e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

DESIGN AND IMPLEMENTATION OF A VOICE ENCRYPTION SYSTEM USING FRACTIONAL-ORDER CHAOTIC MAPS

Abdullah Ali Saeed Alghamdi*1

*1Department Of Electrical And Computer Engineering, King Abdulaziz University, Jeddah, Saudi Arabia.

ABSTRACT

Speech and audio interface systems are widely used in our daily lives. Therefore, most multimedia technology such as speech and audio is paramount, and the telephony, video conference, and news sharing markets are the backbone of their operation. Securing public networks, such as the Internet, via these exchanges is a Classical Algorithm based on Algebraic. These conventional algorithms have however, proven resistant to attacks. Conventional cryptographic methods have only seen for text data. Therefore, they are not equitable for bulk data capabilities. This study proposed a fractional-order chaotic crypto scheme on specialized hardware platforms like DSP or FPGA development boards. In data-secure communication, the value of fractional-order chaotic structures lies in the fact that the security space key expands the fractional-order parameters and thus enhances security. The use of discrete-time fractional-order chaotic schemes for the scrambling of the digitized speech signal envisaged to increase the degree of communication security further. New synchronization schemes for the unpredictable fractional-order method have recently developed. Validation and robustness checking will conducted against threats and will compared to other classical encryption algorithms will carried out.

Keywords: Fractional-Order Systems, Nonlinear Observers, Synchronization, Nonlinear Chaotic Systems, Speech Encryption, Simulink, Android.

I. INTRODUCTION

In our everyday lives, speech and audio communication devices are commonly used. The majority of multimedia technologies, such as speech and audio, are therefore paramount, and their operation is the basis of the telephony, video conferencing, and news exchange industries. It is a requirement to protect these exchanges across public networks like the Internet. Classical algorithms still used today, based on algebraic manipulations. However, these classical algorithms have become vulnerable to attacks with the emergence of increasingly powerful computers. The rapid and increased growth of multimedia data sharing over open networks and the Internet requires secure and robust protection means to provide confidentiality and prevent unauthorized access to the information transferred. The use of data encryption is among many solutions. Encryption sachems are algorithms that alter data (such as text, image, sound, etc.) so that they are unreadable, invisible, or impenetrable during transmission. Nowadays, in different applications, data encryption plays an enormous role, and different encryption systems have developed with the ultimate objective of protecting sensitive data by increasing its protection and confidentiality. Most of the research work aims to provide enhanced consistency of encryption, less execution, and attack security robustness. Chaos-based systems have shown excellent performance compared to conventional encryption schemes, with the demonstrated potential to improve the protection and privacy required by using variable keys. The cornerstone is to use several components of uncertainty to decorate a given scheme's confusion and diffusion capacity. Chaos-based encryption encompasses various multimedia styles in literature, i.e., text, audio, image, and video. Next, a review of the recent literature on a chaotic multimedia encryption application based on maps presented. Today, in telephony, videoconferencing, and news exchange, multimedia applications such as sound and speech are essential. Thus, to prevent interference and listening attacks, the protection of speech communication systems is very critical. As modern voice communication systems require a great amount of information to be shared between local networks and the Internet, the need for encryption and protection has increased [1], [2]. Classical algorithmic based on algebraic manipulations still used today. However, with the advent of increasingly powerful computers, these classical algorithms have become vulnerable to attacks. Moreover, the effectiveness of these conventional cryptographic techniques has proven only for text data. Unfortunately, they are not suitable for bulk data capability. These flaws have pushed research towards the development of new systems. Speech protection also requires dramatically enhanced techniques, such as chaos-based techniques. Techniques based on chaos include methods of encryption that are fast and highly reliable. A significant research subject since the 1990s has been the use of chaos for safe data transmission. From nonlinear systems, chaos obtained. Analog electric oscillators such as Colpitts, Chua, and Qi oscillators or optical and semiconductor devices such as quantum lasers can produce a chaotic signal. A chaotic sequence iterated map can generated numerically in the digital method, for example, by logistical nonlinear differential equations, the Henon map, the Cat map, the Lozi map, etc. The sensitive reliance on initial conditions, similarity to random behavior, and continuous broadband power spectrum characterize these systems. Chaos refers to a stable, probably constrained, but unpredictable behavior that makes it look like a pseudorandom noise. This quality can used to mask or blend information in a safe digital or analog data transmission method [3], [4]. In the literature, chaotic nonlinear systems are well known, [5]-[7]. On the other hand, the analysis of the chaotic behavior of fractional-order discrete-time systems (FOS) has also taken into account in the literature based on the so-called fractional-order calculus. The fractional-order logistic map [8], [9] and the fractional-order Hénon map [10] are among the most important of the fractional-order chaotic maps. Despite its natural application in safe digitalized data communication, the Synchronization of fractional-order discrete-time systems is a very recent research subject [11]-[12]. With few works suggested, fractional-order systems' application to voice encryption is still an open issue [13], [14]. On the other hand, new Synchronization methods of discrete chaotic fractional-order systems dedicated to image encryption have recently proposed. [15] - [17]. The aim of the research project proposed in this paper is to design a new voice encryption, communication scheme based on these methods. The proposed scheme should implemented in a DSP or other micro-controller device. The performance of the new proposed scheme will evaluated and compared to other classical encryption techniques.

II. LITERATURE REVIEW

In the public key cryptosystem, the best-known encryption/decryption algorithm is the RSA due to the inventors' Rivest, Shamir, and Adelman, the Rabin scheme, the Williams scheme, the Elliptic curve. While several of these methods currently used form the foundation of defense, due to the availability of high-speed computers and fast algorithms, none of these can considered 100% safe. [27], [28]. Moreover, if these traditional cryptographic algorithms give good results in the transmission of text messages, they are ineffective for transmitting an audio signal. Audio data encryption is a complicated and complex method compared to the methods used for text data. Audio encryption can be analog or digital. Various analog speech scramblers proposed in the literature [29]. On can cite the time-domain scramblers [30]-[32], the frequency domain scrambler [33], the amplitude scrambling method [34], and the transform domain [35]-[36]. Due to the high redundancy and bulk capacity of voice data, conventional cryptographic algorithms[19]-[27] that are recognized as effective for text data in digital encryption systems fail to provide the same degree of security for audio data. Small block sizes with complex permutation processes used by traditional symmetric key algorithms such as Advanced Encryption Standard (AES), [20], [21] and Data Encryption Standard (DES), [27] to give stable ciphertext. These complicated algorithms are vulnerable to noise attacks, and the characteristics of the audio signs not changed by small blocks. Due to their relatively slow performance due to their complexity, which relies on large number factorization or discrete logarithm problem computing, asymmetric key encryption schemes[19],[21],[28] are not suitable for encrypting large quantities of data and time-sensitive applications such as speech conversation.

By increasing the size of public and private keys to a 1024-bit number, it is also dependent on increasing its stability. Therefore, voice and high-security levels are not suitable and simple algorithms needed. Chaotic systems for voice data seen as an effective technique. The chaotic systems provide high-security strategies due to their high sensitivity to minor changes in the initial state and their pseudorandom actions. The literature suggests many speech encryption schemes using discrete chaotic systems, such as the Hénon map, the Cat map, the Lozi map and the Logistic map. [37] - [49]. Often chaos used to generate the key parameters for the encryption function. The use of chaotic nonlinear systems of fractional order improves the security level of cryptosystems. Nevertheless, few works have been devoted to voice encryption [13]-[14]. Through this abundant literature, it emerges that the theory of the control and design of observers for fractional-order chaotic systems has not investigated in the design of speech secure transmission. Recent methods of synchronizing fractional chaotic systems [15], [16], [17], [50], [51], [52], [53] will be a source of contributions to the design of speech encryption systems. In this sense, a challenge and the main objective of this paper is the

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

proposal for new voice encryption schemes based on the Synchronization of fractional chaotic systems and the software and hardware implementation of the resulting encryption algorithms.

III. RESEARCH DESIGN & METHODOLOGY

Speech Encryption using Fractional-Order Chaos Based Algorithm:

The literature has taken in to account the study of the chaotic behavior of fractional-order discrete-time systems. The fractional-order logistic map [8],[9] and the fractional-order Hénon map [10] are among the most important of the fractional-order chaotic maps. As an example, consider the modified Hénon map of the fractional - order defined by the following equations of fractional differences.

$$\begin{aligned} \Delta^{\alpha_1} x_1(k+1) &= a - x_2^2(k) - b x_3(k) - x_1(k) \\ \Delta^{\alpha_2} x_2(k+1) &= x_1(k) - x_2(k) \qquad (1) \\ \Delta^{\alpha_3} x_3(k+1) &= x_2(k) - x_3(k) \end{aligned}$$

Where the fractional difference operator j of order aj is derived from the Grünwald Letnikov Formulae and is given by:

$$\Delta^{\alpha_j} x(k+1) = x(k+1) - \alpha_j x(k) + \sum_{i=2}^{k+1} (-1)^i \binom{\alpha_i}{i} x(k+1-i) \qquad (2)$$

Note that, in the definition above, the operator of the fractional difference has an infinite memory. We use the short memory concept in practice. That is by replacing the sign number the memory reduced and is finite. Where the finite size of the memory is L. Device (1)'s chaotic behavior is obtained by setting a=1.68, b = 0.1, α_1= 0.97, α_2 = 0.94, α_3= 0.91 and L = 5 inside the odd attractor basin, initial conditions $x_1(0)$ = 0.2, $x_2(0)$ = 0.5 and $x_3(0)$ = 0.1 are chosen. As shown below, the simulation results demonstrate the system's chaotic behavior (1). With respect to the vector parameter a, as can be seen from the bifurcation diagram, seen in Figure 1, when a = 1.3 1.65, system (1) is chaotic. For example, with a = 1.5, Figures 1a and 1b show the phase portrait and state responses of system (1), respectively.

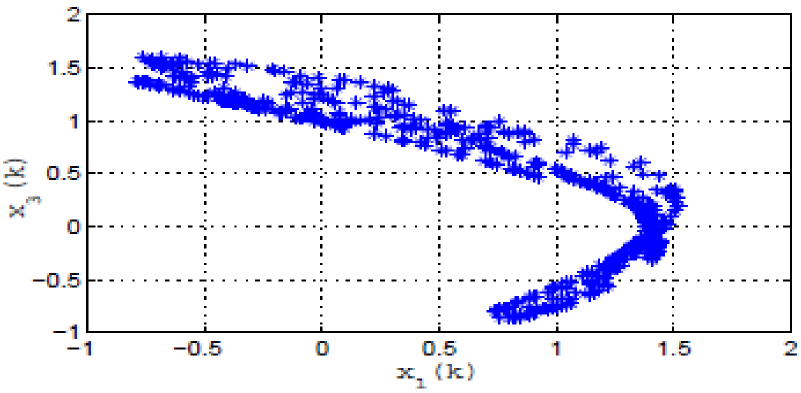

Figure 1: Phase portrait of Fractional-order Modification of Henon map.

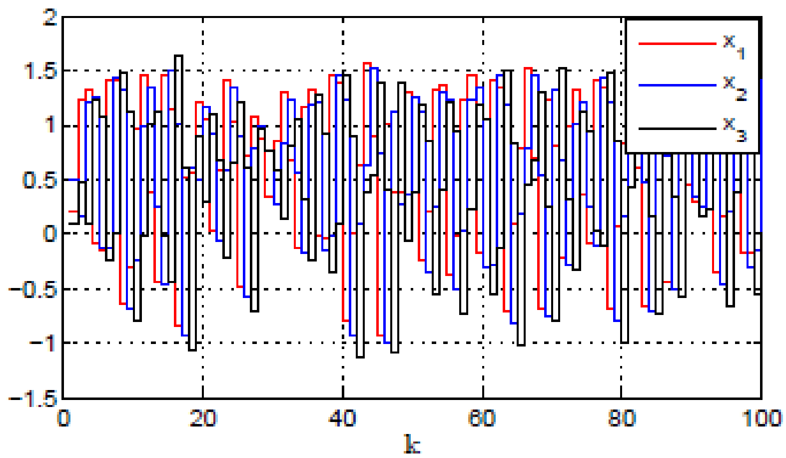

Figure 2: State response of fractional-order Map.

Description of the proposed fractional-order chaotic iterated map base voice encryption System:

The global block-diagram of the proposed scheme has given by Figure 7. It contains two main blocks:
The emitter and the receiver.

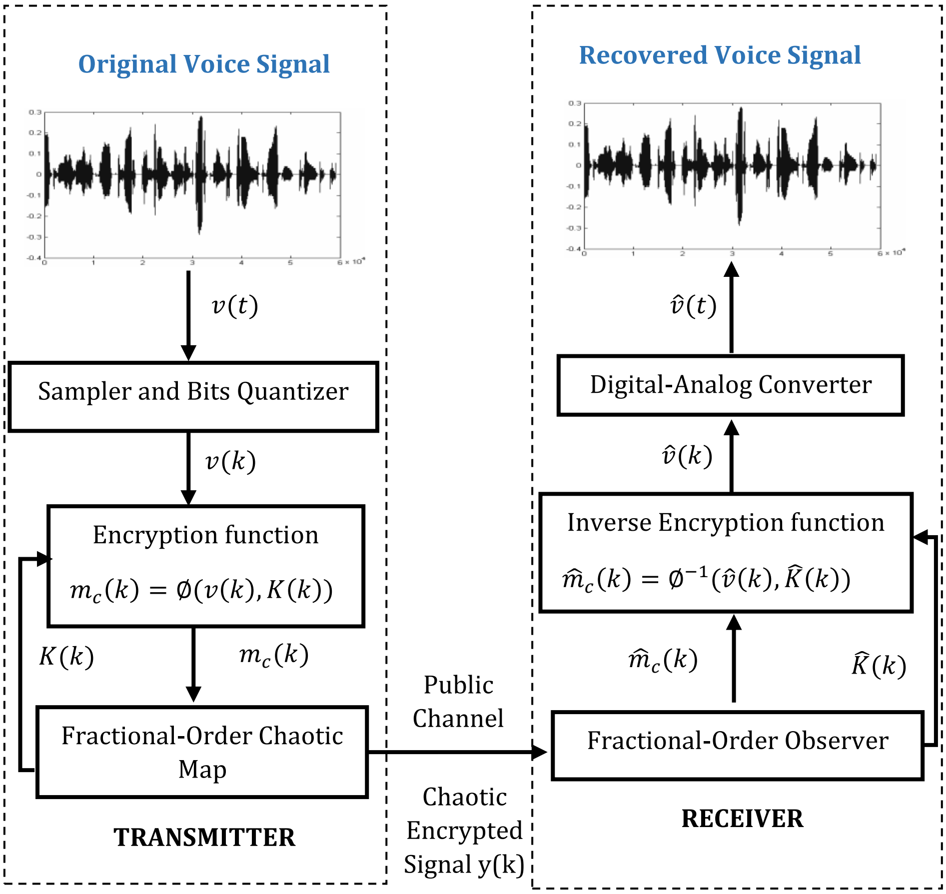

Figure 3: General block diagram of directional-order base chaotic cryptosystem.

Description of the transmitter:

In the sender, first, the voice analog signal has converted to a digital signal after sampling and quantizing process. The digital voice signal has encrypted by using an adequate encryption function. The fractional-order modified Hénon map (1) generates chaotic signals $x_1(k)$, $x_2(k)$ and $x_3(k)$ the generated pseudorandom sequence used to encrypt the key K (k):

$$K(k) = \gamma(x_1(k), x_2(k), x_3(k), p) \quad (3)$$

Where the vector p contains the secret key parameters. The obtained encrypted signal $m_c(k)$ given by:

$$m_c(k) = \emptyset(v(k), K(k)) \quad (4)$$

Where Fiy denotes the function of encryption. The encrypted message $m_c(k)$ inserted by the inclusion method in the same chaotic system dynamics, in the last equation of the third state variable dynamic in order further enhance to the protection and robustness of the transmission system. The original hidden voice signal thus masked by the pseudorandom signal produced by the powered chaotic System (Transmitter), which leads to an unintelligible signal y (k). $x_2(k)$ Transmitted to the chaotic response system via the public channel (receiver).

Description the receiver :

When the transmitter and the receiver synchronized, the retrieval of the original message is possible. Since Pecora and Carrol's groundbreaking work [54] showed the possibility of synchronizing two chaotic systems, the use of chaotic systems in safe communications with different initial conditions has revolutionized conventional encryption methods. As follows, the Synchronization of chaotic systems described. Consider a nonlinear fractional-order chaotic system described by the following state equation:

$$\Delta^{\alpha} x(k+1) = f\big(x(k)\big) \quad (5)$$

$y(k) = h(x(k))$

System (5) represents the transmitter and is designed as the drive (or master) system. Consider the Second nonlinear chaotic System described by:

$$\Delta^{\alpha}\hat{x}(k+1) = f(\hat{x}(k), y(k)) \qquad (6)$$

This second system represents the receiver and designed is as the response (or slave) system. We say that Systems (5) and (6) asymptotically synchronized if the synchronization error:

$$e(k) = x(k) - \hat{x}(k), e(k_0) = x_0 - \hat{x}_0 \neq 0 \qquad (7)$$

Converges to zero as k= 0, and we say that Systems (6) and (7) are synchronized infinite time if There exists a finite time ks > k0 such that e(k) =0 for all ks > k0 .

As pointed out in [55], Synchronization may viewed as an observer design problem. Moreover, in the context of secure communications, the reconstruction of the encrypted message achieved within an unknown input observer [56]. The encrypted message has considered as an unknown input. The objective of the unknown input observer is to estimate both the state and the unknown input. The Synchronization of fractional-order discrete-time chaotic systems with the presence of unknown Inputs will investigated. The Synchronization of fractional-order discrete-time systems is a very recent research topic despite its natural application in secure digitalized data communications such as Image encryption [11], [12].

In this paper, based on the works [15], [50], a step-by-step observer delayed (dead beat Observer), is designed and used to resolve the synchronization problem and to allow the Reconstruction of the states and the unknown input (original voice signal). The fractional-order Observer has given by:

$$\Delta^{\alpha_1}\hat{x}_1(k+1) = a - x_2^2(k) - b\hat{x}_3(k) - \hat{x}_1(k)$$
$$\Delta^{\alpha_2}\hat{x}_2(k+1) = \hat{x}_1(k) - x_2(k) \qquad (8)$$
$$\Delta^{\alpha_3}\hat{x}_3(k+1) = x_2(k) - \hat{x}_3(k)$$

By applying a delayed reconstruction scheme (deadbeat observer), the estimate of the state variables and the encrypted message can obtained from (8) as follows:

$$\hat{x}_2(k) = \emptyset_1\big(y(k)\big) = y(k)$$
$$\hat{x}_1(k-1) = \emptyset_2(y(k), y(k-1))$$
$$\hat{x}_3(k-2) = \emptyset_2(y(k), y(k-1), y(k-2)) \qquad (9)$$
$$\widehat{m}_c(k-3) = \emptyset_3(y(k), y(k-1), y(k-3))$$

After two delay units, the key reconstructed as follows:

$$\widehat{K}(k) = \gamma(\hat{x}_1(k-1), \hat{x}_2(k), \hat{x}_3(k-2), p) \qquad (10)$$

Then, after three delays units, the inversion encryption function used to recover the original digital Voice signal:

$$\hat{v}(k-3) = \emptyset^{-1}(y(k), k(k-1), y(k-3)) \qquad (11)$$

Finally, a digital to analog conversion is module has implemented to recover the original voice signal.

Hardware and software implementation :

The present study should complemented by a real-time implementation followed by a demonstration on speech encryption and decryption application. We can draw inspiration from some works that have dealt with the hardware and software implementation of voice cryptosystems on specialized electronic circuits (DSP, FPGA, or other) [57], [58]. The Tx-Rx system described in the previous sub-section will implemented as software routines in MATLAB to simulate for correctness and suitability for real-time implementation. Once the software implementation is tested and verified in a desktop PC environment using MATLAB, a suitable hardware platform for final deployment will selected. The probable initial candidates for this deployment are Concerto Control Card (DSP TMDSCNCDH52C1) from Texas Instruments, Raspberry Pi (ARMv8-A), or Zedboard (Xilinx Zynq 7000 SoC FPGA) [59]. All of these hardware platforms can programmed via MATLAB/Simulink using a high-level programming paradigm. Thus, the effort spent in tuning the software implementation of the algorithm in MATLAB will put to good use in hardware implementation within a minimal time span.

IV. RESULTS

Simulation Results :

Using the MATLAB Program, a simulation model based on the framework shown in the block diagram has introduced. The voice signal used in this test has a sampling frequency of 8 kHz and a duration of 5 seconds (samples), each using a chaotic map.

Integer Order Encryption :

The diagram below explains the android base integer encryption.

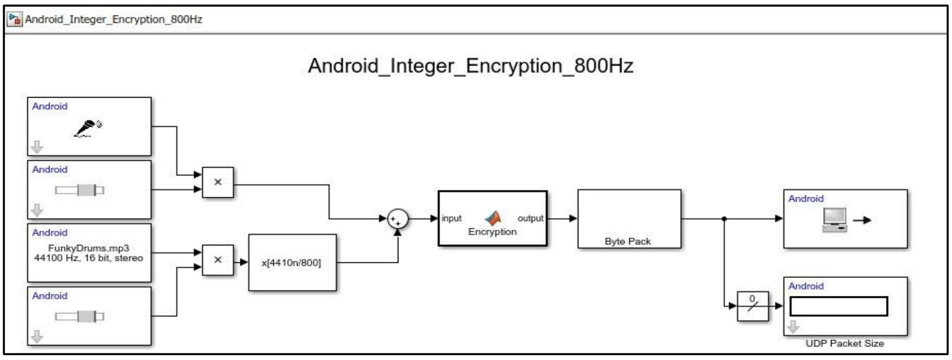

Figure 4: Integer Encryption

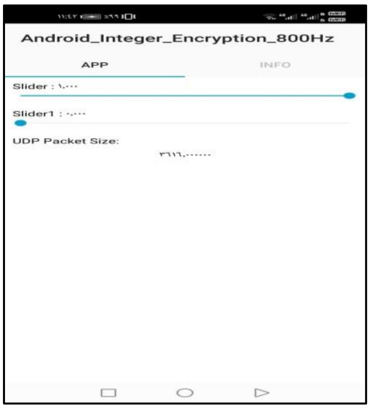

Figure 5: Android Encryption

Integer Order Decryption :

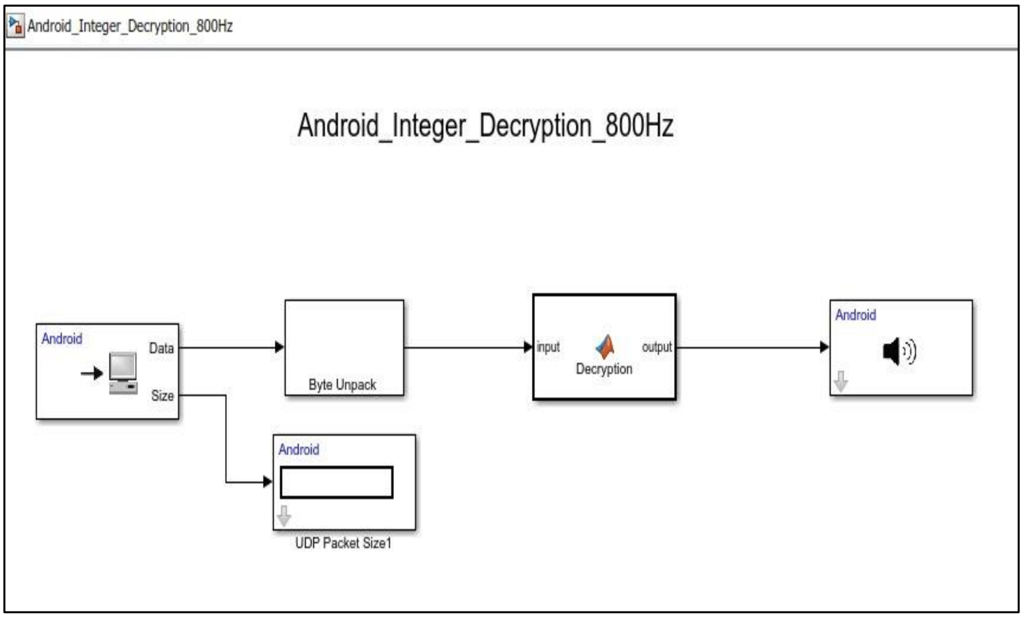

Figure 6: Android Integer decryption

IRJMETS
e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:06/June-2021 Impact Factor- 5.354 www.irjmets.com

Fractional Order Encryption :

The below diagram explains the fractional-order encryption process.

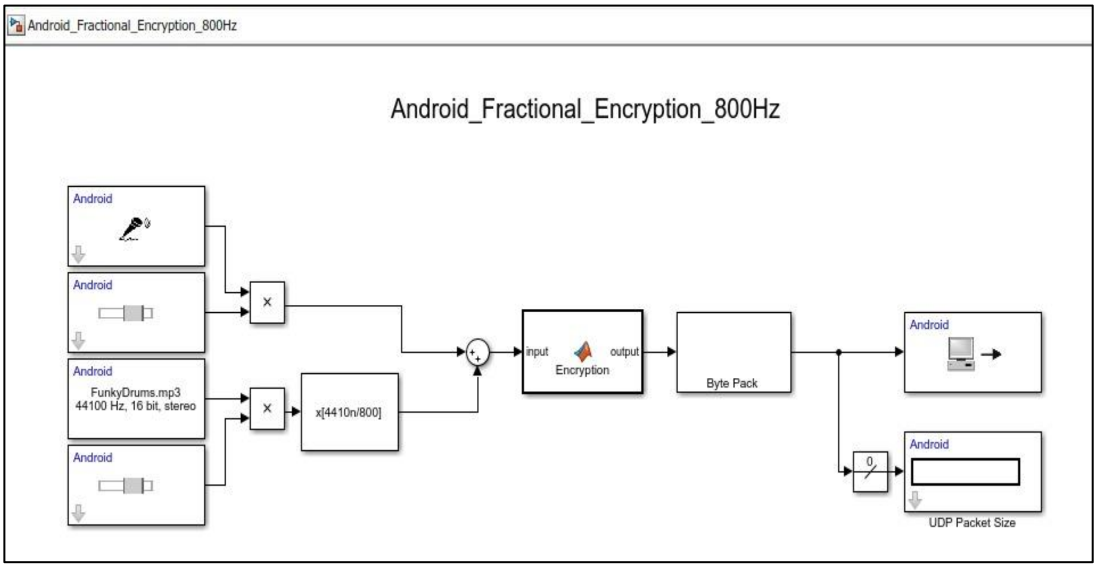

Figure 7: Frictional Encryption

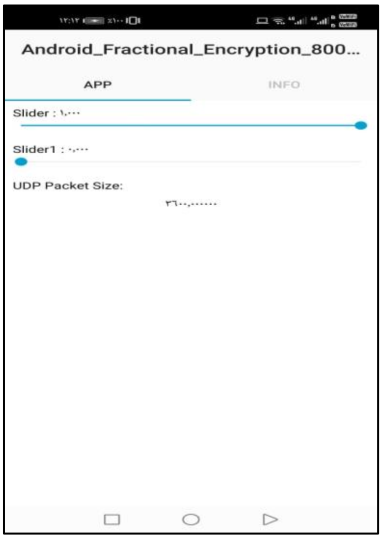

Figure 8: Frictional Encryption

Fractional Order Decryption :

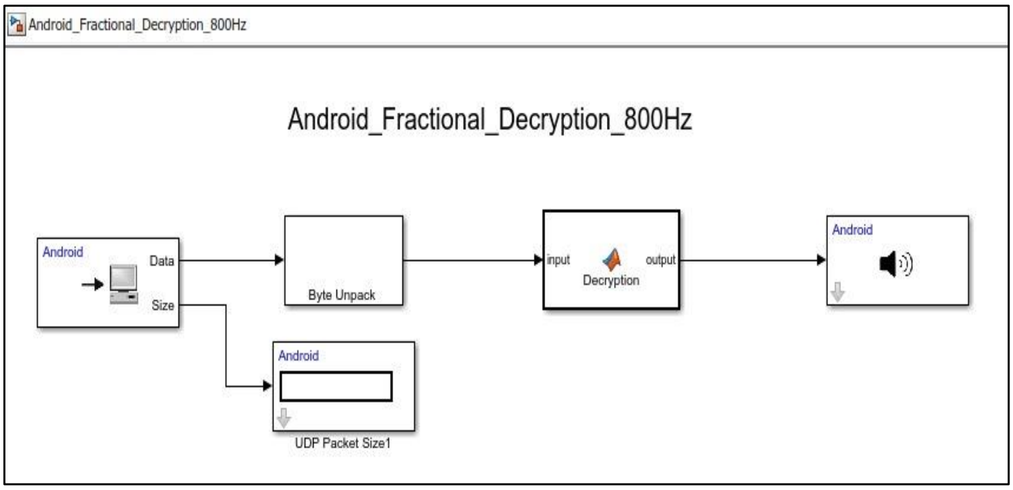

Figure 9: Frictional order Decryption

V. CONCLUSION

This new approach aims to expand compression algorithm functionality to achieve both compression and encryption simultaneously without an additional encryption stage in a single process. The use of the new combined simultaneous compression-encryption approach greatly reduces the encryption resources needed (computational and power resources). Due to such an attractive property, many works are devoted to this subject, some of which also based on chaotic maps. We suggested three strategies for improving different joint compression and encryption schemes based on chaos. The execution time, compression ratio and estimation accuracy of three deferential chaos-based map systems have improved, respectively. All of the above-mentioned works, however, are independent of the plain picture. Therefore, one of our future research guidance is how to build an elective plain image-dependent map framework to further enhancing the security level.

ACKNOWLEDGEMENTS

This project has funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia, under grant no. (KEP-Msc-37-135-38). The authors, therefore, acknowledge with thanks DSR technical and financial support.

VI. REFERENCES

[1] W. Stallings, Cryptography and network security: Principles and practice. Fifth Edition, Prentice Hall, 2010.

[2] D. R., Stinson, Cryptography. Theory and Practice. Third Edition: Chapman & Hall/CRC, 2006.

[3] L. Kocarev and L. Shiguo, Chaos-based Cryptography: Theory, Algorithms and Applications. Series: Studies in Computational Intelligence, Vol. 354, 2011.

[4] S., Banerjee, Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption. IGI Global, 2011.

[5] S. H. Strogatz, Nonlinear dynamics and chaos. Preseus Books Publishing, LLC, 1994.

[6] R. P. Murphy, Chaos Theory, Second edition, Ludwig von Mises Institute, Creative commons attribution License 3.0, 2010.

[7] T. Kapitaniak, Chaos for Engineers Theory, Applications, and Control, Second, Revised Edition Springer-Verlag Berlin Heidelberg 2000.

[8] G. Wu, D. Baleanu, Discrete fractional logistic map and its chaos, Nonlinear Dynamics Vol. 75, pp. 283–287, 2014..

[9] J. Munkhammar, Chaos in a fractional order logistic map, Fract. Calc. Appl. Anal., Vol. 16, pp. 511–519, 2013.

[10] Y. Liu, Discrete chaos in fractional Hénon maps, International Journal of Nonlinear Science, Vol. 18, n°3, pp. 170–175, 2014.

[11] W. Zhen, H. Xia, L. Ning, S. Xiao-Na, Image encryption based on a delayed fractional-order chaotic logistic system, Chinese Physics B Vol. 21, n°5 , 050506, 2012.

[12] G.-C.Wu, D. Baleanu, Z.-X. Lin, Image encryption technique based on fractional chaotic time series, Journal of Vibration and Control Vol. 22, n°8, pp. 2092–2099, 2016.

[13] Maher K. M. Al-Azawi, Jaafar Qassim Kadhim, Speech Scrambling Employing Lorenz Fractional Order Chaotic System, Journal of Engineering and Development, Vol. 17, n°4, pp. 195-211, 2013.

[14] Long Jye Sheu, A speech encryption using fractional chaotic systems, Nonlinear Dynamics, Vol. 65, pp. 103–108, 2011

[15] S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb, A novel secure image transmission scheme based on Synchronization of fractional-order discrete-time hyperchaotic systems, Nonlinear Dynamics, Vol. 88, n°4, pp 2473–2489, 2017

[16] O. Megherb, H. Hamiche, S. Djennoune, M. Bettayeb, A new contribution for the impulsive Synchronization of fractional-order discrete-time chaotic systems, Nonlinear Dynamics, August 2017.

[17] O. Megherb, S. Kassim, H. Hamiche, S. Djennoune, M. Bettayeb, J-P Barbot, Robust image transmission scheme based on coupled fractional-order chaotic maps, SIAM Conference, 2017.

[18] H. Kohad, V. R. Ingle, M. A. Gailwad, Security Level Enhancement in Speech Encryption using Kasami Sequence, Research and Applications (IJERA), Vol.2, n° 4, pp. 1518-1523, 2012.

[19] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communication of the ACM, vol. 2, pp.120-126, 1978.

[20] J. Daemen and V. R. Rijndael, The advanced encryption standard, Dr. Dobb's J. volume 26 No 3, pp. 137–139, 2001.

[21] T. El Gamal, A public-key cryptosystem and signature scheme based on discrete algorithms, IEEE Transactions on Information Theory vol. 31, pp. 469-472, 1985.

[22] F.I.P. Standard, Advanced Encryption Standard (AES), National Institute of Standards and Technology, (NIST), 2001.

[23] B. Schneier, the Blowfish Encryption Algorithm Retriever, October 25, 2008.

[24] A. Kakkar, M. L. Singh, P.K. Bansal, Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network, International Journal of Engineering and Technology, Vol. 2 n° 1, 2012.

[25] V. Gupta, G. Singh, R. Gupta, Advance cryptography algorithm for improving data security, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, n°1, 2001.

[26] H. C. Williams, A modification of the RSA public-key encryption procedure, IEEE Transactions on Information Theory, Vol. 26, pp. 726-729, 1980.

[27] T. Kean and A. Duncan, DES key breaking, encryption and decryption on the XC6216, IEEE Symposium on FPGAs for Custom Computing Machines, Vol. 15-17, pp. 310 - 311, 1998.

[28] M. J. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Transactions Information

[29] H. Kohad, V.R.Ingle, M.A.Gaikwad, An Overview of Speech Encryption Techniques, International Journal of Engineering Research and Development, Vol. 3, n°4, pp. 29-32, 2012.

[30] H. J. Beker and F. C. Piper, Secure Speech Communications, Academic Press, London, UK, 1985.

[31] Q.-H. Lin, F.-L. Yin, T.-M. Mei, and H. Liang, A blind source separation based method for speech encryption, IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 53, n° 6, pp. 1320–1328, 2006.

[32] N. Jayant, B. McDermott, S. Christensen, and A. Quinn, —A comparison of four methods for analog speech privacy, IEEE Transactions on Communications, Vol. COM-29, no. 1, pp. 18–23, January 1981

[33] J. Lee, N. Vijaykrishnan, M.J. Irwin, R. Chandramouli, Block-based frequency scalable technique for efficient hierarchical coding. IEEE Trans. Signal Process. Vol. 54, pp. 2559, 2566, 2006.

[34] Y. Mao, M. Wu, A joint signal processing and cryptographic approach to multimedia encryption. IEEE Trans. Image Process. Vol. 15, pp. 2061–2075, 2006.

[35] M. Ashtiyani, S. Behbahani, S. Asadi, P.M. Birgani, Transmitting encrypted data by wavelet transform and neural network, IEEE Int. Symposium on Signal Processing and Information Technology, pp. 385–389, 2007.

[36] G. Manjunath, G. V. Anand, Speech encryption using circulant transformations, IEEE Int. Conf. Multimedia and Expo., vol. 1, pp. 553–556, 2002.

[37] E. Mosa, W. Messiha, O. Zahran, F. Abd El-Samie, Encryption of speech signal with multiple secret keys in time and transform domains, Springer, 2010.

[38] K. Ganesan, R. Muthukumar, K. Murali, Look-up table based chaotic encryption of audio files, Circuits and Systems, 2006. APCCAS 2006. IEEE Asia Pacific Conference on, volume 5, 2006.

[39] R. Gnanajeyaraman, K. Prasadh, Audio encryption using higher dimensional chaotic map, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[40] J. Liu, FG. Gao, H. Ma, A speech chaotic encryption algorithm based on network, Proceedings of IIHMSP '08, IEEE press, Harbin, China, pp. 283–286, 2008.

[41] Z. Su, G. Zhang, J. Jiang, Multimedia security: a survey of chaos based encryption technology, in book "Multimedia – A multicplinary Approach to Complex Issues", edited by Loannis Karydis, INTECH, March 2012.

[42] A. Musheer, A. Bashir, O. Farooq, Chaos based mixed key stream generation for voice data encryption, International Journal on Cryptography and Information Security (IJCIS),Vol.2, n°1, 2012.

[43] M. Ashtiyani, PM. Birgani, SSK. Madahi, Speech Signal Encryption Using Chaotic Symmetric Cryptography", J. Basic. Appl. Sci. Res., Vol. 2, n°2, pp. 1678-1684, 2012.

[44] S. Najim A. E. Hato , A speech encryption on chaotic maps, International Journal of Computer

Application (0975-8887), Vol. 93, n°4 , pp. 19 – 28, 2014.

[45] H. B. Abdul Wahab , S. I. Mahdi, Modify speech cryptosystem based on shuffling overlapping blocks technique, International Journal of Emerging Trends & Technology in Computer Science, Vol. 4, n°2, pp. 70 – 75, 2015.

[46] A. Mahdi, S. S. Hreshee, Design and implementation of voice encryption system using XOR based on Hénon map, 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and A pplications (AIC-MITCSA) – IRAQ (9-10), 2016.

[47] A. Mahdi, A. K. Jawad, Sa.S. Hreshee, Digital chaotic scrambling of voice based on Duffing map, International Journal of Information and Communication Sciences, Vol.1, n°2, pp. 16-21, 2016.

[48] R.Gnanajeyaraman, K.Prasadh, Dr.Ramar, Audio encryption using higher dimensional chaotic map, International Journal of Recent Trends in Engineering, Vol. 1,n°. 2, 2009.

[49] F. J. Farsana, K. Gopakumar, A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number GeneratorProcedia Computer Science, Vol. 93, pp. 816 – 823, 2016.

[50] M. Bettayeb, U. M. Al-Saggaf, S. Djennoune,, Synchronization of Fractional-Order Discrete-Time Chaotic Systems by Exact Delayed State Reconstructor, submitted to publication.

[51] M. Bettayeb, U. M. Al-Saggaf, S. Djennoune, Single Channel Secure Communication Scheme Based on Synchronization of Fractional-Order Chaotic Chua's Systems, Transaction of the Institute of Measurements and Control, DOI: 10.1177/0142331217729425, 2017.

[52] U. M. Al-Saggaf, M. Bettayeb, S. Djennoune, Super-Twisting Algorithm-Based Sliding-Mode Observer for Synchronization of Nonlinear Incommensurate Fractional-Order Chaotic Systems Subject to Unknown Inputs, Arabian Journal for Science and Engineering, 42(7), pp. 3065-3075, DOI: 10.1007/s13369-017-2548-5, 2017.

[53] M. Bettayeb, U. M. Al-Saggaf S. Djennoune, High gain observer design for fractional-order nonlinear systems with delayed measurements: Application to Synchronization of fractional-order chaotic systems, IET Control and Applications, DOI: 10.1049/iet-cta.2017.0396, 2017.

[54] LM. Pecora and TL. Carrol, Synchronization in chaotic systems, Physical Review Letters 64(8), pp. 821–824, 1990.