Mustansiriyah Journal of Pure and Applied Sciences

www.MJPAS.com

A new Audio Encryption Algorithm Based on Hyper-Chaotic System

H.A. Qasim
Ministry of Education, Baghdad, Iraq(marun_11981@yahoo.com)

A B S T R A C T

a new algorithm for audio encryption is presented in this work, the simple structure chaotic logistic map based to perform permutation mechanism where the position of the audio samples are rearrangement again with the purpose of break correlation, lately based on key stream generated from complex hyper-chaotic system diffusion operation is done with the aim of fill silent periods within the speech conversation to ambiguity the critical information and successful encryption operation.

to ensure the security and efficiency of proposed method many quality metrics analysis are done such as histogram, waveform, entropy, key space, correlation coefficient, differential and speed performance, the experimental results demonstrate that the proposed algorithm characteristics with high level of security, resistant attacks and can realize the real time.

Keywords*: multimedia, cryptography system, diffusion, chaotic , Rössler system*

1. Introduction

In recent years huge amount of multimedia files exchange every day over internet and other network, the need for designing efficient and secure cryptographic system become more and more urgent demand to ensure the security of storage or transmitted such files and keep it secrecy from unauthorized access ,[1].

The most important technique used to exchange information over unsecure environment and preserving the non-repudiation, integrity, authentication and secrecy for information, is cryptography, where the original data is distorted and send with ambiguous form to avoid potential threats from unauthorized access, cryptography can be divided to symmetric and a symmetric, in symmetric cryptography both sides share same secret key to perform encryption and decryption processes, Diffie and Hellman in 1976 proposed asymmetric key cryptography with two different keys, public key for encryption process and private key for decryption process [2]. Some multimedia data like audio file in contrast with text file characteristic's with high repetition and strong correlation between samples, which required more efficient cryptography system to break correlation and hide any statistical information about the nature of original file, that can be used to deduce useful information[3], many scholars suggested utilized of chaotic systems due to excellent properties like extreme sensitivity, ergodicity which corresponding diffusion, confusion respectively in cipher system[4].

With the purpose of ensure the confidentiality of transmitted audio data and efficiency of such technique, anew audio encryption algorithm proposed, utilize the

high randomization of dynamic complex hyper-chaotic system, security and performance analysis show desirable security characteristics, less computational overhead and more resistant attacks.

2.Related work

This section presented brief summary about the suggested audio encryption algorithm that based chaotic map and other techniques with important resulted, for achieve reliable encryption method in [5] Nidaa, Ayad, Mohammed presented an encryption algorithm based low dimension chaotic maps, Henon and Gingerbread, the speech files are rearrange as a cubic form with six sides to scatter speech samples, furthermore the random keys generated from maps used to encrypt each side, results confirm that the proposed algorithm is reliable and more resist attack, reference [6] proposed a novel lossless audio encryption algorithm based on arithmetic operation of an elliptic curve over a finite filed Z_p and binary Galois filed GF(2^n), the proposed algorithm employ special type of curve based on the elliptic curve, which generate high quality sequence of random number with the purpose of defuse the matrix of audio file, finally confusion stage is executed through multiple substitution boxes having higher nonlinearity, the scheme was thoroughly securitized over different simulation analysis, in paper [7] audio samples will permutation employ modified discrete Henon map to break high correlation among adjacent samples, followed by substitution stage which utilize the key sequence generated by modified Lorenz hyper-chaotic system to fill the silent periods with in the speech conversation, with the purpose of execute excellent security performance, various quality metrics analysis is performed to proposed encryption algorithm, results demonstrate its robustness against various cryptography attack.

For realized successful encryption for audio files in paper [8] Permutation-Substitution architecture based to presented a novel encryption algorithm, chaotic circle map and modified rotation equation utilized as a new pseudo-random number generator and used as basis for chaotic bit-level permutation and Substitution, extensive cryptographic analysis done, the resulted proving high level of security.in [9] a novel algorithm for encrypted audio file presented, a mathematical function of chaos theory Ikeda map is used as generator for encryption audio samples, the tested proved that the proposed method characteristics with excellent encryption properties.

3.chaotic system

The complex dynamical system that appear high sensitivity to initial conditions and control parameter called chaotic system, where small error in initial condition can lead to totally different in future behavior of system[10], in cryptography such systems attracts more attention due to is desirable characteristics, which can achieve diffusion and confusion in cryptosystem[11].

A.Logistic map

The first who introduced logistic map is biologist Robert May in 1976,[12] with simple structure and discrete time non-linear dynamical equation, , and expressed by:

$$x_{n+1} = r x_n (1 - x_n) \quad (1)$$

The map display the chaotic behavior when the value of (r) confined between the intervals $[3.57,4]$.

B. Rössler hyper-chaotic system

the chaotic system with more complex behavior such system called hyper-chaotic system, the minimum dimensions for system more than three dimensions, and two equations of system must contain one non-linear term for each[13][14], utilized of such system in cryptography can lead to more advantage like high randomness, unpredictability, desirable security and efficiency, Rössler proposed the first hyper-chaotic system in 1979 that can describe by the following four ordinary differential equations:

$$\begin{aligned} \dot{x} &= -y - z, \\ \dot{y} &= x + ay + w, \\ \dot{z} &= b + xz, \\ \dot{w} &= -cz + dw, \end{aligned} \quad (2)$$

the system exhibit hyper chaotic behavior when the parameter values for a, b, c, d, assumed respectively as $(0.25,3,0.5,0.05)$.

4.Proposed Encryption System

The proposed audio encryption algorithm is achieved two essential processes permutation and diffusion, in permutation stage include rearrange the audio symbols based chaotic random numbers generated from logistic map, lately the value of shuffled symbols modification by applying Exclusive-OR (XOR) with the sequence created by hyper chaotic system and the figure below show the encryption procedure :

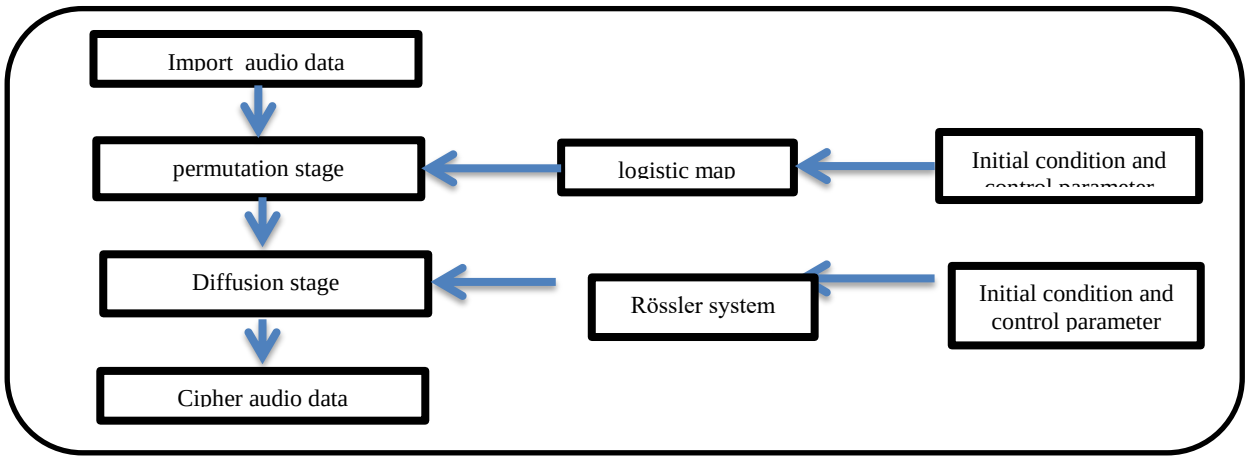

Figure (1): the Block diagram of proposed method

Algorithm (1): Proposed Audio Encryption Algorithm

Input:

- Plain audio data, initial conditions, control parameters

Output :

- Encrypted audio file

Step1: Read audio data X.
Step2: Iterate the equation (1) with initial condition create chaotic sequence Y .
Step3: Sort Y in ascending order manner to create S, for each element i in S, repeat

- locate its position in Y
- Save position in V

Steps4: Rearrange (X) due to V elements.
Steps5: Iterate system (2) create Z, for each i in Z

$$\mathbf{Z(i)} = \mathbf{uint8}((\mathbf{mod}\left(\mathbf{ceil}(\left(\mathbf{i}\times\mathbf{10^{14}}\right)\div\mathbf{64})\right),\mathbf{255}))$$

Where uint8 converts the element into unsigned 8-bit integer, ceil(i) returns the nearest integer less than or equal to i, will mod operation returns the remainder after division returns the remainder after division.
Steps6:perform Xored operation,where $\mathbf{c(i)} = \{\mathbf{X(i)} \oplus \mathbf{Z(i)}\}$
Steps7: Store C**.**
Steps8**:** end.

5.Cryptocrgraphic Analysis

To evaluate the robustness, resistant and efficiency of audio encryption, many metrics are calculated, like Histogram Analysis, Waveform Plotting, Key Space, Correlation Coefficient Analysis, Number of Sample Change Rate (NSCR), and speed performance.

5.1 Key Space Analysis

With the purpose of break and make brute-force attack inefficient, the key space size should be at least 2^{100}[15], the secret key for proposed algorithm represented by initial condition and control parameters (x,y,z,w,a,b,c,d) respectively with precision 10^{-16} for each, the total key space result for proposed algorithm $((10^{16})^{8}) \approx 2^{420}$,which is large enough and can frustrate brute force attack.

Table.1: Key space comparison

Refrence number	Key space
[3]	2^{319}
[8]	2^{149}
Proposed Algorithm	2^{420}

5.2 Histogram Analysis

one aim for ideal encryption is avoid any statistical relationship between the original and encrypted audio files, the histogram for encrypted audio file should has fairly flat form and totally different from corresponding for plain audio file[16], from Figure2(a), Figure2(b) can deduce no statistical relationship, and the intruder cannot get any useful information about the nature of original audio file due to completely uniform distribution of sample values in Figure2(b).

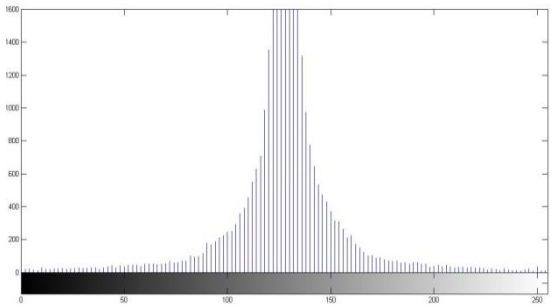

Figure2(a): Plain Audio File

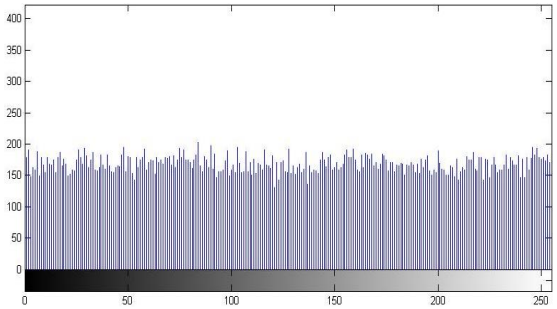

Figure2(b): Encrypted Audio File

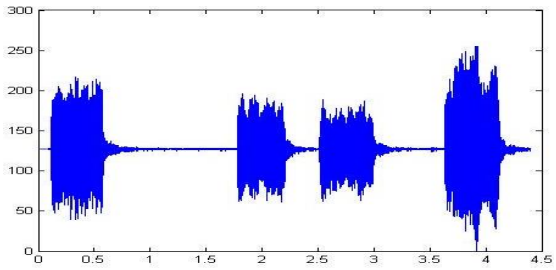

Figure3(a). Plain Audio File

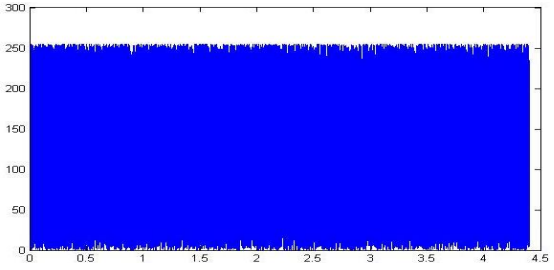

Figure3(b). Encrypted Audio File

5.3 Waveform Plotting

waveform plotting clarify the amplitude of audio signal distributed in time, completely different between Figure3(a) plain audio file and Figure3(b) encrypted audio file, reflected excellent characteristics of the proposed encryption method.

5.4 Correlation Coefficient Analysis

Correlation analysis one aspect for evaluating cryptographic algorithm, that measure the level of likeness between sample values of plain and encrypted audio files, computed by the following equations [17]:

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2\right)}} \quad (3)$$

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

For all tested files in Table-2 can observe that the result correlation values for encrypted audio files close to theoretical value (zero) and the proposed algorithm has good encryption properties.

Table 2. Correlation result values.

Audio name	Size	Correlation coefficient
70bugs	24.8KB	0.0167
Nosign	31.6KB	0.0006
!slap.wav	42.1KB	-0.0047
bird_caw1	43KB	0.0006
Redalert	87.1KB	-0.0010
Toto	102KB	-0.0081
preamble	822KB	0.00008
sea-wave	1254KB	-0.0035
Ref.[3]	43KB	-0.0064
Ref.[5]	138KB	0.290
Ref.[9]	832KB	0.0157

5.5 Information Entropy Analysis

To prevent any degree of predictability that threatened the security of audio file, significance criteria entropy analysis should be done to measure the randomness, which can be measured by following form:

$$H(m) = -\sum_{i=0}^{N-1} P(m_i) log_2[P(m_i)] \quad \textbf{(4)}$$

the entropy value for encrypted audio file should be close to theoretical value (8),the result of applying information entropy analysis listed in Table 3, and the resulted confirm that the encryption algorithm have the required robustness and resistant against entropy attack[18].

Table.3 Information entropy test results.

Audio name	Size	Entropy for original audio	Entropy for encrypted audio
70bugs	24.8KB	5.4592	7.9918
Nosign	31.6KB	6.9430	7.9945
!slap.wav	42.1KB	5.0230	7.9958
bird_caw1	43KB	4.5139	7.9943
Redalert	87.1KB	5.2873	7.9977
Toto	102KB	7.2798	7.9983
preamble	822KB	3.6114	7.9983
sea-wave	1254KB	0.9994	7.9972

5.6 Number of Sample Change Rate

For ensure the quality of encryption algorithm another robust test is done, number of sample change rate(NSCR), which explore the difference in percent's between the sample values for original and encrypted audio file, the formula can be expressed as follow [19]:

$$NPCR(c_1, c_2) = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\% \quad (5)$$

$$D(i,j) = \begin{cases} 0 & if \quad C_1(i,j) = C_2(i,j) \\ 1 & if \quad C_1(i,j) \neq C_2(i,j) \end{cases} \quad (6)$$

the resulted values in Table 4 demonstrate the high difference percentage between original and encrypted audio file.

Table 4. Number of sample change rate.

Audio name	NSCR
70bugs	99.6483
Nosign	99.6044
!slap.wav	99.6177
bird_caw1	99.6068
Redalert	99.6132
Toto	99.6265
preamble	99.6858
sea-wave	99.7916

5.7 Speed Performance

Real-time applications have increased in used exponentially and played major role, the time required encryption and decryption process must be acceptable and within real-time, the program implemented using MATLAP 2013A under Windows 7 ultimate (64-bit) with personal computer Intel® Core™ i7 @2.67GHz and 4GB RAM,

Table 5. present encryption time for different audio files.

Audio name	Size	Encryption time in second
70bugs	24.8KB	0.0687
Nosign	31.6KB	0.0803
!slap	42.1KB	0.1134
bird_caw1	43KB	0.1129
Redalert	87.1KB	0.2340
Toto	102KB	0.2745
preamble	822KB	1.0331
sea-wave	1254KB	0.6475
Ref.[3]	43KB	4.92
Ref.[8]	98.6KB	1.14
Ref.[9]	832 KB	3.691

6. Conclusion

Huge amount of multimedia information exchange every day over unsecure network, which increase demand for cryptography systems that provide reliable confidentiality, With the aim of ensure the secrecy and prevent unauthorized access to confidential audio data, this work presented a new audio encryption algorithm, the proposed method include two stages: permutation and diffusion, at permutation stage the simple structure logistic map utilized to rearrange audio sample values with the aim of break high correlation among them, followed by diffusion stage that used the pseudo-random sequence generated from Rössler hyper-chaotic system to change sample values depending XOR operation, detailed security analysis presented in section 5 show the high resistant ,robustness and randomness of the proposed algorithm, also the resulted show that the encryption process within real time and suitable for real time application, these observations the same for all tested audio files.

7. Reference

[1] Murtala, K., & Adeniyi, A. E. (2017). Message Encryption and Decryption on Mobile Phones. *Tetfund Sponsored Kwara State Polytechnic Journal of Research and Development Studies*, *5*(1), 1-11.

[2] Bahjat, H., & Salih, M. A. (2014). Dynamic Shuffling for Speed Image Encryption. *International Journal of Computer Applications*, *89*(7).

[3] Albahrani, E. A. (2017, March). A new audio encryption algorithm based on chaotic block cipher. In *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)* (pp. 22-27). IEEE.

[4] Tanwar, G., & Mishra, N. (2015). Survey on image encryption techniques. *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, *5*, 12.

[5] Hassan, N. F., Al-Adhami, A., & Mahdi, M. S. (2022). Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps. *Iraqi Journal of Science*, 830-842.

[6] Shah, D., Shah, T., Hazzazi, M. M., Haider, M. I., Aljaedi, A., & Hussain, I. (2021). An efficient audio encryption scheme based on finite fields. *IEEE Access*, *9*, 144385-144394.

[7] Farsana, F. J., Devi, V. R., & Gopakumar, K. (2020). An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. *Applied Computing and Informatics*, (ahead-of-print).

[8] Kordov, K. (2019). A novel audio encryption algorithm with permutation-substitution architecture. *Electronics*, *8*(5), 530.

[9] Stoyanov, B., & Ivanova, T. (2021). Novel implementation of audio encryption using pseudorandom byte generator. *applied sciences*, *11*(21), 10190.

[10] Vaidyanathan, S., Azar, A. T., Rajagopal, K., & Alexander, P. (2015). Design and SPICE implementation of a 12-term novel hyperchaotic system and its synchronisation via active control. *International Journal of Modelling, Identification and Control*, *23*(3), 267-277.

[11] Kamat, V. G., & Sharma, M. (2014). Symmetric Image Encryption Algorithm Using 3D Rossler System. *International Journal of Computer Science and Business Informatics*, *14*(1).

[12] Alligood, K. T., Sauer, T. D., Yorke, J. A., & Chillingworth, D. (1998). Chaos: an introduction to dynamical systems. *SIAM Review*, *40*(3), 732-732.

[13] Vaidyanathan, S. (2016). Hyperchaos, adaptive control and synchronization of a novel 4-D hyperchaotic system with two quadratic nonlinearities. *Archives of Control Sciences*, *26*(4), 471-495.

[14] El-Sayed, H.M. Nour, A.Elsaid, AElsonbaty,"Dynamical Behaviors of A New Hyperchaotic System with One Nonlinear Term," Electronic Journal of Mathematical Analysis and Applications, Volume-3,Number-1,2015.

[15] Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, *16*(08), 2129-2151.

[16] Gupta, K., Gupta, R., Agrawal, R., & Khan, S. (2015). An ethical approach of block based image encryption using chaotic map. *International Journal of Security and Its Applications*, *9*(9), 105-122.

[17] Tao Song, "A Novel Diffusion Approach with Chen System for Chaotic Image Cryptosystems", International Journal of Advancements in Computing Technology (IJACT), Volume-4, Number-20, 2012.

[18] Ahmad, M., & Alam, M. S. (2009). A new algorithm of encryption and decryption of images using chaotic mapping. *International Journal on computer science and engineering*, *2*(1), 46-50.

[19] Gupta, K., & Silakari, S. (2011). New approach for fast color image encryption using chaotic map. *Journal of Information Security*, *2*(04), 139.