Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 14, Issue. 1, January 2025, pg.38 – 49

Audio File Cryptography using Variable Number of Rounds for Blocks Substitution

Prof. Hatim Zaini; Prof. Ziad AlQadi

Taif University, KSA
Albalqa Applied University, Jordan

DOI: https://doi.org/10.47760/ijcsmc.2025.v14i01.004

Abstract: An efficient method of audio file cryptography will be introduced, the method will decrease both the encryption and decryption times comparing with other existing methods, the method will speed up the process of audio file cryptography. The introduced method will use a variable number of rounds for audio file cryptography, each round will use a block size, number of blocks and generated indices keys, these parameters will be variable and change from round to another. The private key will have a variable length, and it will depend on the selected number of rounds (192 bits for each round), this length will be good enough to produce a huge key space capable to resist hacking attacks, the produced decrypted file will be very sensitive to the selected values of the private key. The introduced method will be simple and easy to implement, it will use a simple chaotic logistic map model to generate the required for each round indices key. The introduced method will use a simple substitution operation to apply audio file samples substitution without altering the samples values and without using any extra logical and arithmetic operations (required for other existing methods). The introduced method will be tested and implemented using mat lab; the obtained results will be used to show that the method will satisfy the requirements of good crypto method.

Keywords: Audio file, sample, block, substitution, PK, IK, CK, CLMM.

Introduction

Audio files (AF) are used in various important applications; they might be secret, private, containing confidential data, so they require protection from being hacked especially if the communication network is not secure[1-10].

One of the most popular and easiest techniques used to protect AF is AF cryptography [11-15], this process completely destroy the AF so that it cannot be understood when heard by ear before sending and recovering the original AF after receiving, the sender uses the encryption function and the private key (PK) to produce a cipher encrypted AF, while the receiver uses a decryption function and the PK to produce a decrypted AF [16-22].

A good crypto method must meet the following requirements [23-30]:

- Security, the method must provide a high level of security, this can be achieved by using a PK with length greater or equal 128 bits, this length will be good enough to provide a huge key space capable to resist hacking attacks, the produced decrypted AF must be sensitive to the selected values of the PK [31-37].
- Efficiency, the method must provide a high speed of AF encryption and decryption, it must minimize both the encryption and decryption times [38-42].
- Low quality of the encrypted AF, the mean square error (MSE) [43-50] calculated between the source and the encrypted AFs must be high, while the peak signal to noise ratio (PSNR [51-58) calculated between them must be low.
- Excellent quality of the decrypted AF, the MSE calculated between the original and the decrypted AFs must be zero, while the PSNR value calculated between them must be infinite [59-65].
- Easy to implement, the method must simplify the processes of key generation, AF encryption and AF decryption [66-74].
- Flexibility, the method must be efficient in handling any AF with any size.

The aim of this paper research is to introduce a new method of AF cryptography, which will meet the above mentioned requirements and use a multiple variable number of rounds, variable block size and variable number of blocks,

Related Works

Many methods were introduced for data cryptography, (including AF) [1-10] cryptography, a lot of these methods were based on standard methods of data cryptography such as DES, 3DES, AES, RC2, RC6 and BF, these methods share some features, and some of these features can be considered as weak points, which required enhancements, these features are:

- Data blocking, all of the standard methods allow data blocking, the block size is small and fixed (for DES, 3DES, RC2 and BF the block size equal 64 bits, for AES and RC6 the block size is equal 128 bits), the proposed method will use a variable length block size, it will be selected by the user and can have a length from 1 sample to the AF size.
- PK length, some of the standard methods uses a short PK, while other uses longer PK (DES uses 56 bits PK. while BF uses 448 bits), the proposed method will use 192 bits for each round (768 bits when using 4 rounds).
- Speed, standard methods have a low speed especially when they are used to treat data with big size such as AF, the proposed method will provide a high speed and it will significantly speed up the process of AF cryptography comparing with standard methods.
- Security, these methods provide low level of security (DES based) and moderate level of security, the proposed method will increase the level of security based on the increase in the PK length.
- Rounds, each standard method are applied in a fixed number of rounds, the proposed method will be implemented using variable number of rounds (at least one), this number will be selected by the user.
- In standard method the rounds are used to treat the same block, the proposed method will treat the AF completely.
- Altering the data, all standard based methods change the values of the AF samples, the proposed method will not add any changes to samples values, they will remain the same without any changes, but they will be substituted,

- Simplicity, the standard methods are not simple, they use a complicated sequence of logical and arithmetic operations repeated in each round, the proposed method will replace this sequence by using a simple substitution operation.

The Proposed Method

The proposed method will use a complicated private key (PK) [5-10], this key will contain the values of the blocking factor (P) and the values of chaotic logistic pairs r and x as shown in the example shown in figure 1:

```
P1=0.042;P2=0.06;P3=0.015;P4=0.021;
r1=3.77;x1=0.11;r2=3.82;x2=0.16;
r3=3.67;x3=0.13;r4=3.89;x4=0.26;
```

Figure 1: PK example

The double fractional values of P are to be used to calculate the rounds block sizes (BS) and number of blocks (NB) as shown in figure 2:

```
BS1=fix(L*P1);NB1=fix(L/BS1);
BS2=fix(L*P2);NB2=fix(L/BS2);
BS3=fix(L*P3);NB3=fix(L/BS3);
BS4=fix(L*P4);NB4=fix(L/BS4);
```

Figure 2: Calculating the values of BSs and NBs

Each pair of r and x values with the associated NB value will be used to run a chaotic logistic map model (CLMM) to generate a chaotic key (CK), the CK then will sorted to form the indices key (IK) for the associated round, CLMM is a very simple mathematical model and it can be easily implemented as shown in figure 3]5-13]:

```
for i=1:NB1
  x1=x1*r1*(1-x1);
  CK1(i)=x1;
 end
[ee1 IK1]=sort(CK1);
```

Figure 3: CLMM to generate round IK

The proposed method can be implemented using variable number of rounds, at least one round is required, in the implementation part we will use 4 rounds, here each round will use its own values of BS, NB and IK.
The PK will have a length of 768 bits (192 bits for each round), this length will good enough to provide a huge key space capable to resist any hacking attempts, also the produced decrypted audio file will be very sensitive to the selected values of the PK, any minor changes in the PK in the decryption phase will produce a damaged audio file and these changes will be considered as a hacking attempt.
The encryption and decryption process will be applied by using a simple operation without the need to execute a complicated sequence of logical and arithmetic operations (used in other existing method of audio file cryptography), this operation will substitute the audio file blocks based on the contents of the round‘s IK, figure 4 illustrates an example of using this operation in the encryption and decryption phases:

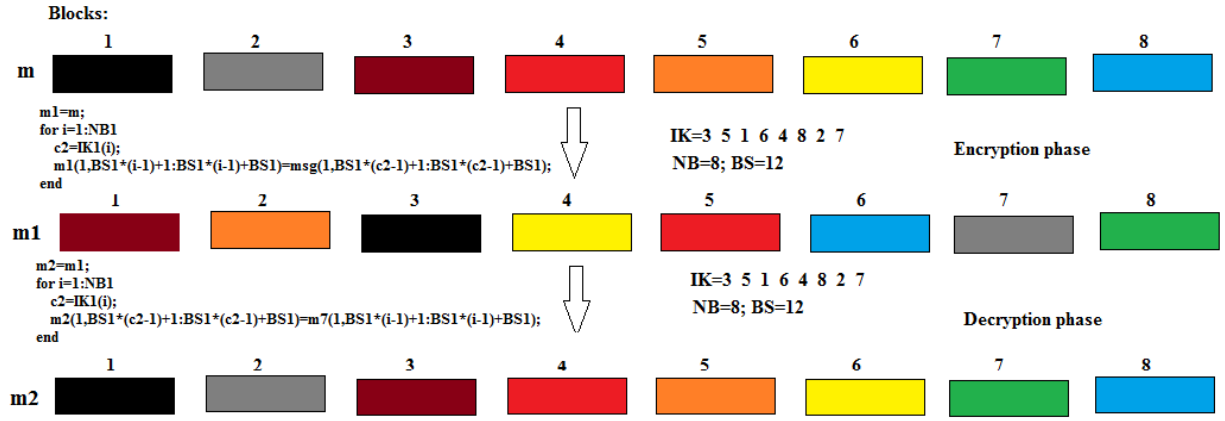

Figure 4: Audio file blocks substitution

The encryption phase of the proposed method will be implemented applying the following steps:

Step 1: Inputs initialization:

a) Get the audio file.

b) Get the audio file size.

c) Reshape the file to one row matrix.

d) Get the PK.

Step 2: Calculation:

a) Calculate BS for each round using the values of P.

b) Calculate the NB values for the rounds.

Step 3: IKs generation:

For each round use the associated NB, r and x to call the key generation function.

Step 4: Encryption:

For each round call the encryption function to apply the round encryption phase.

Step 5: Reshape back the encrypted audio file to original size.

The decryption phase will be implemented applying the same steps as for encryption phase, but instead of using encryption function the decryption function must be used.

Below are the required functions for the proposed method

Encryption algorithm:

Inputs:

NB, BS, IK, Source data (SD)

Output:

Encrypted data (ED)

Process:

I=1;

While i<=NB do

C=IK (I)

ED (1, BS(I-1): BS*(I-1) +BS) = SD (1, BS*(C-1): BS*(C-1) +BS)*

End while

Decryption algorithm:

Inputs:

NB, BS, IK, Encrypted data (ED)

Output:
Decrypted data (DD)
Process:
I=1;
While i<=NB do
C=IK (I)
DD (1, BS(C1): BS*(C-1) +BS) = SD (1, BS*(I-1): BS*(I-1) +BS)*
End while

Indices key generation algorithm:
Inputs:
NB, r, x (ED)
Output:
Indices key (IK)
Process:
I=1;
While i<=NB do
*X=x*r*(1-x)*
CK (I)=x
End while
[SSD IK}=sort (CK)

Implementation and Results Discussion

The proposed method was implemented using mat lab 7 and a PC with the following specifications:

Processor:	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz 2.50 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System
Pen and Touch:	No Pen or Touch Input is available for this Display

The proposed method was tested using various in sizes AFs, the encryption time (ET) was calculated and compared with other methods times, and table 1 shows the obtained results.

Table 1: Obtained ET for various methods

AF size (sample)	Encryption time (second)						
	Introduced in this paper	DES	3DES	AES	RC2	RC6	PF
47315	0.0210	7.835670	9.1080	7.5278	10.9830	4.3705	1.2135
133120	0.0270	12.40491	13.0656	10.7988	15.7554	6.2696	1.7408
145408	0.0290	12.1616	14.1363	11.6837	17.0465	6.7833	1.8835
172032	0.0310	14.5971	16.9673	14.0235	20.4603	8.1418	2.2606
200704	0.0317	17.0184	19.7818	16.3497	23.8542	9.4923	2.6356
212992	0.0320	17.6775	20.5479	16.9829	24.7780	9.8599	2.7377
321536	0.0350	29.5456	34.3431	28.3846	41.4132	16.4796	4.5757
430080	0.0460	42.5104	49.4130	40.8400	59.5855	23.7109	6.5835
Average	0.0316	19.2189	22.1704	18.3239	26.7345	10.6385	2.9539
Average throughput (K samples per	6424.9	010.6	9.2	11.1	7.6	19.1	68.7

second)							
Speed up of the proposed method	1.0000	606.1226	698.3587	578.8198	845.3816	336.3822	93.5211

From table 1 the following are seen:

- The proposed method comparing with other methods decreased the encryption time for various AF sizes (see figure 5).
- The proposed method increased the speed of AF cryptography and it provided a significant speed up comparing with other existing methods of AF cryptography.
- Standard methods require a small time to encrypt-decrypt AF with small sizes, this time will rapidly increase when increasing the AF size, While the proposed method required a small time to encrypt-decrypt AF with small size, and this time is slowly increased when increasing the AF size, so we can recommend using the proposed method to encrypt-decrypt any AF with any size.

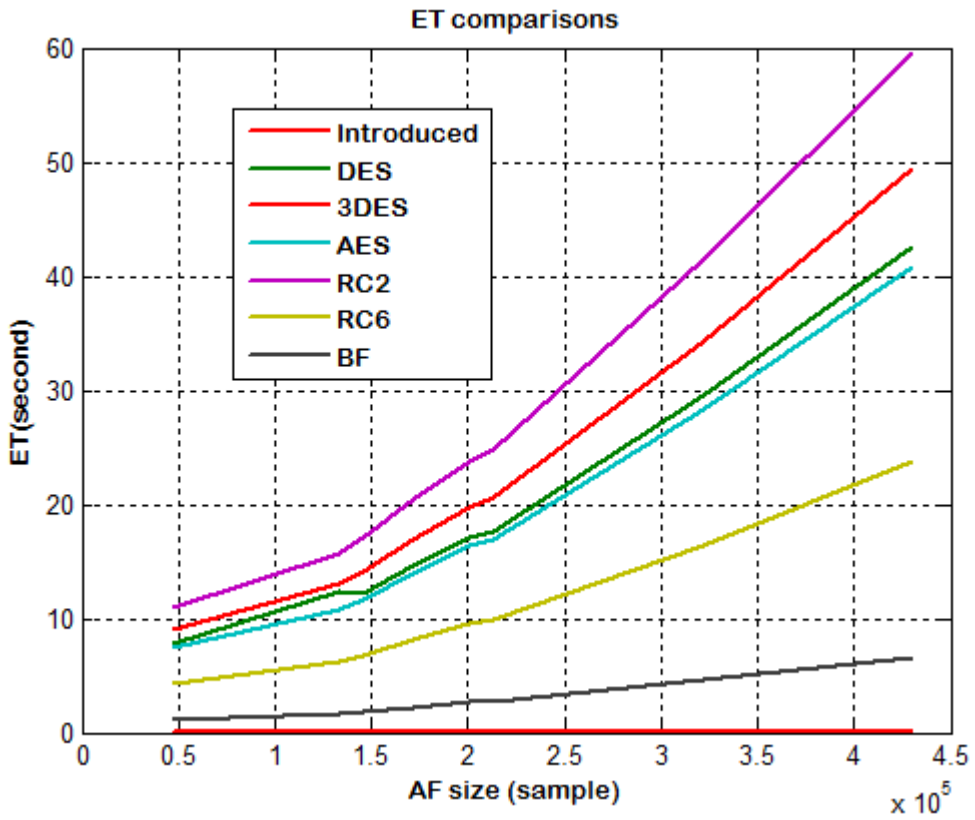

Figure 5: Various methods ET comparisons

AF blocking is required to reduce the encryption-decryption time, increasing the BS will decrease both these times, to show this a AF with 536474 samples was encrypted-decrypted using various BSs, and table 2 shows the obtained speed results:

Table 2: ET when changing the BS

BS1	BS2	BS3	BS4	ET (second)
1(no blocking)	1(no blocking)	1(no blocking)	1(no blocking)	2343.3
53	53	53	53	0.6130
268	268	1126	1663	0.2470
53647	53647	536	53	0.2410
536	536	536	536	0.2230
53647	53647	53647	53647	0.0560
214589	214589	214589	214589	0.0520

An AF with 536474 samples was selected and processed using the proposed method with one round, the value of P was changed to produce various values of NB and BS, the encryption time was calculated and table 3 shows the obtained results:

Table 3: Encryption time using one round and varying the value of P

NB	BS (samples)	ET(seconds)
536474	1(no blocking)	566.5820
134118	4	22.7100
67059	8	2.9170
31557	17	0.6210
15327	35	0.2390
7555	71	0.1610
3777	142	0.1210
1888	284	0.0980
235	2275	0.0350
117	4551	0.0200
58	9102	0.0200
39	13653	0.0200

From table 3 it is shown that the BS must be at least equal 300 samples to optimize the encryption time, here increasing the NB value will increase the encryption time and increasing the BS value will decrease the encryption time as shown in figure 6.

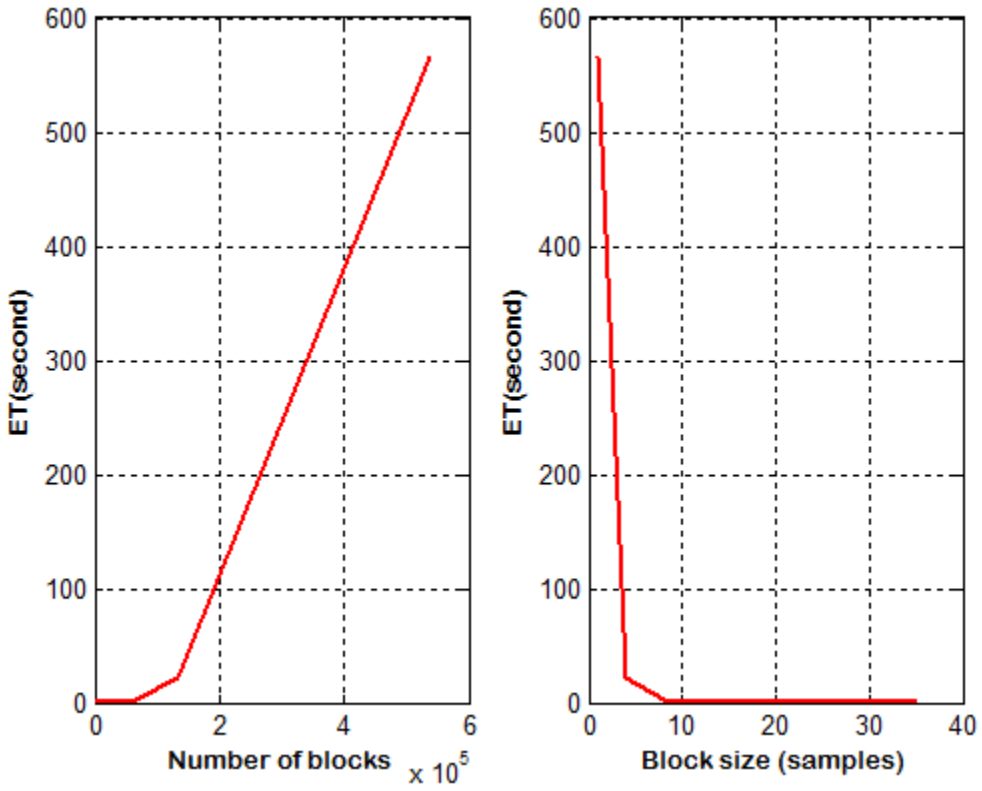

Figure 6: ET vs NB and BS

The quality of the proposed method was tested, the decrypted AFs were always have excellent quality, the NSE value measured between each AF and rhe decrypted AF was always equal zero, while the PSNR value was always equal infinite. The quality of the encrypted AF was always poor, the MSE value measured between the source AF and the encrypted one was always high, while the PSNR value measured between them was always low. Figure 7 and 8 show some example outputs which prove that the proposed method satisfied the quality requirements of good crypto method.

Source DSF		Encrytted DSF		Decrypted DSF	
im(2000:2009,:)		m44(2000:2009,:)		m88(2000:2009,:)	
0.0241	0.0051	0.0251	0.0432	0.0241	0.0051
-0.0094	-0.0118	0.0368	0.0306	-0.0094	-0.0118
-0.0180	0.0050	0.0320	0.0582	-0.0180	0.0050
-0.0157	-0.0027	0.0266	0.0564	-0.0157	-0.0027
-0.0186	0.0029	0.0180	0.0584	-0.0186	0.0029
-0.0040	0.0047	0.0210	0.0800	-0.0040	0.0047
-0.0059	-0.0045	0.0235	0.0985	-0.0059	-0.0045
-0.0019	0.0007	0.0406	0.0866	-0.0019	0.0007
0.0357	0.0140	0.0138	0.0755	0.0357	0.0140
-0.0116	-0.0057	0.0224	0.1227	-0.0116	-0.0057

Figure 7: Sample output samples of the AF

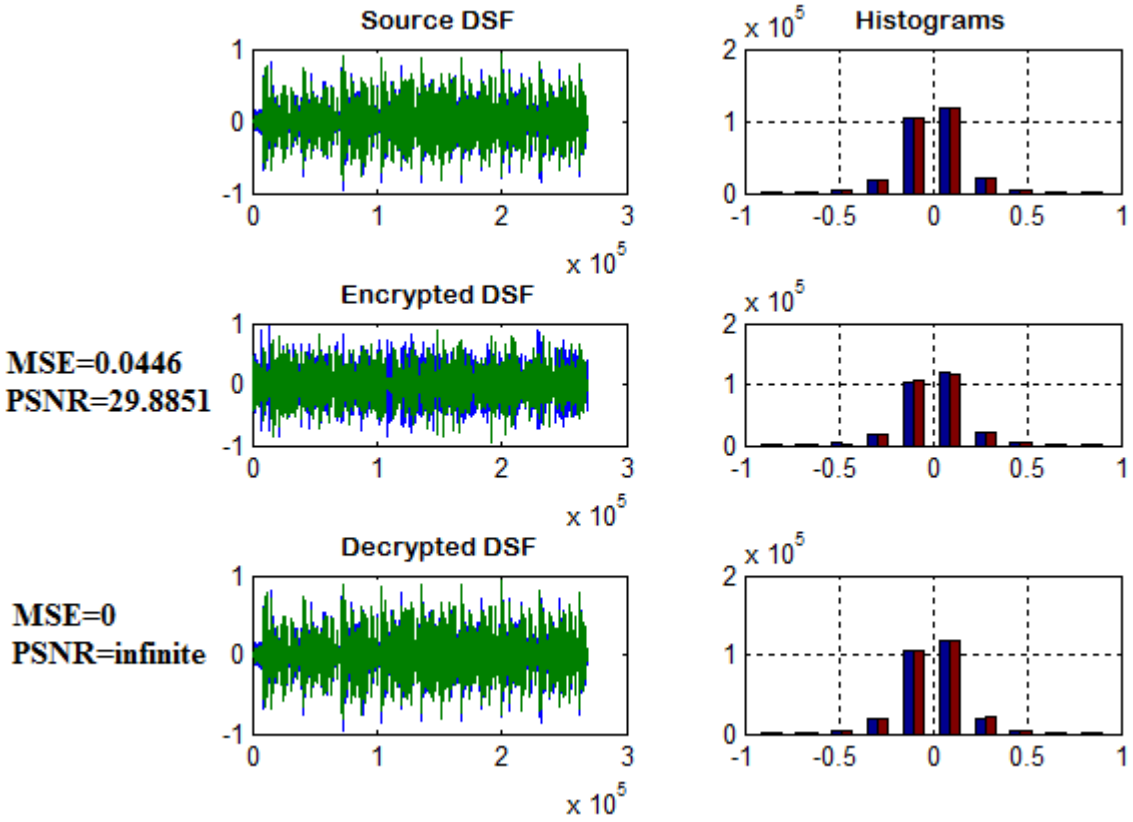

Figure 8: Source, encrypted and decrypted AF samples and the associated histograms

Conclusion

An efficient method of audio file cryptography was proposed, the method comparing with other existing methods reduced the encryption time and the decryption time, and it enhanced the speed of AF cryptography by providing a significant speed up. The obtained results proved the fact that the proposed method satisfied the encryption and decryption quality requirements of good crypto method. The proposed method used a complicated private key with 192 bits and this length was increased when using more than 1 round. The private key was used to divide the AF into blocks, the blocks size in various rounds was variable, the private key was also used to generate a required indices key for the selected round , each indices key was used to substitute the blocks of the associated round, the secret key length was variable and it was generated by running a simple chaotic logistic map model. The proposed method was simple and easy to implement. It used a simple functions for key generation, AF encryption and AF decryption, the encryption and decryption process were applied by using simple blocks substitution operation without altering the AF samples values and with using any logical and arithmetic operations,

The proposed method was tested and implemented using various AFs and the obtained results proved that the proposed method satisfied the quality, speed and security requirements of good crypto method.

References

[1]. Prashanti.G, Deepthi.S & Sandhya Rani.K., "A Novel Approach for Data Encryption Standard Algorithm". International Journal of Engineering and Advanced, Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013, pp. 264.

[2]. Das Debasis, Misra Rajiv. "Programmable Cellular Automata Based Efficient Parallel AES Encryption Algorithm". International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, pp. 204.

[3]. Kalpana Parsi, Singaraju Sudha, "Data Security in Cloud Computing using RSA Algorithm". International Journal of Research in Computer and Communication technology, IJRCCT, ISSN 2278- 5841, Vol 1, Issue 4, September 2012. pp. 145.

[4]. Dr. Prerna Mahajan , Abhishek Sachdeva, Global Journal of Computer Science and Technology Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013,Type: Double Blind Peer Reviewed International Research Journal ,Publisher: Global Journals Inc. (USA).

[5]. 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

[6]. Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.

[7]. 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.

[8]. X. Zhang and X. Wang, *Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System*, Springer, New York, NY, USA, 2019.

[9]. 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.

[10]. Mua'ad M. Abu-Faraj, Khaled Aldebe, Ziad A. Alqadi, Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography, Traitement du signal 39(1):173-178, DOI: 10.18280/ts.390117

[11]. Kanika Sharma and Nischay Bahl, Taxonomy of Cryptography Techniques for Network Security, International Journal of Engineering and Computer Science, ISSN: 2319-7242, Volume 5 Issue 8, August 2016, Page No. 17787-17793.

[12]. 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.2009.10.3.

[13]. 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.

[14]. 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.

[15]. Abomhara, M., Zakaria, O., Khalifa, O.O., Zaidan, A.A.,Zaidan, B.B. (2022). Enhancing selective encryption forH. 264/AVC using advanced encryption standard. International Journal of Computer and Electrical Engineering (IJCEE), 2(2): arXiv:2201.03391.https://doi.org/10.48550/arXiv.2201.03391arXiv:2201.03391.https://doi.org/10.48550/arXiv.2201.03391.

[16]. Naji, A.W., Hameed, S.A., Zaidan, B.B., Al-Khateeb,W.F., Khalifa, O.O., Zaidan, A.A., Gunawan, T.S.(2009), Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques. International Journal of Computer Science and Information Security (IJCSIS), 3(1): 73-78.arXiv:0908.0216.

[17]. Hamdan, A., Jalab, H.A., Zaidan, A.A., Zaidan, B.B.(2010). New frame work of hidden data within no multimedia file. Int. J. Comput. Netw. Secur, 2(1): 46-54.

[18]. Taqa, A., Zaidan, A.A., Zaidan, B.B. (2009), New framework for high secure data hidden in the MPE Guising AES encryption algorithm. International Journal of Computer and Electrical Engineering, 1(5): 1793-8163.

[19]. Zaidan, A.A., Zaidan, B.B., Jalab, H.A. (2010). A new system for hiding data within (unused area two+ image page) of portable executable file using statistical technique and advance encryption Standared. International Journal of Computer Theory and Engineering, 2(2): 218.

[20]. Ignatiev, A., Morgado, A., Marques-Silva, J. (2019).RC2: An efficient MaxSAT solver. Journal on Satisfiability, Boolean Modeling and Computation, 11(1):53-64

[21]. Verma, P., Shekhar, J., Preety, A.A. (2015), A survey for performance analysis various cryptography techniques digital contents. International Journal of Computer Science and Mobile Computing, 4(1): 522-531.https://doi.org/10.3233/SAT190116.

[22]. Alanazi, H., Zaidan, B.B., Zaidan, A.A., Jalab, H.A.,Shabbir, M., Al-Nabhani, Y. (2010), New comparative study between DES, 3DES and AES within nine factors, Journal of Computing, 2(3). arXiv:1003.4085.

[23]. Thakur, J., Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. International Journal of Emerging Technology and Advanced Engineering, 1(2):6-12 .

[24]. Jorstad N., and Landgrave.: Cryptographic algorithm metrics. In 20th National Information Systems Security (1997)

[25]. Mushtaq, M. F., Akram, U., Khan, I., Khan, S. N., Shahzad,A., and Ullah, A.: Cloud computing environment and security challenges: A review. International Journal of Advanced Computer Science and Applications, vol. 8(10), pp. 183-195(2017)
[26]. Hercigonja, Z., Gimnazija, D., and Varazdin, C.: Comparative analysis of cryptographic algorithms and advanced cryptographic algorithms. International Journal of Digital Technology & Economy, vol. 1(2),pp. 1-8 (2016)
[27]. Stallings, W.: Cryptography and Network Security: Principles and Practice, 5th ed. Prentice Hall Press (2010)
[28]. William, E. B., Barker, C.: Recommendation for the tripledata encryption algorithm (TDEA) block cipher. NISTSpecial Publication 800-67 (2012)
[29]. Maqsood, F., Ali, M. M., Ahmed, M., and Shah, M. A.: Cryptography: A comparative analysis for modern techniques. International Journal of Advanced Computer Science and Applications, vol. 8(6), pp. 442-448 (2017)
[30]. Alshahrani, A. M., and Walker, S.: Implement a novel symmetric block cipher algorithm. International Journal on Cryptography and Information Security, vol. 4 (4), pp. 1-11(2014)
[31]. Smid M. E., and Branstad D. K.: Data Encryption Standard: past and future. In Proceedings of the IEEE, vol. 76 (5), pp.550-559 (1988)
[32]. N. I. of S. and T. NIST: Data Encryption Standard (DES).Federal Information Processing Standards Publication (FIPSPUB 46-3), vol. 25(10), pp. 1-22 (1999)
[33]. Dworkin, M.: Recommendation for block cipher modes of operation, NIST Spec. Publ. 800-38B, (2005)
[34]. Patil, P., Narayankar, P., Narayan, D. G., and Meena, S. M.:A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. In Procedia Computer Science, vol. 78, pp.617-624 (2016)
[35]. Faiqa Maqsood, Muhammad Ahmed, Muhammad Mumtaz Ali, Munam Ali Shah, Cryptography: A Comparative Analysis for Modern Techniques, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017.
[36]. Mua'ad M. Abu-Faraj, Ziad A. Alqadi, Using Highly Secure Data Encryption Method for Text File Cryptography, IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.11, November 2020.
[37]. Ziad alqadi, Analysis of stream cipher security algorithm, Journal of Information and Computing Science, vol. 2, issue 4, pp. 288-298, 2007.
[38]. 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.
[39]. 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.
[40]. 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.
[41]. 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.
[42]. 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.
[43]. 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.
[44]. 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.
[45]. Ashraf Abu-Ein, Ziad AA Alqadi, Jihad Nader, A TECHNIQUE OF HIDING SECRETE TEXT IN WAVE FILE, International Journal of Computer Applications, 2016.
[46]. 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.
[47]. 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.
[48]. 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.
[49]. 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.
[50]. 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.
[51]. 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.
[52]. 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.
[53]. 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.
[54]. 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.

[55]. 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.
[56]. 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.
[57]. 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.
[58]. 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.
[59]. Prof. Ziad Alqadi, Hybrid, Secure and Highly Speed Method for Color Image Cryptography, International Journal of Computer Science and Mobile Computing, vol. 12, issue 9, pp. 15-38, 2023.
[60]. Adnan Manasreh, Nasser Abdellatif, Ziad A. Alqadi, SPEECH FILES CRYPTOGRAPHY USING IMAGE KEY AND INDICES KEY, ARPN Journal of Engineering and Applied Science, vol. 18, issue 13, pp. 1508-1517, 2023.
[61]. Prof. Ziad Alqadi; Dr. Mohammad Sleman Khrisat, Analysis of Methods used to Create Digital Signals Fingerprints, IJCSMC, Vol. 12, Issue. 8, August 2023, pg.84 – 97.
[62]. [61] Nasser Abdellatif and Ziad A. Alqadi Adnan Manasreh, SECURING LSB STEGANOGRAPHY USING BITE SUBSTITUTION AND IMAGE BLOCKING, ARPN Journal of Engineering and Applied Science, vol. 18. Issue 7, pp. 743-758, 2023.
[63]. Nasser Abdellatif Adnan Manasreh, Mohammad S. Khrisat, Hatim Ghazi Zaini, Ziad A. Alqadi, IMPROVED MEDIAN FILTER TO ELIMINATE SALT AND PEPPER NOISE IN DIGITAL, ARPN Journal of Engineering and Applied Science, vol. 18, issue 4, pp. 310-316, 2023.
[64]. Ziad A. Alqadi and Nasser Abdellati Adnan Manasreh, Mohammad S. Khrisat, Hatim Ghazi Zaini, IMPROVING DATA STANDARD METHODS OF CRYPTOGRAPHY, ARPN Journal of Engineering and Applied Sciences, vol. 17, issue 24, pp. 2077-2088, 2023.
[65]. 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.
[66]. 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.
[67]. Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," Information Sciences, vol. 480, pp. 403–419, 2019.
[68]. 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.
[69]. X. Zhang and X. Wang, Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System, Springer, New York, NY, USA, 2019.
[70]. 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.
[71]. Pleacher, D. (n.d.), Calculating password entropy. Retrieved February 16, 2023, from https://www.pleacher.com/mp/mlessons/algebra/entropy.htmlPotter,
[72]. Shaza D. Rihan, Ahmed Khalid Saife, Eldin F. Osman, A Performance Comparison of Encryption Algorithms AES and DES, International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 IJERTV4IS120227 www.ijert.org (This work is licensed under a Creative Commons Attribution 4.0 International License.) Vol. 4, Issue 12, December-2015.
[73]. Aamer Nadeem and Muhammad Younus Javed, A Performance Comparison of Data Encryption Algorithms, International Conference on Information and Communication Technologies, 2005, pp. 84-89, https://api.semanticscholar.org/CorpusID:14441015.
[74]. Manreet Sohal, Sandeep Sharma, and BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing, Journal of King Saud University –Computer and Information Sciences, 2018.
[75]. Hamdy M. Mousa, DNA-Genetic Encryption Technique, I. J. Computer Network and Information Security, 2016, 7, 1-9 Published Online July 2016 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2016.07.01.

