Signal extraction based on chaos masking

Chao Li, Jiayin Yu, Shiyu Guo, Mengna Shi, Erfu Wang*

Electronic Engineering College, Heilongjiang University, Harbin, Heilongjiang, 150080, China
efwang_612@163.com

Abstract. As chaotic masking signal refers to a seemingly random and irregular signal occurring in a deterministic system, it is highly confidential to load the signal needed to be transmitted into chaotic masking signal as a carrier signal for transmission. In this paper, an improved information encryption based on Lorenz chaotic masking system and speech signal extraction based on joint diagonalization blind extraction algorithm are designed. The performance comparison between the proposed algorithm and FastICA blind extraction algorithm based on negative entropy maximization is analyzed quantitatively and qualitatively in the simulation experiment. The effectiveness of information encryption under chaos masking and the reliability of the algorithm based on joint diagonalization blind extraction are verified.

1. Introduction

Under the background of the increasingly complex communication environment and the trend of the globalization of economy and information, information has become one of the most important strategic resources in today's society. In order to improve the security of information transmission, it is necessary to encrypt or mask the transmitted signal[1]. By taking advantage of the high energy characteristics of chaotic signal, the transmitted signal is completely covered before transmission, which can play a role of confidentiality[2]. In the case of unknown channel, blind source extraction technology is adopted to extract the signal and extract the signal we need[3, 4].

This paper analyzes the improved Lorenz chaos theory cover system and joint evaluation index diagonalization algorithm theory and signal extraction performance. Then, using the generated mask signal improved Lorenz chaotic signals transmitted signals hidden in the respective dimension of the chaotic system, chaotic masking the transmitted signal. Finally, the experimental analysis of simulation results demonstrate the effect of chaos under cover information encrypted and based on joint diagonalization algorithm to extract the observed performance mixed-signal location.

2. Theoretical analysis

2.1 Chaos cover system

Chaos cover characteristics of the system can not be completely thorough understanding of the definition of chaotic systems cover existing only been a widely accepted system masked by chaos mathematics \( Li − Yorke \) definition[5, 6].
Provided \( f(x) \) is a section \([a, b]\) to its continuous mapping, if \( f(x) \) life-cycle point of all cycles, and the presence of \( I \) uncountable subset \( S \subset I \), \( S \) does not contain periodic points, such that for each a \( x, y \in S, x \neq y \), namely:

\[
\begin{align*}
\liminf \left| f^{(n)}(x) - f^{(n)}(y) \right| &= 0 \\
\limsup \left| f^{(n)}(x) - f^{(n)}(y) \right| &> 0
\end{align*}
\]

For each \( x \in S \) at the period point \( P \in I \)

\[
\limsup \left| f^{(n)}(x) - f^{(n)}(P) \right| > 0
\]

When \( f(x) \) meets the above conditions, the corresponding state of \( f(x) \) at this time is chaotic state.

The classical Lorenz chaos equation was derived by Lorenz, a meteorologist, when he studied the atmospheric convection model, and the three-dimensional equation and the dynamic behavior of "butterfly effect", which laid a solid foundation for the development of chaos theory\[^{[7]}\]. The chaotic masking system used in this paper is an improvement on the traditional lorenz chaotic system, and the nonlinear phase \( xy \) in the traditional system is changed into \( x^2 + y^2 \).

\[
\begin{align*}
\dot{x} &= 10(y - x) \\
\dot{y} &= 16x - xz + 2y \\
\dot{z} &= x^2 + y^2 - 8z / 3
\end{align*}
\]

Figure 1 is the improved Lorenz chaotic system's 3d attractor, figure 2 is the improved 2d attractor.

Figure 3 is the time domain response diagram corresponding to x, y and z directions of the improved Lorenz chaotic system. In this paper, the chaotic signal of x channel is selected as the chaotic masking signal to mask and encrypt the signal.
2.2 Signal masking

The signal that needs to be transmitted and the chaotic signal that needs to be concealed are regarded as the source signal for linear mixing in the blind extraction of chaotic masking. The signal to be transmitted is \( s(t) = [s_1(t), s_2(t), \ldots, s_n(t)] \), chaotic masking signal \( m(t) \), and the signal observed through chaotic masking \( x(t) = [x_1(t), x_2(t), \ldots, x_m(t)] \).

\[
x(t) = A\begin{bmatrix} s_1(t), s_2(t), \ldots, s_n(t), m(t) \end{bmatrix}
\]

(4)

Where \( A \) is a randomly generated matrix.

2.3 Joint approximation diagonalization algorithm

The key to the signal extraction under the cover of chaos is the learning algorithm of unmixing matrix. In general signal extraction problems, the mixed mode of signal is not known, and it is difficult to obtain the mixed matrix directly by observing the signal. This paper adopts the blind beam extraction method based on the fourth-order cumulant proposed by Cardoso and Souloumiac, namely the JADE feature matrix joint similarity diagonalization algorithm\(^{[8-11]}\). The JADE algorithm schematic diagram is shown in the figure 4. In the figure \( x(t) \) is the signal needed to be masked, \( m(t) \) is the chaotic masked signal, \( x(t) \) is the observed signal, \( W \) is obtained through the JADE algorithm, and \( y(t) \) is the extracted signal.

\[
y(t) = Wx(t) = WAx(t)
\]

(5)

2.4 Extraction performance test

The performance of an algorithm is usually judged quantitatively by observing the similarity coefficient and performance index of the signal before and after extraction. Let \( \xi_{ij} \) be the similarity coefficient to extract the expected signal \( s' \) and the source signal \( s_i \).
When $\xi_{ij} = 1$, it indicates that the extracted signal is exactly the same as the source signal, which is an ideal situation. In the actual extraction process, it is inevitable that external factors and various errors will affect the performance of the algorithm. In other words, when $\xi_{ij}$ approaches 1, it means that the extraction effect is good.

3. Simulation experiment and result analysis
Choose male and female voice signal in the voice database as a source of information we need to hide, an improved lorentz chaotic masking system signal was randomly selected as the masking signal for the experiment.

| Signal                  | Sampling frequency/Hz |
|------------------------|-----------------------|
| Male voice signal      | 8000                  |
| Female voice signal    | 8000                  |
| Chaotic masking signal | 8000                  |

Figure 5 is the speech signal and the chaotic masking signal observed before the chaotic masking. Figure 6 shows the signal observed by us after the chaotic masking processing. It can be seen from the figure that the speech signal tested in the experiment was completely covered by the chaotic masking signal, and the waveform of the signal changed, improving the confidentiality of the signal in the transmission process.

Figure 7 is the two-way male and female voice signals that we carry out chaotic masking through FastICA blind extraction algorithm based on negative entropy maximization. Figure 8 is the scatter diagram of the extracted voice signal and male and female voice signals.
Figure 9 is the two-way male and female voice signals that we carry out chaotic masking through extraction based on the joint diagonalization blind extraction algorithm. Figure 10 is the scatter diagram of the extracted voice signal and male and female voice signals.

It can be seen from figure 8 that the source information is not in line with the scatter diagram of the extracted signal, and the signal cannot be completely extracted. Figure 10 shows that the scatter diagram of the source signal and the extracted signal is a thin straight line, and the signal can be raised. It can be seen from table 2 that after chaotic masking processing, the performance of the joint diagonalization blind extraction algorithm is better than that of FastICA blind extraction algorithm based on negative entropy maximization.

| Table 2. Similarity coefficient. |
|----------------------------------|
|                                | Blind extraction algorithm of | Based on the joint |
|                                | FastICA based on negative      | diagonalization blind |
|                                | entropy maximization           | extraction algorithm |
| Speech signal of Male           | 0.8411                        | 0.9596               |
| Speech signal of Female         | 0.8907                        | 0.9826               |

4. Conclusion
The safe transmission of information has become the primary consideration in real social life. Due to the energy aggregation characteristics of chaotic masking signal, it is possible to take chaotic masking signal as the carrier signal and load the transmitted signal. Chaotic masking signal can completely cover the transmitted signal. In this paper, the improved Lorenz chaotic system is adopted to generate the chaotic masking signal and the joint diagonalization blind extraction algorithm is adopted to extract the required signal. From the observed signal, it can be seen that the masking signal has been
completely covered and the signal transmission is concealed. Compared with the performance of FastICA blind extraction algorithm based on negative entropy maximization, the performance of FastICA blind extraction algorithm based on joint diagonalization is proved to be superior quantitatively and qualitatively.

Acknowledgments
This work was mainly supported by the National Natural Science Foundation of China under the registration numbers 61571181.

References
[1] Chen, T.M., Ge, L. (2013) Chaos-based encryption and message authentication algorithm for wireless sensor network. Journal on Communications, 34: 113-120.
[2] Wang, E.F., Wang, D.Q., Ding, Q. (2011) New time-frequency method of harmonic signal extraction in chaotic secure communication system. Journal on Communications, 37: 191-198.
[3] He, F.T., Zhang, M., Bai, K., Sun, L. (2016) Image encryption method based on laser speckle and Henon mapping. Infrared and Laser Engineering, 45: 268-272.
[4] Jia, H.Y., Tao, Q., Chen, Z.Q., Xue, W. (2015) Analysis and Synchronization of the Fractional-order Chen System and its Implementation in Confidential Communication. Journal of Tianjing University of Science & Technology, 30: 66-71.
[5] Yin, J.D., Zhou, Z.L. (2010) Quasiweak chaotic equivalent system defined almost periodic point. Journal of Systems Science and Mathematical Sciences, 30: 1156-1162.
[6] Schweizer, B., Smítal, J. (1994) Measures of chaos and a spectral decomposition of dynamical systems on the interval. Trans. Amer. Math. Soc., 344: 737-754.
[7] Zhou, Z.L. (1997) Symbolic dynamics. Shanghai Science and Technology Education Publishing, Shanghai.
[8] Cheng, G.H., Wang, L.J. (2014) Directororthogonal algorithm of joint diagonalization for blind source separation. Journal of University of Electronic Science and Technology of China, 43: 359-362.
[9] Zheng, X.P. (2014) JADE sparse signal of improved performance comparison algorithm. Electronic Technology & Software Engineering, 22: 58-59.
[10] Yang, F.S., Hong, B. (2006) Independent component analysis principles and applications. Tsinghua University Publishing, Beijing.
[11] Zhan, L.J., Peng, L., Ye, X.F. (2017) JADE used to extract heart rate signals from color video. Physical Experiment of College, 30: 7-11.
[12] Zhao, Z.J., Huang, Y.B., Qiang F.F., Yang, A.F. (2019) Single channel blind source separation algorithm based on feedback variational mode decomposition. Journal of Vibration and Shock, 38: 268-273.