Hindawi
Complexity
Volume 2021, Article ID 6627804, 21 pages
https://doi.org/10.1155/2021/6627804

Research Article

Quantum Particle Swarm Optimization Extraction Algorithm Based on Quantum Chaos Encryption

Chao Li, Mengna Shi, Yanqi Zhou, and Erfu Wang

Electrical Engineering College, Heilongjiang University, Harbin 150080, China

Correspondence should be addressed to Erfu Wang; wangerfu@hlju.edu.cn

Received 3 October 2020; Accepted 30 January 2021; Published 12 February 2021

Academic Editor: Akif Akgul

Considering the highly complex structure of quantum chaos and the nonstationary characteristics of speech signals, this paper proposes a quantum chaotic encryption and quantum particle swarm extraction method based on an underdetermined model. The proposed method first uses quantum chaos to encrypt the speech signal and then uses the local mean decomposition (LMD) method to construct a virtual receiving array and convert the underdetermined model to a positive definite model. Finally, the signal is extracted using the Levi flight strategy based on kurtosis and the quantum particle swarm optimization optimized by the greedy algorithm (KLG-QPSO). The bit error rate and similarity coefficient of the voice signal are extracted by testing the source voice signal SA1, SA2, and SI943 under different SNR, and the similarity coefficient, uncertainty, and disorder of the observed signal and the source voice signal SA1, SA2, and SI943 verify the effectiveness of the proposed speech signal extraction method and the security of quantum chaos used in speech signal encryption.

1. Introduction

With the widespread popularity of multimedia services, speech as a real-time business form is still one of the main ways for people to communicate. According to statistics, hundreds of millions of sensitive speech data are being transmitted through open and shared networks every second. So, the encrypted transmission for speech information is an important way to ensure the safe and effective speech information from the sending end to the receiving end. In recent years, scholars have proposed many methods for encrypted transmission of speech signals, such as chaotic masking encryption. At the same time, the related methods of blind signal processing are also concerned by scholars and introduced into related research in this field in order to solve the problem that the number of receiving elements is small in the actual application environment, and the channel conditions are missing or the channel parameters are unknown.

At present, scientific researchers have proposed many signal encryption methods. Sun et al. proposed signal encryption based on random signals and block changes [1]. Shah et al. proposed a method for encrypting signals through Mobius changes and Hénon mapping [2]. Bhattacharya et al. proposed a GPU network encryption method based on the PCA-Firefly's XGBoost new classification model [3]. However, speech signals have some inherent characteristics that are different from other multimedia information, such as large capacity and high redundancy. The traditional speech signal encryption algorithm often has the problem of low security. Considering the actual hardware overhead of the receiving array element, designing a new encryption algorithm that can ensure a sufficient security level is always a huge challenge for researchers. In recent years, chaotic signals have outstanding performance in signal encryption due to their pseudo-randomness, ergodicity, and initial sensitivity. Hongjun and Xingyuan proposed color image encryption based on one-time keys and robust chaotic maps [4] and proposed color image encryption using spatial bit-level arrangements and high-dimensional chaotic systems [5]. Hamed and Ali proposed a speech signal encryption algorithm based on Logistic mapping and three-dimensional matrix [6]. Sathiyamurthi and Ramakrishnan used chaotic shift keying

to encrypt speech signals [7]. Mosa et al. used chaotic Baker mapping in the time domain and transform domain of speech signals to perform permutation and mask replacement [8]. Hamza and Titouna used Zaslavsky mapping as a pseudo-random number generator when encrypting speech signals [9]. In addition, some researchers used direct chaotic modulation of Lorenz or hyperchaotic Qi system to set information into a variable of the system to achieve the encryption of the speech signal in the communication system [10]. However, the above studies are all based on one-dimensional, two-dimensional, three-dimensional, or multidimensional hyperchaos, whose chaotic models are relatively fixed. How to use chaotic signals in a more difficult-to-understand format and how to build a more secure chaotic dynamic system are the primary problems in designing higher security for chaotic masking speech signal encryption algorithms. The quantum chaos for concealed transmission is proposed, which selects the system parameter values with highly complex structure and high security through the analysis of its chaotic characteristics, laying the foundation for designing a speech signal encryption algorithm with a better security level.

There are two main methods for extracting speech signal s from a chaotic background: the method based on phase space reconstruction and the method based on geometric features of singular attractors. Both methods are based on a positive definite mixed model; that is, the number of receiving array elements is equal to the number of transmitting array elements. However, this is obviously not guaranteed in actual communication. When the number of receiving array elements is less than the number of sending in actual communication, the form of underdetermined is often taken. Therefore, the achievement of separation and extraction of speech signals must change underdetermined to positive definite by the model conversion. The method based on the geometric characteristics of chaotic signals is more widely used in the positive definite model extraction method, to avoid the difficult problem of selecting the embedding dimension and delay parameter in the phase space reconstruction [11–13].

Sadhu et al. used the minimum phase space volume method to study the parameters of the autoregressive model and the frequency of the sinusoidal signal under the chaotic background [14]. Fu et al. combined the method of Tim-Sauer and Robert-Cawley to successfully extract harmonic signals from the chaotic background [15]. Li adopted the time-frequency joint algorithm to realize harmonic signal extraction [16]. Unfortunately, the above algorithms cannot effectively extract the transmitted speech signal in the underdetermined channel model, especially in the case of mixing additive white Gaussian noise. A method of constructing virtual receiving array elements is proposed, which decomposes the observation signal to supplement the missing array elements, and then the blind extraction of low-element speech signals is realized.

Independent component analysis technology [17] is a new signal processing technology that emerged in the 1990s, which calculates the high-order statistical characteristics of the signal to separate each source signals from multiple mixed signals without other prior knowledge. Hesse and James proposed the FastICA algorithm with spatial constraints in biomedical signal processing [18]. Ahmad et al. proposed an improved FastICA algorithm based on kurtosis contrast function to separate mixed EEG signals [19]. Li et al. used the FastICA algorithm to process optical signals [20]. Labounek et al. used the Group ICA method to estimate the stable EEG spatial distribution [21]. Aiming at the problems of poor robustness and low convergence accuracy of existing ICA methods, a quantum particle swarm optimization algorithm based on the kurtosis Levy flight strategy greedy algorithm (KLG-QPSO) is proposed. First, the proposed LMD algorithm is used to decompose the observed signal and to supplement the missing array elements, converting the underdetermined model into a positive definite model. Then, the KLG-QPSO algorithm is used to separate the signal from the chaotic occlusion to recover the source signal. In this paper, the concealed encrypted transmission and recovery extraction of three speech signals are realized in the underdetermined model using three-way speech signals as transmission objects and utilizing quantum chaotic signals as carriers.

The main contributions of this article are as follows

(A1) The quantum chaotic signal generated by the Harper model is used as a masking signal in the secure transmission of voice signals, and the highly complex structure of the quantum is used to completely cover the voice signal so that the encryption of the voice signal has a better security level.

(A2) In the underdetermined channel model mixed with additive white Gaussian noise, a new virtual receiving array element construction method LMD is used to decompose the observation signal, supplement the missing elements, and convert the underdetermined model into a positive definite model.

(A3) A quantum particle swarm optimization algorithm (KLG-QPSO) based on kurtosis-based Levi's flight strategy and greedy algorithm is proposed. The algorithm is used to extract observation signals, and then the blind extraction of low-level speech signals is realized.

The rest of the paper is organized as follows. Section 2 describes the theoretical basis of the underdetermined transmission model, Harper model, and its characteristics of generating quantum chaos. Section 3 discusses the

processing methods of nonstationary signals and the construction of virtual array units based on LDM. Section 4 describes the proposed positive definite blind source separation algorithm KLG-QPSO. Section 5 describes pseudo code of the proposed algorithm and performance evaluation. Section 6 gives the results of simulation experiments and analyzes the safety performance of the system. Section 7 summarizes our conclusions.

2. Theoretical Basis

This part will construct the mixing and separation model of multiple speech signals and one quantum chaotic signal in the underdetermined model channel mixed with Gaussian white noise to realize the safe transmission of speech signals. In addition, this section will describe the quantum chaotic signal generated by the Harper model.

2.1. Underdetermined Transmission Model. The underdetermined transmission model refers to separating and recovering a relatively independent source signal from the observed multisource mixed signal under the condition that the number of observations is less than the number of source signals. The schematic diagram of the underdetermined transmission model is shown in Figure 1.

Assuming that M mutually independent and non-Gaussian observation signals are a mixture of N source signals, the underdetermined transmission model is described as follows [22]:

$$x_i(t) = \sum_{k=1}^{N} a_{ik} s_k(t) + n_i(t), \tag{1}$$

where $x_i(t)$ represents the i-th observation signal received by the sensor at the receiver; $s_k(t)$ represents the k-th source signal; $n_i(t)$ represents the Gaussian white noise mixed in $x_i(t)$; and N represents the number of source signals.

Equation (1) can also be written as follows:

$$x(t) = As(t) + n(t), \tag{2}$$

where $x(t) = [x_1(t), x_2(t), \ldots, x_M(t)]^T$ and $s(t) = [s_1(t), s_2(t), \ldots, s_N(t)]^T$ represent the observed signal vector and the source signal vector, respectively; $A = [a_1, a_2, \ldots, a_N] \in R^{M\times N}$ $(M < N)$ represents the mixing matrix; and $n(t)$ represents the noise vector.

2.2. Harper Model and Characteristics of Quantum Chaos. The Harper model was proposed in 1955 [23] to describe the motion state of electrons in a two-dimensional lattice perpendicular to the direction of the magnetic field. The Hamiltonian of the system is shown in the following equation:

$$H_0(p, \theta) = \cos(p) + \cos(\theta), \tag{3}$$

where p, θ is a pair of regular conjugate variables.

By adding a periodic driving term to the Harper model, the model can be expanded from a pure integrable system to a complex dynamic system that exhibits chaotic motion as

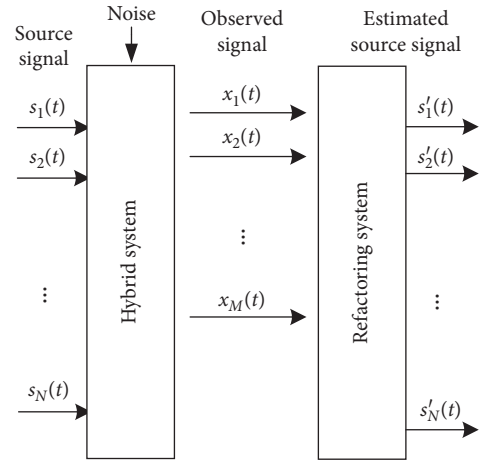


Figure 1: Model of underdetermined transmission.

parameters change. The Hamiltonian of the period-driven quantum Harper model is shown in the following equation:

$$H(p, \theta, t) = L\cos(p) + K\cos(\theta)\sum_{m}\delta(t - m\tau), \tag{4}$$

where L and K are system parameters; $\delta(t)$is the δfunction; $m$takes any integer; and $\tau$is the drive period. The discontinuous area-preserving mapping equation that the system evolves in a driving cycle is shown in the following equation:

$$\begin{cases} p_{n+1} = p_n + K\sin(\theta_n), \\ \theta_{n+1} = \theta_n - L\sin(p_{n+1}). \end{cases} \tag{5}$$

2.3. Characteristics of Harper Model Produced Chaotic. The form of the period-driven Harper model is simple, but as the parameters change, it has complex dynamic behavior in the phase space. In the asymmetric case $(L \neq K)$, if L and K are relatively small, the phase space is divided into multiple layers by the KAM torus. In Figure 2(a),$L = 0.05$ and $K = 0.01$; in Figure 2(b), $L = 0.03$ and $K = 0.07$; when the values of L and K are not equal, the phase space is divided into multiple layers by the KAM torus, showing different states.

In the case of symmetry, when $L = K \longrightarrow 0$, the system is classical integrable. As $L = K$ increases, the KAM torus is continuously destroyed and chaos will appear in the phase space diagram. In Figure 3(a), $L = K = 0.2$; in Figure 3(b), $L = K = 0.4$; in Figure 3(c) $L = K = 0.63$; with the gradual increase in $L = K$, the phenomena of regular motion and chaotic motion appear simultaneously in the phase space. When $L = K > 0.63$, there will be a wide range of chaotic motions, and the system appears exponentially sensitive to the initial state due to the enhancement of nonlinear effects. In Figure 3(d), $L = K = 4$; in Figure 3(e), $L = K = 10$; the motion of the system will be chaotic, and as the value of $K = L$ increases, the chaotic state of the system will strengthen.

Chaos refers to a seemingly random phenomenon that appears random in a deterministic system. Chaos is not simply disordered, there is no obvious period and symmetry

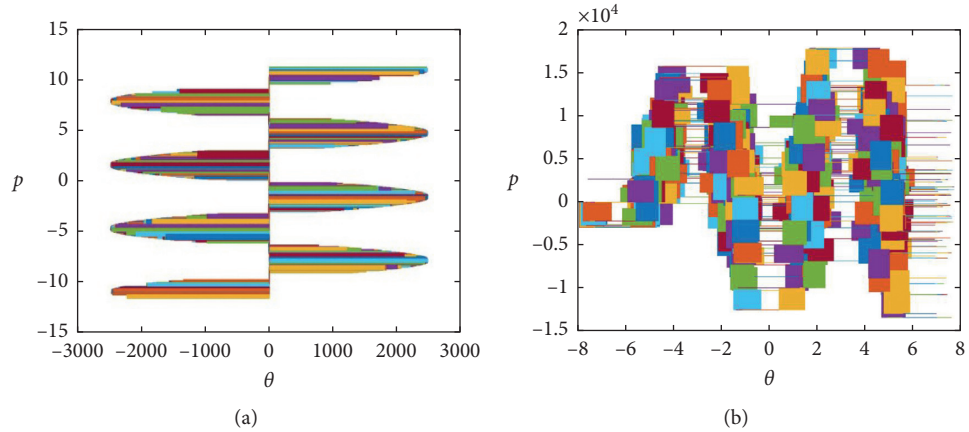


Figure 2: Model of underdetermined transmission: (a) $L = 0.05$ and $K = 0.01$; (b) $L = 0.03$ and $K = 0.07$.

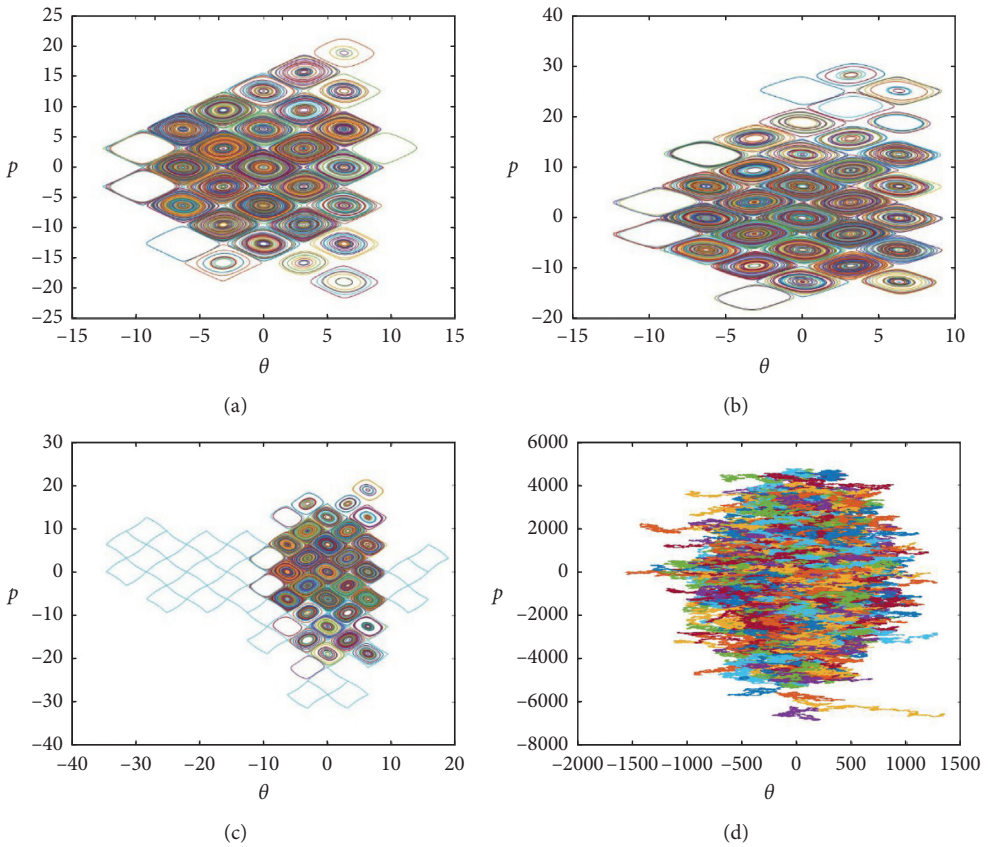
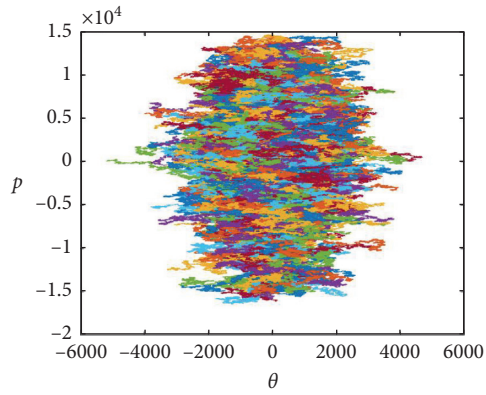


Figure 3: Continued.



(e)

Figure 3: Harper model phase space diagram of symmetrical case: (a) $L = K = 0.2$; (b) $L = K = 0.4$; (c) $L = K = 0.63$; (d) $L = K = 4$; (e) $L = K = 10$.

on the surface, but it is an ordered structure with rich internal levels, and it is a new form of existence for nonlinear systems. This paper uses two chaos test methods: 0-1 test method [24] and Lyapunov exponential method [25] to test the characteristics of the chaos produced by the Harper model. Now, the Harper model is tested 0-1 when the parameters $L = 0.05$ and $K = 0.01$; $L = K = 0.63$; $L = K = 4$; and $L = K = 10$. When $L = 0.05$ and $K = 0.01$; $L = K = 0.63$, it is judged as "0"; when $L = K = 4$; $L = K = 10$, it is judged as "1," which corresponds to the periodic state and the chaotic state, respectively. The 0-1 test is shown in Figure 4, describing periodic motion and chaotic motion, respectively.

The spectrum of Lyapunov exponent with the number of iterations of the Harper model when $K = L = 10$ is shown in Figure 5. The blue and red curves in Figure 5 represent the variation of the two positive Lyapunov exponents with the number of iterations when the Harper model produces chaotic signals when $K = L = 10$. And, they are greater than 0, indicating that it is chaotic movement and the structure is complicated.

By observing the chaotic spatial phase diagram generated by the Harper model, it can be found that there is an energy accumulation region in quantum chaos. This part of the signal has the characteristics of broadband and high energy, and the digital speech signal is a small signal with low energy. Therefore, the speech signal can be well hidden in the quantum chaotic signal to achieve the purpose of encrypted transmission. In this paper, when $L = K = 10$, the quantum chaos generated by the Harper model is used to mask the encrypted transmission of the three speech source signals.

3. Low-Element Receiving Model Conversion

3.1. Speech Signal and LMD Decomposition. Empirical mode decomposition (EMD) [26] is a common processing method for speech signal extraction and separation under the underdetermined model. EMD decomposes a series of intrinsic mode functions (IMFs) from high frequency to low frequency from the observed signal and extracts different IMF according to the different proportional characteristics of each source signal. However, the problem of endpoint effect exists in EMD. LMD adopted in this paper can overcome the problem of endpoint effect caused by EMD. In this paper, LMD is used to process the observed signal and decompose the signal to generate a virtual receiving data array.

The LMD algorithm is an adaptive decomposition based on the information of the signal itself. The algorithm can separate the envelope signal and the frequency modulation signal from the original signal, and the product function components generated by these two signals have practical physical meaning. The obtained time-frequency distribution can clearly and accurately reflect the distribution of signal energy on different spatial scales. LMD can calculate the instantaneous amplitude and frequency, respectively, which can effectively avoid the mixing phenomenon of the two, and the decomposition speed is fast. For any signal, the LMD decomposition process is as follows:

(i) Calculate all extreme points n_i in the signal $x(t)$ and calculate the average value m_i of the sum of the two adjacent extreme points n_i and n_{i+1}, as shown in the following equation:

$$H_0(p, \theta) = \cos(p) + \cos(\theta). \tag{6}$$

The mean m_i between all adjacent points is connected in series with a straight line and smoothed by the moving average method to obtain a smooth local mean function $m_{11}(t)$.

(ii) By subtracting the two adjacent extreme points and dividing the absolute value by 2, the estimated value

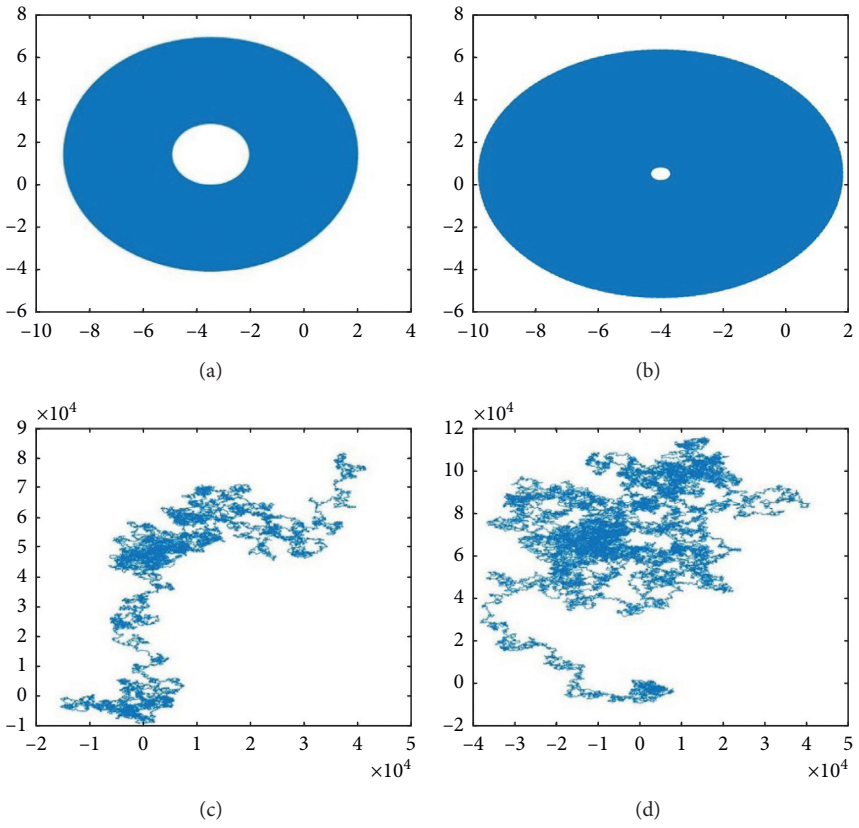


Figure 4: The result of the 0-1 test: (a) $L = 0.05$ and $K = 0.01$; (b) $L = K = 0.63$; (c) $L = K = 4$; (d) $L = K = 10$.

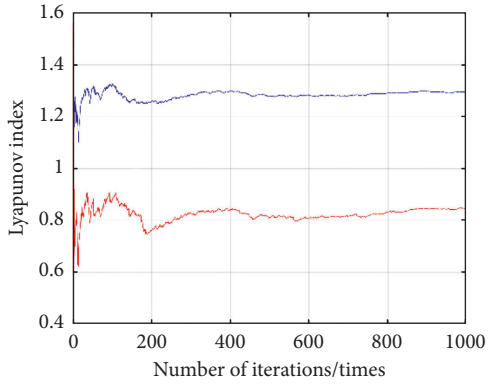


Figure 5: Spectra of Lyapunov exponent.

of the signal envelope is a_i, as shown in the following equation:

$$a_i = \frac{|n_i - n_{i+1}|}{2}. \tag{7}$$

All the two adjacent envelope estimates a_i are connected by straight lines and smoothed by moving average. The smoothed envelope estimation function $a_{11}(t)$ is obtained.

(iii) The smooth local mean function $m_{11}(t)$ is removed from the original signal $x(t)$, as shown in the following equation:

$$h_{11}(t) = x(t) - m_{11}(t). \tag{8}$$

(iv) The demodulation of $h_{11}(t)$ is achieved by dividing $h_{11}(t)$ by the smooth envelope estimation function $a_{11}(t)$, as shown in the following equation:

$$s_{11}(t) = \frac{h_{11}(t)}{a_{11}(t)}. \tag{9}$$

(v) Calculate the envelope estimation function $a_{12}(t)$ of $s_{11}(t)$; if $a_{12}(t) \neq 1$, $s_{11}(t)$ is not a pure FM signal. Repeat the above demodulation process until $s_{1n}(t)$ becomes a pure FM signal (i.e., $-1 \leq s_{1n}(t) \leq 1$ and its envelope function $a_{1(n+1)} = 1$), as shown in the following equation:

$$\begin{cases} h_{11}(t) = x(t) - m_{11}(t), \\ h_{12}(t) = s_{11}(t) - m_{12}(t), \\ \vdots \\ h_{1n}(t) = s_{1(n-1)}(t) - m_{1n}(t), \end{cases} \tag{10}$$

where

$$\begin{cases} s_{11}(t) = \dfrac{h_{11}(t)}{a_{11}(t)}, \\ s_{12}(t) = \dfrac{h_{12}(t)}{a_{12}(t)}, \\ \vdots \\ s_{1n}(t) = \dfrac{h_{1n}(t)}{a_{1n}(t)}, \end{cases} \tag{11}$$

where the iteration termination condition is

$$\lim_{n \longrightarrow \infty} a_{1n}(t) \approx 1. \tag{12}$$

(vi) Multiply the obtained envelope estimation function for each time to obtain the envelope signal $a_1(t)$ of the first component, as shown in the following equation:

$$a_1(t) = a_{11}(t), a_{12}(t), \ldots, a_{1n}(t) = \prod_{p=1}^{n} a_{1n}(t). \tag{13}$$

(vii) The product function PF of the original signal is obtained by multiplying the envelope signal $a_1(t)$ by the pure modulation signal $s_{1n}(t)$, as shown in the following equation:

$$\mathrm{PF}_1(t) = a_1(t) s_{1n}(t). \tag{14}$$

(viii) Separate the first component $\mathrm{PF}_1(t)$ from $x(t)$ to obtain a new signal $u_1(t)$. Use $u_1(t)$ as the original data and repeat the above steps and cycle N times, until $u_N(t)$ becomes a monotonic function, as shown in the following equation:

$$\begin{cases} u_1(t) = x(t) - \mathrm{PF}_1(t), \\ u_2(t) = u_1(t) - \mathrm{PF}_2(t), \\ \cdots \\ u_N(t) = u_{N-1}(t) = \mathrm{PF}_N(t). \end{cases} \tag{15}$$

Finally, the decomposition results of LMD are shown in the following equation:

$$x(t) = \sum_{i=1}^{p} \mathrm{PF}_i + u_p(t). \tag{16}$$

3.2. Virtual Array Construction Based on LMD. The proposed model mixes and separates multiple speech signals and one quantum chaotic signal in an underdetermined model channel mixed with Gaussian white noise. The traditional algorithm based on positive definite mixed channel cannot achieve blind separation and extraction of source signals. So, a virtual array element construction method based on LMD is proposed. The idea is to repeat the decomposition process of LMD and use the first component of each decomposition process as the virtual receiving array element to supplement the observed signal. Combined with the actual observation array element, a positive definite hybrid model is constructed. Then, the proposed KLG-QPSO algorithm is used to extract the speech signal which is covered by chaotic signal. The block diagram of the system model is shown in Figure 6.where $\mathbf{A} = [A_1, A_2, \ldots, A_N]$ is a $M * N$ $(M < N)$ channel mixing matrix randomly generated by the RAND function; $s(t) = [s_1(t), s_2(t), \ldots, s_N(t)]^T$ represents $\mathbf{N}$ unknown source signal vectors; $x(t) = [x_1(t), x_2(t), \ldots, x_M(t)]^T$ is the mixed signal vector; $n(t)$ is a Gaussian white noise vector added to the channel, $\mathbf{Y} = [y_1, y_2, \ldots, y_m]^T$ is the observed signal vector; and $Y' = [y_1, y_2, \ldots, y_n]^T$ is the observed signal vector obtained by $\mathbf{Y}$ after **LMD** processing.

$$Y = x(t) + n(t) = As(t) + n(t), \tag{17}$$

$$Y \xrightarrow{\mathrm{LMD}} Y', \tag{18}$$

4. KLG-QPSO Algorithm

In the traditional quantum particle swarm optimization algorithm [27], the potential well center can be continuously adjusted according to the change of the particle self-cognition level, but it is always limited to the local optimal position and the global optimal position. The potential well center update strategy relies too much on the local optimal position and the global optimal position, the single information sharing mechanism between particles which leads to

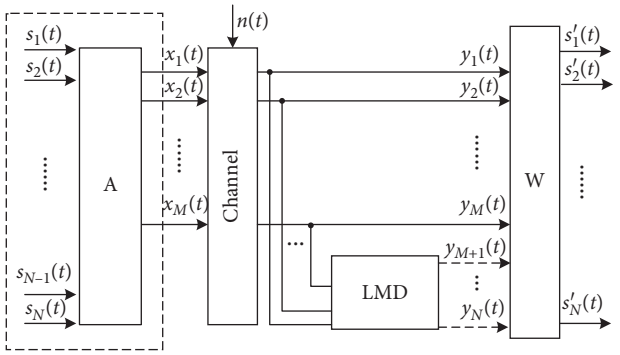


Figure 6: System model.

the slow evolution or even premature convergence of the population. This paper proposes a new positive definite blind source separation algorithm, which is a quantum particle swarm optimization algorithm based on the Levy flight strategy greedy algorithm of kurtosis (KLG-QPSO). Focusing on the update method of the potential well center, the improved quantum particle swarm algorithm takes kurtosis as the fitness function, introduces Levy flight strategy and greedy algorithm to overcome the shortcomings of the traditional quantum particle swarm optimization algorithm in the optimal particle renewal, and further improves the convergence accuracy and speed of the algorithm.

4.1. QPSO. Clerc proposed aggregation in the study of particle convergence behavior in the PSO algorithm [28]. Aggregation is the most essential characteristic of a group of intelligent creatures. As the population iteratively evolves, all particles will converge to the vicinity of their respective local attractor. The position of the attractor is shown in the following equation:

$$p_{i,j}(t) = \frac{c_1 r_{1,j}(t) P_{i,j}(t) + c_2 r_{2,j}(t) G_j(t)}{c_1 r_{1,j}(t) + c_2 r_{2,j}(t)}, \tag{19}$$

where $1 \le j \le N$; $p_{i,j}(t)$ represents the local attractor of particle i; $P_{i,j}$ represents the local optimal position of the particle; $G_j(t)$ represents the global optimal position of the population; $r_{1,j}$ and $r_{2,j}$ represent the mutually independent random nonnegative real numbers within (0,1), c_1 represents local cognitive ability and its function is to regulate the speed of particles moving to their best position, and c_2 represents the overall cognitive ability and its function is to control the speed of particles moving to the global optimal position.

According to the theory of quantum mechanics, the dynamic behavior of particles in quantum space can generally be described by the Schrödinger equation, as shown in the following equation:

$$j\hbar \frac{\partial}{\partial t}\psi(r,t) = \left(-\frac{\hbar^2}{2m}\nabla^2 + V(r)\right)\psi(r,t), \tag{20}$$

where $\hbar$ is Planck's constant; m is the particle mass; $V(r)$ is the energy distribution function of the potential field; and $\psi(r,t)$ is the wave function.

In the quantum space, the Delta potential well is selected as the PSO potential well model, and the potential energy distribution of the Delta potential well is shown in the following equation:

$$V(r) = -\gamma\delta(r), \tag{21}$$

where γ is the depth of the potential well.

Solve the wave function by substituting equation (21) into equation (20), as shown in the following equation:

$$\psi(r) = \frac{1}{\sqrt{L}} e^{-|r|/L}, \tag{22}$$

where $L = \hbar^2/m\gamma$ is the characteristic length of the Delta potential well. The probability density function of the particle at r is shown in the following equation:

$$Q(r) = \frac{1}{L} e^{-2|r|/L}. \tag{23}$$

In the potential well space, the position of the particle has a high degree of randomness, following Schrodinger's theorem. In actual operation, it is generally realized by the Monte Carlo method. Let $u = e^{-2|r|/L}$, where u is a random number randomly selected in [0,1]:

$$r = \pm \frac{L}{2} \ln\left(\frac{1}{u}\right). \tag{24}$$

So, the position of the particle in quantum space is as follows:

$$x = p \pm \frac{L}{2} \ln\left(\frac{1}{u}\right). \tag{25}$$

The position of the particle is time-varying in equation (25), and it is ensured that the particle converges to the respective local attractor p; that is, the L in equation (25) must also be time-varying. Let $L = L(t)$, and the position update in any dimension is shown in the following equation:

$$X(t+1) = p(t) \pm \frac{L(t)}{2} \ln\left(\frac{1}{u(t)}\right), \quad u(t) \in U(0,1). \tag{26}$$

Quantum space is a kind of multidimensional space. The convergence of the position of particles in multiple dimensions can be transformed into the convergence of particles in one-dimensional space. So, the position of particles in quantum space is shown in the following equation:

$$X_{i,j}(t+1) = p_{i,j}(t) \pm \frac{L_{i,j}(t)}{2} \ln\left(\frac{1}{u(t)}\right), \quad u(t) \in U(0,1). \tag{27}$$

In quantum space, introduce an average position and record its position coordinate as $C(t)$:

$$C(t) = \left(\frac{1}{N} \sum_{i=1}^{N} P_{i,1}(t), \frac{1}{N} \sum_{i=1}^{N} P_{i,2}(t), \ldots, \frac{1}{N} \sum_{i=1}^{N} P_{i,D}(t) \right), \tag{28}$$

where D is the particle dimension and N is the population size.

Now, the length of the potential well is shown in the following equation:

$$C(t) = \left(\frac{1}{N} \sum_{i=1}^{N} P_{i,1}(t), \frac{1}{N} \sum_{i=1}^{N} P_{i,2}(t), \ldots, \frac{1}{N} \sum_{i=1}^{N} P_{i,D}(t) \right), \tag{29}$$

where $L_{i,j}(t)$ is the potential well length in quantum space and α is the contraction expansion coefficient.

By substituting equation (29) into equation (27), the position of the particle in the quantum space is obtained as shown in the following equation:

$$X_{i,j}(t+1) = p_{i,j}(t) \pm \alpha \left| C_j(t) - X_{i,j}(t) \right| \ln\left(\frac{1}{u_{i,j}(t)} \right), \tag{30}$$

where $p_{i,j}(t)$ is the local attractor, which represents the center of the potential well, and its position determines the direction of the particle in the quantum space; $u_{i,j}(t)$ is a random number in [0,1].

4.2. Levy Flight Strategy. Levy flight was proposed by Paul Levy [29], which is a type of non-Gaussian random walk process with Markov properties characterized by occasional long-range jumps. Levi's flight step length follows the Levy distribution, which is a probability distribution proposed by the French mathematician Levy. The expression of the power form of Levy distribution is $\text{Levy}(\lambda) \sim |d|^{-\lambda}$, in which d is random step size and λ is power $1 < \lambda \leq 3$.

$$\text{Levy}(s, \kappa, \mu) = \begin{cases} \sqrt{\frac{\kappa}{2\pi}} \exp\left[-\frac{\kappa}{2(s-\mu)} \right] \frac{1}{(s-\mu)^{3/2}}, & 0 < \mu < s < \infty, \\ 0, & s \leq 0. \end{cases} \tag{31}$$

In the equation, s is the Levy flight step length, μ is the displacement parameter, and κ is the scale parameter, which determines the distribution scale.

In order to apply Levy flight to the QPSO algorithm, it is necessary to discretize Levy flight and then combine equation (30) to obtain the global optimal position after Levi flight update, as shown in the following equation:

$$X_g(t) = X(t) + \beta \oplus \text{Levy}(\lambda), \tag{32}$$

where $X_g(t)$ is the global optimal position of the particle after the Levy flight update, $\beta = \beta_0 \times (X(t) - X_{\text{worst}})$ is the step size control factor, β_0 is the initial value, X_{worst} is the position of the worst particle in the contemporary, and the size step is used to fly to the original small probability exploration area, making the search area more uniform, $\text{Levy}(\lambda)$ is the random search path, and $\oplus$ is the dot product operation.

The Levy distribution is very complex; its flight path is commonly simulated by the Mantegna algorithm as shown in the following equation:

$$\text{Levy}(\lambda) = \mu / |v|^{1/\chi}, \tag{33}$$

where χ satisfies $0 < \chi \leq 2$ and $\lambda = 1 + \chi$ andμ, $v$both follow the normal distribution of the following equation:

$$\begin{cases} \mu \sim N\left(0, \sigma_\mu^2\right), \\ v \sim N\left(0, \delta_v^2\right), \end{cases} \tag{34}$$

where

$$\begin{cases} \delta_\mu = \left[\Gamma(1+\lambda) \sin(\pi\lambda/2) / \left(\Gamma[(1+\lambda)/2] 2^{(\lambda-1)/2} \lambda \right) \right], \\ \delta_v = 1, \end{cases} \tag{35}$$

where Γ is the gamma function.

In order to illustrate the superiority of Levy flight, the flight path of particles in two-dimensional space is shown in Figure 7, and the particle position changes in 1000 generations are recorded. The flight step distribution is shown in Figure 8.

It can be seen from Figures 7 and 8 that frequent short-distance search in Levy flight can be carefully searched around the current optimal solution to improve the search ability, and the occasional long-distance jump search can expand the range of particle search, which is conducive to enhancing the diversity of particles, avoiding the algorithm falling into the local optimum, and improving the convergence accuracy of the algorithm.

Substituting equations (33)–(35) into equation (32), the global optimal position of the updated Levy flight can be obtained by simplification as shown in the following equation:

$$X_g(t) = X(t) + \beta \oplus \frac{\mu}{|v|^{1/\chi}} \left[X(t) - X_{\text{worst}} \right]. \tag{36}$$

4.3. Greedy Algorithm. Although Levy flight can make the particles get rid of local optimum, it cannot guarantee that the updated particle position is better than the original position. For this problem, the greedy algorithm [30] is introduced to decide whether to update the optimal particle position. When the updated position is better than the original position, the position is updated; otherwise the

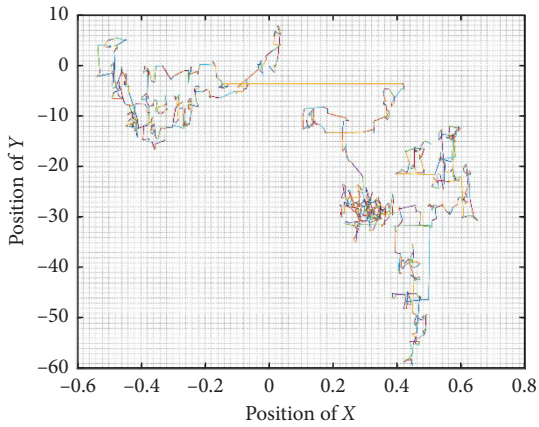


Figure 7: Particle flight path in two-dimensional space.

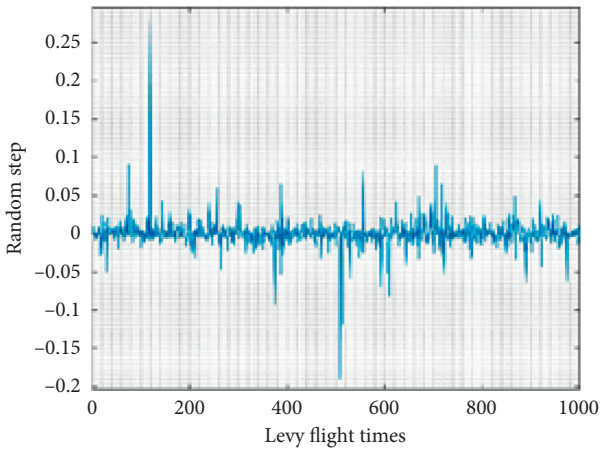


Figure 8: Random step distribution of Levy flight.

original position is retained, and the implementation process is shown in the following equation:

$$X_g^{\text{new}}(t) = \begin{cases} X_g(t), & f\left(X_g(t)\right) > f\left(X(t)\right), \\ X(t), & f\left(X_g(t)\right) < f\left(X(t)\right), \end{cases} \tag{37}$$

where $X_g^{\text{new}}(t)$ is the updated particle position of the greedy algorithm and $f(\cdot)$ is the fitness function. The evaluation strategy based on the greedy algorithm enables the quantum particle swarm optimization algorithm based on Levy flight strategy to guide other particles to search by using the optimal particles of each generation in the evolution process so that the algorithm can achieve better convergence accuracy and speed.

4.4. Fitness Function. In this paper, kurtosis [31] is taken as the fitness function. Kurtosis is a classical non-Gaussian measure. The existence of non-Gaussian signal is the basis of applying ICA to BSS. Define the kurtosis of the signal as shown in the following equation:

$$\text{kurt}(y) = E\left[y^4\right] - 3\left(E\left[y^2\right]\right)^2, \tag{38}$$

where $\text{kurt}(\cdot)$ represents the kurtosis of the signal and $E(\cdot)$ represents the mean value, and normalization of equation (38) can obtain the following equation:

$$\text{kurt}(y) = \frac{E\left[y^4\right]}{E\left[y^2\right]^2} - 3. \tag{39}$$

In order to reduce the calculation, the signal is centered and whitened. The mean value of the signal after the center whitening is zero and the variance is 1, as shown in the following equation:

$$\text{kurt}(y) = E\left[y^4\right] - 3. \tag{40}$$

If the signal is a Gaussian signal, its kurtosis value is zero. For most non- Gaussian signals, the signal whose kurtosis value is greater than zero is called a super-Gaussian signal; for example, the sound signal is a super-Gaussian signal, while the signal whose kurtosis value is less than zero is called a sub-Gaussian signal, and the image signal is a sub-Gaussian signal. Because of the nonzero kurtosis of the signal, the absolute kurtosis will be used as the non-Gaussian measure of the signal in blind source separation. For the signal requiring blind separation, the greater the absolute value of kurtosis is, the stronger the non-Gaussian nature of the signal is and the better the separation will be. The flow chart of the KLG-QPSO algorithm is shown in Figure 9.

In the block diagram of the system model in Figure 6, the key step is to use the nonstationary signal processing method described in Section 3.1: LDM algorithm to decompose the observed signal. For example, $n = m + 1$, select the PF1 component and a positive definite model can be constructed. The reason is that the first component in the decomposition process can well represent the characteristics of **Y** signal of observation signal. According to the blind source separation theory, use the KLG-QPSO algorithm to construct the positive definite mixed model separation matrix **W**:

$$s'(t) = WY', \tag{41}$$

where $s'(t) = [s_1'(t), s_2'(t), \ldots, s_N'(t)]^T$ is the estimated signal of the source signal.

5. Algorithm Complete Pseudo Code and Performance Evaluation

Combined with the system model shown in Figure 6, the simulation flow chart studied in this paper can be obtained as shown in Figure 10.

The pseudo codes of the virtual array construction based on LMD and the speech signal mask encryption transmission and the extraction algorithm based on the KLG-QPS algorithm under the quantum chaos mask are as follows (Algorithm 1):

The secret transmission of speech signals under the conceal of quantum chaos is the main research content.

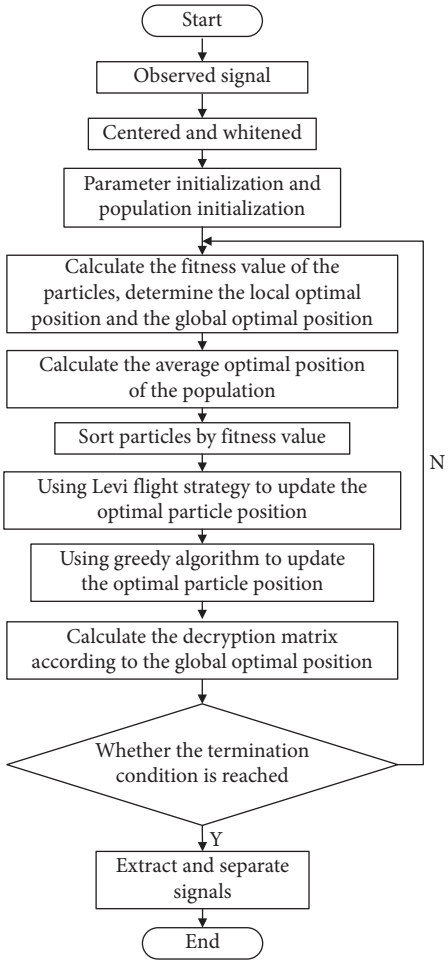


Figure 9: KLG-QPSO algorithm flow chart.

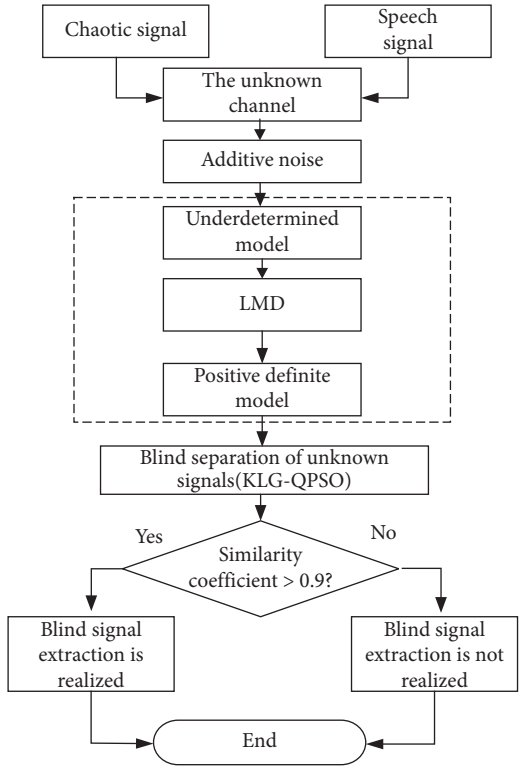


Figure 10: Simulation flow chart.

When analyzing the performance of the proposed system, similarity coefficients and signal-to-interference ratio (SIR) will be used for quantitative evaluation. s_i' and s_j represent source signal and separated signal, respectively. The similarity coefficient can be expressed as the following equation:

$$\xi_{ii} = \xi\left(s_i'(t)s_i(t)\right) = \frac{\left|\sum_{i=1}^{n} s_i'(t)s_i(t)\right|}{\sqrt{\sum_{i=1}^{n} s_i'^{2}(t)\sum_{j=1}^{n} s_i^{2}(t)}}. \tag{42}$$

The similarity coefficient between the source speech signal $s_i(t)$ and the extracted separated speech signal $s_i'(t)$ is between 0 and 1. When the two signals are completely correlated, the similarity between the source speech signal and the extracted and separated speech signal will be higher. At this time, ξ_{ij} is close to 1, indicating that the proposed algorithm has better extraction and separation performance. Otherwise, the smaller the similarity coefficient, the separation effect of the algorithm will be worse.

If $s_{ii}'(t)$ is the part of the extracted separated speech signal that belongs to the source speech signal $s_i(t)$ and $s_{ij}'(t)$ is the part of the extracted separated speech signal that does not belong to the source speech signal $s_i(t)$, then the SIR can be as shown in the following equation:

$$\mathrm{SIR}_i = 10\log 10\frac{\sum_i s_{ii}'^{2}(t)}{\sum_i\sum_j s_{ij}'^{2}(t)}, \tag{43}$$

where $s_{ii}'(t)$ represents the energy from the source speech signal $s_i(t)$ in the extracted and separated speech signal $s_i'(t)$ from the source speech signal $s_i(t)$ and $s_{ij}'(t)$ represents the interference energy from the source speech signal $s_i(t)$ in the extracted and separated speech signal $s_i'(t)$ from other source speech signal. If the value of SIR is larger, the degree of crosstalk suppression is higher and the performance of the system for extracting and separating speech signals will be better.

6. Simulation Experiment and Performance Analysis

The speech in the international standard TIMIT speech database is selected as the source speech signal for encrypted transmission. The length of the signal is 3.6 s, and the sampling frequency is $f_c = 8$ KHz. The number of iterations of the KLG-QPSO algorithm is set to $M = 40$, the population size is set to $N = 40$, the shrinkage expansion coefficient is $\alpha = 0.5, \lambda = 1.5$, and the step size control factor is set $\beta = 1.7$.

(1) **Input:** speech signal (SA1, SA2, SI943), chaotic signal, H, α, λ, β, M, N
(2) Speech signal 8 kHz sampling quantization BPSK, chaos signal quantization BPSK
(3) Obtain observed signal Y with equation (17)
(4) **For** $i = 1{:}n$ **do**
(5) **when** $a_{1i}(t) \neq 1$
(6) $m_{1i}(t)$, $a_{1i}(t) \leftarrow$ AveMove (Y) by equations (6) and (7);
(7) $h_{1i}(t) \leftarrow$ Cal $(Y, m_{1i}(t))$ by equation (8);
(8) $s_{1i}(t) \leftarrow$ Cal $(h_{1i}(t), a_{1i}(t))$ by equation (9);
(9) **Until** $a_{1i}(t) = 1$
(10) $\mathrm{PF}_i(t) \leftarrow$ Cal $s_{1i}(t)$ by equation (14);
(11) **For** $i = 1{:}N$ **do**
(12) $u_i(t) = Y - \mathrm{PF}_i(t)$
(13) **Until** $u_i(t)$ is a monotonic function
(14) **End for**
(15) **End for**
(16) Obtain Y' by equations (16) and (18)
(17) $[m, n] = size[Y']$;
(18) Initialize particle position $P_i = [P_{i1}, P_{i2}, \ldots, P_{i\,D}]$, $1 \leq i \leq N$, $D = m \times n$;
(19) **For** $i = 1{:}M$ **do**
(20) Calculate the adaptation value by equation (40);
(21) Update particle position by equations (36) and (37)
(22) Find the global optimal particle P_g;
(23) $W \leftarrow P_g$;
(24) Calculate $s'(t)$ by equation (41);
(25) **Until** stopping criterion is satisfied;
(26) **End for**
(27) **Output:** $s'(t)$

Algorithm 1: Information hiding transmission and extraction.

6.1. Encryption Analysis of Speech Signal Underdetermined Model. This study only considers the additive white Gaussian noise in the channel and does not consider the internal noise in the chaotic system. Three speech signals SA1, SA2, and SI943 are selected in the speech database. And, the other way selects the quantum chaotic signal generated by the Harper model when $L = K = 10$as the mask signal. There are two array elements $M = 2$ at the receiver. When the SNR is 20 dB, the underdetermined model channel mixing matrix $\mathbf{H}$ of 2×4 is randomly generated:

$$\mathbf{H} = \begin{bmatrix} 0.9115 & 0.5874 & 0.4082 & 0.0359 \\ 0.3422 & 0.1407 & 0.9291 & 0.5777 \end{bmatrix}. \tag{44}$$

The three-way speech is all from women, and their frequency range is roughly the same, which increases the difficulty of separation in a certain extent. Figures 11(a)–11(c) show the time-domain wave diagrams of three speech signals in the source signal, Figures 12(a)–12(c) show the histogram corresponding to three speech signals in the source signal, and Figures 13(a)–13(c) show the spectrum corresponding to three speech signals in the source signal.

These four-way speech signals at the transmitter are mixed with underdetermined model channels to obtain two signals. The two signals are converted into 8 bit data and output in parallel, and PCM decoding is performed to obtain two observation signals. Figures 14(a) and 14(b) show the time-domain waveform of the observed signal, Figures 14(c) and 14(d) show the histogram of the observed signal, and Figures 14(e) and 14(f) show the spectrum of the observed signal.

It can be seen from Figure 14 that the three-way source speech signal is completely hidden by the quantum chaotic signal, and the subjective discrimination ability of the human eye cannot distinguish the useful speech signal information. It proves the validity and reliability of the proposed use of quantum chaotic signal to cover the speech signal in encrypted transmission.

Since the number of observation signals is less than the number of source signals, the virtual array unit is supplemented by LMD, and the underdetermined model is transformed into the positive model to construct the virtual receiving array. Then, the KLG-QPSO algorithm is used to process the four-channel observed signal, and the estimated signal is obtained. The extracted estimated signal is processed by parallel serial transformation and PCM decoding, and the three-way extracted and separated speech signal is shown in Figure 15. Figures 15(a)–15(c) are time-domain waveform corresponding to the three extracted speech signals, Figures 16(a)–16(c) are the histogram corresponding to the extracted three speech signals, and Figures 17(a)–17(c) are the spectrum corresponding to the three speech signals after extraction.

According to the separation result, the time-domain waveform, histogram, and spectrogram of the extracted speech signal are very close to the time-domain waveform, histogram, and spectrogram of the source speech signal. The useful information in the speech signal information can be

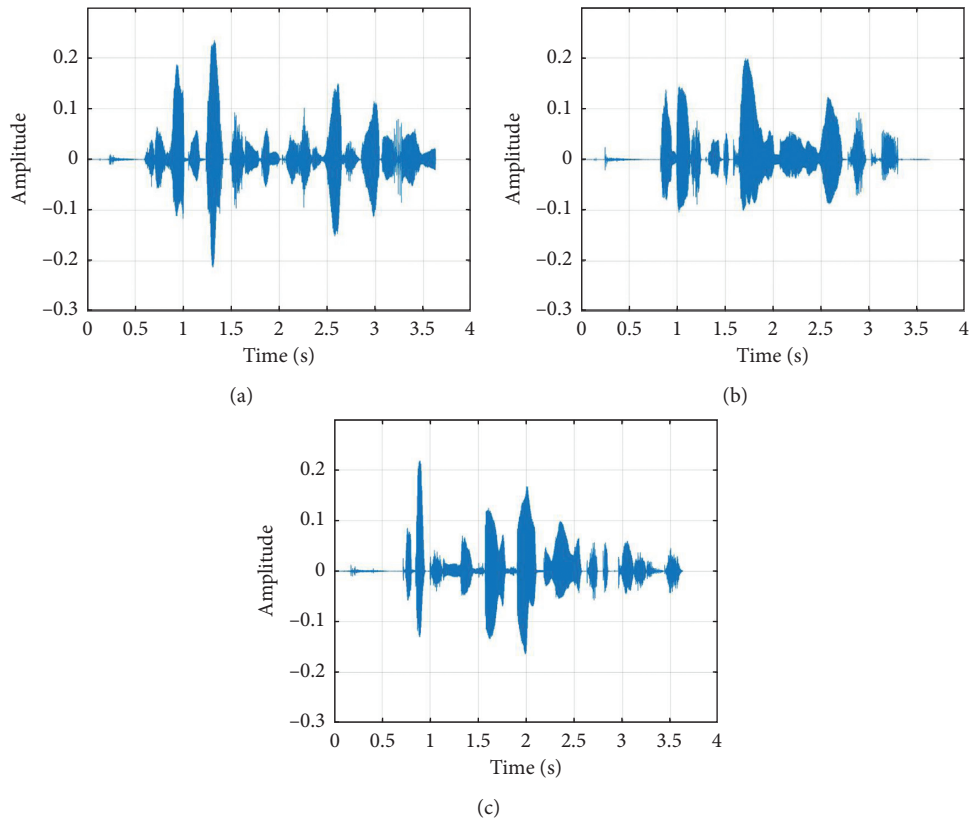


Figure 11: Time-domain waveforms of source signals (three speech signals): (a) SA1 speech signal; (b) SA2 speech signal; (c) SI943 speech signal.

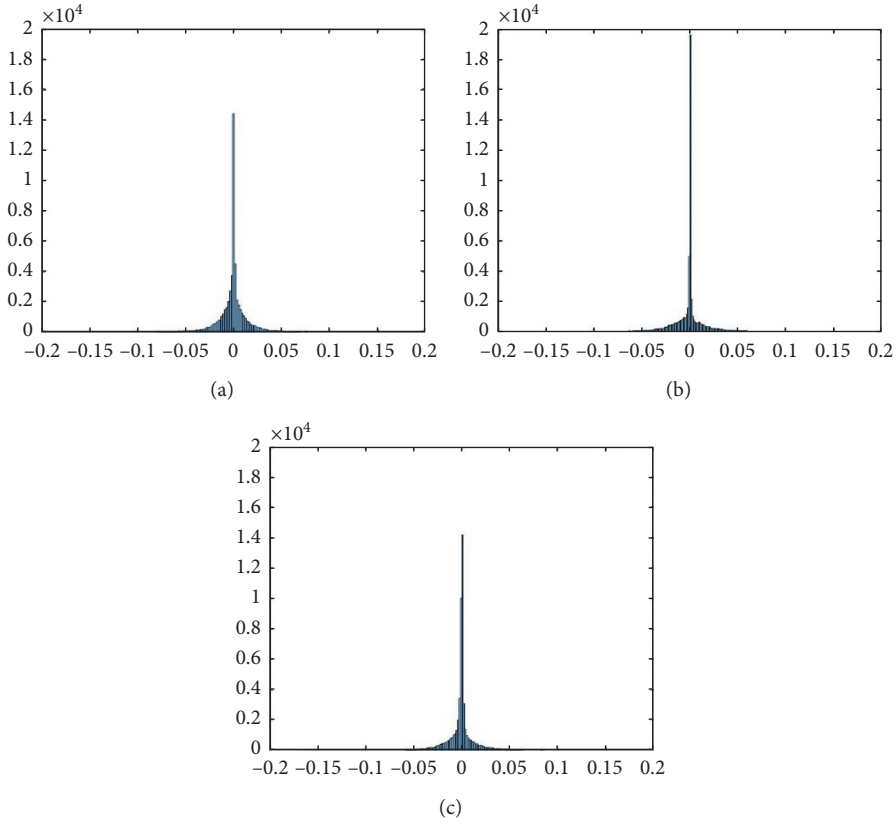


Figure 12: Histograms of source signals (three speech signals): (a) SA1 speech signal; (b) SA2 speech signal; (c) SI943 speech signal.

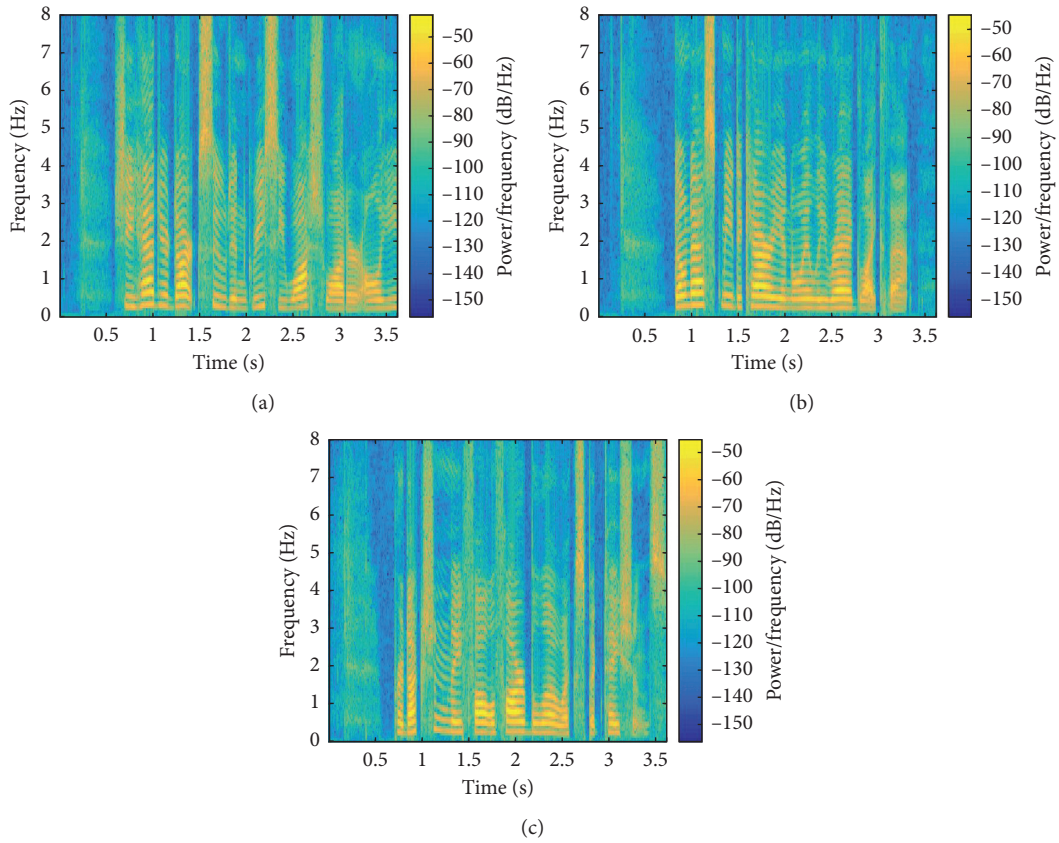


Figure 13: Spectrograms of source signals (three speech signals): (a) SA1 speech signal; (b) SA2 speech signal; (c) SI943 speech signal.

distinguished by the subjective distinguishing ability of the human eye. The similarity coefficient and SIR to evaluate the performance of the extracted speech signal are shown in Table 1.

Table 1 shows the data results of the similarity coefficient and SIR of each speech signal under the condition of SNR = 20 dB. It can be seen that the speech signal extraction and separation algorithm proposed in this paper have better performance.

By changing the value of SNR, repeat the above experiment, test the bit error rate under different SNR conditions, and extract the similarity coefficient between the speech signal and the source speech signal and the change of SIR. The bit error rate of the extracted speech signal under different SNRs, the similarity coefficient of the extracted speech signal and the source speech signal, and the change curve of SIR are shown in Figures 18–20, respectively.

It can be seen from Figure 18 that with the increase in SNR, the channel environment has been improved, and the overall bit error rate has shown a downward trend. The bit error rate is about without modulation. It can be seen from Figure 19 that as the SNR increases, the similarity coefficient between the extracted speech signal and the source speech signal shows an overall upward trend. When SNR = 24 dB, the similarity coefficient between the extracted speech signal and the source speech signal is already very close to 1. As can be seen from Figure 20, as the SNR increases, the SIR also gradually increases. The reason for the above results is that when the SNR increases, the signal propagation environment is improved. At this time, the influence of noise or interference is reduced, and the effectiveness of the extraction and separation algorithm is naturally improved.

6.2. Performance Analysis. This part will analyze the security of using quantum chaotic signals as masking signals to mask and encrypt speech signals and the complexity of the proposed speech signal extraction and separation algorithm.

6.2.1. Encryption Effect Analysis. The proposed speech signal encryption method uses the quantum chaotic signal generated by the Harper model as a mask signal to mask and encrypt the speech signal to convert it into an incomprehensible signal. Comparing the time-domain waveform (Figure 11), histogram (Figure 12), and spectrogram (Figure 13) of the source speech signal with the time-domain waveform, histogram, and spectrogram (Figure 14) of the encrypted speech signal, it can be seen that the source speech signal cannot be distinguished from the observation signal. The performance of the proposed encryption method is evaluated by comparing whether the disorder or uncertainty level of the observed signal is higher than that of the source signal. In this paper, entropy (H) [32, 33] and disorder levels (DLs) [34] will be used to evaluate the level of uncertainty and disorder. Table 2 shows the entropy (H) and disorder levels (DLs) between the source speech signal and the

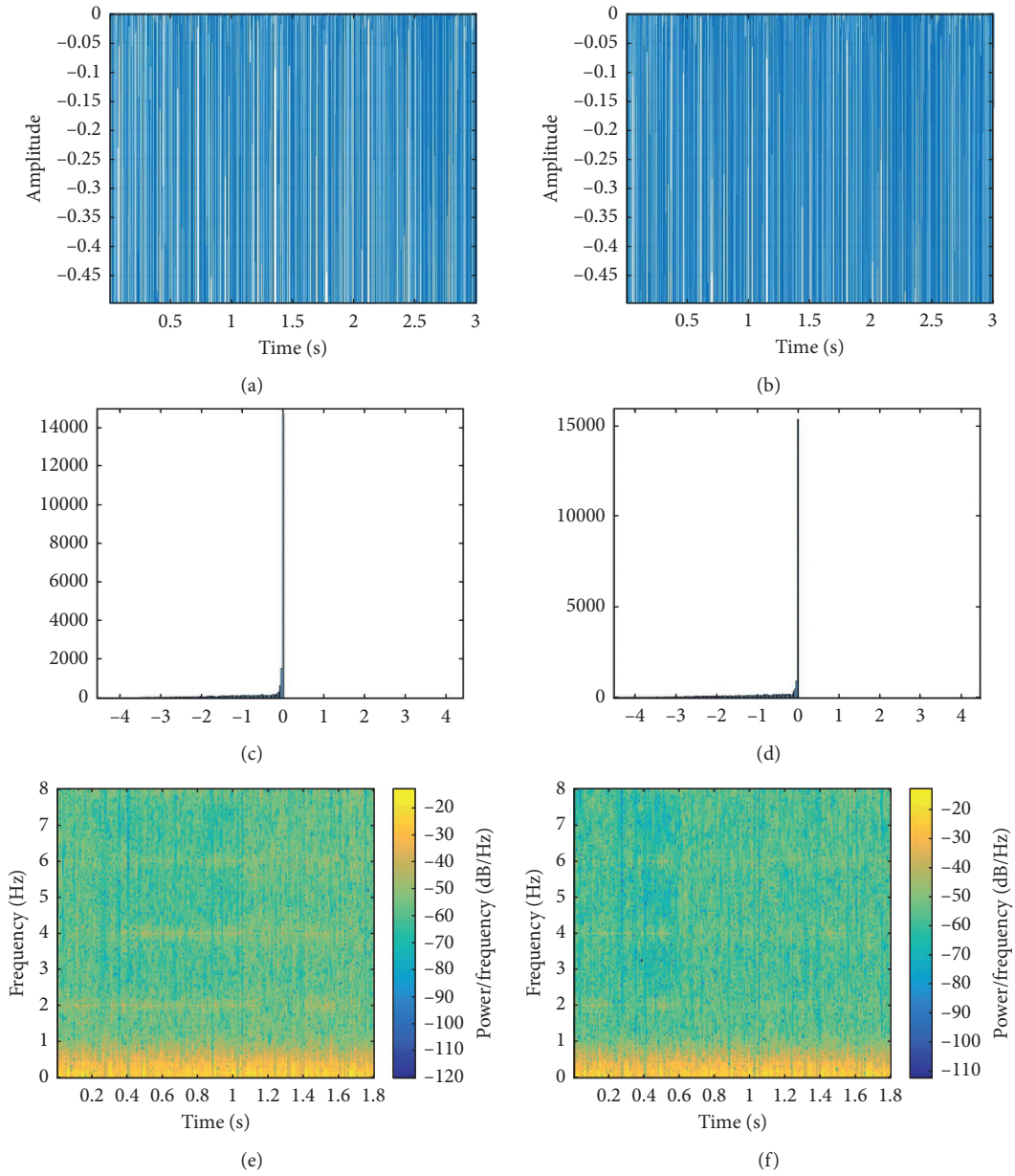


Figure 14: Observed signal: (a) time-domain waveforms of the first observation signal; (b) time-domain waveforms of the second observation signal; (c) histograms of the first observation signal; (d) histograms of the second observation signal; (e) spectrograms of the first observation signal; (f) spectrograms of the second observation signal.

observed signal, and Table 3 shows the similarity coefficient between the source speech signal and the observed signal.

Tables 2 and 3 compare H, DL, and similarity coefficient of source speech signal and observed signal, respectively. According to the data in Table 2, the entropy of the observed signal is about 30% higher than that of the source speech signal, which means that the uncertainty of the observed signal is much higher. The DL of the observed signal is about 6 times that of the source speech signal, which means that the amplitudes of the adjacent samples in the observed signal are more variable. The entropy (H) of the observed signal is about 7.4824 and the degree of disorder (DL) is about 1.1979, which are similar to the maximum possible entropy and maximum possible disorder of 8 and 2, respectively [33].

From the data in Table 3, it can be seen that the similarity coefficient between the source speech signal and the observed signal is almost zero, which means that they are independent of each other.

This paper compares the proposed method with several other methods and compares the similarity coefficient between the source speech signal and the observed signal. The encryption algorithm based on Zaslavsky chaotic map [9], the speech encryption method based on cosine number transformation [35], the method of using the multiscroll

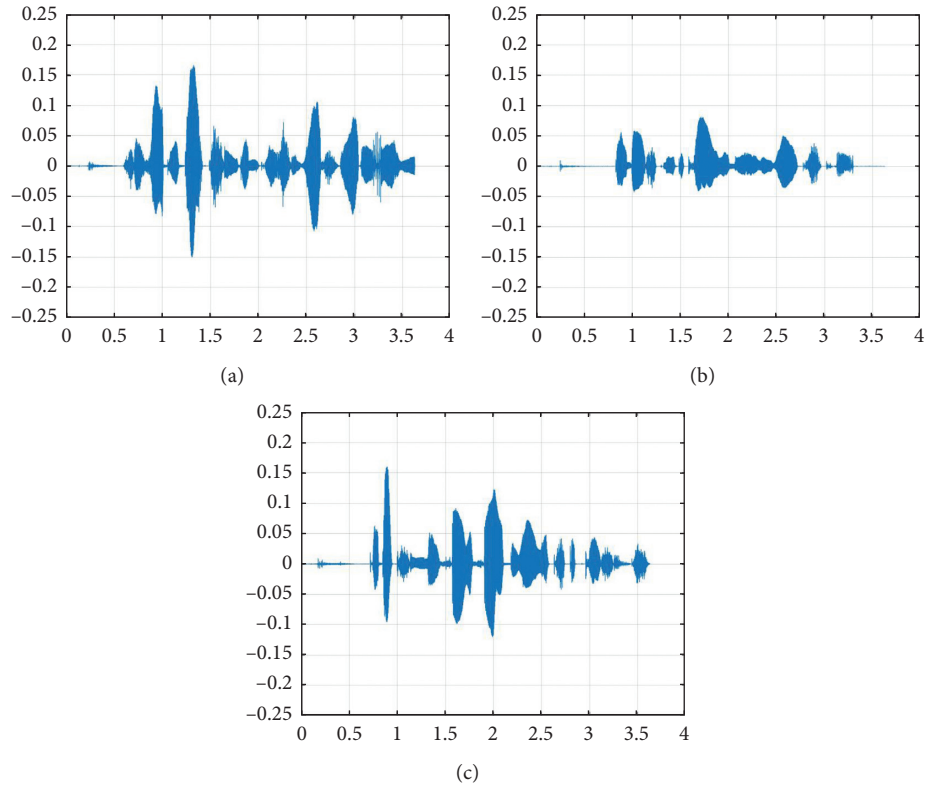


Figure 15: Time-domain waveform diagram of speech signal extraction under quantum chaos: (a) SA1 speech signal; (b) SA2 speech signal; (c) SI943 speech signal.

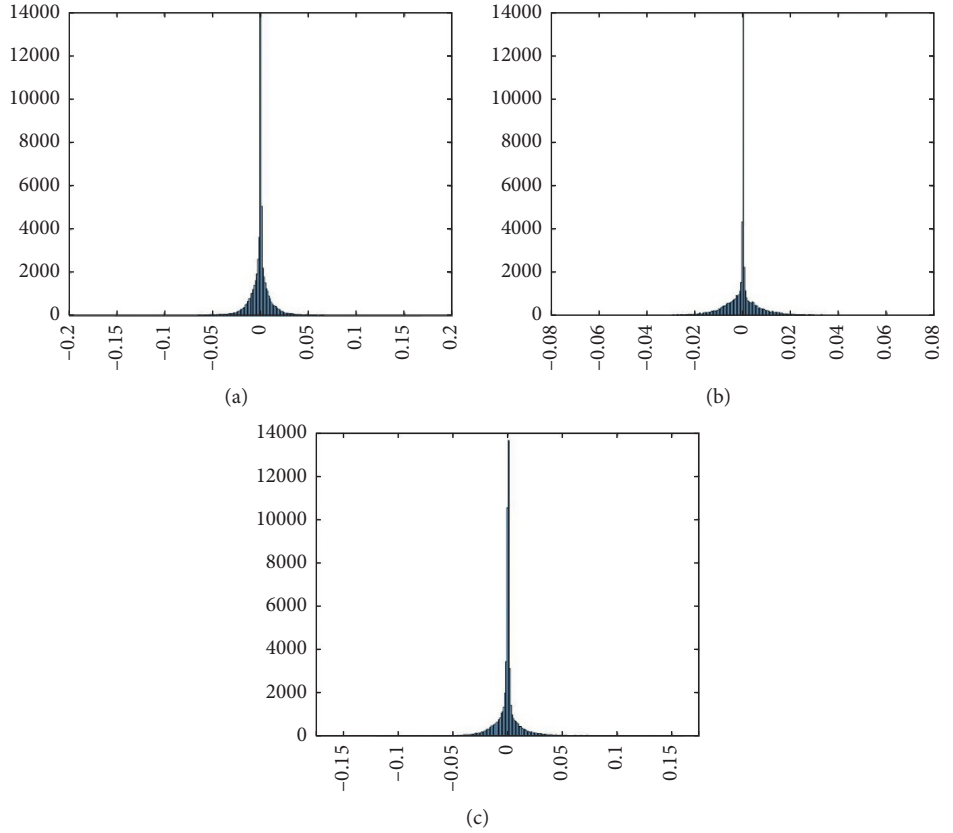


Figure 16: Histogram of speech signal extraction under quantum chaos: (a) SA1 speech signal; (b) SA2 speech signal; (c) SI943 speech signal.

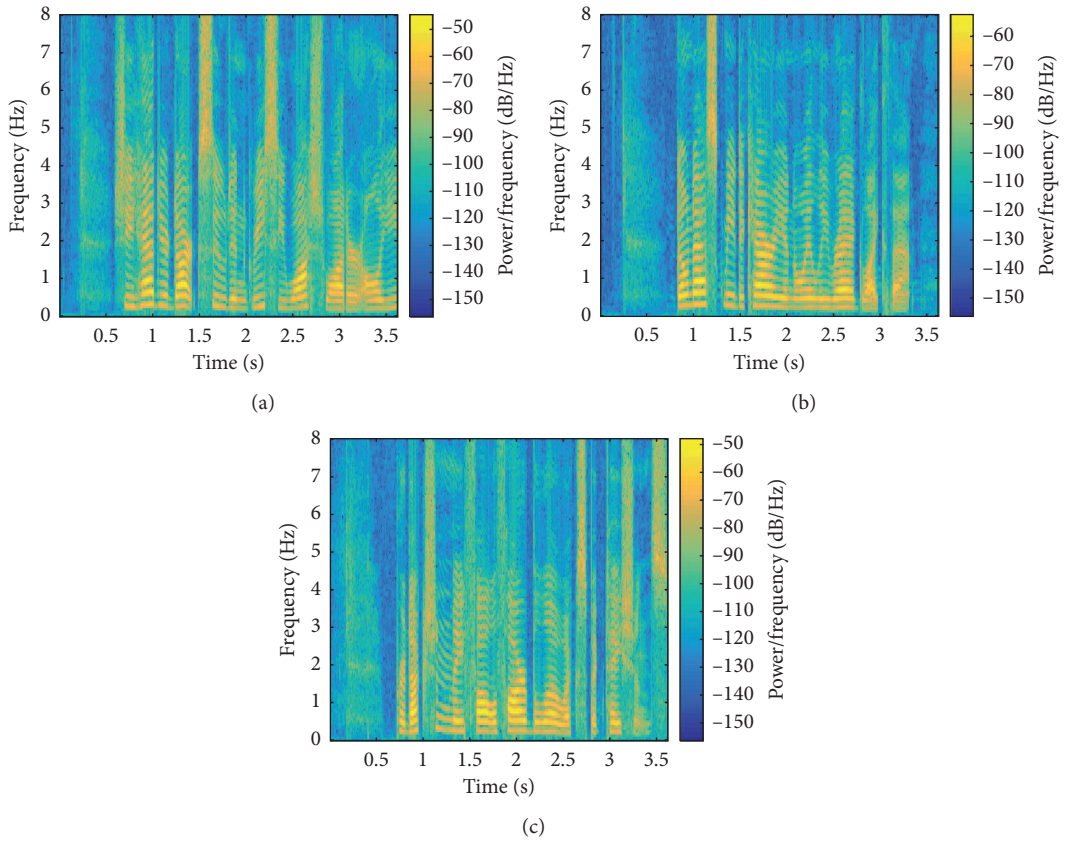


Figure 17: Spectrum diagram of speech signal extraction under quantum chaos: (a) SA1 speech signal; (b) SA2 speech signal; (c) SI943 speech signal.

Table 1: Characteristics needed to detect interfloor.

Signal	Similarity coefficient	SIR
SA1	0.9629	20.9843
SA2	0.9457	20.8865
SI943	0.9416	20.8023

chaotic system to confuse and diffuse speech data [36], and the audio encryption algorithm based on DNA coding and chaotic system [37] are compared. The comparison of the correlation coefficient between the observation signal and the source signal obtained after using these encryption methods to encrypt the source speech signal is shown in Table 4. The closer the correlation coefficient is to 0, the lower the correlation between the two, and the encryption effect will be better.

Table 4 shows the similarity coefficients of the source speech signal and the observed signal under different encryption methods. Correlation (1st) represents the similarity coefficient between the original speech signal and the first observation signal. Correlation (2rd) represents the similarity coefficient between the original speech signal and the second observation signal. It can be seen from the table that under the three source speech signals of SA1, SA2, and SI943, the correlation coefficient of the two observation signals processed by the proposed method is about 0.00042; The correlation coefficient of the two observation signals processed by the Hamza and Titouna method is about 0.001243; the Lima and da Silva Neto method is about 0.0017783, and the Hongjun et al. method is about 0.003215, and the correlation coefficient of the Wang and Su method for processing the two observation signals is about 0.001467. From the data results, it can be seen that compared with the other four methods, the similarity coefficient between the observed signal and the source speech signal of the proposed method is closer to 0, showing good encryption performance, which verifies that quantum chaotic signals have outstanding performance in speech signal encryption.

6.2.2. Key Sensitivity Analysis. To measure an encryption algorithm, the sensitivity of key needs to be tested [38]. If the key is sensitive, then a small change in the key will cause a significant change in the output. The quantum chaotic signal generated by the Harper model will produce different

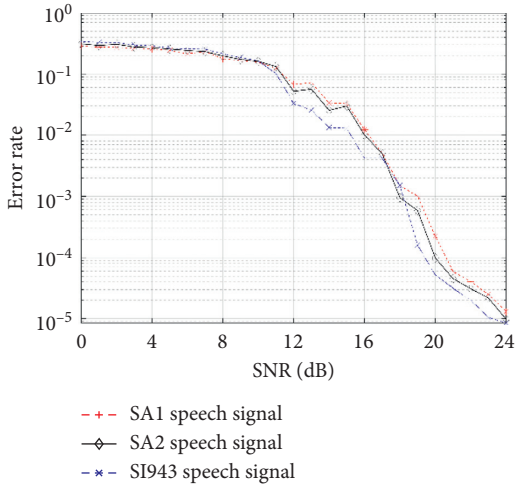


Figure 18: Bit error rate of speech signal.

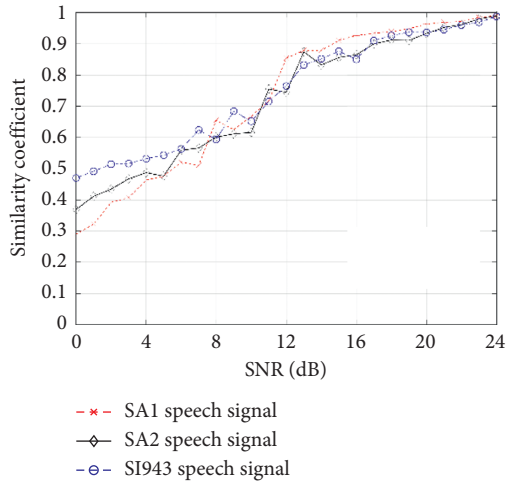


Figure 19: Similarity coefficient of speech signal.

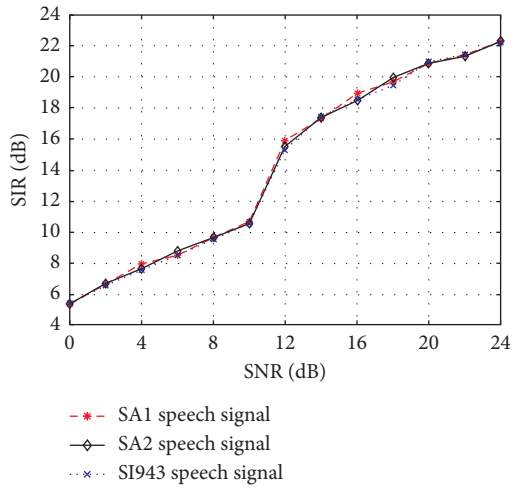


Figure 20: SIR of speech signal.

Table 2: Entropy (H) and disorder levels (DLs) between source speech signal and observed signal.

	Original signal			Observation signal	
	SA1	SA2	SI943	First observed	Second observed
H	5.1327	5.4812	5.2043	7.3847	7.5801
DL	0.2165	0.2043	0.2174	1.1943	1.2014

Table 3: Similarity coefficient of source speech signal and observed signal.

	Original signal		
	SA1	SA2	SI943
First observed	0.00056	0.00023	0.00048
Second observed	0.00043	0.00045	0.00037

Table 4: Similarity coefficients between source speech signal and observed signal.

	SA1		SA2		SI943	
	Correlation (1st)	Correlation (2rd)	Correlation (1st)	Correlation (2rd)	Correlation (1st)	Correlation (2rd)
Hamza and Titouna [9]	0.00067	0.00197	0.00127	0.00095	0.00131	0.00129
Lima and da Silva Neto [35]	0.00167	0.00145	0.00175	0.00184	0.00195	0.00201
Hongjun et al. [36]	0.00431	0.00358	0.00218	0.00231	0.00364	0.00327
Wang and Su [37]	0.00086	0.00186	0.00073	0.00138	0.00219	0.00148
Proposed	0.00056	0.00043	0.00023	0.00045	0.00048	0.00037

Table 5: Similarity coefficient between encrypted signal and source speech signal.

	$K = L = 10$	$K = L = 7$	$K = L = 4$
Similarity coefficient	0.00032	0.00094	0.00262

Table 6: Complexity of speech signal extraction and separation algorithm.

Step	Complexity
1.LMD	$C_1 = O(M_{\text{Original}} \cdot M_{\text{Observed}} \cdot \log(H))$
2.KLG-QPSO	$C_2 = M * O(N^2)$

chaotic signals when the parameter $L = K$ is set to different values, as shown in Figure 3. In order to study the sensitivity of using quantum chaotic signal as a key, the paper adds that when $L = K$ is equal to 10, 7, and 4, the chaotic signal generated by the Harper model encrypts the SA1 speech signal, and the similarity coefficient of encrypted signal and the source signal is compared and analyzed as shown in Table 5. From the data in Table 5, it can be seen that the encryption effect is different when $L = K$ is set to a different value. The chaotic signal generated when $L = K = 10$ has a significantly higher encryption effect on the SA1 voice signal than $L = K = 7$ or 4. Because with the increase in the value of $L = K$, the quantum chaotic signal generated by the Harper model is more complex and has a higher high-energy density, which can effectively encrypt the signal. In Table 5, the difference between $K = L = 10$ and $K = L = 7$ is 3, and the encrypted signal is 99.01432%; $K = L = 7$ and $K = L = 4$ are also 3, and the encrypted signal is 99.18651%; the difference between $K = L = 10$ and $K = L = 4$ is 6, and the difference between the encrypted signal is 99.8642%, which proves that using the quantum chaotic signal as the key to encrypt the speech signal has a high sensitivity. Table 5 shows similarity coefficient between encrypted signal and source speech signal $K = L = 10$, $K = L = 7$, and $K = L = 4$, which is 0.00032, 0.00094, and 0.00262, respectively.

6.2.3. Algorithm Complexity Analysis. This section analyzes and calculates the complexity of the proposed LMD-KLG-QPS algorithm. Suppose the number of iterations based on the KLG-QPSO algorithm is M, and the population number is N; the number of runs of LMD to construct a virtual receiving array is H; the number of source signals is M_{Original}; the number of observation signals is M_{Observed}. The complexity of the speech signal extraction and separation algorithm is shown in Table 6.

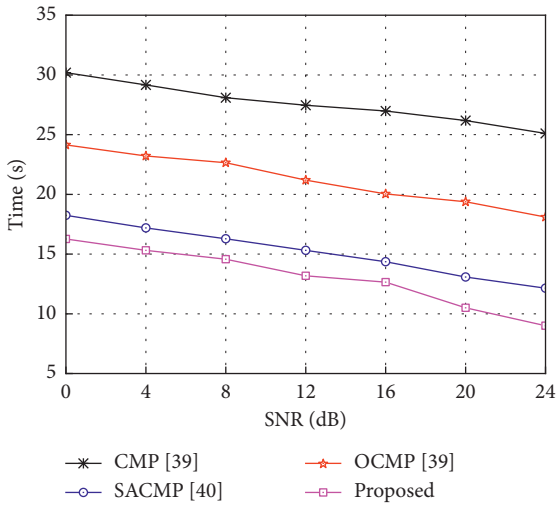


Figure 21: Computational time based on SNR of different algorithms.

These analyses were performed on a PC equipped with a Windows 10 64 bit operating system, a 1.80 GHz Intel(TM) i7-8550U 4-core processor, and Matlab 2016a 8 GB RAM.

The complexity of the proposed LMD-KLG-QPS algorithm is as follows:

$$C = C_1 + C_2. \tag{45}$$

It can be seen from Table 6 that the complexity of the proposed LMD-KLG-QPS algorithm is $O(M_{\text{Original}} \cdot M_{\text{Encrypted}} \cdot \log(H)) + M * O(N^2)$. We also use CMP [39], OCMP [39], and SACMP [40] algorithms to extract separate source speech signals. The calculation time of these algorithms under different SNRs is shown in Figure 21. Compared with CMP, OCMP, and SACMP, the proposed algorithm reduces the calculation time by 23.6, 13.5, and 5.2%, respectively. It can be seen from the data results that the proposed method consumes less calculation time compared with the other three methods. The computational complexity is significantly better than the other three algorithms, which verifies that the proposed algorithm has good performance.

7. Conclusions

Speech signal encryption technology has been widely used in enterprises and military fields. Using a secure password system to protect speech signals in wired and wireless communications is very important. This paper proposes a speech signal encryption transmission method based on the underdetermined model under the cover of quantum chaotic signal. The quantum chaotic signal generated by the Harper model when $L = K = 10$ is used as a masking signal to mask and encrypt the speech signal to be transmitted. Then, a virtual receiving array is constructed by the LMD method, converting the underdetermined model into a positive definite model. Lastly, the KLG-QPSO algorithm is used to process the signal to realize the encrypted transmission and blind extraction of the speech signal. The simulation experiment verifies the validity and reliability of the proposed LMD-KLG-QPSO algorithm. By comparing the entropy (H) and disorder degree (DL) with maximum possible entropy and maximum possible disorder and comparing with other methods, it is verified that the proposed method is more secure. In addition, compared with CMP, OCMP, and SACMP, the time cost of the proposed algorithm is smaller.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the Natural Science Foundation of Heilongjiang Province, China (no. LH2019F048), Heilongjiang University Outstanding Youth Science Foundation, and the National Natural Science Foundation of China (nos. 61801173 and 61771186).

References

[1] S. Sun, Y. Guo, and R. Wu, "A novel plaintext-related image encryption algorithm based on stochastic signal insertion and block swapping," *IEEE Access*, vol. 7, pp. 123049–123060, 2019.

[2] D. Shah, T. shah, and S. S. Jamal, "Digital audio signals encryption by Mobius transformation and Hénon map," *Multimedia Systems*, vol. 26, pp. 235–245, 2020.

[3] S. Bhattacharya and P. K. R. Maddikunta, "A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU," *Electronics*, vol. 9, no. 2, pp. 219–235, 2020.

[4] L. Hongjun and W. Xingyuan, "Color image encryption based on one-time keys and robust chaotic maps," *Computers and Mathematics with Applications*, vol. 59, pp. 3320–3327, 2010.

[5] L. Hongjun and W. Xingyuan, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Optics Communications*, vol. 287, no. 16-17, pp. 3895–3905, 2010.

[6] Y. M. Hameed and N. H. M. Ali, "An efficient audio encryption based on chaotic logistic map with 3D matrix," *Journal of Theoretical and Applied Information Technology*, vol. 96, no. 16, pp. pp5142–5152, 2018.

[7] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *Eursip J Audio Speech Music Process*, vol. 2017, 2017.

[8] E. Mosa, N. W. Messiha, O. Zahran, and F. E. Abd El-Samie, "Chaotic encryption of speech signals," *International Journal of Speech Technology*, vol. 14, no. 4, pp. 285–296, 2011.

[9] R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," *Information Security Journal: A Global Perspective*, vol. 25, no. 4–6, pp. 162–179, 2016.

[10] Z. Fangfang and L. Shutang, "Self-time-delay synchronization of time-delay coupled complex chaotic system and its applications to communication," *International Journal of Modern Physics C*, vol. 25, no. 3, 2014.
[11] L. Xiaofeng, "Locating and imaging contact delamination based on chaotic detection of nonlinear Lamb waves," *Mechanical Systems & Signal Processing*.vol. 109, pp. 58–73, 2018.
[12] A.-O. Boudraa and J.-C. Cexus, "EMD-based signal filtering," *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no. 6, pp. 2196–2202, 2007.
[13] Y. Guo, G. R. Naik, and H. Nguyen, "Single channel blind source separation based local mean decomposition for Biomedical applications," *IEEE Engineering in Medicine and Biology Society*, vol. 2013, pp. 6812–6815, 2013.
[14] A. Sadhu, S. Narasimhan, and J. Antoni, "A review of output-only structural mode identification literature employing blind source separation methods," *Mechanical Systems and Signal Processing*, vol. 94, no. 15, pp. 415–431, 2017.
[15] W. Fu, B. Nong, X. Zhou, J. Liu, and C. Li, "Source recovery in underdetermined blind source separation based on artificial neural network," *China Communications*, vol. 15, no. 1, pp. 140–154, 2018.
[16] J. Li, "The study of blind source separation based on sparsity and decorrelation," *IOP Conference Series Materials Science and Engineering*, vol. 394, no. 5, pp. 394–399, 2018.
[17] P. Comon, "Independent component analysis, A new concept?" *Signal Processing*, vol. 36, no. 3, pp. 287–314, 1994.
[18] C. W. Hesse and C. J. James, "The FastICA algorithm with spatial constraints," *IEEE Signal Processing Letters*, vol. 12, no. 11, pp. 792–795, 2005.
[19] T. Ahmad, H. N. B. Alias, and M. Ghanbari, "Separation of the EEG signal using improved FastICA based on kurtosis contrast function," *Australian Journal of Basic and Applied Sciences*, vol. 5, no. 9, pp. 2152–2156, 2011.
[20] Q. Li, Z. Wang, Z. Huang, K. Guo, and L. Liu, "Implementation of blind source separation for optical fiber sensing," *Applied Optics*, vol. 53, no. 9, pp. 1832–1837, 2014.
[21] R. Labounek, D. A. Bridwell, R. MareEk et al., "Stable scalp EEG spatiospectral patterns across paradigms estimated by group ICA," *Brain Topography*, vol. 31, no. 5, pp. 76–89, 2017.
[22] V. G. Reju, S. N. Koh, and I. Y. Soon, "An algorithm for mixing matrix estimation in instantaneous blind source separation," *Signal Processing*, vol. 89, no. 9, pp. 1762–1773, 2009.
[23] L. Benjamin and G. Bertrand, "Quantum computation of a complex system: the kicked harper model," *Physical Review E*, vol. 70, 2004.
[24] G. A. Gottwald and I. Melbourne, "A new test for chaos in deterministic systems," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 460, no. 2042, pp. 603–611, 2004.
[25] C. An and T. Xueting, *Laypunov Irregular Points with Distributional Chaos*, Dynamical Systems, London, UK, 2019.
[26] U. Nathaniel, N. Beloff, and N. George, "Instantaneous frequency and wave mode identification in a magnetosheath using few spatial points," *Chinese Physics B*, vol. 22, no. 8, 2013.
[27] W. Tailai, "Feature extraction of electronic nose signals using QPSO-based multiple KFDA signal processing," *Sensors*, vol. 18, no. 2, p. 388, 2018.
[28] M. Clerc and J. Kennedy, "The particle swarm-explosion, stability, and convergence in a multidimensional complex space," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 1, pp. 58–73, 2002.
[29] B. Ming, "Cascade reservoir operation optimization based-on improved Cuckoo Search," *Journal of Hydraulic Engineering*, vol. 46, pp. 341–349, 2015.
[30] X. Zhao, "A greedy genetic algorithm for unconstrained global optimization," *Journal of Systems Science and Complexity*, vol. 18, no. 1, pp. 102–110, 2005.
[31] E. Eweda, N. J. Bershad, and J. C. M. Bermudez, "Stochastic analysis of the LMS and NLMS algorithms for cyclostationary white Gaussian and non-Gaussian inputs," *IEEE Transactions on Signal Processing*, vol. 66, no. 18, pp. 4753–4765, 2018.
[32] D. Robinson, "Entropy and uncertainty," *Entropy*, vol. 10, no. 4, pp. 493–506, 2008.
[33] D. Renza, S. Mendoza, and D. M. Ballesteros, "High-uncertainty audio signal encryption based on the Collatz conjecture," *Journal of Information Security and Applications*, vol. 46, pp. 62–69, 2019.
[34] D. M. Ballesteros, J. Peña, and D. Renza, "A novel image encryption scheme based on collatz conjecture," *Entropy*, vol. 20, no. 12, 2018.
[35] J. B. Lima and E. F. da Silva Neto, "Audio encryption based on the cosine number transform," *Multimedia Tools and Applications*, vol. 75, no. 14, pp. 8403–8418, 2015.
[36] L. Hongjun, K. Abdurahman, and L. Yanling, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik*, vol. 127, no. 19, pp. 7431–7438, 2016.
[37] X. Wang and Y. Su, "An audio encryption algorithm based on DNA coding and chaotic system," *IEEE Access*, vol. 8, pp. 9260–9270, 2019.
[38] Zh. Ying Qian and W. Xing Yuan, "A new image encryption algorithm based on non-adjacent coupledmap lattices," *Applied Soft Computing*, vol. 26, pp. 10–20, 2015.
[39] G. Rath and C. Guillemot, "Complementary matching pursuit algorithms for sparse approximation," 2008.
[40] D. Wei, J. Mao, and Y. Liu, "An improved complementary matching pursuit algorithm for compressed sensing signal reconstruction," 2011.