Audio Encryption Scheme based on Pseudo-orbit of Chaotic Map

Magalhães, E.P.[1] **, Santos, T.A.**[1] **, Nepomuceno, E.G.**[1*]

[1]Control and Modelling Group (GCOM)
Department of Electrical Engineering
Federal University of São João del-Rei
Pça. Frei Orlando, 170 - Centro - 36307-352 - São João del-Rei, Minas Gerais, Brasil

eduardopintomagalhaes@gmail.com, contato@tsantos.com.br, nepomuceno@ufsj.edu.br

Abstract. *Chaos-based encryption uses a chaotic dynamic system to encrypt a file. The aim of this study was to investigate the use of the chaotic Cubic Map to encrypt data, in particular, audio files. A simple algorithm was developed to encrypt and decrypt an audio data. The effectiveness of the method was measured by means of the correlation coefficient calculation, spectral entropy and also by comparing waveforms. The measurements were shown to lead to satisfactory confusion levels of the original data, within a few seconds. This indicates that the Cubic Map can be used as a source for encryption keys, with as good or better security indicators when compared to other schemes.*

1 Introduction

Chaos-based encryption has received much attention since the work of Matthews [8], and has been persistently studied ever since. An encrypted data is obtained from the logical exclusive or operation between some data and a chaotic pseudo-orbit. Chaos-based encryption has many possible uses in the digital security field and different chaotic systems have also been investigated as a potential improvement to security and performance [4, 13, 2, 14, 6, 3].

Several works regarding cryptography using dynamic chaotic systems were proposed in the literature. For example, Sheu [12] proposed a speech encryption algorithm using fractional chaotic systems and Kordov and Bonchev [5] proposed an algorithm of audio-based encryption using a circular map. However, to the best of the authors knowledge and bibliographic review, no application of the Cubic Map was developed for this purpose.

This research aims to apply the Cubic Map to a very simple encryption algorithm and measure its performance by comparing the results with more complex schemes already published. This paper is organized as follows: Section 2 deals with the preliminary concepts; Section 3 discusses the proposed methodology for cryptography and statistical analysis; Section 4 presents the results, as well as their analyzes and finally in Section 5, the conclusion of this work.

*This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001, the Ministry of Science, Technology, Innovation and Communications (MCTI) and the Federal University of São João del Rei.

2 Preliminary Concepts

In this section, the theoretical concepts needed to carry out this work are presented.

2.1 Chaotic dynamic systems

Chaotic dynamic systems have been studied from the work of [7]. The accepted definition of chaos found in the literature can be properly explained by Banks et al.

Definition 1: *[1]. Let $f : X \to X$ be a chaotic system. This system is chaotic when it has the three following properties, such as being transitive, dense in X and sensitive to the initial conditions: f is transitive; the periodic orbits of f are dense in X and f is sensitive to the initial conditions.*

2.2 Cubic Map

The Cubic Map is a map that has a chaotic behavior from the value r, known as the bifurcation parameter. This map is a discrete and dynamic system described by the equation below:

$$f_r(x) = rx^3 + (1 - r)x \tag{1}$$

3 Methodology

3.1 Audio Encryption Process

The current study required simulating and analyzing audio file encryption and decryption as if in a real-world file exchange. Countdown for a space launch was chosen as subject as it has subtle and strong features. The audio was obtained through NASA's website and refers to the liftoff of Atlas V from Cape Canaveral [1]. One interval extensions of the Cubic Map was simulated using a set of conditions and parameters known to be chaotic, and care was taken to analyze chaotic indicators [10, 9].

The pseudo-orbit was simulated using $r = 3.6$ and 1900 initial conditions varying linearly from -1 to 1, on MATLAB R2018a running on a GNU Linux machine with Intel(R) Core(TM) i7-7700HQ CPU @

[1]All the audio files referenced in this work can be acessed through: `https://bit.ly/2JOlbEF`.

2.80GHz. Having more initial conditions means reducing the length of each simulation, yielding more precise results [10].

By obtaining the same numerical type, the encryption process could begin. This consists of applying logical Exclusive Or ($\oplus$) operation bit by bit. So, the encrypted audio is obtained by Equation 2.

$$EncryptedAudio = \sigma_{Norm} \oplus ConvertedAudio \quad (2)$$

Encrypted data was then statistically analyzed and searched for vulnerabilities and similarities with the original data.

The encryption process wouldn't be successful if the data could not be recovered. Thus, by simulating the same pseudo-orbit and applying Exclusive Or operation again, as in Equation 3 the data was restored to its original state.

$$ConvertedAudio = \sigma_{Norm} \oplus ConvertedAudio \quad (3)$$

In order for the file to be readable, the inverse process of audio conversion must be made, converting it back to double precision, subtracting 32768 and converting back to 16 bit signed integer.

3.2 Spectral Entropy

The spectral entropy of the signal was defined as the energy distribution as a function of frequency. Therefore, the frequency spectrum was calculated by FFT (Fast Fourier Transform). However, large FFT sizes can produce high-frequency resolutions, while low FFT sizes have the opposite effect. In order to achieve a high resolution in the frequency axis, the overlay percentage feature was used. This feature allows the frequency axis to be stretched on the spectrogram graph by processing parts of the frequency series. The resolution was then set in a window size of 2048 points and a percentage of overlap in 75%. The spectral spectrum is normalized between 0 and 1. Thus, the spectral entropy was normalized between 0 (total regularity) and 1 (maximum irregularity).

4 Results

4.1 Waveform Analysis

The waveform plots can be seen in Figure 1. The graph represents the audio amplitude distributed in time. It can be observed that the original data in Figure 1 (a) loses its features and cannot be distinguished in Figure 1 (b). By means of the Figure 1 (b) it is observed that the encrypted signal remains secure under the data transmission process, since the keyspace that is based on the initial conditions of the Cubic Map and the bifurcation parameter r was determined to be large enough.

The Figures 2 (a) and (b) illustrate the main band occupied by the signals. The frequency of the signal occupying 99% of its band is 5.148 kHz, while the frequency of the cryptographic signal occupying 99% of its band is 21.894 kHz.

5 Conclusion

A new scheme for chaos-based encryption was developed. The XOR encryption scheme together with the Cubic Map is investigated analytically and compared with other results on the literature [5, 11]. The Cubic Map proved to be robust under the aspect of the secure key from its initial conditions since it was possible to satisfactorily describe the complexity of the regularity of the original and cryptographic signal.

References

[1] John Banks, Jeffrey Brooks, Grant Cairns, Gary Davis, and Peter Stacey. On devaney's definition of chaos. *The American mathematical monthly*, 99(4):332–334, 1992.

[2] X Chai, Y Chen, and L Broyde. A novel chaos-based image encryption algorithm using dna sequence operations. *Optics and Lasers in engineering*, 2017.

[3] R Guesmi, MAB Farah, A Kachouri, and M Samet. A novel chaos-based image encryption using dna sequence operation and secure hash algorithm sha-2. *Nonlinear Dynamics*, 2016.

[4] Z Hua and Y Zhou. Image encryption using 2d logistic-adjusted-sine map. *Information Sciences*, 2016.

[5] Krasimir Kordov and Lachezar Bonchev. Using circle map for audio encryption algorithm. *Mathematical and Software Engineering*, 3(2):183–189, 2017.

[6] W Liu, K Sun, and C Zhu. A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering*, 2016.

[7] Edward N Lorenz. Deterministic nonperiodic flow. *Journal of the atmospheric sciences*, 20(2): 130–141, 1963.

[8] Robert Matthews. On the derivation of a "chaotic" encryption algorithm. *Cryptologia*, 13 (1):29–42, January 1989.

[9] Eduardo M. A. M. Mendes and Erivelton G. Nepomuceno. A very simple method to calculate the (positive) largest lyapunov exponent using interval extensions. *International Journal of Bifurcation and Chaos*, 26(13):1650226, December 2016.

[10] E.G. Nepomuceno, S.A.M. Martins, G.F.V. Amaral, and R. Riveret. On the lower bound error for discrete maps using associative property. *Systems Science & Control Engineering*, 5(1):462–473, January 2017.

[11] Animesh Roy and A. P. Misra. Audio signal encryption using chaotic hénon map and lifting

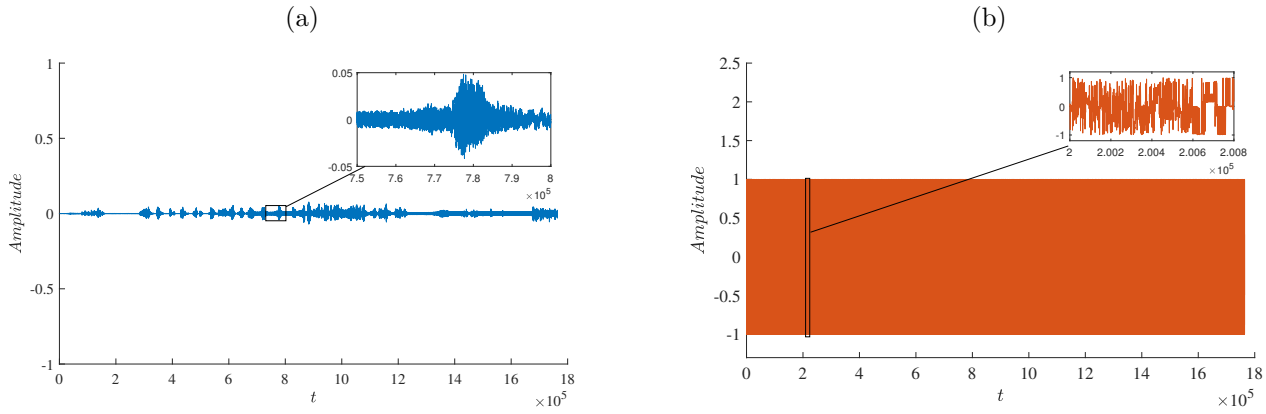

Figure 1: Wave forms (amplitude vs time) [(a) and (b)]. It should be noted that (a)'s amplitude is considerably lower than (b). Also, one should observe that, due to the encryption process, the original data (a) cannot be recognized in (b), as it lost all of its features.

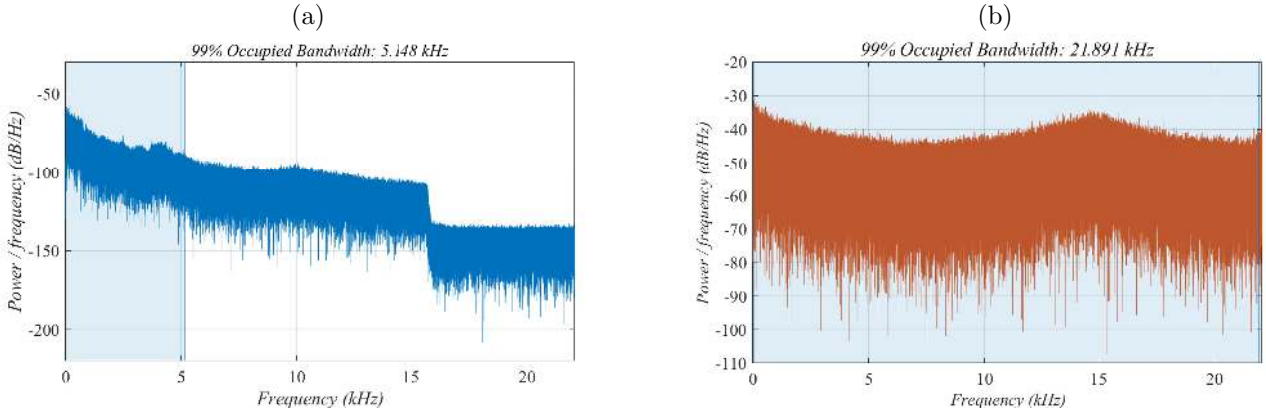

Figure 2: Occupied bandwidth (power/frequency vs frequency) [(c) and (d)] of the original and encrypted audio signals. As can be seen, the signal after the encryption becomes an audio with noise.

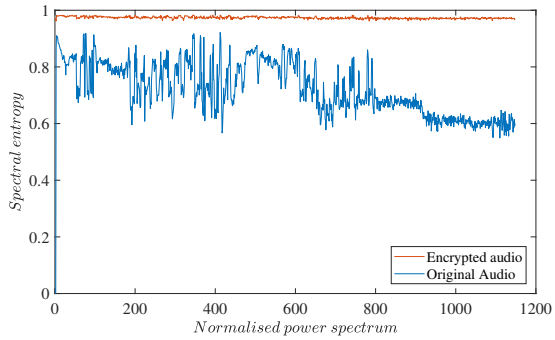

Figure 3: Spectral entropy of the original (blue) and encrypted (brown) audio signals with the following spectral values: between 0,809 and 0,591 for the encrypted signal and 0,9736 (mean value) for the original signal (close to 1). Entropy shows high homogeneous leves of disorder on the encrypted audio, in contrast with the original one.

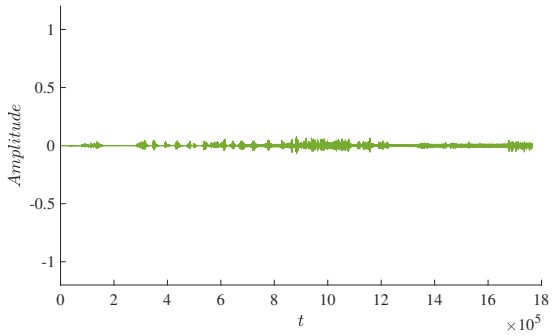

Figure 4: Waveform (amplitude vs time) of the decrypted audio. As can be seen, the audio has been completely decrypted without any loss of information.

wavelet transforms. 2017. doi: 10.1140/epjp/i2017-11808-x.

[12] Long Jye Sheu. A speech encryption using fractional chaotic systems. *Nonlinear dynamics*, 65 (1-2):103–108, 2011.

[13] L Xu, Z Li, J Li, and W Hua. A novel bit-level image encryption algorithm based on chaotic maps. *Optics and Lasers in Engineering*, 2016.

[14] N Zhou, S Pan, S Cheng, and Z Zhou. Image compression–encryption scheme based on hyperchaotic system and 2d compressive sensing. *Optics & Laser Technology*, 2016.