(i,SB:SB+BSL-1),NRLD);
end
S2=bin2num(q,S1);
S3=reshape(S2,nn1,nn2);
    
```

```

;Decryption
S4=reshape(S3,1,L1);
S5=num2bin(q,S4);
BSL=30;
SB=2;
NRLD=23;
for i=1:L1
    S5(i,SB:SB+BSL-1)=rotl(S5(i,SB:SB+BSL-1),BSL-NRLD);
end
S6=bin2num(q,S5);
S7=reshape(S6,nn1,nn2);

function res=rotl(bin, d) % % Left rotation of d bits
if d>1
    res=rotl([bin(2:end) bin(1)], d-1);
else
    res=[bin(2:end) bin(1)];
end
end
    
```

Implementation and Results Discussion

A set of DSF were selected, table 4 shows the basic information of these files:

Table 4: Selected DSF basic information

DSF number	Size	Length in sample	Length in bytes
1	64448x1	64448	515584
2	82880x1	82880	663040
3	160768x2	321536	2572288
4	100352x2	200704	1605632
5	113664x2	227328	1818624
6	215040x2	430080	3440640
7	86016x2	172032	1376256
8	66560x2	133120	1064960
9	106496x2	212992	1703936
10	136192x2	272384	2179072

The main objective of the crypto system is to produce a damaged encrypted data, the method of cryptography can be evaluated based on the degree of file destruction, a good method of cryptography must maximize the MSE value and must minimize the PSNR value measured between the source and the encrypted DSFs.

Several values of the starting bit of the set of bits to be rotated were selected as follows:

- Low index bit (High order of LSB).
- Medium index.
- High index.

The selected DSF were processed using the following PK:

PK:
BSL=30;
SB=2; Low index (high LSB order)
NRLD=23;

Table 5 shows the obtained quality parameters measured between the source and the encrypted DSFs, while figure 6 shows a sample outputs:

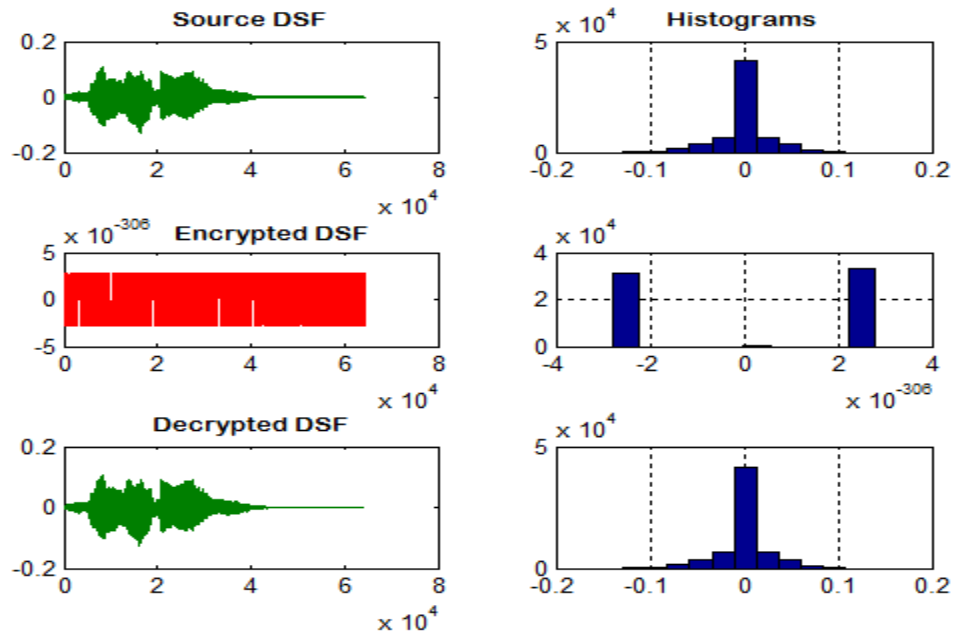


Figure 6: Sample outputs using BS=2

Different indexes of SB were used and the selected DSF were implemented using these bits, and tables 5 and 6 show the obtained quality results:

Table 5: Quality parameters using low ordered index BS

DSF number	Used SB	MSE	PSNR
1	3	0.0010	42.3624
2	4	6.3281e-004	45.1077
3	5	7.4867e-004	43.5608
4	6	9.7069e-004	44.3725
5	7	2.0667e-004	35.6258
6	8	1.9001e-004	30.4175
7	9	2.7587e-004	42.1592
8	10	1.9106e-004	50.4415
9	2	2.6946e-004	38.6548
10	2	5.8637e-004	29.8751

Table 6: Quality parameters using high ordered index BS

DSF number	Used SB	MSE	PSNR
1	15	9.8398e-006	88.9695
2	16	1.5704e-006	105.0964
3	25	1.2099e-013	269.0192
4	26	0	Infinity
5	30	0	Infinity
6	31	0	Infinity
7	32	0	Infinity
8	33	0	Infinity
9	34	0	Infinity
10	35	0	Infinity

From tables 5 and 6 we can see the following:

- Using low ordered bits of the speech samples values will increase The MSE value and at the same time decrease the value of PSNR, so to achieve a high degree of destruction in the encrypted DSF it is recommended to use the low ordered indexes bit in the crypto process.
- Using high ordered indexes of the speech sample binary values will add a minor changes to the samples values, so theses bits are not recommended to be used in the crypto method , they keep the MSE low and keep the PSNR high, they can be efficiently use in a stego system [70-82].

Conclusion

A simple method of digital speech cryptography was proposed; the method used a simple rotate left operation to apply speech encryption-decryption. The rotation operation was implemented based on the private key values, these values were used to determine the starting bit in the samples binary values where to start rotating, the number of digits for rotating was also determined and the set of the bits to be rotated.

The proposed method was tested and implemented using various digital speech file. The quality of the encrypted files was examined and it was shown that using the low ordered indexes of the binary values of the speech samples is the best choice to achieve a high degree of destruction in the obtained encrypted files.

References

- [1]. 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>
- [2]. 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
- [3]. 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>
- [4]. EE. KisikChang, J. Changho, & L. Sangjin, "High Quality Perceptual Steganographic Techniques", Springer. 2939, pp.518-531, 2004. doi: 10.1007/978-3-540-24624-4_42, <http://www.springerlink.com/content/c6guuj5xnyy4wj3c/>
- [5]. C. Kessler, "Steganography: Hiding Data within Data" An edited version of this paper with the title "Hiding Data in Data", Windows & .NET Magazine, 2001. [Online] Available: <http://www.garykessler.net/library/steganography.html> (October 4,2011)
- [6]. Gandharba Swain, & S.K. lenka, "Steganography-Using a Double Substitution Cipher", International Journal of Wireless Communications and Networking. 2(1), pp.35-39, 2010. ISSN: 0975-7163. <http://www.serialspublications.com/journals1.asp?jid=436&jtype>

- [7]. Hideki Noda, Michiharu Nimi, & Eiji Kawaguchi, "High-performance JPEG steganography using Quantization index modulation in DCT domain", *Pattern Recognition Letters*, 27, pp.455-46, 2006. <http://ds.lib.kyutech.ac.jp/dspace/bitstream/10228/450/1/repository6.pdf>
- [8]. Kathryn, "A Java Steganography Tool", 2005. <http://diit.sourceforge.net/files/Proposal.pdf>
- [9]. Motameni, M. Norouzi, M. Jahandar, & A. Hatami, "Labeling method in Steganography", *Proceedings of world academy of science, engineering and technology*, 24, pp.349-354, 2007. ISSN 1307-6884. <http://www.waset.org/journals/waset/v30/v30-66.pdf>
- [10]. Mohammed A.F Al Husainy, "Message Segmentation to Enhance the Security of LSB Image Steganography", *International Journal of Advanced Computer Science and Applications*, 3(3): 57-62, 2012. <http://www.ijacsa.thesai.org>
- [11]. Mohammed A.F Al Husainy, "Developed Segmented LSB Image Steganography", *International Science and Technology Conference (ISTEC 2012)*, Dubai, December 13-15, 2012. <http://www.iste-c.net>
- [12]. Afjal H. Sarower; Rashed Karim; Maruf Hassan, An Image Steganography Algorithm using LSB Replacement through XOR Substitution, *Computer Science:2019 International Conference on Information and Communications Technology (ICOIACT)*, DOI:10.1109/icoiact46704.2019.8938486.
- [13]. Rashad J. Rasras¹, Mutaz Rasmi Abu Sara², Ziad A. AlQadi³, 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, 2019, <https://doi.org/10.30534/ijatcse/2019/64832019>
- [14]. Ziad A. Alqadi, Majed O. Al-Dwairi, Amjad A. Abu Jazar and Rushdi Abu Zneit, 2010, Optimized True-RGB color Image Processing, *World Applied Sciences Journal* 8 (10): 1175-1182, ISSN 1818-4952.
- [15]. Waheeb, A. and Ziad AlQadi, 2009. Gray image reconstruction, *Eur. J. Sci. Res.*, 27: 167-173.
- [16]. Akram A. Moustafa and Ziad A. Alqadi, Color Image Reconstruction Using A New R'G'I Model, *Journal of Computer Science* 5 (4): 250-254, 2009 ISSN 1549-3636. <https://doi.org/10.3844/jcs.2009.250.254>
- [17]. Musbah J. Aqel, Ziad AlQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, *International Journal of Engineering & Technology*, 7(3.13) (2018) 104-107. <https://doi.org/10.14419/ijet.v7i3.13.16334>
- [18]. 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.
- [19]. Khaled Matrouk, Abdullah Al-Hasanat, Haitham Alasha'ary, Ziad Al-Qadi, Hasan Al-Shalabi, Analysis of Matrix Multiplication Computational Methods, *European Journal of Scientific Research*, ISSN 1450-216X / 1450-202X Vol.121 No.3, 2014, pp.258-266.
- [20]. Ziad A.A. Alqadi, Musbah Aqel, and Ibrahiem M. M. ElEmary, Performance Analysis and Evaluation of Parallel Matrix Multiplication Algorithms, *World Applied Sciences Journal* 5 (2): 211-214, 2008.
- [21]. Z Alqadi, A Abu-Jazzar, Analysis of program methods used in optimizing matrix multiplication, *Journal of Engineering*, 2005.
- [22]. Musbah J. Aqel, Ziad A. Alqadi, Ibraheem M. El Emery, Analysis of Stream Cipher Security Algorithm, *Journal of Information and Computing Science* Vol. 2, No. 4, 2007, pp. 288-298.
- [23]. 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*, Vol. 96. No. 13, pp. 4081-4091, 2018.
- [24]. 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.
- [25]. 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.
- [26]. 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>
- [27]. 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
- [28]. 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.
- [29]. Zhou X, Gong W, Fu W, Jin L. 2016 An 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>

- [30]. Wu D-C, Tsai W-H. A stenographic method for images by pixel value differencing. *Pattern Recognition. Lett.* 24, 1613–1626. 2003 [https://doi.org/10.1016/S0167-8655\(02\)00402-6](https://doi.org/10.1016/S0167-8655(02)00402-6)
- [31]. 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>
- [32]. M. Abu-Faraj, and Z. Alqadi, “Image Encryption using Variable Length Blocks and Variable Length Private Key,” *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 11, Iss. 3, pp. 138-151, 2022.
- [33]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, “A Dual Approach for Audio Cryptography,” *Journal of Southwest Jiaotong University*, vol. 57, no. 1, pp. 24-33, 2022.
- [34]. 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.
- [35]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, “Simple, Efficient, Highly Secure, and Multiple Pur- posed Method on Data Cryptography,” *Traitement du Signal*, vol. 39, no. 1, pp. 173-178, 2022.
- [36]. M. Abu-Faraj, Khaled Aldebe, 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, 2021.
- [37]. M. Abu-Faraj, Z. Alqadi, and K. Aldebei, “Comparative Analysis of Fingerprint Features Ex- Traction Methods,” *Journal of Hunan University Natural Sciences*, vol. 48, iss. 12, pp. 177-182, 2021.
- [38]. M. Abu-Faraj, and Z. Alqadi, “Improving the Efficiency and Scalability of Standard Meth- ods for Data Cryptography,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 21, no.12 , pp. 451-458, 2021.
- [39]. Abdullah N. Olimat, Ali F. Al-Shawabkeh, Ziad A. Al-Qadi, Nijad A. Al-Najdawi, Forecasting the influence of the guided flame on the combustibility of timber species using artificial intelligence, *Case Studies in Thermal Engineering*, Volume 38, 2022, 102379, ISSN 2214-157X, <https://doi.org/10.1016/j.csite.2022.102379>.
- [40]. M. Abu-Faraj, and Z. Alqadi, “Image Encryption using Variable Length Blocks and Variable Length Private Key,” *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 11, Iss. 3, pp. 138-151, 2022.
- [41]. M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, “A Dual Approach for Audio Cryptography,” *Journal of Southwest Jiaotong University*, vol. 57, no. 1, pp. 24-33, 2022.
- [42]. 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.
- [43]. M. Abu-Faraj, K. Aldebei, and Z. Alqadi, “Simple, Efficient, Highly Secure, and Multiple Purr- posed Method on Data Cryptography,” *Traitement du Signal*, vol. 39, no. 1, pp. 173-178, 2022.
- [44]. M. Abu-Faraj, Khaled Aldebe, 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, 2021.
- [45]. M. Abu-Faraj, and Z. Alqadi, “Improving the Efficiency and Scalability of Standard Meth- odds for Data Cryptography,” *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 21, no.12 , pp. 451-458, 2021.
- [46]. J. Vilkamo and T. Bäckström, “Time-Frequency Processing: Methods and Tools,” in *Parametric Time-Frequency Domain Spatial Audio*, V. Pulkki, S. Delikaris-Manias, and A. Politis, Eds. Wiley, 2017, pp. 3–24.
- [47]. K Matrouk, A Al-Hasanat, H Alasha'ary, Ziad Al-Qadi, H Al-Shalabi, Speech fingerprint to identify isolated word person, *World Applied Sciences Journal*, 31 (10), 1767-1771, 2014.
- [48]. Ziad alqadi, Analysis of stream cipher security algorithm, *Journal of Information and Computing Science*, vol. 2, issue 4, pp. 288-298, 2007.
- [49]. Jamil Al-Azzeh, Bilal Zahran, Ziad Alqadi, Belal Ayyoub, Muhammed Mesleh, A Novel Based On Image Blocking Method to Encrypt-Decrypt Color, *International Journal on Informatics Visualization*, vol. 3, issue 1, pp. 86-93, 2019.
- [50]. Musbah J Aqel, Ziad ALQadi, Ammar Ahmed Abdullah, RGB Color Image Encryption-Decryption Using Image Segmentation and Matrix Multiplication, *International Journal of Engineering and Technology*, vol. 7. Issue 3.13, pp. 104-107. 2018.
- [51]. Jihad Nadir, Ashraf Abu Ein, Ziad Alqadi, A Technique to Encrypt-decrypt Stereo Wave File, *International Journal of Computer and Information Technology*, vol. 5, issue 5, pp. 465-470, 2016.
- [52]. Saleh Khawatreh, Belal Ayyoub, Ashraf Abu-Ein, Ziad Alqadi, A Novel Methodology to Extract Voice Signal Features, *International Journal of Computer Applications*, vol. 975, pp. 8887, 2018.
- [53]. 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 9, pp. 4092-4098, 2019.

- [54].Aws Al-Qaisi, Saleh A Khawatreh, Ahmad A Sharadqah, Ziad A Alqadi, Wave File Features Extraction Using Reduced LBP, International Journal of Electrical and Computer Engineering, vol. 8. Issue 5, pp. 2780-2787, 2018.
- [55].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.
- [56].Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016
- [57].Ismail Shayeb, Ziad Alqadi, Jihad Nader, Analysis of digital voice features extraction methods, International Journal of Educational Research and Development, vol. 1, issue 4, pp. 49-55, 2019.
- [58].Jihad Nader Ahmad Sharadqah, Ziad Al-Qadi, Bilal Zahran, Experimental Investigation of Wave File Compression-Decompression, International Journal of Computer Science and Information Security, vol. 14m issue 10, pp. 774-780, 2016.
- [59].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.
- [60].Majed O Al-Dwairi, A Hendi, Z AlQadi, an efficient and highly secure technique to encrypt-decrypt color images, Engineering, Technology & Applied Science Research, vol. 9, issue 3, pp. 4165-4168, 2019.
- [61].Amjad Y Hendi, Majed O Dwairi, Ziad A Al-Qadi, Mohamed S Soliman, a novel simple and highly secure method for data encryption-decryption, International Journal of Communication Networks and Information Security, vol. 11, issue 1, pp. 232-238, 2019.
- [62].Prof. Ziad Alqadi, Dr. Mohammad S. Khrisat, Dr. Amjad Hindi, Dr. Majed Omar Dwairi, USING SPEECH SIGNAL HISTOGRAM TO CREATE SIGNAL FEATURES, International Journal of Engineering Technology Research & Management, vol. 4, issue 3, pp. 144-153, 2020.
- [63].M. Abu-Faraj, Z. Alqadi, and K. Aldebei, "Comparative Analysis of Fingerprint Features Extraction Methods," Journal of Hunan University Natural Sciences, vol. 48, iss. 12, pp. 177-182, 2021.
- [64].Alqadi, Z. (2019). A new method for voice signal features creation. International Journal of Electrical and Computer Engineering (IJECE), 9(5): 4092-4098. <https://doi.org/10.11591/ijece.v9i5.pp4092-4098>.
- [65].Alqadi, Z. (2009). 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.
- [66].Zaini, H., Alqadi, Z.A. (2021). Efficient WPT based speech signal protection. IJCSMC, 10(9): 53-65. <https://doi.org/10.47760/ijcsmc.2021.v10i09.006>.
- [67].Zneit, R.A., Khrisat, M.S., Khawatreh, S.A., Alqadi, Z.(2020). Two ways to improve WPT decomposition used for image features extraction. European Journal of Scientific Research, 157(2): 195-205.
- [68].Hindi, A., Qaryouti, G.M., Eltous, Y., Abuzalata, M., Alqadi, Z. (2020). Color image compression using linear prediction coding. International Journal of Computer Science and Mobile Computing, 9(2): 13-20.
- [69].Zaidan, A.A., Majeed, A., Zaidan, B.B. (2009). High securing cover-file of hidden data using statistical technique and AES encryption algorithm. World Academy of Science Engineering and Technology(WASET), 54: 468-479.
- [70].Zaidan, A.A., Zaidan, B.B. (2009). Novel approach for high secure data hidden in MPEG video using public key infrastructure. International Journal of Computer and Network Security, 1(1): 1985-1553.
- [71].Khalifa, O.O., Naji, A.W., Zaidan, A.A., Zaidan, B.B., Hameed, S.A. (2010). Novel approach of hidden data in the (unused area 2 within EXE file) using computation between cryptography and steganography. Int. J. Comput.Sci. Netw. Secur, 9(5): 294-300.
- [72].Majeed, A., Mat Kiah, M.L., Madhloom, H.T., Zaidan, B.B., Zaidan, A.A. (2009). Novel approach for high secure and high rate data hidden in the image using image texture analysis. International Journal of Engineering and technology, 1(2): 63-69. <http://eprints.um.edu.my/id/eprint/4951>.
- [73].Zaidan, A.A., Othman, F., Zaidan, B.B., Raji, R.Z., Hasan, A.K., Naji, A.W. (2009). Securing cover-file without limitation of hidden data size using computation between cryptography and steganography. In Proceedings of the World Congress on Engineering, 1: 1-7.
- [74].Aos, A.Z., Naji, A.W., Hameed, S.A., Othman, F., Zaidan, B.B. (2009). Approved undetectable-antivirus steganography for multimedia information in PE-file. In 2009 International Association of Computer Science and Information Technology-Spring Conference, pp. 437-444. <https://doi.org/10.1109/IACSIT-SC.2009.103>.
- [75].Zaidan, A.A., Zaidan, B.B., Abdulrazzaq, M.M., Raji, R.Z., Mohammed, S.M. (2009). Implementation stage for high securing cover-file of hidden data using computation between cryptography and steganography. International Association of Computer Science and Information Technology (IACSIT), indexing by Nielsen, Thomson ISI (ISTP), IACSIT Database, British Library and EI Compindex, 19: 482-489.

- [76].Naji, A.W., Zaidan, A.A., Zaidan, B.B., Muhamadi, I.A.(2010). Novel approach for cover file of hidden data in the unused area two within EXE file using distortion techniques and advance encryption standard. Proceeding of World Academy of Science Engineering and Technology (WASET), 56(5): 498-502.
- [77].M. Bala Kumara, P. Karthikkab , N. Dhiviyac , T. Gopalakrishnan, A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 2, February – 2014.
- [78].Lee Mariel Heucheun Yepdia, Alain Tiedeu, and Guillaume Kom, A Robust and Fast Image Encryption Scheme Based on a Mixing Technique, Security and Communication Networks, Volume 2021 |Article ID 6615708 | <https://doi.org/10.1155/2021/6615708>.
- [79].Z. Hua, Y. Zhou, and H. Huang, “Cosine-transform-based chaotic system for image encryption,” Information Sciences, vol. 480, pp. 403–419, 2019.
- [80].M. Asgari-chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, “A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation,” Signal Processing, vol. 157, p. 1, 2019.
- [81].X. Zhang and X. Wang, Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System, Springer, New York, NY, USA, 2019.
- [82].J. S. Zhenjun and R. Sun, “Multiple-image encryption with bit-plane decomposition and chaotic maps,” Optics and Lasers in Engineering, vol. 80, pp. 1–11, 2016.