An Audio Data Encryption with Single and Double Dimension Discrete-Time Chaotic Systems

[1]Akif Akgül, [1]Sezgin Kaçar, [1]İhsan Pehlivan

[1] Department of Electrical and Electronics Engineering, Sakarya University, 54187, Turkey
E-mail: aakgul@sakarya.edu.tr, skacar@sakarya.edu.tr, ipehlivan@sakarya.edu.tr

Abstract— In this article, a study on increasing security of audio data encryption with single and double dimension discrete-time chaotic systems was carried out and application and security analyses were executed. Audio data samples of both mono and stereo types were encrypted. In the application here, single and double dimension discrete-time chaotic systems were used. In order to enhance security during encryption, a different method was applied by also using a non-linear function. In the chaos based application realized with the method developed, analyses results were achieved with common security analyses such as key space, key sensitivity, chaos effect and histogram. Several examinations on the safety of chaotic systems in the application were carried out with these analyses results.

Key words— Audio Data Encryption, Chaos Based Encryption, Information Security, Security Analyses

Introduction

A safe communication is one of the most significant needs of our era. Many studies on hiding data types like text, audio, image and so on have been carried out in order to meet such need. In this article, a study on increasing the security of audio data has been executed. Many studies on audio data encryption have appeared in the literature so far (Gopalan et al., 2012, Chang et al., 2003, Chen et al., 2007, Dipu & Alam, 2007). Some of these included directly hiding audio files while others included methods of hiding the information by embedding some other data in the audio files. The general objective of all these studies is to prevent the possession of data by undesired people. Today, telephone conversations and conversations in any other place can easily be monitored with the help of some certain technological devices. It has become a necessity to take many security precautions to protect such information. Although people try to protect data by encrypting, it is generally accepted that they can still be decrypted in a certain amount of time with some techniques. Factors like the complexity of the encrypted data and algorithms used during encryption have become important in encryption. Contrary to recently used standard encryption algorithms, number of studies with chaotic systems has starting increasing. Chaotic systems have become more popular in encryption as they can successfully maintain infusion and diffusion, the basic components of encryption, by providing complexity with activities like noise and being sensitive to primary conditions.

There are numerous encryption and signal hiding studies in the literature used with the chaos technique. In some of their studies about signal hiding, Pehlivan and his colleagues employed masking technique that included adding information signals to chaotic signals (Pehlivan & Uyaroglu, 2007, Cicek et al., 2013, Pehlivan & Wei, 2012, Pehlivan & Uyaroglu, 2012). Sakthidasan and Santhosh; carried out encryption with chaos by mixing original data and data from chaotic system (Sakthidasan & Santhosh, 2011). Oğraş and Türk achieved encryption by making use of a non-linear function. (Ogras & Turk, 2012). To decrypt data which has been encrypted this way, one needs to know the non-linear function and all the parameters in it. By combining chaotic system based and non-chaotic encryption algorithms, Fındık performed text encryption (Fındık, 2004). In real environment applications, since image, video, audio and such data are big in size, encryption with such method is disadvantageous in terms of speed. Yardım and Afacan carried out some studies on timing in encryption and decryption by applying delay and switching on chaotic signal data (Yardim & Afacan, 2010). In order to decrypt data encrypted this way, one needs to know which data has been encrypted when and in which order. Any mistake will hinder the decryption of the encrypted data. Sohby and Shehata achieved chaos based encryption by adding the data to be encrypted to the Lorenz system (Sobhy & Shehata, 2001).

There are many few studies on hiding audio data by using chaotic systems. Abdulkareem and Abduljaleel developed a new encryption method by using single dimension chaos generator and non-chaotic encryption method Blowfish algorithm and combining audio data with chaos and non-chaos algorithm (Maysaa & Iman, 2013). Zhang and Min developed a non-symmetrical numerical encryption algorithm for audio communication and also made the security analyses of their system (Zhangx, 2005). Gnanajeyaraman and his colleagues carried

out audio encryption studies by employing multiple dimension chaotic system for safer communication (Gnanajeyaraman et al., 2009). Prabu and his colleagues carried out an audio encryption study with single dimension discrete chaotic Logistic Map system and realized a real time application (Prabu et al., 2012). Ganesan and his colleagues' audio encryption study included a simple double dimension chaotic system (Ganesan et al., 2006).

In this study, chaos based encryption applications were done for the safe transmission of mono and stereo audio data. Single and double dimension discrete chaotic systems, which have a simple structure and are very affective for encryption, were preferred. Key space, key sensitivity, chaos effect and histogram analyses about the success of the encryption procedures were performed with MATLAB programme. Codes written with Matlab is convertible to C/C++ codes and codes can be gathered and run in other environments without Matlab being installed, which are two important advantages of Matlab.

The second part of the article includes information about single and double dimension discrete chaotic systems used in chaos based encryption applications. In part 3, application method was explained and realized. In part 4, security analyses were performed. The last part covers the results and evaluations.

Discrete-Time Chaotic Systems Used In Encryption Applications

Single dimension Logistic Map and double dimension Arnold's Cat Map chaotic systems, which are very common in the literature, were used in this study.

Logistic Map

Logistic Map is a very commonly used single dimension chaotic system. Figure 1 exhibits bifurcation diagram that shows at which intervals Logistic Map enters chaos. r parameter was examined between 0-4 values. Bifurcation diagram in Figure 1 shows that r value must be chosen 3.5699-4 so that the system can enter chaos. Otherwise, the system will not enter chaos and keys necessary for encryption will not be produced and thus chaotic encryption will not be possible.

$$Xn + 1 = r * Xn * (1 - Xn) \quad (1)$$

X value represents the system variable, and r represents the system parameter in Equation 2. n value is changeable according to the data to be encrypted. Value of n depends on how many bits of data will be encrypted.

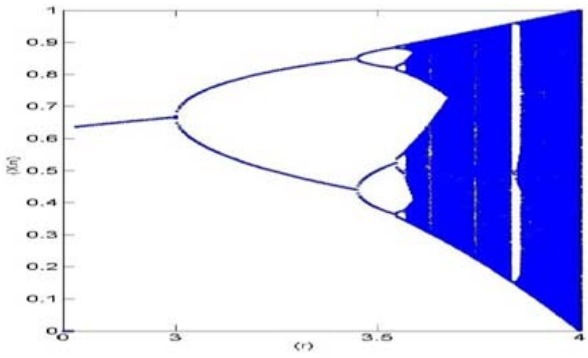


Figure 1: Logistic Map bifurcation diagram

Arnold's Cat Map

Another chaotic system utilized for encryption in this study is Arnold's Cat Map. Arnold's Cat Map is a double dimension chaotic system, therefore it is represented by two different equations in Equation 3 and 4 below.

$$Xn + 1 = Xn + Yn \pmod 1 \quad (2)$$

$$Yn + 1 = Xn + k * Yn \pmod 1 \quad (3)$$

x and y variables in Equation 3 and 4 are the system variables like in Logistic Map and n value is the number of repetition. k value is the system parameter. x(0) and y(0) initial values must be defined so that the encryption with Arnold's Cat Map can be started.

Chaos Based Encryption Application And Security Analyses

Method

A non-linear equation was used in order to increase security in encryption. One needs to know a and b parameters and also know what kind of equation was used in order to decrypt data encrypted with the function in Equation 5. "x" value in the function represents the keys produced with chaos generators and "m" value represents the audio data to be encrypted in bits.

$$f(x,m) = \frac{2x(1 + xm + (1 - m)) + a}{b} \quad (4)$$

In this study, a parameter is 0.9 and b parameter is 4.8. Choosing an appropriate value range for equation and parameters is necessary for achieving a chaos based encryption. When certain limits are exceeded, the system will get out of chaos and thus chaos based encryption will not be achieved.

Figure 2 exhibits the general block diagram of encryption application for safe transmission of any audio data. As can be seen on the block diagram, audio data and keys produced with chaotic systems are encrypted with the help of a function. Data encrypted later in the block diagram can be decrypted with the inverse of the function. In order to decrypt audio data encrypted in the application in this figure, one needs to know keys produced for each bit (46000 keys for 46000 bits of audio data) and the order of these keys, the chaotic system used, parameters in the chaotic system and initial values, and also non-linear equation and all parameters employed in this equation. Otherwise, it will not be possible to decrypt the encrypted data.

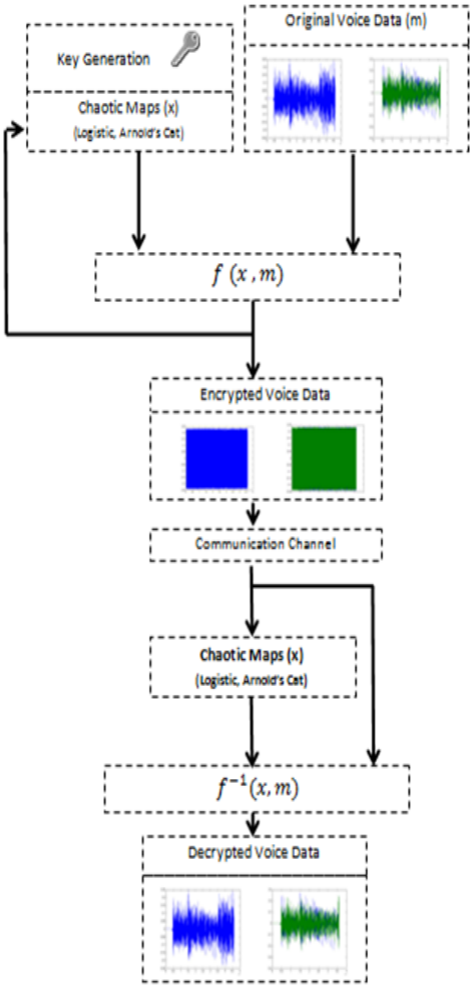


Figure 2: Block Diagram of Encryption and Decryption Audio Data

Encryption Applications on Mono and Stereo Audio Data

Figure 3 and 4 show 46000 bits mono and stereo audio data to be encrypted. Although green signal seems dominant in stereo audio data in Figure 4, in fact there are two separate signals as green and blue.

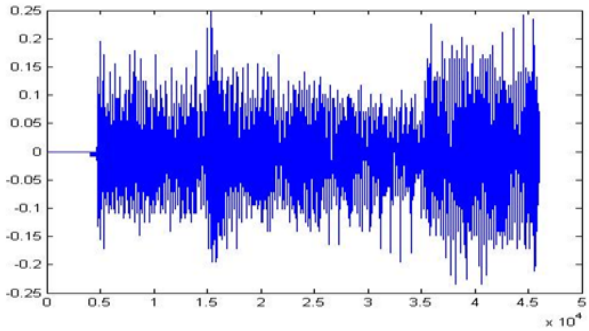


Figure 3: Mono Original Audio Data

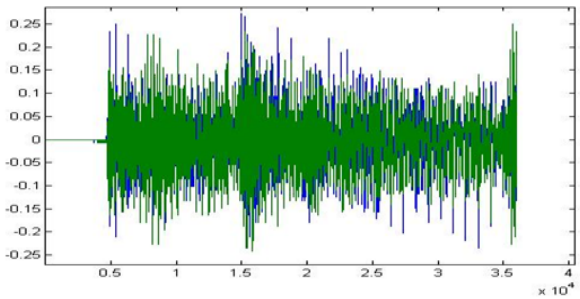


Figure 4: Stereo Original Audio Data

Original mono and stereo audio data in Figure 3 and 4 were encrypted by using two different chaotic systems, as explained in Part 3.1. As for chaotic systems, discrete-time single dimension Logistic Map and discrete-time double dimension Arnold's Cat Map, which are both very common in the literature, were utilized. Encrypted audio data from the encryption done with Logistic Map is as shown in Figure 5 and 6.

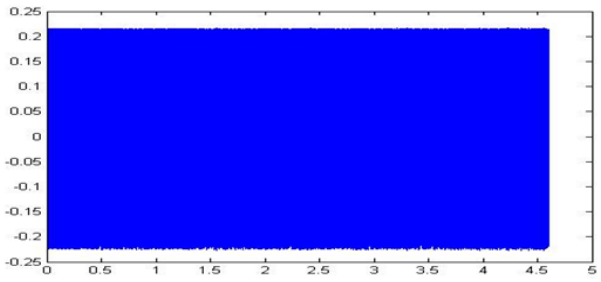


Figure 5: Mono audio data encrypted with Logistic Map

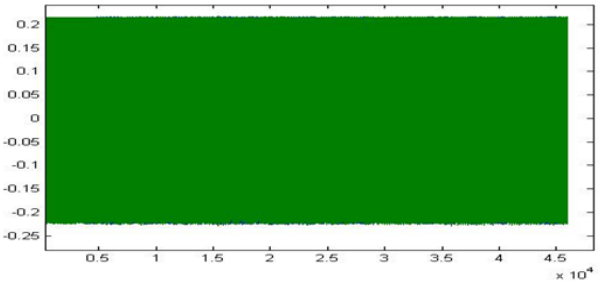


Figure 6: Stereo audio data encrypted with Logistic Map

Figure 7 and 8 exhibit audio data encrypted with Arnold's Cat Map chaotic system. In the encryption of stereo audio data by Logistic Map and Arnold's Cat Map, green audio data is dominant in encrypted data, yet at the background there is also very little blue encrypted audio data in Figure 8.

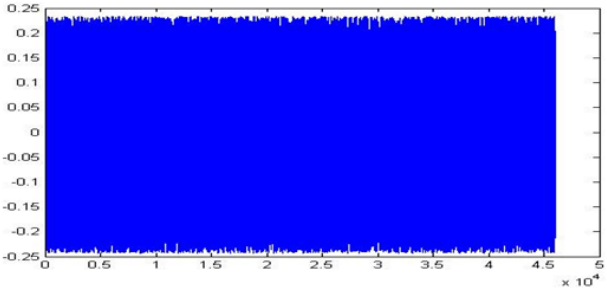


Figure 7: Mono audio data encrypted with Arnold's Cat Map

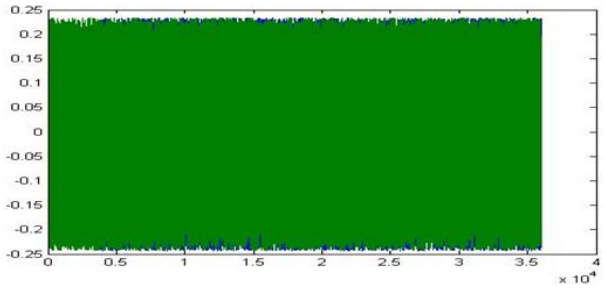


Figure 8: Stereo audio data encrypted with Arnold's Cat Map

Figure 9 and 10 show decrypted audio data obtained from the decryption process which was performed as explained on the block diagram in part 3.1. There was no corruption in the audio data, which proves that both encryption and decryption processes were performed successfully.

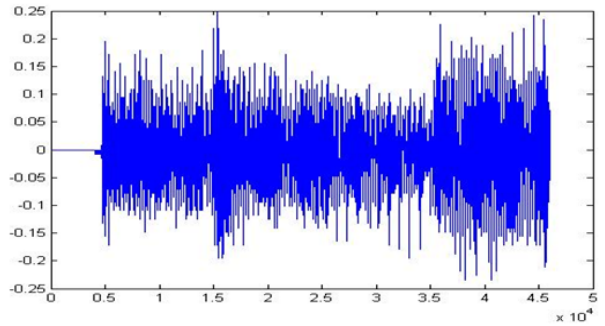


Figure 9: Decrypted mono audio data

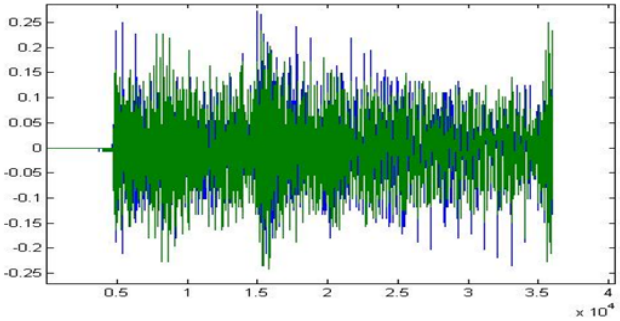


Figure 10: Decrypted stereo audio data

Security Analyses of Encryption Applications

Encryption processes may have been performed successfully. Yet, security analyses must be carried out in order to assess the reliability of encryption processes. Encrypted data with disappointing results in security analyses will not be preferred as they are so vulnerable to be decrypted. Key space analysis, key sensitivity analysis, chaos effect and histogram were performed in order to compare the chaotic systems utilized in this study.

Key Space Analysis

Key space needs to be large enough to prevent strong attacks. As size and other variables increase in chaotic systems, key space increases, too. When there is only one variable, key space can have 10^{14} different values. For instance, in a three dimension chaotic system with just one variable, total key space will be 10^{56} as initial conditions can be 10^{42} because of the size and 10^{14} because of the parameter. In such an application, key spaces

will vary due to size, depending on Logistic Map or Arnold's Cat Map chaotic system. Key space for Logistic Map is 10^{28}, according to r parameter and x(0) initial value. Key space for Arnold's Cat Map is 10^{42} according to k parameter, x(0) and y(0) initial values. Based on these results, it can be concluded that a encryption with Arnold's Cat Map will be more reliable than the one with Logistic Map.

Key Sensitivity Analysis

While encrypted data is being decrypted, a small change in the key leads to different results during the decryption. In a safe encryption, a very small change in keys must prevent attacks. This shows why chaos encryption is so important. Change in one of the keys directly affects the result; in other words, encrypted data can not be decrypted even if only one key has been changed. One needs to know all the keys to decrypt the encrypted data because different keys are produced for each data. It is also necessary to know the order of the keys. Knowing all the keys will not suffice because if the decryption does not happen in the correct order, the data cannot be decrypted. In some studies, more than one audio data or other data are processed for encryption. Therefore, sensitivity may increase as a result of a small change in any data since other data are included in encryption. Decrypted data is what counts as the result in analysis. If any small change prevents obtaining the original data, analysis result is successful. For instance, during the decryption of encrypted mono audio data from Arnold's Cat Map in Figure 7, data on the 10000th bit was changed and as a result of this change, corrupted signal was obtained as in Figure 11.

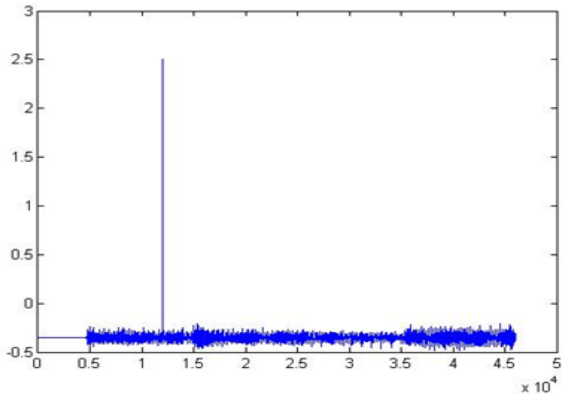


Figure 11: Corrupted audio data as a result of changing a bit while mono audio data was being decrypted.

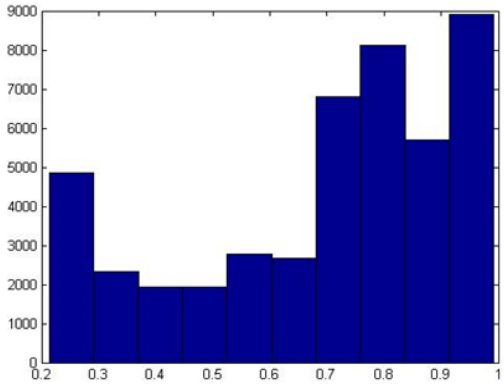
Chaos Effect (Encryption Effect Analysis)

The effect of chaos during encryption is called chaos effect. Examining encrypted audio data to see chaos effect in application, one can observe that encryption was performed in a very complex way with both systems. Audio data seemed dominant at all intervals and also very dominant sounds were obtained when encrypted audio data was listened to. It will not be easy for cryptanalysts to decrypt data encrypted with chaotic systems because encrypted audio data are very complex.

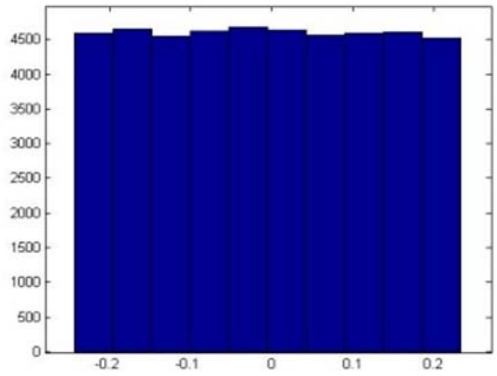
Histogram Analysis

Distributions of data values in a system comprise the histogram. Histogram analyses can be made by examining data distributions in many different fields. In encryption practices, if the distributions of numbers that represent encrypted data are close, this means encryption has been performed well. The closer the data distributions are, the more difficult it will be to decrypt the encrypted data.

Examining the histogram diagrams of mono audio data in Figure 12. a) and b), one can see that the distribution by Arnold's Cat Map in Figure 12.b) is much better than the one by Logistic Map in Figure 12.a). Therefore, it can be concluded that encryption with Arnold's Cat Map is better than encryption with Logistic Map and that it will be more difficult to decrypt data encrypted with Arnold's Cat Map.



a)



b)

Figure 12: Histogram Diagrams for Mono Audio Data **a)** Logistic Map **b)** Arnold's Cat Map

Figure 13 and 14 show the histogram diagrams of stereo audio data encrypted with Logistic Map and Arnold's Cat Map, respectively. Since stereo audio data have two different signals, two different histogram diagrams were included here. Not only for mono audio data but also for stereo audio data, histogram distributions in encryption with Arnold's Cat chaotic system are much better for both signals (blue and green).

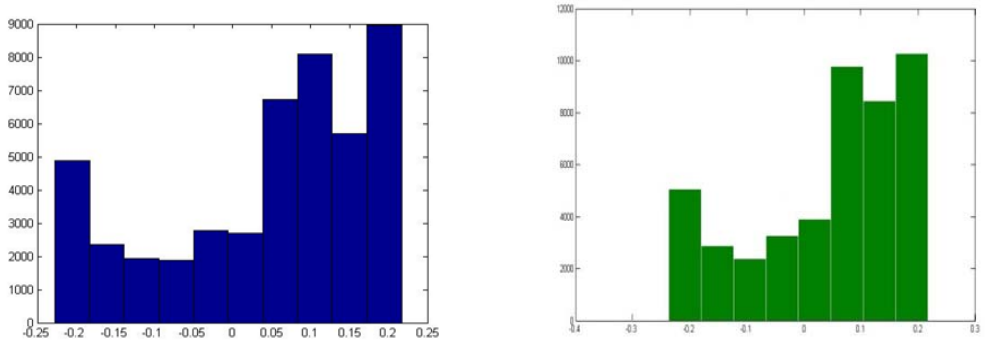


Figure 13: Histogram Diagrams of stereo audio data encrypted with Logistic Map

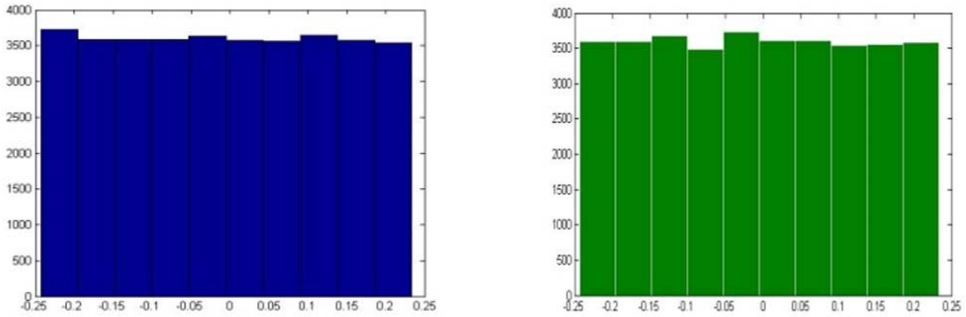


Figure 14:. Histogram Diagrams of stereo audio data encrypted with Arnold's Cat Map

Results and Evaluation

Safe communication is one of the many areas of application of chaotic systems. In this article, two different discrete-time chaotic systems were used to increase security of audio data and security analyses were executed. In order to decrypt the encrypted data in chaos based encryption applied here, one needs to know which chaotic systems were used, keys produced and their order, all parameters and initial values in chaotic systems, the non-linear equation used and all parameters belonging to this equation. Because of any mistake during the decryption of the encrypted data, such as changing even just one key data (as seen in key sensitivity analysis), encrypted data can not be decrypted and the original audio data can not be retained.

Based on the key space and histogram analysis, it is clear that double dimension Arnold's Cat Map can provide safer encryption than single dimension Logistic Map. As Part 4.1 explains, key space of double dimension Arnold's Cat Map chaotic system is larger than that of single dimension Logistic Map. As the histogram analysis in Part 4.4 shows, Arnold's Cat Map has a much better distribution and is better than Logistic Map and thus decryption the data will be more difficult.

When security analysis results for a encryption application on a chaotic system are better than that of another system, other analyses reveal similar results. For example, Arnold's Cat Map chaotic system in this study showed better histogram analysis results, and it also showed better results in all analyses. Since software necessary for the chaos based encryption method used here take up very small ram space, excluding audio data, (1KB for mono, 2KB for stereo), it will be more advantageous to use them in real environment applications. Moreover, this study was encrypted in Matlab, codes can be converted to C/C++ and codes can be gathered and be run in other environments without Matlab being installed, which are other advantages of this application.

References

Gopalan KG, Benincasa DS, Wenndt SJ (2001). Data embedding in audio signals. IEEE Aerospace Conference Proceedings (Cat. No.01TH8542). Vol. 6, pp. 2713–2720.

Chang CC, Lee RTC, Xiao GX, Chen TS (2003). A new Speech Hiding Scheme based upon sub-band coding. Proceedings of the 2003 Joint Conference of the Fourth International Conference on Information, Communications and Signal Processing and Fourth Pacific Rim Conference on Multimedia. Vol. 2, pp. 980–984.

Chen S, Leung H, Ding H (2007). Telephony Speech Enhancement by Data Hiding. IEEE Transactıons On Instrumentatıon And Measurement. Vol. 56, no. 1, pp. 63–74.

Dipu KHM, Alam SB (2010). Hardware based real time, fast and highly secured speech communication using FPGA. IEEE International Conference on Information Theory and Information Security, pp. 452–457.

Pehlivan I, Uyaroğlu Y (2007). Simplified Chaotic Diffusionless Lorenz Attractor and its Application to Secure Communication Systems. IET Communications, pp: 1015-1022.

Cicek S., Uyaroğlu Y., Pehlivan I (2013). Simulation and Circuit Implementation Of Sprott Case H Chaotic System And Its Synchronization Application For Secure Communication Systems. Journal of Circuits, Systems and Computers. Vol.22, No.04, 1350022_1-1350022_15 DOI: 10.1142/S0218126613500229.

Pehlivan I, Wei Z (2012). Analysis, Nonlinear Control and Circuit Design of an Another Strange Chaotic System. Turkish Journal of Electrical Engineering & Computer Sciences.Volume 20, Issue sup2, 1229-1239.

Pehlivan I, Uyaroğlu Y (2012). A New 3D Chaotic System with Golden Proportion Equilibria: Analysis and Electronic Circuit Realization. Computers & Electrical Engineering, Vol. 38, Issue 6 , 1777-1784.

Sakthidasan K, Santhosh BV (2011). A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images, International Journal of Information and Education Technology. Vol. 1, no.2, pp: 137-141.

Ogras H, Turk M (2012). Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function. World Academy of Science Engineering and Technology. Stockholm.

Findik O (2004). Şifrelemede Kaotik Sistemin Kullanılması. M.S. thesis, Comp. Dept., Selçuk. Univ., Konya.

Yardim FE, Afacan E (2010). Lorenz-Tabanlı Diferansiyel Kaos Kaydırmalı Anahtarlama (Dcsk) Modeli Kullanılarak Kaotik Bir Haberleşme Sisteminin Simülasyonu. Gazi¨ Univ. Müh. Mim. Fak. Der., Vol. 25, no.1, pp: 101-110.

Sobhy MI, Shehata AR (2001). Chaotic Algorithms for Data Encryption, Acoustics, Speech, and Signal Processing. IEEE International Conference on, Salt Like City.

Maysaa A, Iman Q (2013). A.,Speech Encryption Using Chaotic Map and Blowfish Algorithms, Journal of Basrah Researches.Vol. 39. No. 2,pp. 68-76.

Zhangx M (2005). Ageneralized Chaos Synchronization Based Encryption Algorithm For Sound Signal Communication. Circuits Systems Signal Processing. Vol. 24. No. 5, pp. 535-548.

Gnanajeyaraman R, Prasadhk, Ramar (2009). International Journal of RecentTrends in Engineering. Audio encryption using higher dimensional chaotic map. Vol. 1. No. 2, pp. 103-107.

Prabu AV, Srinivassaraos, Apparao T, Jaganmohan M, Babu RK (2012). International Journal of Computer Applications. Audio Encryption in Handsets. Vol. 40. No. 6, pp. 40-45.

Ganesan K, Muthukumarr, Murali K (2006). Look-up Table Based Chaotic Encryption of Audio Files, Circuits and Systems. APCCAS 2006. IEEE Asia Pacific Conference, Singapore, pp: 1951-1954.

