Efficient speech encryption using chaotic cat map for code-excited linear prediction (CELP) based coders in packet networks

Fatiha Merazka

Citation: Proc. Mtgs. Acoust. **19**, 055063 (2013); doi: 10.1121/1.4800747
View online: https://doi.org/10.1121/1.4800747
View Table of Contents: https://asa.scitation.org/toc/pma/19/1
Published by the Acoustical Society of America

Proceedings of Meetings on Acoustics

Volume 19, 2013 http://acousticalsociety.org/

ICA 2013 Montreal
Montreal, Canada
2 - 7 June 2013

Signal Processing in Acoustics
Session 2pSP: Acoustic Signal Processing for Various Applications

2pSP6. Efficient speech encryption using chaotic cat map for code-excited linear prediction (CELP) based coders in packet networks

Fatiha Merazka*

***Corresponding author's address: Telecommunications, University of Science & Technology Houari Boumediene, P.O.Box 32 El Alia, Algiers, 16111, Bab Ezzouar, Algeria, fmerazka@usthb.dz**

The increasing importance of multimedia applications is placing a great insist on content protection and customer privacy. Communications can be intercepted, especially over wireless links. Since encryption can effectively prevent eavesdropping, its use is widely advocated. The codec G. 729 based CS-ACELP algorithm is standardized as voice codec by ITU-T for multimedia and Voice over Internet Protocol (VoIP) applications. In this paper we introduce a speech encryption method based chaotic cat map algorithm. Cat map extended to two-dimensional NxN matrix. It takes concepts from linear algebra and uses them to change the positions of the values of the matrix. The result after applying the Cat Map will be shuffled signals that contain the same values of the original signals. We applied our encryption scheme to the standard ITU-T G.729 standard speech coder to evaluate its performance. Simulation results show that G.729 based cat map encryption is very efficient since the encrypted speech is similar to a white noise. The perceptual evaluation of speech quality (PESQ) and enhanced modified bark spectral distortion (EMBSD) tests for speech extracted from TIMIT database confirm the efficiency of our proposed scheme.

Published by the Acoustical Society of America through the American Institute of Physics

 [DOI: 10.1121/1.4800747]
Received 23 Jan 2013; published 2 Jun 2013

INTRODUCTION

Most multimedia applications such as speech and audio are essential, and their service is the basis in telephony industry, video conference and news broadcasting. Thus, the encryption of speech or audio is very important.

The field of encryption and security is becoming very important in the twenty first century when a massive amount of information is transmitted over the Local Area Networks as well as the Internet.

Encryption is the process of transforming information (plaintext) into a special form called Cipher by using some type of algorithm to make it unreadable to anyone except those who have the knowledge of the algorithm and its secret keys [1]. Militaries, governments, private companies have used the encryption for a long time to facilitate secret communication. Traditional symmetric key algorithms like Advanced Encryption Standard (AES) and Data Encryption Standard (DES) use small blocks size with complex permutations process to give secure ciphertext [2-4]. The Linear Feedback Shift Register (LFSR) has been one of the most popular encryption techniques widely used in speech communication. LFSR algorithms have found wide applications in wireless communication, including scrambling, error correction coding, encryption, testing, and random number generation [5-8].

Chaotic maps algorithms are very suitable for various data encryption schemes. In particular, chaotic maps are easy to be implemented by microprocessors and personal computers. Therefore, chaotic cryptosystems generally have high speed with low cost, which makes them better candidates than many traditional ciphers for multimedia data encryption. In this work, we consider the use of chaotic cat map encryption, first proposed by Vladimir Arnold in the 1960s, for the standard ITU-T G.729. The paper is organized as follows. In section 2, we derive the chaotic cat map algorithm. We give a brief description the standard IUT-T G.729 in section 3. We present the simulation results to demonstrate its performance in section 4. Concluding remarks are provided in section 4.

ENCRYPTION BASED CHAOTIC CAT MAP

The signal is scaled by a matrix NxN. If M is the message size, $N = \lfloor M^{(1/2)} \rfloor$. In our case, we work with frames of 80 bits. The encryption function is represented by the equation 1

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = A \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N) \tag{1}$$

The matrix A is chosen such as $|A| = 1$. Thus, the confusion key of cat map is composed of the parameter a and b. The matrix A is of the form given by equation 2

$$A = \begin{bmatrix} ab+1 & a \\ b & 1 \end{bmatrix} \tag{2}$$

where a and b are two values selected randomly between 0 and 256. Indeed, the Cat Map performs a permutation. The coordinates (x_n, y_n) of a given bit in the original signal become (x_{n+1}, y_{n+1}) in the encrypted signal. The matrix obtained from encryption equation is transformed into encrypted vector to generate the encrypted message. Decryption is done by the same equation except that the matrix A is replaced by its inverse [9]. Decryption is done by the same equation except that the matrix A is replaced by its inverse [9]

OVERVIEW OF THE STANDARD G.729

The standard G.729 speech coder is an 8 kbps Conjugate-Structure Algebraic-Code-Excited Linear Prediction (CS-ACELP) speech compression algorithm approved by ITU-T. G.729 offers high quality, robust speech performance at the price of complexity. It requires 10 ms input frames and generates frames of 80 bits in length. With the G.729 coder processing signals in 10 ms frames and 5 ms look-ahead, the total algorithmic delay is 15 ms.

each 80 bit frame produced contains linear prediction coefficients, excitation code book indices, and gain parameters that are used by the decoder in order to reproduce speech. The inputs/outputs of this algorithm are 16 bit linear PCM samples that are converted from/to an 8 kbps compressed data stream. G.729 is mostly used in Voice over IP (VoIP) applications for its low bandwidth requirement [10].

SIMULATIONS AND RESULTS

In this section, several experiments are carried out to test the encryption efficiency of the proposed speech cryptosystem. The quality of both the encrypted and decrypted speech signals is assessed. Simulations and results of our implemented method are given in this section. The speech used is extracted from TIMIT database [11]. The original speech and its spectrogram are given in FIGURES 1 and 2 respectively for comparison later with the decrypted speech. After the speech is coded with the ITU-T G.729, it is encrypted based chaotic cat map algorithm. The encrypted speech and its spectrogram are presented in FIGURES 3 and 4 respectively.

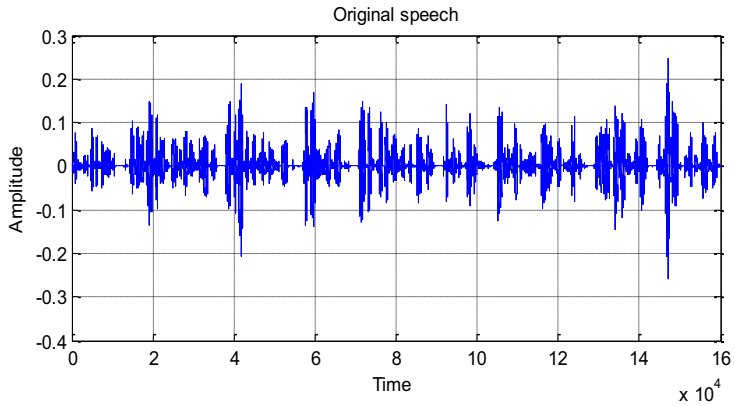

FIGURE 1. Waveform of original speech

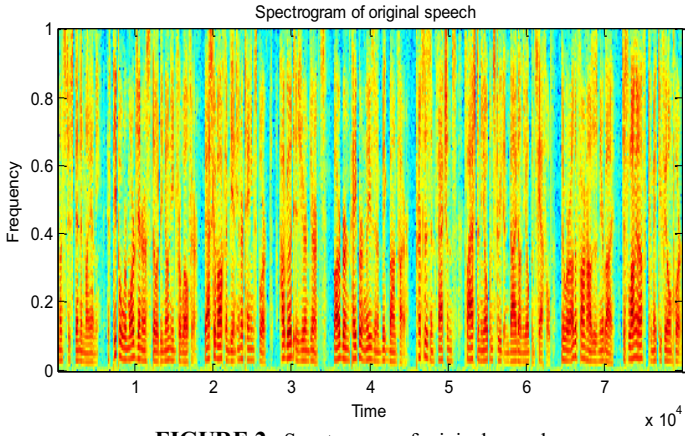

FIGURE 2. Spectrogram of original speech.

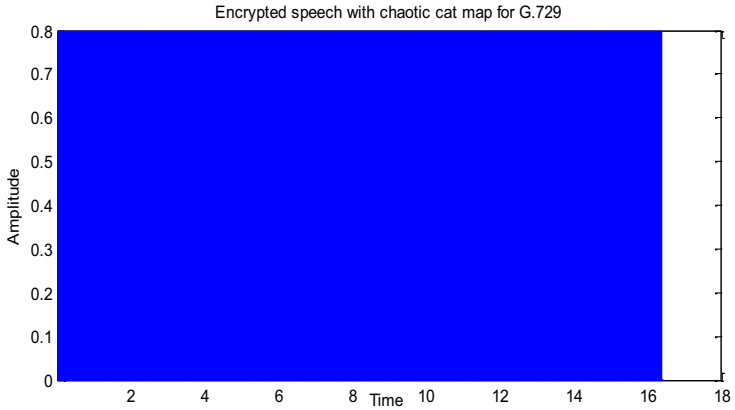

FIGURE 3. Speech encrypted based chaotic cat map algorithm

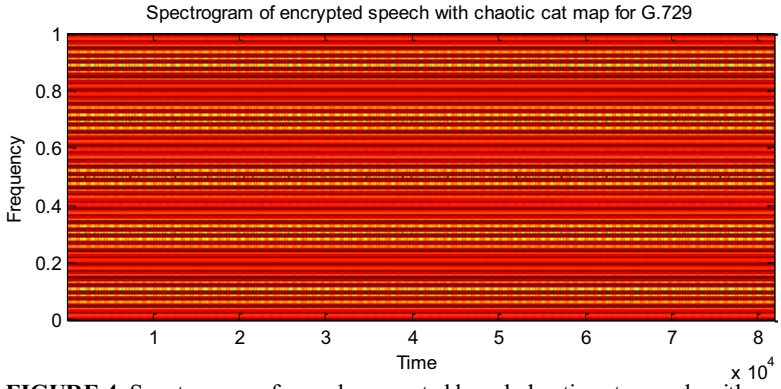

FIGURE 4. Spectrogram of speech encrypted based chaotic cat map algorithm

We can see from FIGURES 3 and 4 that the encrypted speeches signal is obviously similar to the white noise which indicates that no residual intelligibility can be useful for eavesdroppers at the communication channel.

The decrypted and decoded speech with G.729 and its spectrogram are presented in FIGURES 5 and 6 respectively.

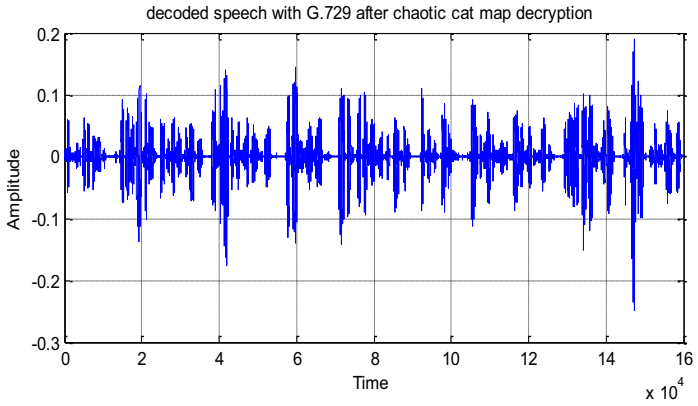

FIGURE 5. Waveform of decrypted speech

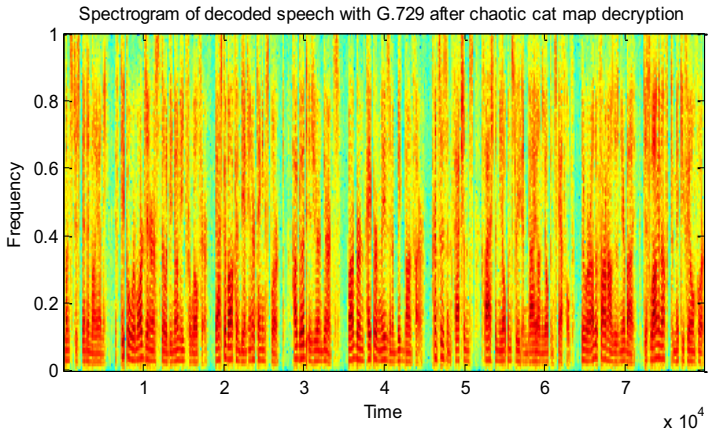

FIGURE 6. Spectrogram of decrypted speech

Comparing FIGURES 1 and 5, we can see clearly that the decoded speech signal is the same as the original one with hardly noticeable differences. The spectrograms of the original speech (FIGURE 2) and the decrypted speech (FIGURE 6) are identical and also with unnoticeable differences.

We use PESQ for an objective quality measure [12] and EMBSD tests [13]. The obtained results are summarized in TABLE 1.

TABLE 1. PESQ and EMBSD results

Algorithm	PESQ	EMBSD
G. 729 alone	3.322	1.636
G. 729 + chaotic cat map	3.322	1.636

Results from TABLE 1 confirm the efficiency of the chaotic cat map based algorithm for the standard ITU-T G.729 since the same values are obtained with and without encryption with the chaotic cat map algorithm.

CONCLUSION

We have presented an efficient way of encryption and decryption of speech signals for the ITU-TG. 729 codec based on chaotic cat map. From our results, it is obvious that even with insignificant differences in speech quality; the presented method performs well with the standard ITU-T G. 729 for the encryption and decryption of speech.

REFERENCES

1. U. Sahu, K. S. Dash, “Image Encryption, and Authentication Using Orthogonal Transformation on Residual Number System”, National Institute of Technology of Rourkela, 2008.
2. Advanced Encryption System, Federal Information Processing Standards Publication 197, 2001
3. J. Daemen and V. R. Rijndael, "The advanced encryption standard", Dr. Dobb’s J. volume 26 No 3, pp. 137–139 , 2001.
4. National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standards Publication. 46, U.S. Government Printing Office, Washington, DC (1977)
5. IEEE Std. 802.11–2007, Part 11: “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” IEEE Std. 802.11, 2007.
6. G. C. Ahlquist, M. Rice, and B. Nelson, “Error Control Coding in Software Radios: An FPGA Approach,” in Proc. of the IEEE Personal Communications, 1999; 6(4): 35-39.

7. V. Sriram and D. Kearney, ”An FPGA Implementation of a Parallelized MT19937 Uniform Random Number Generator,” EURASIP Journal on Embedded Systems. 7, 1-6. (2009).
8. K. K. Saluja and C.-F. See, "An Efficient Signature Computation Method," IEEE Design and Test of Computers, 9(4), 22-26 (1992).
9. Zhaopin Su,“Selective Encryption for G.729 Speech Using Chaotic Maps”, International Conference on Multimedia Information Networking and Security, 488–492 (2009).
10. ITU, ITU-T G.729: CS-ACELP Speech Coding at 8 kbit/s (ITU 1998).
11. NIST,Timit Speech Corpus (NIST 1990).
12. ITU-T Draft Rec P.862 Perceptual evaluation of speech quality (PESQ), an objective method of end-to-end speech quality assessment of narrowband telephone networks and speech codecs (May. 2000).
13. W. Yang, *Enhanced Modified Bark Spectral Distortion (EMBSD): An Objective Speech Quality Measurement Based on Audible Distortion and Cognition Model* (Ph.D. dissertation, Temple University, USA, May 1999).