Application of Compound Chaotic Mapping in Voice Encryption Algorithm

Ruishan Du.Yang Li

School of Computer and Information Technology, Northeast Petroleum University, Daqing, 163318 China

Summary
Using the Devaney chaos theory, designed a compound chaotic mapping as the encryption function, and had proven that the track was non-periodic for the initial value of a finite decimal. We have designed an encryption algorithm successively according to this, and realized the encryption for sound documents. Afterward the simulation experiment has been set on. We realized the key sensitivity analysis, the statistical analysis, as well as the correlation analysis of definite text and secret text. The experimental result showed that this system has the good cryptology performance, produces the large key space. Meanwhile, it has excellent avalanche effect, resists exhaustion and the statistical analysis effectively.

Key words:
Compound chaos, Speech coding, Pronunciation encryption, Key analysis

1. Introduction

The needs of language communication are gradually increased with the development of society, the development of language communication technology is also accelerating, however, attacks against it are more and more serious, so information security has attracted increasing attention of people [1,2].

Chaotic dynamics have been widely used in the encryption algorithm. The features of chaotic map include sensitivity to initial conditions, topological transitivity and density of periodic points, chaotic sequence generated by it is a pseudo-random sequence which has better randomness, correlation, and complexities, but structure is complex and difficult to analyze and predict, so the chaotic sequence generated by chaotic dynamical systems to achieve encryption can meet the safety requirements of sequence encryption algorithm [3]. Document [4] proposed an algorithm of composite nonlinear chaotic pseudo-random number generator, however, due to the limited accuracy of the computer, it's difficult to avoid short-cycle effects. So, in this paper, improved the designed a hybrid chaotic system pseudo-random code generator which can avoid short-cycle effectively, and proved it is no periodic in theory, and then it is applied to the voice encryption, by the experiments, the cipher text has better distribution characteristics, it can resist statistical analysis effectively, thus ensuring the encryption system is high security.

2. Definition and characteristics of chaos

At present, there is no uniform definition of chaos, here introduced the definition of Devaney[5]: set V is a metric space, X , Y are any open subset of V , f is a continuous mapping: $V \to V$, if meets the following three conditions, it is said f is chaotic on the V .

(1) f has sensitive dependence on initial conditions. That is $\forall \varepsilon > 0,$ for any $x \in V$,there is $\delta > 0,$ and there is y and natural numbers n in the neighborhood δ of x , and $d(f^n(x) - f^n(y)) > \varepsilon$ is right.

(2) f has topological transitivity, that is to say $\forall X, Y \subset U,$ $K > 0$, make $f^k(X) \cap Y \neq \Phi$.

(3) The periodic point set T of f is dense on the V . That is to say there is $\forall x \in V, \forall \varepsilon > 0,$ and there is any $y \in T$ make the inequality $|y - x| < \varepsilon$ right.

Wealthy chaotic characteristics: the sensitivity to the parameters and initial values, the ergodic and the randomness

3. The design hybrid chaotic system

A hybrid chaotic system is designed :

$$F(x_{n+1}, y_{n+1}) = \begin{cases} x_{n+1} = f(x_n) = 3.999\ x_n(1 - x_n) \\ y_{n+1} = G(y_n) = \begin{cases} f_0(y_n) = 8y_n^4 - 8y_n^2 + 1, x_n \geq 0.5 \\ f_1(y_n) = 4y_n^3 - 3y_n, x_n < 0.5 \end{cases} \end{cases}$$

The selection of dynamic generated chaotic sequence between

$$f_0(y) = 8y^4 - 8y^2 + 1$$

Manuscript received August 5, 2014
Manuscript revised August 20, 2014

$f_1(y) = 4y^3 - 3y$

The select conditions determined by the chaotic sequence of $f(x) = 3.999x(1-x)$, chaotic sequence flow $\{y_n\}$ as the password flow, the orbit generated by the system is more complex than a single chaotic system, and it also has better randomness. The hybrid chaotic system of random number generator mentioned by Literature [4] is :

$$\begin{cases} f_0(y_{n-1}) = 8y_{n-1}^4 - 8y_{n-1}^2 + 1 \\ f_1(y_{n-1}) = 4y_{n-1}^3 - 3y_{n-1} \\ y_n = F(y_{n-1}) = \begin{cases} f_0(y_{n-1}), y_{n-1} < 0 \\ f_1(y_{n-1}), y_{n-1} \geq 0 \end{cases} \end{cases}$$

It is a system determined, set the initial value is y_0, once appears cyclical phenomenon due to the limited accuracy of the computer, there is y_N ,and $y_N = y_0$, and then the chaotic sequence must be in cycle N , but for the composite chaotic system in this paper, even though there is $y_N = y_0$,it is difficult to ensure $(x_i - 0.5)$ and $(x_{N+i} - 0.5)$ is the same sign, once appears x_{N+j} , make the $(x_j - 0.5)$ and $(x_{N+j} - 0.5)$ is the different sign, sequence will jump out of the original periodic orbit. It is should be noted that due to the limited of precision of the machine, $F(x, y)$ performance cycle behavior in the computer inevitably. However, due to its complex dynamical behavior, it is can be guaranteed that there is still large enough cycle even in the limited accuracy of the computer, and it can resist the statistical analysis effectively.

4. The algorithm description of encrypt and decrypt which use mixed chaotic function to language files

4.1 The design of voice files encryption

(1) Set S is the sampling points sequence of audio files, that is to say $S = s_1 s_2 \cdots s_n$,and s_i is the value of the sampling points of voice files, and $s_i \in [-1,1]$, and $i = 0,1,\cdots,n$.

(2)Encode for S , can get the plaintext sequence $M = [N \times S]$,and $[\bullet]$ is the rounding operation, N is an integer, and set $N = 255$, thus the plaintext sequence is $M = m_1 m_2 \cdots m_n$, $m_i \in [-255,255]$, $i = 1,2,\cdots,n$.

(3)Select the initial $x_0 \in [0,1], y_0 \in [-1,1]$,that is the key, the chaotic sequence $y_1, y_2, \cdots, y_n$ generated by iterative to $F(x, y)$, encoded by the encoding method described above, then get the password flow. $P = p_1, p_2, \cdots, p_n, p_i = [255 \times y_i]$, $i = 1,2,\cdots,n$.

(4)Then encrypt the plaintext stream, $c_i = p_i \oplus m_i$,get the cipher text streams $C = c_1 c_2 \cdots c_n$,, $\oplus$ "is the XOR operation.

4.2 Decryption design

As $c_i = p_i \oplus m_i$, So $m_i = c_i \oplus p_i$, in fact the decryption process is the inverse process described in (4), at last encode to the decrypt files:

$$S' = \frac{M}{255}$$

5. The analysis and simulation results of encryption performance

(1) The analysis of key space

The key space is $10^{14} \times 2 \times 10^{14}$ due to the system key is the initial of chaotic map, and they are the decimals between -1 and 1, and the accuracy is 10^{-14} . The key space is equivalent to providing a 94-bit binary key. The key space is so large that can resist brute-force attacks of the hardware.

(2) Time and frequency domain analysis of encrypted information

In order to analyze encrypted files in the time and frequency domain, we did the appropriate simulation experiments with MALAB, and the original speech signal format to be tested is PCM, the sampling frequency is 44KHz, sampling accuracy is 16 bit, bit rate is 1411kbps, and voice file format is Wav. Analyzed time domain and frequency domain between before and after encryption of recording "Chaos" and the key is $x_0 = 0.34521$, $y_0 = 0.33129$:

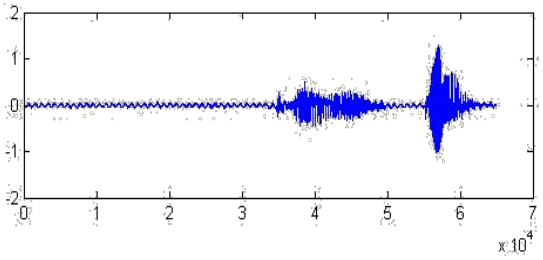

Fig 1. The original speech signal

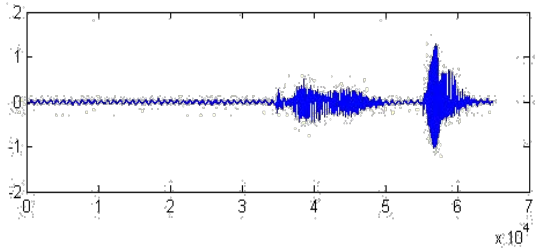

Fig 2. Encrypted voice files

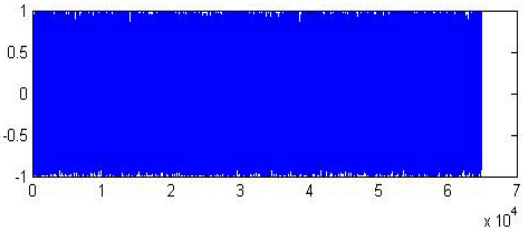

Fig 3. The decrypted audio file

(3) The analysis of key sensitivity:
Good password system should be extremely sensitive to the key changes, that is to say the avalanche phenomenon of key. Here is the test of sensitive to the initial by the algorithm, by using $(x_0^{'}, y_0)$ and $(x_0, y_0^{'})$,and decrypt the encrypted files with ($x_0^{'} - x_0 = 10^{-11}$, $y_0^{'} - y_0 = 10^{-11}$) as the key and (x_0, y_0) as the encryption key.

(4) Correlation Analysis:
It is necessary to reduce the correlation between adjacent data in order to damage statistics attack due to the high correlation of the adjacent data of audio file. Select 2,000 pairs of adjacent data as (x_i, x_{i+1}) randomly when tests the voice segment, and x_i, x_{i+1} are the voice data values of the position, and then calculate the correlation coefficient of them. We can get the correlation coefficient of the selected data is 0.9927 before encryption and 0.0280 after encryption by calculating. It is can be seen that data correlation before encryption is strong, but it is destroyed after encryption from the figure. Data is distributed to the entire space.

6. Conclusion

A voice encryption system is designed based on chaos theory in this paper. Encryption of original file is achieved by the cipher text generated by the chaotic sequence flow generated by a complex chaotic mapping, and then coded, XOR to the encoded audio files. The experimental results show that the system has high security, its keys have a good avalanche effect, and cipher text has good statistical properties randomly.

Acknowledgments

This paper is supported by Scientific Research Fund of Heilongjiang Provincial Education Department (NO: 12521055) and Youth Foundation of Northeast Petroleum University (NO: 2012QN117).

References

[1] LiCuiyan,GaoFei. A Voice Encryption Algorithm Based on Hyperchaos Mackey-G lass System [J].Telecommunication Engineering, 2007, 47(1) :117-121.
[2] J.M.Amigo,L.Kocarev,J.Szczepanski. Theory and practice of chaotic cryptography[J]. Physics Letters A, 2007,366 (3):211-216.
[3] HeXiping.Study on the Chaos-based Algorithms Applied to Image Security[D].Chongqing University,2006.
[4] XiaoJun Tong, MingGeng,Cui. Image encryption with compound chaotic sequence cipher shifting dynamically [J]. Image vicion computing, 2008, 26(6): 843~850.
[5] R.Devany. Chaotic Dynamics [M].Shanghai, Shanghai Translation Publishing Company, 1990.