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. 13, Issue. 2, February 2024, pg.13 – 26

LSB8 using DSF to Hide Secret Message

Prof. Ziad Al Qadi; Hussein Najeeb Hatamleh

Al Balqa Applied University, Faculty of Engineering Technology, Jordan-Amman

DOI: https://doi.org/10.47760/ijcsmc.2024.v13i02.002

Abstract:
An efficient method of message steganography will be proposed, the method will use 8 bits from the speech sample binary value to hold one character from the secret message, thus the capacity hiding will equal the covering DSF size. Using lower LSBs of the speech sample binary value will not much affect the sample value, so the quality of the stego DSF will be excellent and the stego file will be closed to the covering file. The proposed method will add an extra security issues by using a private key, this key will be used to calculate the starting sample where to start characters hiding, it will determine the starting LSB to get the set of 8 LSBs, and it will be also used to generate eight element chaotic key, this key will be converted to 8 orders of LSBs to hide the bits of characters, these bit will be not consecutive. The PK will a long enough long provide a good key space capable to resist hacking attempt and the extracted message will be very sensitive to the selected values of the private key.
The proposed method will provide enhancements in the quality, security, speed and sensitivity of message steganography, these enhancements will be proved based on the discussing of obtained experimental results.
Keywords: Steganography, SM, DSF, stego file, covering file, PK, CK, IKEY, LSB8.

Introduction

Message steganography [11-20] shown in figure 1 is the process of securing the message by hiding it in a covering media before message transmission and extracting it from the stego media after receiving the stego media. Message hiding is usually implemented by a hiding function (See figure 1 (a)), this function processes the secret message, the covering media and the private key (PK) to produce a stego media, while the extracting function processes the stego media and the PK to produce a secret image (see figure 1 (b)) [21-25[.

.The digital speech file (DSF) is an excellent and convenient media to be used as a covering media for the following reasons [26-31]:

- Easy to get the speech file.
- A huge size of the DSF allows providing a big hiding capacity; it can be easily used to hide ahort and long messages.
- The binary value of the speech sample gives us a flexibility of using 1 or more bits for message hiding.

- Changing some bits (as we will see later in this section) in the speech sample binary value will not much affect the speech value, thus will keep the stego file with excellent quality [32-40].

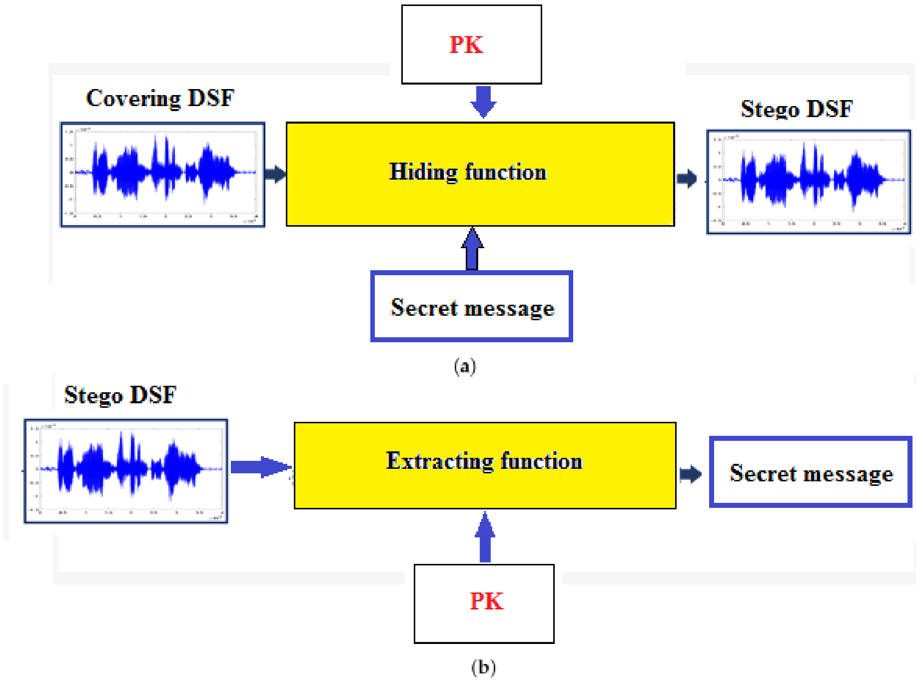

Figure 1: Process of message steganography diagram

Steganography refers [1-10] to the process of concealing a secret message (with no traceability) in a manner that it will make no meaning to anyone else except the intended recipient, and it has the features listed in table 1 [11-17].

Table 1: Steganography vs cryptography [43-50]

Feature	Steganography
Meaning	Covered writing
Data altering	Structure of data is not usually altered.
Supports	Supports **Confidentiality** and **Authentication** security principles
Needs for mathematics	Not much mathematical transformations are involved.
Action on data	The information is hidden.
Data visibility	Hidden information is not visible
Confidentiality	Provides Confidentiality only
Algorithm	Doesn't have specific algorithms
Goal	is to make the information invisible to anyone who doesn't know where to look or what to look for

A good stego system must satisfy the following requirements [41-46]:

1) Quality:

- The extracted message must be the same as the source message, the mean square value (MSE) measured between the source and the extracted message must be equal zero, while the peak signal to noise ratio (PSNR) measured between them must be equal infinity (see table 2) [47-52].

- The stego DSF must be closed to the covering file, the MSE measured between them must be very low, while the PSNR must be very high (see table 2) [53-60].

Table 2: Quality requirements [61-65]

Quality Parameter	Measured between covering and stego DSFs	Measured between source and extracted SMs
MSE	**Very low**	**Zero**
PSNR	**Very high**	**Infinity**
Remarks	**Stego file must be closed to covering one**	**Extracted message must be identical to the source one**

2) **Speed:**
The stego system must decrease both the hiding and extracting times and increase the throughputs of message hiding and message extracting (K characters processed in a second).

3) **Extra security issues:**
The stego system in addition to data hiding must used a private key to protect the hidden message from being hacked; the key must provide a good key space capable to resist hacking attacks [66-70].

4) **Flexibility:**
The stego system must be able to process any message (short and long), changing the message must not require any changes in the hiding and extracting functions.

5) **Simplicity:**
The hiding and extracting functions must minimize the code required to apply message hiding and message extracting.
Secret message (SM) is a set of characters which forms a one row matrix, it can be easily processed and it can be presented as shown in figure 2 by the characters, the decimal values and the message binary matrix (MBM).

```
Message='Steganography';
Decimal=uint8(Message)
Decimal =

  83  116  101  103   97  110  111  103  114   97  112  104  121

MBM=dec2bin(Decimal,8)

MBM =

01010011
01110100
01100101
01100111
01100001
01101110
01101111
01100111
01110010
01100001
01110000
01101000
01111001
```

Message binary matrix (MBM) ←

Figure 2: SM presentation

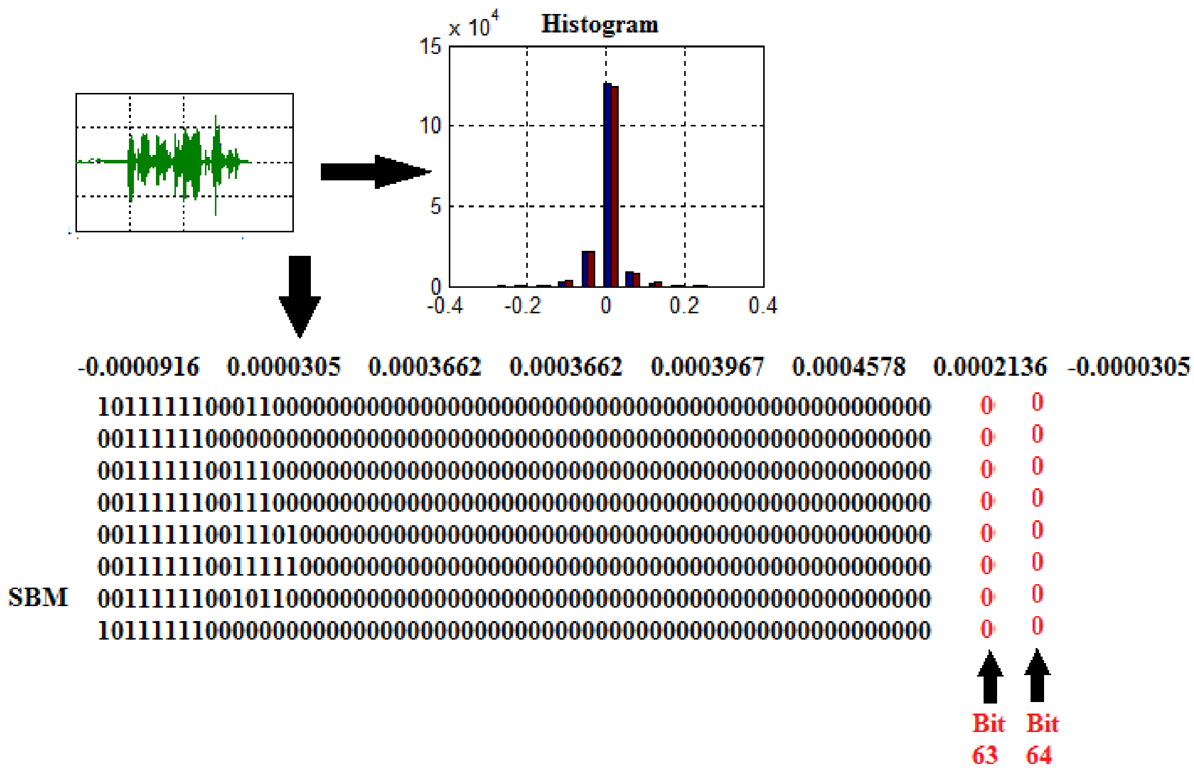

Figure 3: DSF presentation

Digital speech file (DSF) [70-80] is a set of samples values, these values are organized in one or two columns matrix, this file can be presented by the speech wave, histogram, decimal matrix and the speech binary matrix (SBM) as shown in figure 3. DSF has the following features:

- Huge size, the size of the DSF can be increased by increasing the recording time and/or the sampling frequency.
- Decimal fractional value of the speech sample is represented by a 64 bits binary number, this number as shown in figure 4 provide a flexibility to select one or more bits for MBM bits hiding.

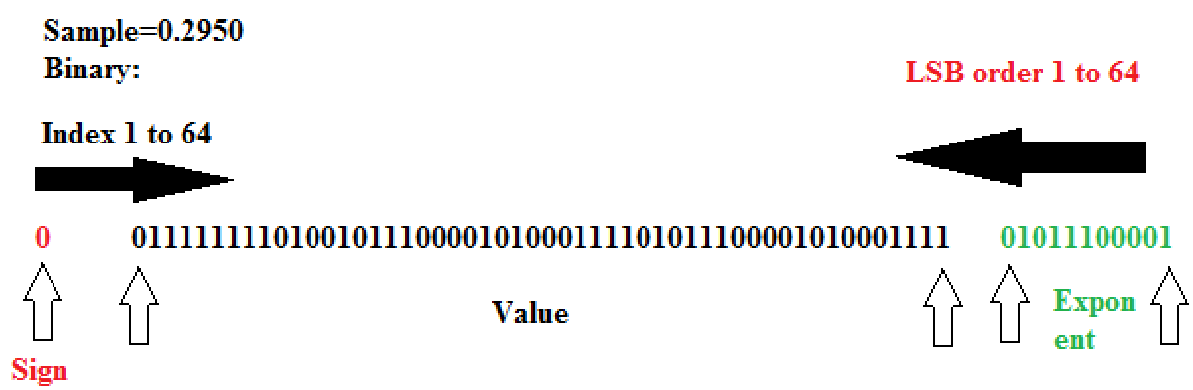

Figure 4: 64_bits binary value of the DSF sample

- Changing the low ordered LSBs of the speech sample values will not much affect the sample value, this will give use the ability to use one or more LSBs for message hiding. Table 3 shows the effects of changing 8LSBs of the speech sample value using different orders of LSB8[1-10]:

Table 3: Effects of replacing different ordered LSB8s sets of the speech sample

Sample=0.294
Character 'Z'
Decimal=90
Binary=01011010

Changed orders bits	New value	MSE	PSNR
1-8	**3.2607e+129**	**1.0632e+259**	**0**
2-9	**2.3092e-090**	**0.0864**	**0**
3-10	**6.1454e-200**	**0.0864**	**0**
4-11	**5.3766e-100**	**0.0864**	**0**
5-12	**2.5145e-050**	**0.0864**	**0**
25-32	0.2940	1.0983e-009	181.8118
26-33	0.2940	1.7826e-010	199.9942
27-34	0.2940	1.2367e-011	226.6764
28-35	0.2940	1.9620e-012	245.0872
29-36	0.2940	3.5527e-015	308.2271
30-37	0.2940	3.7326e-013	261.6816
40-47	0.2940	1.7809e-019	407.2365
57-64	**0.2940**	**3.7748e-030**	**653.0085**
56-63	**0.2940**	**5.2077e-029**	**626.7648**
55-62	**0.2940**	**8.3323e-030**	**645.0906**
54-61	**0.2940**	**5.3327e-028**	**603.5017**
53-60	**0.2940**	**2.5630e-027**	**587.8026**

From table 3 we can see that the best choice is to select the bits 57-64 for message steganography, but we can use other lower ordered LSBs, but the MSE will grow, while the PSNR will drop down, and these values will be acceptable.

Several methods [1-10]were introduced for message steganography, most of these methods were based on LSB and LSB2 methods, and mostly these methods used digital image as a covering media [1-7], increasing the message length will negatively affect the quality of the stego image [77-82].

The Proposed Method

The proposed method has the following features:

- It uses 8 consecutive bits from each covering speech sample value to hide one character from the SM.
- The set of 8 bits starting bit (SB) is from 25 to 57.
- The capacity hiding of the covering DSF equals the speech size in samples.
- Using high ordered bits will enhance the quality of the stego file.
- The PK is used to generate an 8 elements chaotic logistic key, this key will be converted to indices key, the last order of the bit in the set of 8 LSBs will be added to this key to form a new indices key, this key will be used to arrange the character bits as illustrated in the example shown in figure 5.
- The PK contains 4 components: a pair of chaotic parameters r and x, the starting position (POS), and the last bit order in the set of LSB8 (LB). r and x are used to run a chaotic logistic map model (CLMM) to generate a chaotic key (CK), POS is used to calculate the starting position of the covering-stego samples, while LB is used to adjust the contents of the generated from CK indices key.

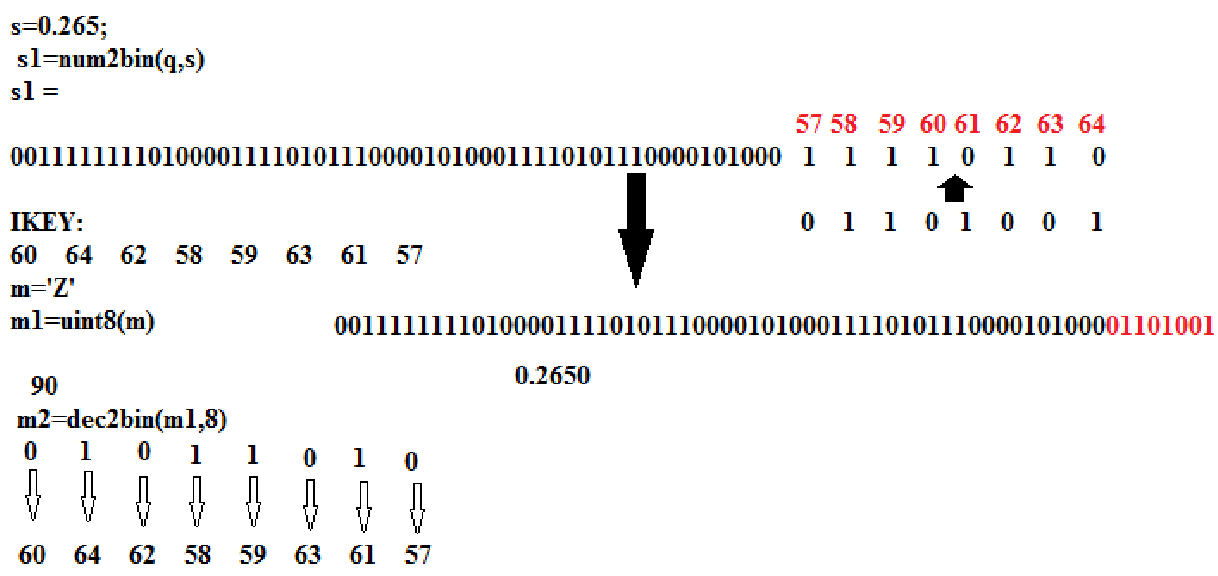

Figure 5: Example of character bits hiding

The proposed method will implemented applying the following tasks:

Hiding process:

Task1:

Input preparation:

1) Get the covering DSF.
2) Get the file size.
3) Reshape DSF matrix to one row matrix.
4) Get the SM.
5) Get the length of the message.
6) Convert the message to decimal.
7) Get the PK.

Task2:

PK processing:

1) Use r and x values to run CLMM to generate CK.
2) Sort this key to get the indices key.
3) Subtract the contents of the indices key from LB and add 1 to the results to get the secret key.
4) Compute the starting position of the covering samples by multiplying the POS value with the DSF size and taking the integer value of the results.

Task 3:

Message hiding:

1) Get the covering samples.
2) Convert the covering samples to binary to get the SBM.
3) Convert the decimal matrix to binary to get the MBM.
4) For each row in MBM insert the bit in the sample LSB8 bits using the secret key.
5) Convert the resulting covering samples to decimal to get the stego samples.
6) Return the stego samples back to the DSF row matrix.
7) Reshape back the row matrix to the original size to get the stego DSF.

The extracting process:

Task1 1:

Input preparation:

1) Get the stego DSF.
2) Get the file size.
3) Reshape the file matrix to one row matrix.

Task2:

PK processing:

This task will be implemented using the same procedures as for data hiding process.

Task3:

SM extraction:

1) Get the stego samples.
2) Convert the stego samples.
3) Extract the LSB8 of each sample using the secret key to form MBM.
4) Convert MBM to decimal.
5) Convert the decimal matrix to characters to get the SM.

The following mat lab code can be useful to test and implement the proposed method:

```
;Hiding process
m1='LSB8 message hiding';
m2=uint8(m1);
LM=length(m1);
[c1 fs1]=wavread('C:\Users\win 7\Desktop\voices\a1.wav');
[nn1 nn2 nn3]=size(c1);L1=nn1*nn2;
c2=reshape(c1,1,L1);
r1=3.77;x1=0.11;POS=0.179;LB=64;
q1 = quantizer('double');
m3=dec2bin(m2,8);
for i=1:8
      x1=r1*x1*(1-x1);
      CK(i)=x1;
end
[ff IKEY]=sort(CK);
STP=fix(L1*POS);
P=LB+1-IKEY;
covs=c2(1,STP+1:STP+LM);
covsb=num2bin(q1,covs);
for i=1:LM
   for j=1:8
      covsb(i,P(j))=m3(i,j);
   end
end
stegos=bin2num(q1,covsb)';
c2(1,STP+1:STP+LM)=stegos;
c3=reshape(c2,nn1,nn2);
```

```
;Extracting process
c4=reshape(c3,1,L1);
r1=3.77;x1=0.11;POS=0.179;LB=64;
for i=1:8
    x1=r1*x1*(1-x1);
    CK(i)=x1;
end
[ff IKEY]=sort(CK);
STP=fix(L1*POS);
P=LB+1-IKEY;
s1=c4(1,STP+1:STP+LM);
s2=num2bin(q1,s1);
for i=1:LM
   for j=1:8
      m4(i,j)=s2(i,P(j));
   end
end
m5=bin2dec(m4)';
char(m5)
```

Implementation and Results Discussion

A good method of message steganography must produce a stego file with excellent quality, the stego file must be closed to the covering file. The quality of the proposed method was tested, several messages were selected and processed using the proposed method, figure 6 shows a sample outputs of the method implementation, this figure shows that even the hidden message was long the quality of the stego file is excellent and the stego file is closed to the covering one, and this prove the fact that the proposed method satisfies the quality requirements.

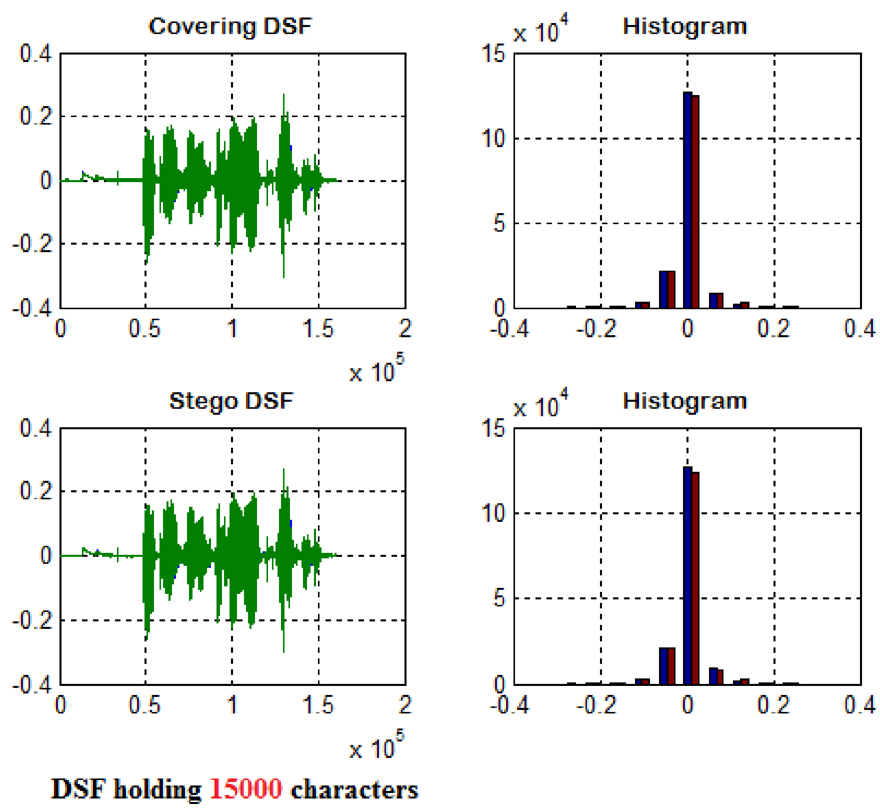

Figure 6: Produced sample outputs

The MSE and PSNR values measured between the covering and stego files were calculated and the obtained values of these parameters also prove that the proposed method satisfies the quality requirements (see table 4), (the covering DSF size was equal

Table 4: Quality parameters measured between covering and stego DSFs

Message length (byte)	MSE	PSNR
100	1.2363e-036	800.4879
200	1.2921e-036	800.0468
400	4.2597e-036	788.1174
500	4.2223e-036	788.2056
750	5.8444e-036	784.9546
1000	7.7495e-036	782.1331
1500	1.4803e-034	752.6352
5000	8.5328e-033	712.0926
10000	2.6270e-032	700.8476
20000	4.2875e-032	695.9489
Remarks	Low	High

The low values of MSE and high values of PSNR prove that the proposed method satisfies the quality requirements, the obtained quality parameters are better than the parameters of other methods introduced in [1-10], the quality of the stego file keeps excellent even if we hide a long message (see figure 7).

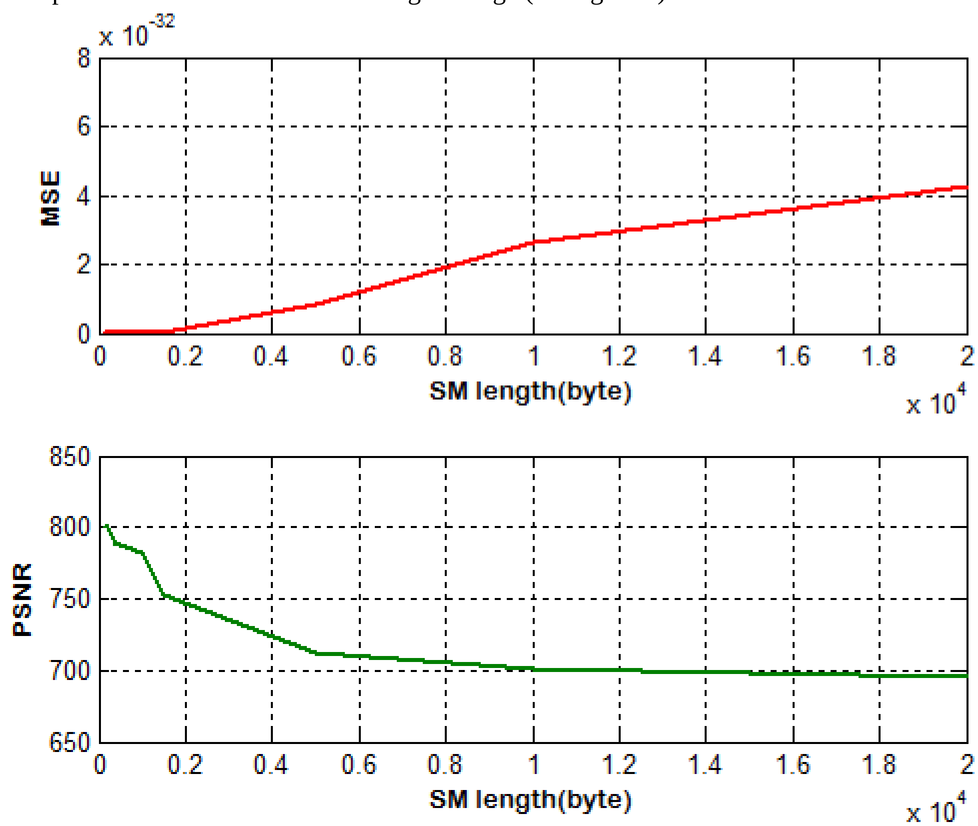

Figure 7: MSE and PSNR vs SM length

The proposed method provided a good speed, several messages were processed, the hiding time in seconds (HT), the extracting time in seconds (ET), the hiding throughput in K bytes per second (HTP) and the extracting throughput in K bytes per second (ETP) were calculated and table 5 shows the obtained results:

Table 5: Obtained speed results

SM length (byte)	HT	ET	HTP	ETP
100	0.0580	0.0110	1.6837	8.8778
500	0.0740	0.0250	6.5984	19.5313
750	0.0820	0.0380	8.9320	19.2743
1000	0.0910	0.0560	10.7315	17.4386
1500	0.1170	0.0700	12.5200	20.9263
5000	0.2580	0.1980	18.9256	24.6607
10000	0.4660	0.5250	20.9563	18.6012
20000	0.8780	1.6660	22.2452	11.7234
25000	1.0800	2.5230	22.6056	9.6766
50000	2.5110	12.1770	23.4638	4.0099
100000	4.1300	53.8210	23.6456	1.8145

The obtained speed results are acceptable and they are closed to the results of other existing methods of message steganography using digital image as a covering media.
The proposed method is sensitive to the selected values of the PK, any changes in the PK in the extracting process will produce a damaged extracted message as shown in the obtained results shown in table 6.
The message "LSB8 steganography" was hidden using PK1, the hidden message was extracted by each of the following PKs, and table 6 shows the obtained results:

PK1:
r1=3.77;x1=0.11;
POS=0.179;LB=64;
PK2:
r1=3.87;x1=0.11;
POS=0.179;LB=64;
PK3:
r1=3.77;x1=0.19;
POS=0.179;LB=64;
PK4:
r1=3.77;x1=0.11;
POS=0.279;LB=64;
PK5:
r1=3.77;x1=0.11;
POS=0.179;LB=63;

Table 6: Sensitivity results

Used PK in the extraction function	Extracted message	MSE between the source and the extracted messages	PSNR between the source and the extracted messages	Remarks
PK1	LSB8 steganography	0	Infinity	Correct
PK2	#´$ @srôôpvr@aqbqgv	3545.7	28.2085	Damaged
PK3	&i(§£éé «£ ¤¥¢¥®«	5874.7	22.2366	Damaged
PK4	Unreadable	8764.8	4.1137	Damaged
PK5	8 T<< tT D t	3521	26.9219	Damaged

Conclusion

A simple method of secret message steganography was proposed, the method used simple assignment operations to apply bits hiding and bits extracting. The proposed method used 8 bits from the covering sample binary value to hide one character, making the capacity hiding equal the digital speech file size in samples, the bits can be selected anywhere but it recommended to use the least significant 8 bits to get the best quality of the stego file. The proposed method used a complicated private key with four values, the first two values are a chaotic logistic parameters, which were used to run a CLMM to generate a chaotic key, the chaotic key was transformed to secret indices key to apply message bits hiding in the associated bits of the speech sample, the third value was used to calculate the starting position of the covering-stego samples where to start hiding-extracting, and the fourth value was used to determine the set of used 8 bits for data steganography.

The method was tested and implemented using various messages and the obtained results were used to prove the fact that the method satisfies the requirements of good stego system in quality, speed and sensitivity.

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, &GadielSeroussi,"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, MichiharuNimi, &EijiKawaguchi,"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 Journal8 (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 ANDSEGMENTATIONMETHODS 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, HaithamAlasha'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 ofParallel 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, Ibraheim M. El Emary, 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. 2016An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15thInt. 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. 2003https://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 Sharadqh, 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 TOCREATE 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 Ex- Traction 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 inthe (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-antivirussteganography 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 Compendex, 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. Dhivyac , 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.