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. 5, May 2024, pg.24 – 42

Secure Stego Method to Protect SMS Transmission

Mohanad Ahmad Bashir Bashir

Al-Balqa Applied University, Zarqa University College, Jordan-Zarqa

DOI: https://doi.org/10.47760/ijcsmc.2024.v13i05.002

Abstract:

A novel method of message steganography will be proposed. The method will use a digital speech file as a covering media. The 32 binary bits of each speech sample will be used for data hiding, using these bits will increase the hiding capacity, and changing them will not much affect the sample value, thus the quality of the stego file will be always high. The proposed method will use a private key to protect the hidden message, the protection will be applied by shuffling the rows of the speech binary matrix using the contents of the generated indices key, The induces key will be generated by running a chaotic logistic map model using the values of the chaotic parameters included in the private key. The proposed method will be tested and implemented using various messages, the quality, sensitivity and speed of the proposed method will be analyzed to prove the enhancements provided by the proposed method.

Keywords: Steganography, DSF, SMS, MBM, SBM, shuffling, PK, CK, indices key.

Introduction

Short secret message (SMS) [20-25] are considered one of the most widely used types of digital data and circulated through various social media platforms [14-19]. Since some of these means of communication are unsafe and there are many people lurking about the data to hack it and disrupt its content, it is necessary to protect the text message and transform the communication environment from an unsafe environment to a safe environment as shown in figures 1 and 2.

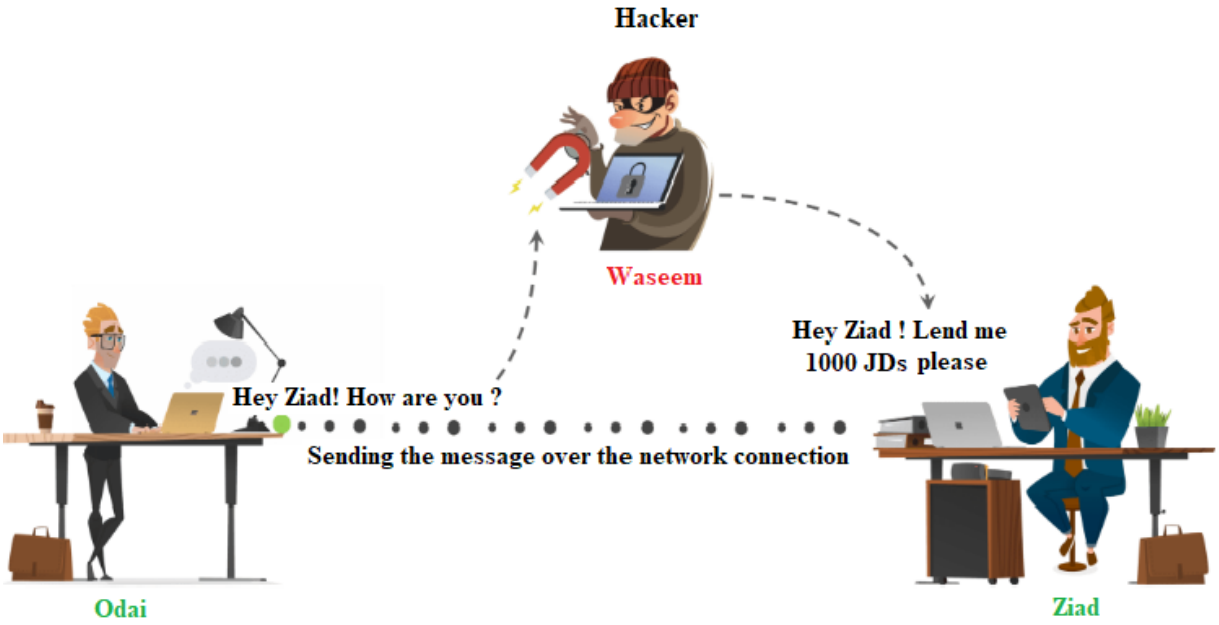

Figure 1: Unsafe SMS transmission media

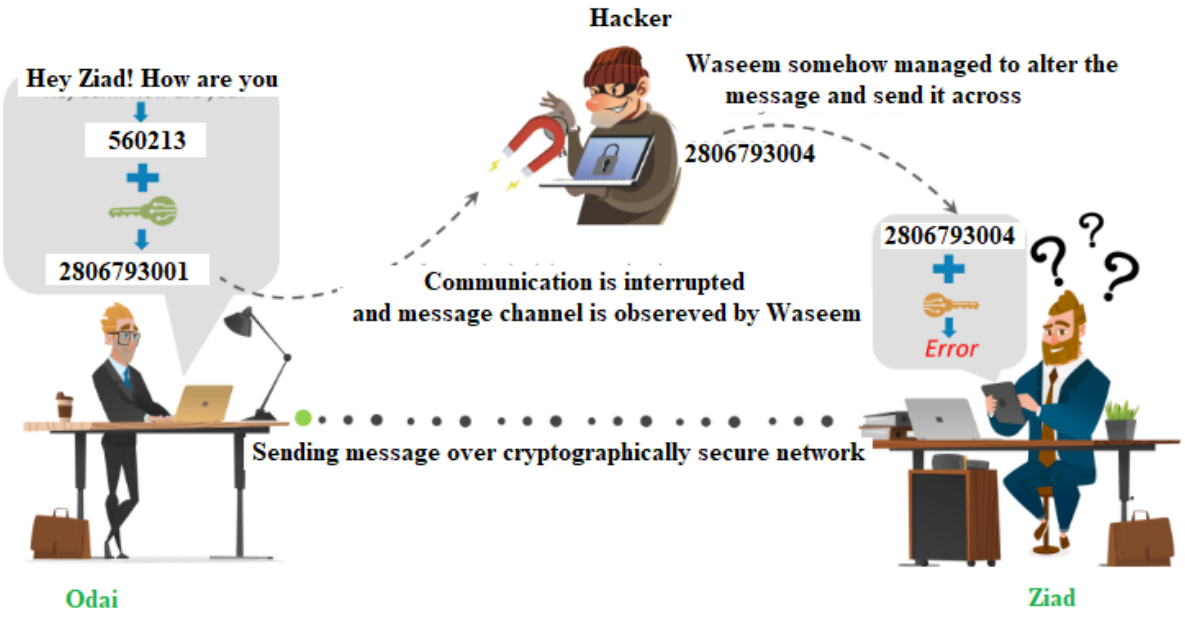

Figure 2: Safe SMS transmission media

SMS protection and securing is required because SMS may be private, or may be secret or the communication media may be unsafe. Protecting and securing the message can be achieved by using message steganography [26-30]. SMS steganography means hiding a message in a covering digital media without affecting much this media, the produced stego media must be closed to the covering media [36-40]. The stego media will be used to extract an SMS which must be identical to the source hidden SMS, the hiding and extracting processes are maintained by hiding and extracting functions as shown in figure 3 [31-35].

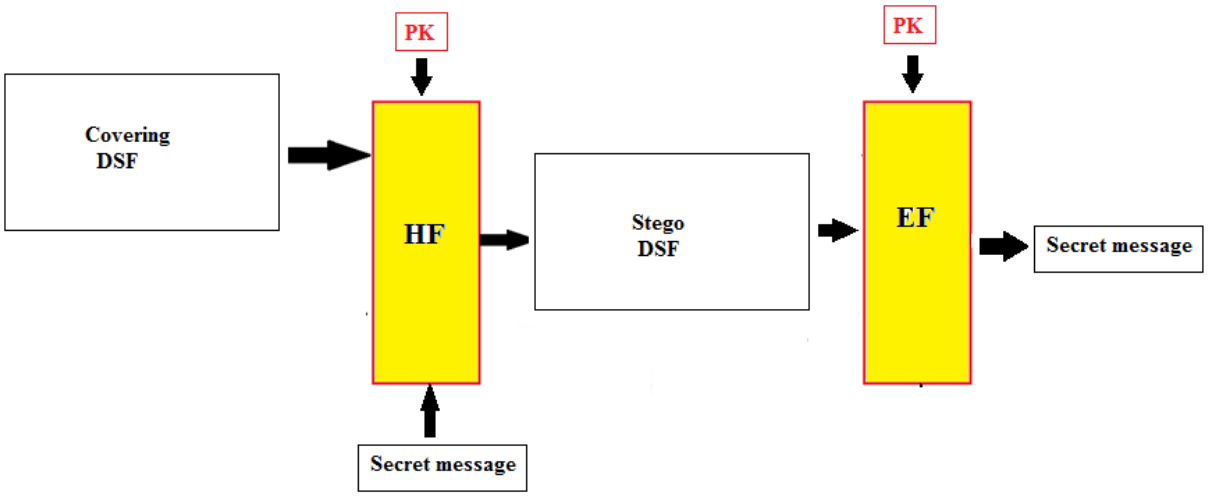

Figure 3: Stego system diagram

In this paper research the process of steganography will combined with a simple message cryptography using a private key, this key will be used to shuffle the columns of each row in the digital speech file binary matrix (SBM). Combining the crypto and stego processes will expand the security enhancements by combining the features of data steganography and cryptography, these features are listed in table 1:

Table 1: Steganography and cryptography features [43-50]

Factor of comparison	Steganography	Cryptography
Meaning	Covered writing	Secret writing
Data altering	Structure of data is not usually altered.	Structure of data is altered.
Mean square error(MSE)	MSE measured between covering and stego DSFs must be low, while MSE between source and extracted message must be zero [77-82].	MSE measured between source and encrypted data must be high, while MSE between source and decrypted data must be zero [70-76].
Peak signal to noise ratio (PSNR)	PSNR measured between covering and stego DSFs must be high, while PSNR between source and extracted message must infinity [65-70].	PSNR measured between source and encrypted data must be low, while PSNR between source and decrypted data must be infinity [60-65].
Supports	Supports **Confidentiality** and **Authentication** security principles	Supports **Confidentiality** and **Authentication** security principles as well as **Data integrity** and **Non-repudiation**
Needs for mathematics	Not much mathematical transformations are involved.	Involves the use of number theory, mathematics etc. to modify data
Action on data	The information is hidden.	The information is transformed
Data visibility	Hidden information is not visible	Transformed information is visible
Confidentiality	Provides Confidentiality only	Provides Confidentiality, Integrity, Non-repudiation
Algorithm	Doesn't have specific algorithms	Has Various recognized and approved algorithms
Goal	is to make the information invisible to anyone who doesn't know where to look or what to look for[50-55]	is to keep the contents of the message secret from unauthorized access [46-50]

SMS is a set of characters organized in one row matrix, the values of this matrix can be easily represented by decimal values (ASCII), these values can be easily converted to binary using 8_bits binary representation to form the message binary matrix (MBM). MBM is a 2D matrix with 8 columns and number of rows equals the messages

length, this matrix can be easily reshaped to form a new matrix with a selected number of columns as shown in figure 4.

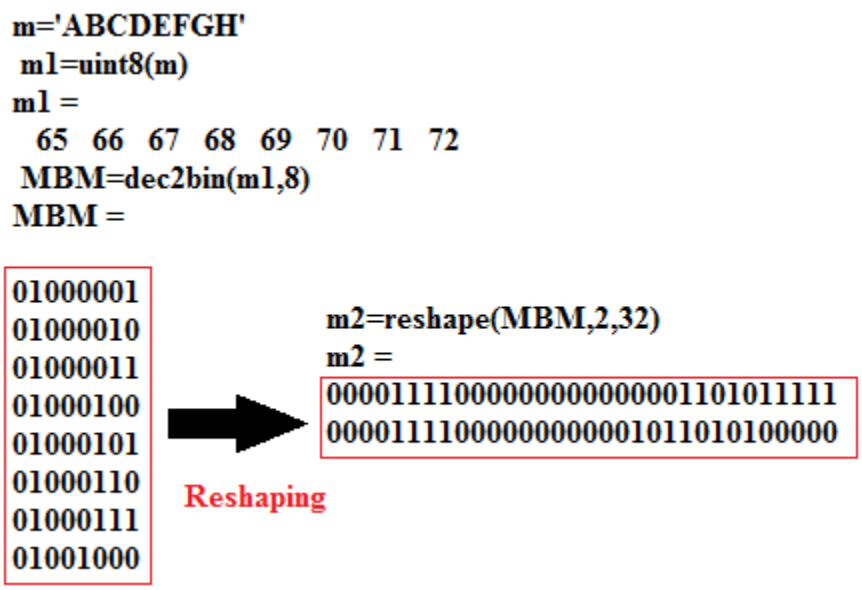

Figure 4: SMS presentation

Digital speech file (DSF) [11-20]is a set of double type values (samples) organized in one column or two columns matrix, these values can be easily converted to binary using 64_bits representation. The sample binary value is divided into three parts (sigh digit, 52 bits for the sample value and 11 bits for the exponent value).
DSF as shown in figure 5 can be presented by the speech wave, histogram, decimal matrix and speech binary matrix (SBM). SBM is a 2D matrix with 64 columns and number of rows equals the DSF size [21-30].

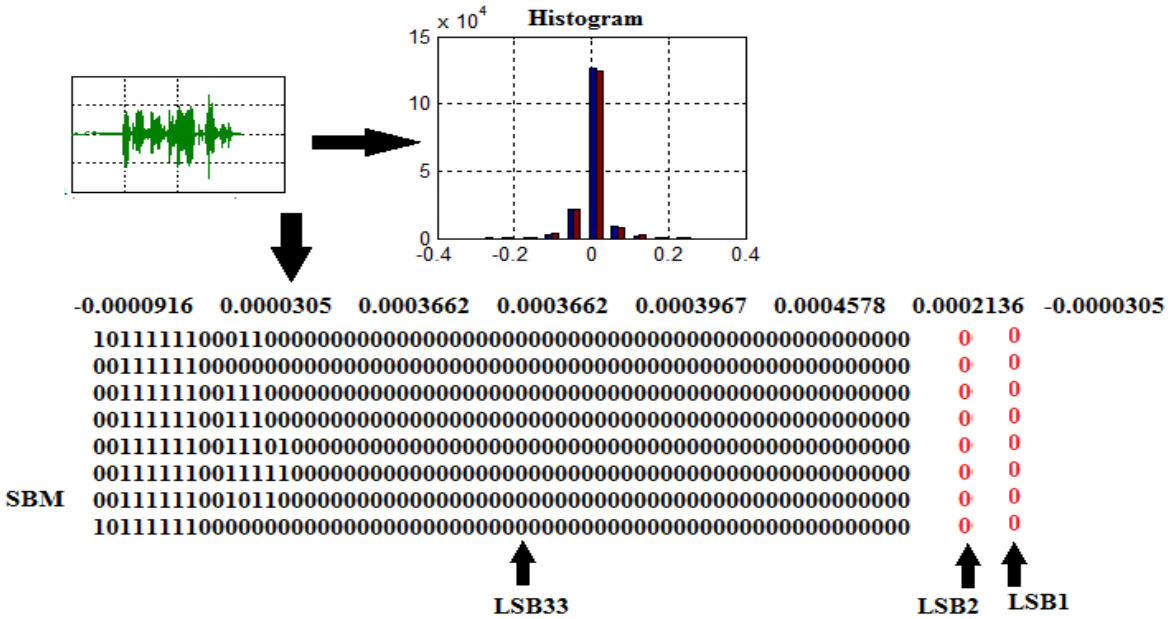

Figure 5: DSF presentation

The sample binary value has an interesting feature, changing the lower bits in this value will not much affect the sample value; this will keep the stego sample closed to the covering sample.
Figures 6, 7 and 8 show the effects of changing some bits in the sample binary value [40-50]:

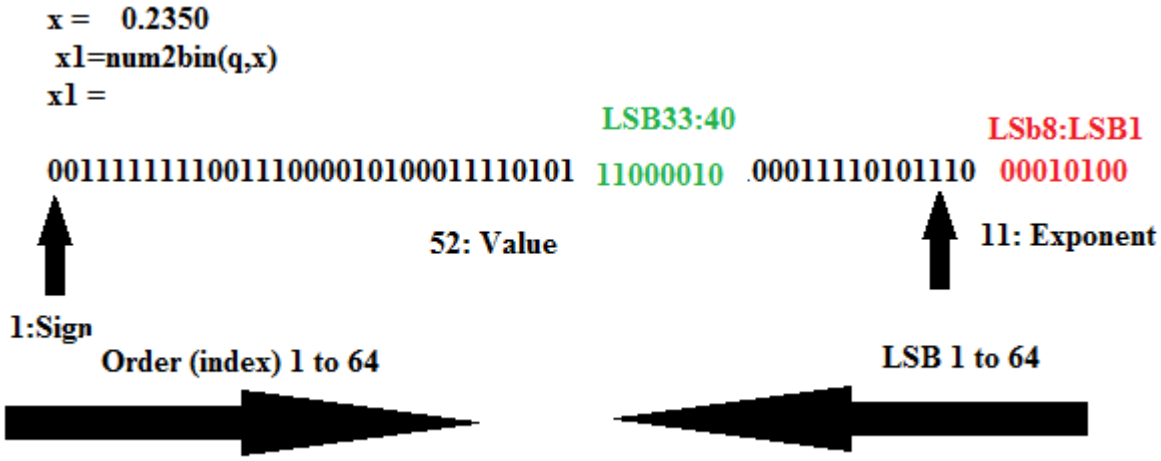

Figure 6: DSF sample values

```
w=65
01000001
x =
   0.2350
x1=num2bin(q,x)
0011111111001110000101000111101011100001010001111010111000010100
x2=x1
x2 =
0011111111001110000101000111101011100001010001111010111000010100
x2(:,57:64)=w   LSB57:LSB1
x2 =
0011111111001110000101000111101011100001010001111010111001000001
x3=bin2num(q,x2)
   0.2350
[r1 r2]=PSNR_RGB(x3,x)
MSE=6.8541e-029
PSNR=648.0815
```

Figure 7: Using lower 8 bits (LSB8) for data hiding (example)

```
w=65
01000001
x =
   0.2350
x1=num2bin(q,x)
00111111110011100001010001111010111000010100011110101110000101000
x2=x1
x2 =
00111111110011100001010001111010111000010100011110101110000101000

 x2=x1
00111111110011100001010001111010111000010100011110101110000101000
x2(:,33:40)=w  LSB33:LSB40
x2 =
00111111110011100001010001111010010000010100011110101110000101000
x3=bin2num(q,x2)
x3 =
 0.2350
MSE =  5.5511e-015
PSNR =  299.2844
```

Figure 8: Using LSB33 to LSB40 for data hiding (example)

In the proposed method the 32 lower bits of each DSF sample binary value will be used for data hiding, and this will provide the following enhancements:

- Each sample can be used to hold 4 characters; this will increase the capacity hiding to reach the DSF size in samples multiplied by 4.
- Changing the 32 bits of the samples binary values will keep the stego samples closed to the covering samples, thus the MSE value measured between the covering DSF and the stego DSF will be minimized, while the value of PSNR will be maximized.

The proposed method will use a chaotic logistic map model (CLMM) parameters r1 and x1 to generate a chaotic key (CK), this key will be sorted to generate the indices key, required to apply SBM rows shuffling.

The CK has the following features:

- Easy to generate, the following mat lab code uses the CLMM equation to run a CLMM to generate a key with length equal NB:

```
; CK generation
r1=3.77;x1=0.19; NB=4000;
for i=1:NB
x1=r1*x1*(1-x1);
ck(i)=x1;
end
;Converting CK to indices key
[ee key]=sort(ck);
```

- The generated key is very sensitive to the selected values of r1 and x1, any minor changes in the value of r1 and/or changes in x1 will change the key, figure 9 shows the sensitivity of the generated keys:

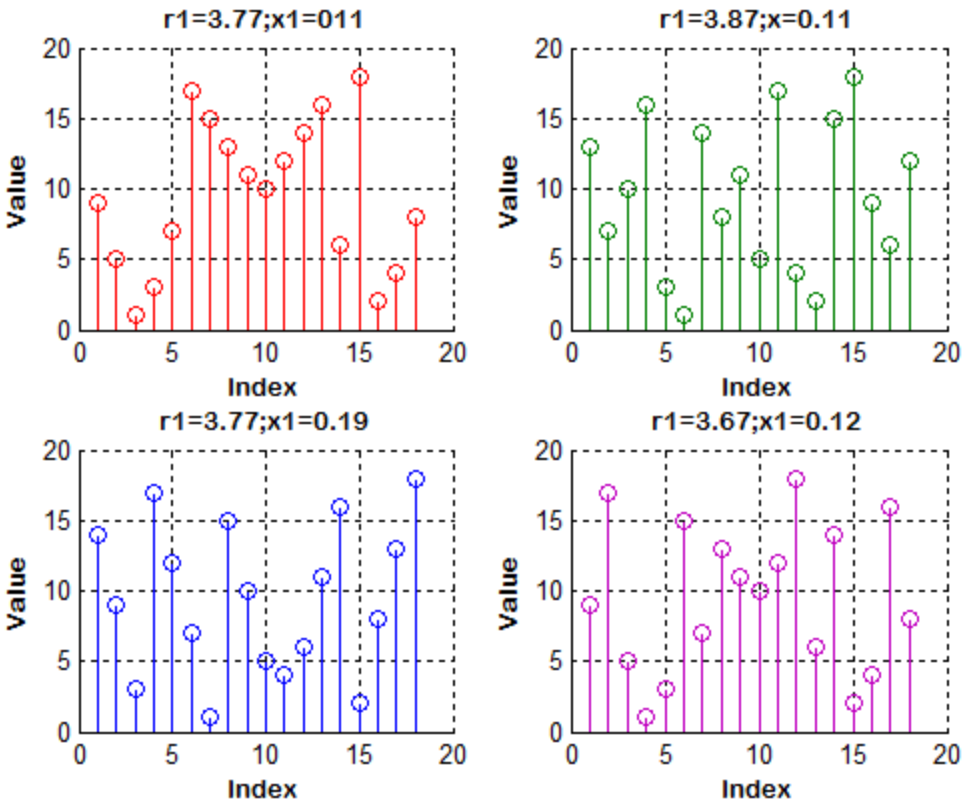

Figure 9: Indices key sensitivity

- CK generation require a key generation time (KGT), this time will rapidly increase when increasing the key length as shown in table 2 and figure 10:

Table 2: Indices key KGT

Key length	KGT (second)	Key length	KGT (second)
100	0.0010	5000	0.0690
500	0.0050	10000	0.1060
1000	0.0160	25000	0.3850
2000	0.0530	50000	1.5740
4000	0.0610	100000	11.3170

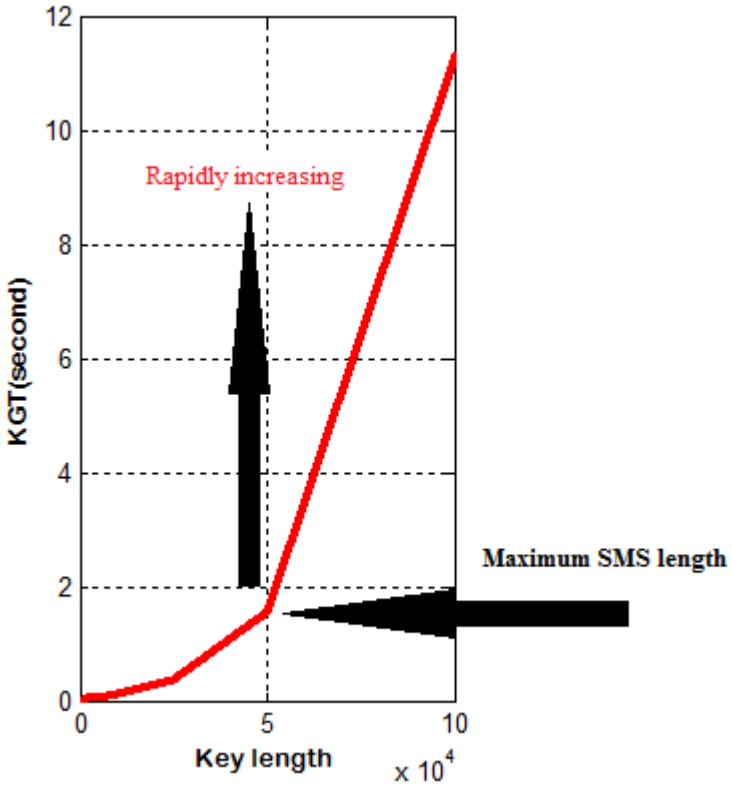

Figure 10: KGT vs key length

Referring to the results shown in table 2 and figure 10 we will consider a message SMS with length not greater than 4 K bytes, for longer messages it is recommended to divide the message into blocks, or to change the method of key generation to achieve the best speed of message steganography [31-36].

Many authors [1-10] introduced various methods of message steganography, many of these methods were based on least significant bit (LSB1) method and two least significant bits (LSB2) methods, theses methods have some features, which required to be enhanced, and table 3 shows these features and the enhancements ,which will be provided by the proposed method [77-82]:

Table 3: Stego methods features [26-30]

Feature	LSB1	LSB2	Proposed LSB32
Used covering media	Mainly color image	Mainly color image	DSF
Used bits	1	2	32
Required byte to hide one character	8	4	0.25 sample
Capacity hiding	Image size divided by 8	Image size divided by 4	DSF size multiplied by 4
Maximum change	1	3	0.0001
Minimum change	-1	-3	-0.0001
Quality of Stego media	Good for short messages, increasing the message length will increase MSE and decrease PSNR	Good for short messages, increasing the message length will increase MSE and decrease PSNR	Excellent when using short and long message, increasing the message length will keep MSE low and PSNR high

The Proposed Method

The proposed method uses a private key (PK), which contains the values of three parameters: Two chaotic parameters r1 and x1 and the POST parameter, which will be used to calculate the starting position of the covering samples. The PK will be used to secure the hidden message, this key will have a length of 192 bits, this length will be capable to create a huge key space capable to resist hacking attempts, this space can be calculated using equation 1 below:

$$\text{Key space} = 2^{64x3}$$

$$= 2^{192}$$

$$6.277101735386680763835789423207 7x10^{57} \text{ Combinations} \quad (1)$$

The PK will be used to generate indices key by sorting the generated CK, the length of this key will equal the message length divided by 4 , this key will be used to shuffle the rows of the SBM, this operation will be implemented based on the contents of the indices key, these contents will used as indexes to put the required row of the SBM in the hiding process and to get the row of the SBM in extracting process.

The proposed method hiding process will be implemented applying steps:

Step1: Input data preparation

1) Get the covering DSF.
2) Get the DSF size (LS).
3) Reshape DSF matrix into one row matrix.
4) Get the SMS.
5) Get the length of message (LM).
6) Get the PK.

Step2: Input preprocessing

1) Convert the message to decimal.
2) Convert the decimal message to binary to get MBM.
3) Reshape MBM to 32 columns.
4) Calculate the starting position of the covering sample s by taking the integer value of the result of multiplication POS value with LS.
5) Extract the covering samples.
6) Convert the covering samples to binary using 64_bits binary representation.
7) Use r1 and x1 to generate the secret indices key.

Step 3: SMS hiding:

1) Let the 32 bits of each row of SBM equal the reshaped MBM.
2) Use the indices key to shuffle the rows of the SBM to get the stego bytes.
3) Convert the stego bytes to decimal.
4) Return the stego bytes to the DSF row matrix.
5) Reshape the matrix back to original sizes to get the stego DSF.

Figure 11 illustrates an example of applying hiding process:

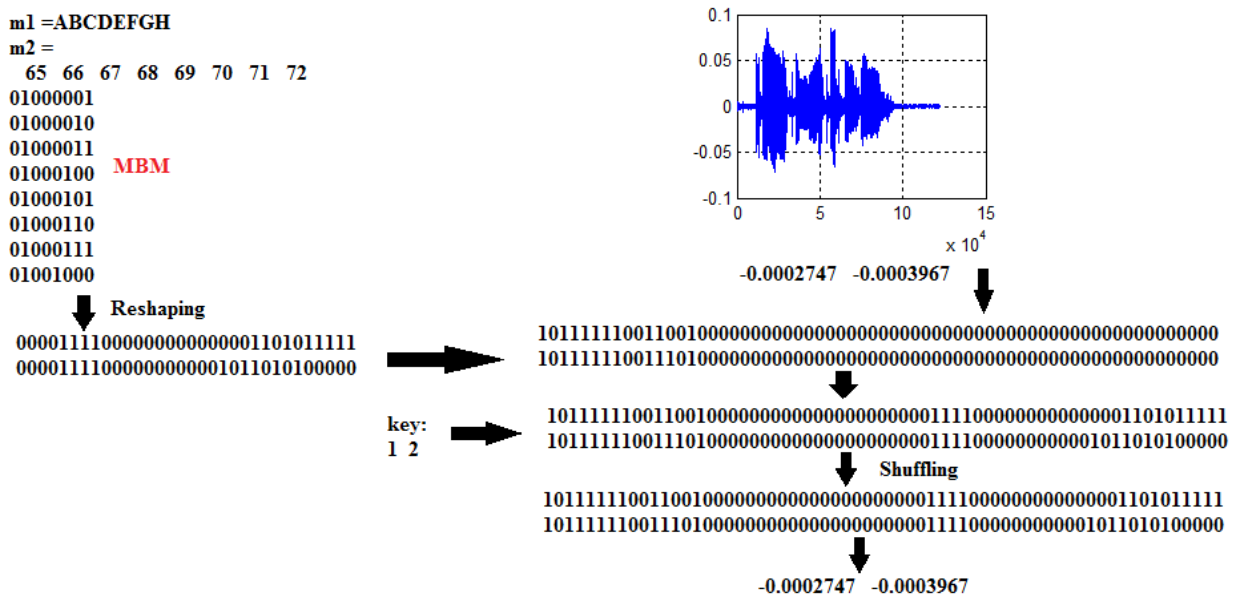

Figure 11: Hiding process example

The extracting process can be implemented applying the following steps:

Step 1: Input preparation:

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

Step2: Input preprocessing:

1) Use r1 and x1 to run a CLMM to generate the indices key.
2) Calculate the starting position of the stego samples.
3) Extract the stego samples.

Step 3: SMS extracting:

1) Convert the stego samples to binary using 64_bits binary representation.
2) Extract the lower 32 bits from the binary matrix.
3) Use the indices key to shuffle the rows of the matrix.
4) Reshape the matrix to 8 columns matrix.
5) Convert the matrix to decimal.
6) Convert the decimal matrix to characters to get the SMS.

Figure 12 illustrates an example of applying message extractions process:

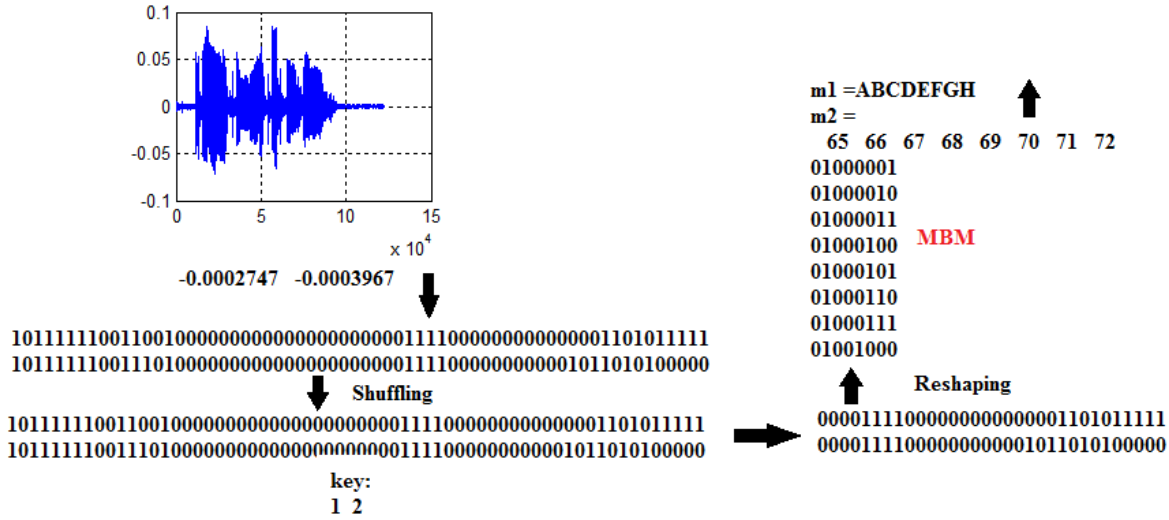

Figure 12: Message extracting process example

Below is a mat lab source code which can be used to test and implement the proposed method:

```
;SMS hiding process
q=quantizer('double');
r1=3.77;x1=0.19;POS=0.109;
[cc1 fs1]=wavread('C:\Users\win 7\Desktop\voices\f3.wav');
[nn1 nn2]=size(cc1);LS=nn1*nn2;
s1=reshape(cc1,1,LS);SP=fix(POS*LS);
m1='ABCDEFGHIGKLMNOPQRST';
m2=uint8(m1) ;
LM=length(m2); NB=LM/4;
for i=1:NB
x1=r1*x1*(1-x1);
ck(i)=x1;
end
[ee key]=sort(ck);
s2=s1(1,SP+1:SP+NB) ;
s3=num2bin(q,s2) ;
m3=dec2bin(m2,8);
m4=reshape(m3,NB,32) ;
s4=s3;
for i=1:NB
   k=find(key==i);
   s4(k,33:64)=m4(i,:);
end
s5=bin2num(q,s4)';
s1(1,SP+1:SP+NB)=s5;
s6=reshape(s1,nn1,nn2);
```

```
;SMS extracting process
rr1=3.77;xx1=0.19;POS=0.109;
SP=fix(POS*LS);
for i=1:NB
xx1=rr1*xx1*(1-xx1);
ck1(i)=xx1;
end
[ee key1]=sort(ck1);
s7=reshape(s6,1,LS);
s8=s7(1,SP+1:SP+NB);
s9=num2bin(q,s8);
for i=1:NB
   f=find(key1==i);
   m5(i,:)=s9(f,33:64);
end
m6=reshape(m5,LM,8);
m7=bin2dec(m6)'; m8=char(m7);
```

Implementation and Results Discussion

The proposed method was implemented using various SMS, the sensitivity was tested and the obtained results showed that the hiding process and the extracting process must use the same PK, any changes in the PK in the extracting process will produce a damaged extracted message, The message 'ABCDEFGHIGKLMNOPQRST' was hidden using the following PK, the hidden message was extracted by applying the changes shown in table 4:

```
PK:
r1=3.77;x1=0.19;
POS=0.109;
```

Table 4: Method sensitivity

Changes in the PK	MSE	PSNR	Remarks
No changes	0	Infinity	Correct
r1=3.91	0.7000	92.1831	Damaged
x1=0.29	4.4000	73.8003	Damaged
POS=0.09	5561.8	2.3797	Damaged

The quality of the stego DSF was tested, the obtained results showed that even in the message is long, the values of MSE were very low and the values of PSNR are very high, thus the stego DSF always has an excellent quality, and the stego file is always closed to the covering 1. Table 5 shows the obtained quality parameter values measured between the stego and the covering DSFs, and figure 13 shows a sample outputs, here the stego file is very closed to the covering file:

Table 5: Quality results

Message length (K bytes)	MSE	PSNR
0.25	5.2829e-021	417.5797
0.5	1.2719e-020	408.7933
1	1.5126e-020	407.0600
2	3.7574e-020	397.9613
4	5.4181e-020	394.3010
8	8.1197e-020	390.2556
16	2.6018e-018	355.5850
25	6.2453e-018	346.8285
50	1.5850e-017	337.5150
100	2.1579e-017	334.4295
Remarks	Low	High

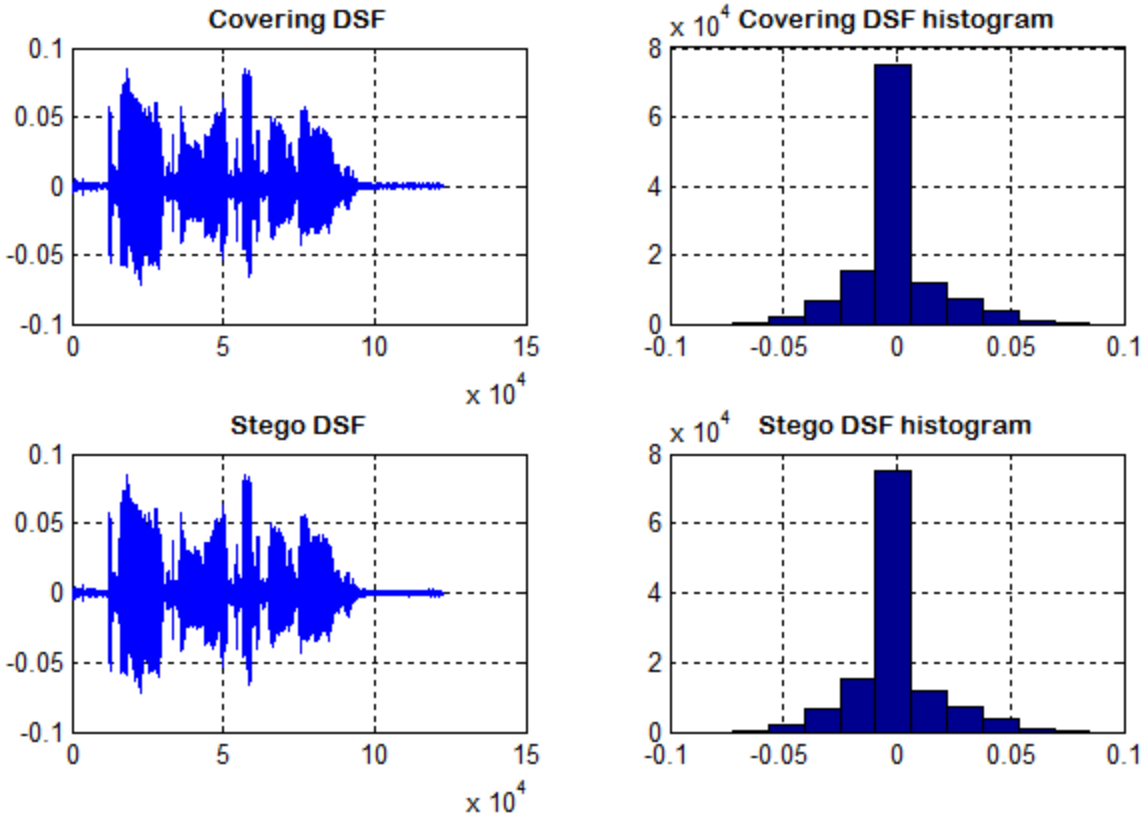

Figure 13: Stego DSF holding 10000 characters

From table 5 it is shown that increasing the message length will keep the value of MSE low and it will keep the value of PSNR high and this is shown in figure 14:

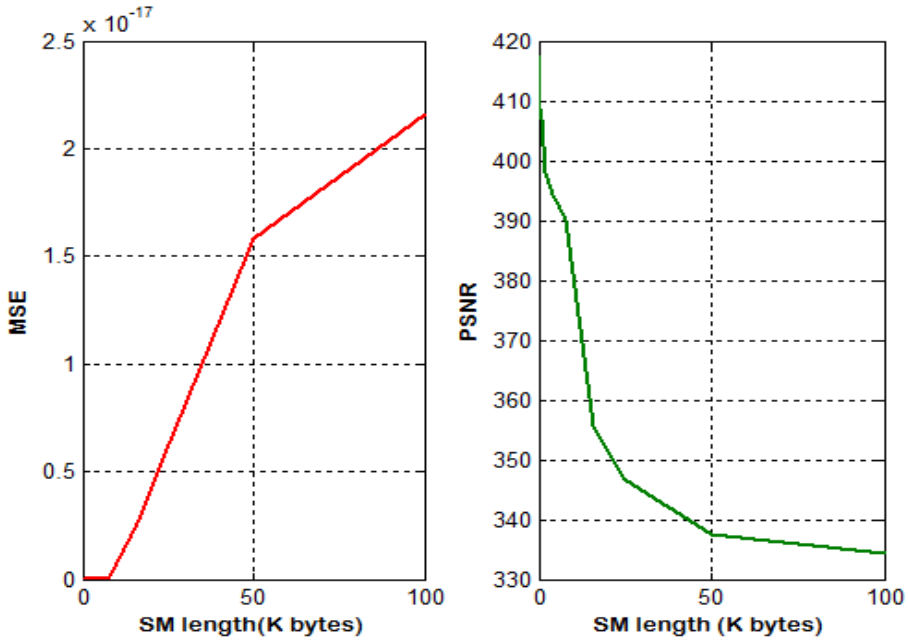

Figure 14: Quality parameters VS SMS length

The speed of the proposed method was tested, 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 6 and 7 show the obtained speed results.

Table 6: ET, DT results

Message length (K bytes)	HT	ET
0.25	0.0540	0.0110
0.5	0.0580	0.0160
1	0.0640	0.0270
2	0.0800	0.0430
4	0.1250	0.0860
8	0.2410	0.2300
16	0.4760	0.6000
25	0.8270	1.2740
50	2.5930	5.1940
100	6.5620	19.7940

Table 7: ETP, DTP results

Message length (K bytes)	HTP	ETP
0.25	4.6296	22.7273
0.5	8.6207	31.2500
1	15.6250	37.0370
2	25.0000	46.5116
4	**32**	**46.5116**
8	33.1950	34.7826
16	33.6134	26.6667
25	30.2297	19.6232
50	19.2827	9.6265
100	15.2393	5.0520

From tables 6 and 7 we can see that for short messages, the method provides a good speed, the speed will get worst when increasing the message length (over 4 K bytes length) as shown in figure 15 and for long messages we recommend dividing the message into blocks to minimize the time required for key generation.

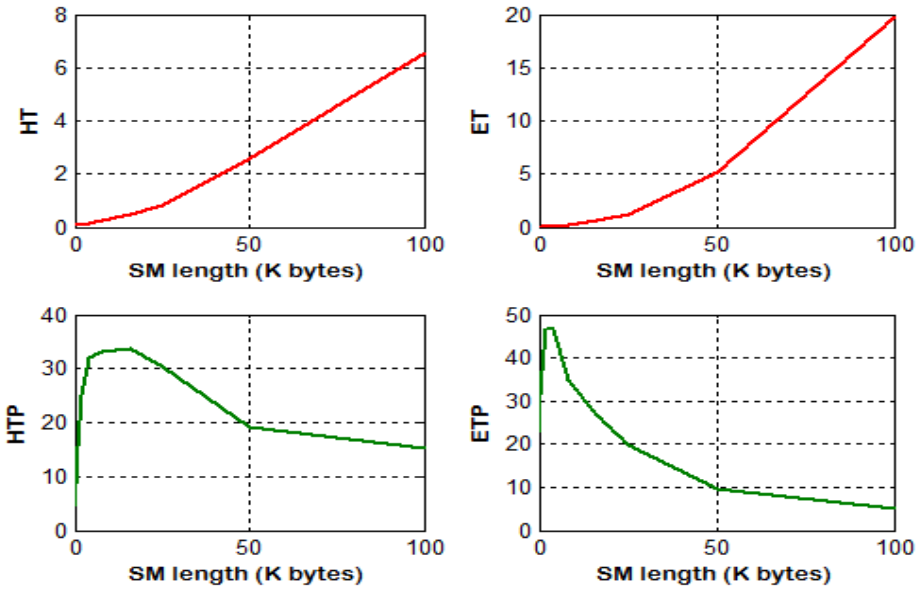

Figure 15: Speed parameters vs message length

Conclusion

An efficient method of message steganography was proposed, the method used digital speech file as a covering media, and 32 bits of each sample were used for data hiding, thus the capacity hiding was increased to reach the speech file size multiplied by 4. It was shown that changing the 32 bits of the speech sample will not much affect the sample value, thus the quality of the stego file was kept high and the stego file was always closed to the covering file regardless the hidden message length. The proposed method added an extra protection by using a private key, this key provided a good key space and the extracted message was very sensitive to the selected values of the private key. The rows of the speech binary matrix were shuffled based on the contents of the indices key generated by running a chaotic logistic map model.

The proposed method was tested and implemented using various messages, the obtained results were used to prove the sensitivity, quality and speed of the proposed method.

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.

