Optik 127 (2016) 7431–7438

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys

Hongjun Liu[a,b,*], Abdurahman Kadir[c], Yanling Li[a,b]

[a] School of Information Engineering, Weifang Vocational College, Weifang 261041, China
[b] Modern Logistics Information Engineering Technology Research Center of Weifang, Weifang 261041, China
[c] School of Computer Science and Engineering, Xinjiang University of Finance and Economics, Urumqi, 830012, China

ARTICLE INFO

Article history:
Received 25 March 2016
Accepted 23 May 2016

Keywords:
Audio encryption
Confusion and diffusion
Multi-scroll chaotic system
One-time keys

ABSTRACT

Here is a proposal of lossless dual-channel audio encryption scheme based on one-time keys, the novelty is to apply chaotic system with changeable multi-scroll to generate key stream to confuse and diffuse audio data, and the one-time keys, such as initial values of state variables, scroll number and initial iteration times of the chaotic system, are dependent on both external keys and hash value of the plain audio file, to make the chaotic trajectory more unpredictable. The algorithm owns large key space to make brute-force attack impossible. Statistical analysis demonstrates the effectiveness for fast audio encryption, and the scheme can also be applied in encrypting audio with more channels.

1. Introduction

The confusion and diffusion of secure communication theory can also be applied in audio encryption. Akgül et al. [1] proposed an audio data encryption with single and double dimension discrete-time chaotic systems, audio data samples of both mono and stereo types were encrypted, and a non-linear equation was used to increase security in encryption. Sadkhan et al. [2] designed pseudo-random bit generator based on Unified chaotic map and applied it in digital voice encryption. Tamimi et al. [3] employed a shuffling procedure to encrypt audio with stream cipher method, the private key is key dependent and data dependent. Lima et al. [4] introduced an audio encryption scheme based on the cosine number transform (CNT), the transform is defined over a finite field, and is recursively applied to blocks of samples of non-compressed digital audio signal, the blocks are selected using a simple overlapping rule, which provides diffusion of the ciphered data to all processed blocks. Ciptasari et al. [5] aimed to construct a resilient audio ownership protection scheme to enhance the security by integrating the discrete wavelet transform and discrete cosine transform, visual cryptography, and digital time stamps, the watermark does not require to be embedded within the original audio but is used to generate a secret image and a public image, the scheme can be widely applied to the area of audio ownership protection.

In cryptography, chaotic maps, such as Chebyshev map [6], Tent map, and chaotic systems, such as Lorenz system [7] and Chen system [8], are usually employed to generate pseudo-random sequence as key stream, for tiny change of one of the initial values can lead to completely different trajectory. Augustine et al. [9] presented an audio encryption scheme using compressive sensing (CS) and Arnold transform-based scrambling, compressive sensing is done by using a key-based measurement matrix and the scrambling is carried out with the help of a key-based Arnold matrix, whose initial state is

[*] Corresponding author at: School of Information Engineering, Weifang Vocational College, Weifang 261041, China.
E-mail address: smithliu@126.com (H. Liu).

http://dx.doi.org/10.1016/j.ijleo.2016.05.073
0030-4026/© 2016 Elsevier GmbH. All rights reserved.

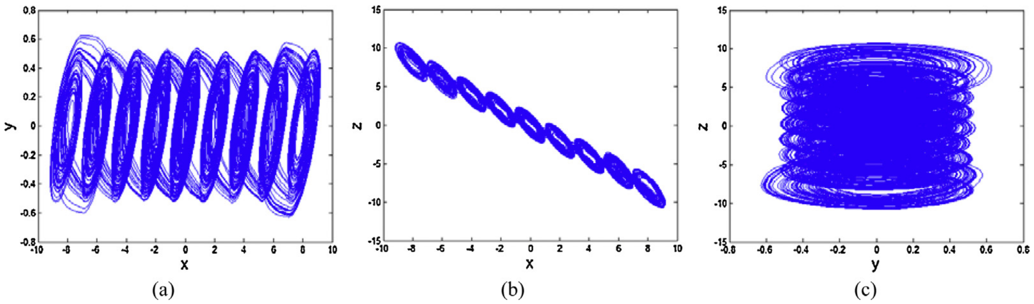

Fig. 1. The chaotic attractors when $n = 9$.

generated by a piece wise linear chaotic map (PWLCM), using three 32-bit keys. Eldin et al. [10] provided a new technique for audio for TV cloud computing, encrypting the audio signals is addressed based on chaotic map and the algorithm was tested using an audio tone (AT) to evaluate the performance, the software of encrypt audio using AT based on chaotic map is specially designed to meet the needs of ClComp of Egyptian Radio and Television Union (ERTU).

In recent years, as the important part of post-quantum cryptography, hash-based cryptography has been applied in image encryption schemes [11–13], in these schemes. The hash value of the plain-text can be transformed into one-time keys, to make the differential attacks ineffective.

In this paper, we design a novel dual-channel audio encryption scheme based on multi-scroll chaotic system, the algorithm is designed to confuse and diffuse the audio matrix by the sequences generated by chaotic system, whose initial conditions dependent on both the hash value of the plain audio and external keys. The diffusion process is implemented by a nonlinear equation. Audio file with more channels can also be encrypted by this algorithm. Security analysis demonstrates that the algorithm is very sensitive to tiny change of the keys, and statistical analysis, such as correlation, histogram and peak signal-to-noise(PSNR), shows that the algorithm can resist against statistical attacks. Experimental results demonstrate the effectiveness of the audio encryption scheme.

2. The multi-scroll chaotic system

The three dimension (2N + 1)-scroll chaotic system [14] using sign functions can be described by Eq. (1).

$$\begin{cases} \dot{x} = A[y - bx - 0.5(a - b)f(x)] \\ \dot{y} = x - y - z \\ \dot{z} = -By \end{cases} . \tag{1}$$

The nonlinear sign function is given by Eq. (2).

$$f(x) = \sum_{i=0}^{(n-3)/2} [sgn(x + (2i + 1)) + sgn(x - (2i + 1))]. \tag{2}$$

Here $\mathbf{X} = [xyz]^{\mathrm{T}}$ are state variables, $a$and $b$are control parameters. Moreover, the control factor n is the number of multi-scroll, $n = 3, 5, 7, 9, 11, \ldots$.When $a = -2/7, b = 2/7, A = 9$ and $B = 15$, the system can generate (2N + 1)-scroll chaotic attractor only by adjusting the control factor n. When we set $n = 11$, the chaotic attractors of x-y, x-z and y-z directions are shown in Fig. 1.

The Lyapunov exponents can be utilized to measure the exponential rates of divergence and convergence of nearby trajectories in state space [15]. Fig. 2 demonstrates that the system maintains chaotic state when $n \in [3, 335]$, because the largest Lyapunov exponents are always greater than zero. So we can make the scroll number change dynamically dependent on the plain audio, to enhance the randomness of trajectory.

3. Chaos-based audio encryption and decryption scheme

3.1. Generating the initial conditions

Here we utilize a 256-bit external secret key H, which is the hash value of the plain audio A_P by SHA-256, to generate the initial conditions. Two audio files with only a bit difference can get two completely different hash values.

The 256-bit hash value can be expressed as hexadecimal number array H.

$\boldsymbol{H} = [h_1, h_2, \ldots, h_{64}]$.