基于改进 Henon 映射和超混沌的双重语音加密算法

张秋余，宋宇杰
（兰州理工大学计算机与通信学院，甘肃 兰州 730050）

摘　要：针对现有语音混沌加密算法密钥空间小、安全性差、加密效率低且无法实现密钥复杂度与加密效率的权衡等问题，提出了一种改进 Henon 映射和超混沌的双重语音加密算法。首先，为了使 Henon 映射具有更大的混沌空间和更高的混沌复杂度，通过扩展控制参数范围将非线性三角函数作为输入参数变量等手段对经典 Henon 映射进行了改进；其次，利用改进的 Henon 映射生成伪随机序列，并对语音数据进行单次不重复置乱加密，获得语音数据的初次加密结果；最后，利用 Lorenz 超混沌系统对初次加密后的语音数据进行 Arnold 二次置乱加密和异或扩散加密，获得最终的密文语音数据。实验结果表明，与现有方法相比该算法具有更大的密钥空间和更高的加密效率，且对各种密码攻击拥有更好的鲁棒性。

关键词：语音加密；改进的 Henon 映射；Lorenz 超混沌系统；Arnold 变换；鲁棒性
中图分类号：TP309
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021271

A dual speech encryption algorithm based on improved Henon mapping and hyperchaotic

ZHANG Qiuyu, SONG Yujie
School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

Abstract: Aiming at the problems of small key space, poor security, low encryption efficiency, and the inability to realize the trade-off between key complexity and encryption efficiency of existing speech chaotic encryption algorithms, a dual speech encryption algorithm based on improved Henon mapping and hyperchaotic was proposed. Firstly, the traditional Henon mapping was improved by extending the control parameter range and taking the nonlinear trigonometric function as the input parameter variable, which made the Henon mapping have larger chaotic space and higher chaotic complexity. Secondly, the improved Henon mapping was used to generate pseudorandom sequence, and the speech data was encrypted single time without repeated scrambling to obtain the first time encryption results of the speech data. Finally, Lorenz hyperchaotic system was adopted to encrypt the speech data after the first time encryption by Arnold secondary scrambling encryption and XOR diffusion encryption to obtaining the final ciphertext speech data. The experimental results show that, compared with the existing methods, the proposed algorithm have larger key space, higher encryption efficiency, and stronger robustness against various cryptographic attacks.

Key words: speech encryption, improved Henon mapping, Lorenz hyperchaotic system, Arnold transform, robustness

收稿日期：2021−09−09；**修回日期**：2021−12−10
基金项目：国家自然科学基金资助项目（No.61862041）
Foundation Item: The National Natural Science Foundation of China (No.61862041)

1 引言

随着云存储、计算机网络的快速发展，多媒体技术已经在人类的日常生活中发挥了重要作用[1]。其中，语音具有表义功能而被广泛关注，如会议录音、法庭证据等，这些应用都体现了语音内容的重要性，如何确保语音数据的安全传输成为研究热点之一。

目前，学者们提出了许多用于保护语音数据的加密方法。常用的加密方法有混沌映射加密[2]、置乱加密、同态加密[3]、AES 加密[4]、RSA 加密[5]、DES 加密[6]等，这些加密方法使加密后的语音数据变得杂乱无章，有效地保护了语音数据免受不法分子的破译和篡改。混沌系统生成的随机序列因其对初值敏感性、密钥不可预测性和良好的统计特征，被广泛地应用于图像、音频、视频等多媒体加密[7]。经典的混沌系统主要包括一维的 Logistic 映射[8]、二维的 Henon 映射[9]、三维的 Lorenz 映射[10]以及基于改进的超混沌系统。但现有低维的混沌映射大多存在周期性短、混沌区间小、复杂度低等问题，无法实现对多媒体数据的安全加密；高维的混沌映射又普遍存在算法复杂度高、加密效率低等问题，无法实现海量多媒体数据的安全存储。因此，学者们对常用的混沌加密算法进行了改进和创新，并取得了众多成果。通常混沌加密算法的改进主要分为两类：一类是通过优化改进适用于语音加密的伪随机序列；另一类是针对加密算法的设计结构改进和创新。

针对第一类语音加密方案中，不少学者在保证不改变系统变量的情况下，对经典的混沌映射进行改进，创建了具有系统复杂度更高的混沌系统用以实现对多媒体数据加密。Sayed 等[11]提出一种具有 3 个独立参数改进的混沌映射，并利用该算法与置换网络实现了语音加密。改进的混沌映射增强了混沌特性，简化了映射方程的取模运算，有效地克服了控制参数范围限制和动态退化问题。Farsana 等[12]提出一种基于音频置乱的语音加密方案，该方案在经典 Henon 映射的基础上对算法进行优化改进，改进后的算法具有更大的混沌区间和更高的系统复杂性，使用改进的 Henon 映射对语音数据执行置乱操作，结合 Lorenz 超混沌系统进行替换操作，实现了语音数据高效安全的加密。Hamdi 等[13]通过改进 Henon 映射，增大了混沌参数区间，减小了周期窗口，扩展了密钥空间。为避免长时间使用固定混沌序列作为密钥带来的安全隐患，该方法增加混沌序列的随机性，并利用动态分组加/解密系统良好的保密性，有效防止了基于混沌的模型重构方法带来的攻击，提高了算法的鲁棒性。Zghair 等[14]提出一种具有 12 个正参数的七维三阶非线性超混沌系统，该算法增加了语音的密钥空间，提高了算法的鲁棒性，但高维数的混沌系统增加了算法复杂度，降低了加密效率。

另一类语音加密方案是通过对现有的加密结构设计优化，用以实现更高效安全的多媒体信息加密。如 Shah 等[15]提出一种新的三维混沌映射的语音加密方案，首先将语音分成 8 位序列和 7 位序列，随后对分离的序列用不同高质量的替换盒进行替换，并将替换盒通过伽罗瓦域上 Mobius 变换生成密文语音，能够抵抗统计攻击和差分攻击，具有较强的鲁棒性。Imran 等[16]提出一种非对称密钥语音加密模型，发送方使用生成的公钥对语音加密，接收方使用生成的私钥解密并实现语音重构，具有较高的安全性。Elsafty 等[17]提出一种基于动态 S-box 的语音加密算法，该算法提出 S 盒中的数据并不是固定不变的，而是利用混沌系统生成的伪随机序列对 S 盒中的数据进行动态变换，用以实现语音数据加、解密。

综上所述，为了解决现有基于混沌映射的语音加密算法大多存在密钥空间和加密算法复杂度等问题，本文给出了一种基于改进 Henon 映射和超混沌的双重语音加密算法，该算法在确保语音

加密系统拥有较大密钥空间的同时，降低了语音数据的加密时间，增加了算法的鲁棒性，实现了高效安全的语音加密。本文的主要创新工作如下。

（1）为了解决现有混沌系统控制参数多、混沌区间小等问题，通过扩展控制参数范围、将非线性三角函数作为输入参数变量等手段对经典 Henon 映射进行了改进，增大了混沌序列的伪随机性。

（2）利用改进 Henon 映射生成的伪随机序列对语音数据实现单次不重复置乱加密，克服了传统随机置乱加密中对单列数据重复置乱的缺点，减少了语音的加密时间，提高了语音加密效率。

（3）为了提高加密算法的密钥空间、鲁棒性和安全性，将改进 Henon 映射与 Lorenz 超混沌加密系统相结合，采用改进的广义 Arnold 置乱算法，实现了语音数据双重加密。

2　预备知识

2.1　改进的 Henon 混沌系统

经典的 Henon 映射函数[18]表达式如式（1）所示。

$$\begin{cases} x_{n+1} = 1 + y_n - ax_n^2 \\ y_{n+1} = bx_n \end{cases} \tag{1}$$

其中，x 和 y 为输入参数，n 为迭代次数，a、b 为系统参数。当 a=1.4、b=0.3 时，系统处于混沌状态。

本文改进的 Henon 混沌映射是在经典的 Henon 混沌映射的基础上对函数表达式和系统参数进行改进，改进的 Henon 映射表达式如式（2）所示。

$$\begin{cases} x_{n+1} = 1 - a_1 \cos y_n - a_1 \sin x_n \\ y_{n+1} = x_n + b_1 \end{cases} \tag{2}$$

其中，a_1 和 b_1 是混沌系统的控制参数，x 和 y 是系统的输入参数并作为加密算法的密钥。

算法改进：在式（1）的基础上，将 y_n 替换为非线性项 $-a_1 \cos y_n$；将 ax_n^2 替换为非线性 $a_1 \sin x_n$ 项；将 $y_{n+1} = bx_n$ 替换为 $y_{n+1} = x_n + b_1$，从而构建出一个新的二维 Henon 混沌映射，引入非线性混沌函数解决了经典混沌函数的线性局限性，相较于经典混沌函数拥有更大的伪随机性和混沌空间。本文选择 a_1=5、b_1=0.3，Henon 映射改进前后的混沌区间如图 1 所示，Henon 映射改进前后的 Lyapunov 指数图如图 2 所示，Henon 映射改进前后的相空间图如图 3 所示。从图 1 可知，当 0≤ a ≤5 时，经典的混沌空间取值范围 $a \in [1.05,1.4]$，而改进的 Henon 映射混沌空间的取值范围 $a_1 \in [1.402,5]$，与经典的 Henon 映射相比，改进的算法具有更大的混沌空间。图 2 中当 a_1=1.402、b_1=0.3 时，存在一个正的 Lyapunov 指数 LE1=0.147 379 47 和一个负的 Lyapunov 指数 LE2=−0.434 224 26，此时系统处于混沌状态。随着 a 值的增加，Lyapunov 指数也相应地增大。当 $a_1 \in [1.402, +\infty]$时，混沌空间均有有效值，且随着 a_1 的增加，相应的 Lyapunov 指数、混沌空间随之增大。

从图 3 中可以看出，改进的 Henon 映射相空间图相比于经典的 Henon 映射相空间图具有更大的混沌区间、更复杂的混沌特性。因此，本文改进的 Henon 混沌映射具有更大的随机性、低互相关性和遍历性，更适用于语音加密系统。

2.2　Lorenz 超混沌系统

Lorenz 超混沌系统是在经典 Lorenz 混沌系统[19]的基础上进行改进和优化[20]，并利用附加的状态变量将原始的三维系统改进为四维超混沌系统。本文引用 Lorenz 超混沌系统，不仅增大了加密算法的密钥空间和伪随机性，同时增加了算法的鲁棒性和安全性。Lorenz 超混沌系统函数表达式如式（3）所示。

$$\begin{cases} \dot{x}_2 = c\left(y_2 - x_2\right) + w_2 \\ \dot{y}_2 = ex_2 - x_2 z_2 - y_2 \\ \dot{z}_2 = ey_2 - dz_2 \\ \dot{w}_2 = -y_2 z_2 + fw \end{cases} \tag{3}$$

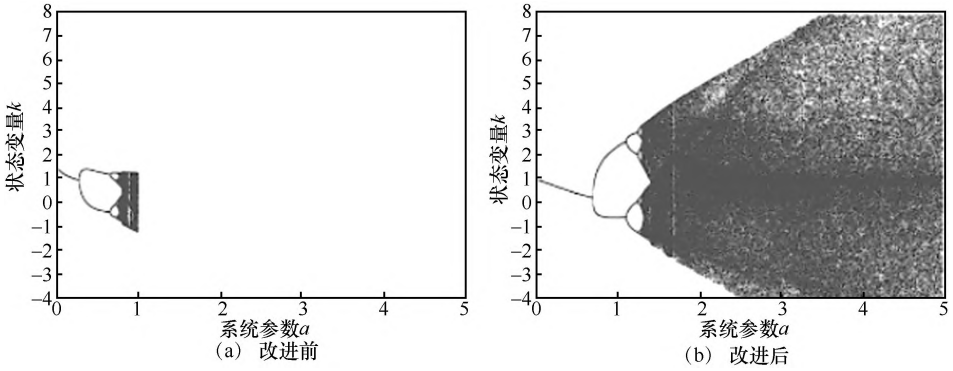

图 1　Henon 映射改进前后的混沌区间

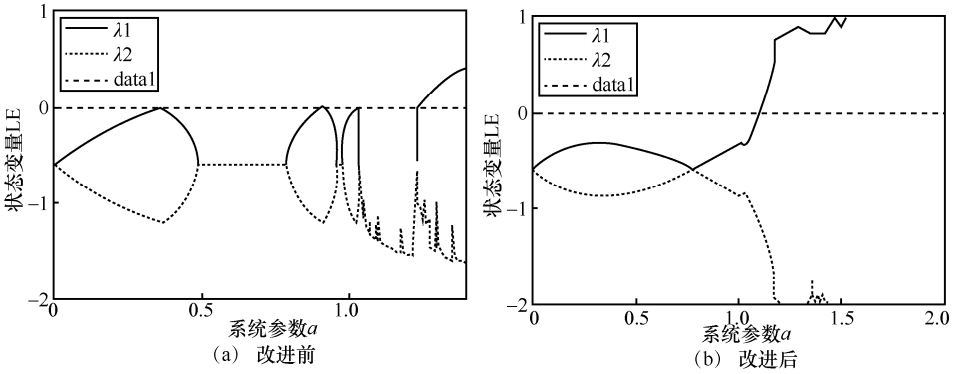

图 2　Henon 映射改进前后的 Lyapunov 指数图

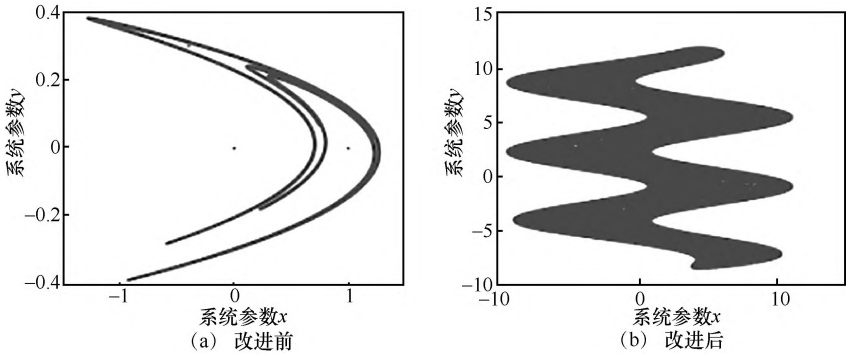

图 3　Henon 映射改进前后的相空间图

其中，x_2、y_2、z_2 和 w_2 是系统的状态变量；c、d、e 和 f 为系统参数，且当 $-1.52 \leqslant f \leqslant -0.06$ 时，系统处于超混沌状态。

2.3　改进的 Arnold 变换算法

本文对经典的 Arnold 变换算法[21]进行优化，将传统的二维矩阵转化为一维向量进行置乱操作。具体方案如下。

（1）经典的二维不等长 Arnold 置乱算法定义如式（4）所示。

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \boldsymbol{T} \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \bmod \begin{bmatrix} M \\ N \end{bmatrix} \tag{4}$$

其中，$\boldsymbol{T}$ 为变换矩阵，1、p、q、pq+1 是变换矩阵的参数，M 和 N 是输入语音数据的行列数，x_0 和 y_0 是原始的数据点坐标，经过变换矩阵后，生成新的数据点 x_1 和 y_1，实现置乱加密。

（2）将 M 行 N 列的矩阵数据转化为一维向量 $\boldsymbol{S}$，记为 $\boldsymbol{A}$，则 $\boldsymbol{A}$ 的长度为 $M \times N = j$。此时，需要加密的数据变为 1 行 j 列。

（3）通过计算式（4）可得，$x_1 = 1 + qj$；$y_1=p+(p\times q+1)$。本文仅考虑 y_1，可以通过伪随机变量 p、q 实现对加密数据$(1, j)$和$(1, y_1)$之间的数据转换。与此同时，将 $p\times q+1$ 定义为一个新的随机数，记为 u，按式（5）进行表达式转换。

$$u\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \boldsymbol{T}\begin{bmatrix} 1 \\ j \end{bmatrix}(\mathrm{mod}\, N) = \begin{pmatrix} 1 & q \\ p & u \end{pmatrix}\begin{bmatrix} 1 \\ j \end{bmatrix}(\mathrm{mod}\, N) \tag{5}$$

（4）Arnold 置乱数据序列表达式为式（6）的定义，其中，p、q 为加密的随机变量，x_1 和 y_1 为变换后的加密数据。

$$y_1\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_1 = 1 + qj \\ y_1 = p + uj \end{bmatrix} \tag{6}$$

（5）Arnold 置乱反变换：在使用伪随机矩阵进行语音置乱加密时，由于置乱算法本身是可逆的，在对数据进行解密时，只需要对 Arnold 置乱变换的加密数据按语音数据长度进行反向置乱即可恢复原始语音数据。

本文改进的 Arnold 置乱加密算法相比较于传统的 Arnold 行列置乱加密算法，有效地克服了传统 Arnold 置乱加密中存在周期短、安全性差等问题，并且将数据转换为一维向量，有效地减少了加密时间，提高了加密效率。

3　算法设计

3.1　语音初次加密算法

语音初次加密算法处理流程如图 4 所示，主要包括：语音数据预处理、模数转换、置乱加密、数模转换、密文语音输出等步骤，具体过程如下。

（1）语音预处理。对明文语音信号 $\boldsymbol{P}=\{\boldsymbol{P}(i)|1<i<L\}$进行预加重，分帧处理，帧长 M=256，帧位移 N=256。

（2）模数转换。对原始语音数据 $\boldsymbol{P}$ 通过模数转换为小数点后 15 位的普通数据 $\boldsymbol{P}'$，并将其转化为一维列向量。

（3）混沌序列生成。对改进的 Henon 映射输入密钥$[K_1, K_2]$，按式（7）生成长度为 $M\times N$ 的伪随机序列 $\boldsymbol{xx}$，其中，将重复出现的随机数保留其中一个，对未出现的随机数按照从小到大的顺序在末尾补齐。

$$\boldsymbol{XX}' = \mathrm{mod}(\mathrm{floor}(\mathrm{XX}(1:M\times N) + 100\times 10^{10}), M\times N) + 1 \tag{7}$$

（4）单次不重复置乱加密。利用生成的伪随机序列 $\boldsymbol{xx}$ 对语音数据 $\boldsymbol{P}'$ 进行置乱操作，生成置乱后的语音数据 $\boldsymbol{P}'' = [M\times N, 1]$。

（5）数模转换。对加密后的语音数据 $\boldsymbol{P}''$ 进行数模转换，生成密文语音信号 $\boldsymbol{Q}$，完成语音信号加密。

（6）语音解密。语音初次加密算法为对称加密算法，故解密为加密的逆过程。

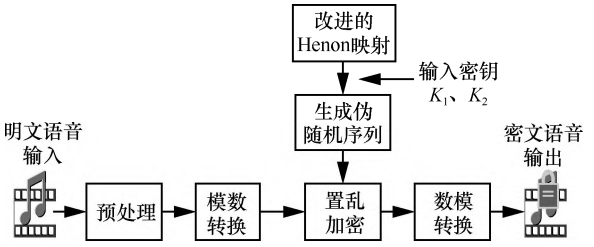

图 4　语音初次加密算法处理流程

3.2　双重语音加密算法

本文提出的双重语音加密算法处理流程如图 5 所示，主要包括：密钥生成、改进的 Henon 置乱加密、Lorenz 超混沌系统中 Arnold 置乱加密、异或扩散加密等步骤。

3.2.1　密钥生成

改进 Henon 混沌系统输入密钥参数为 $K_1 = 1.1$、$K_2 = 2.2$；Lorenz 超混沌系统的输入密钥参数为：$K_3 = 3.3$、$K_4 = 4.4$、$K_5 = 5.5$、$K_6 = 6.6$。

本文提出的加密系统属于对称加密系统，解密密钥和加密密钥必须完全相同才能正确解密。

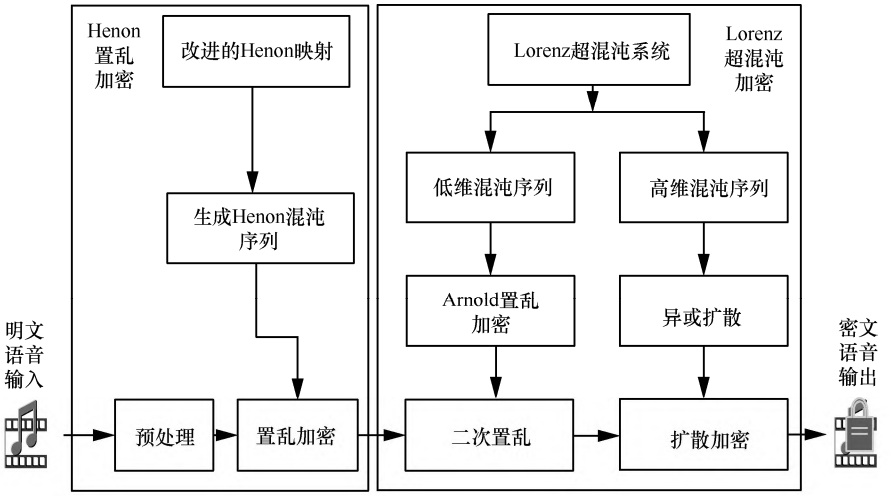

图 5　双重语音加密算法处理流程

3.2.2　改进的 Henon 置乱加密

通常语音加密系统需要对语音数据先进行预处理操作。将模拟信号转换为数字信号，再利用混沌映射生成伪随机序列对语音数据加密。具体步骤包括以下几个。

（1）原始语音信号预处理。对语音信号 $\boldsymbol{P}=\{P(i)|1<i<L\}$ 进行不重叠分帧，语音信号长度为 L，每帧长为 256，帧位移为 256，共计分为 $M=L/(256\times256)$ 个语音帧。

（2）生成混沌序列。对改进的 Henon 混沌映射输入系统参数 $[a_1,b_1]$ 和密钥 $[K_1,K_2]$，生成长度为 $M\times N$ 的混沌序列 $\boldsymbol{XX}$。其中，对伪随机序列 $\boldsymbol{XX}$ 中所有重复的随机数只保留其中一个，最后将未出现的随机数按照从小到大的顺序补齐，按式（7）定义生成最终的混沌序列 $\boldsymbol{XX}'=y\{x(i)|1<i<L\}$。

（3）单次不重复置乱加密。将分帧后语音数据展开成一维列向量，得到新的语音序列 $\boldsymbol{P}=[M\times N,1]$。利用生成的混沌序列 $\boldsymbol{XX}'$ 对 $\boldsymbol{P}'$ 按位进行置乱操作，得到置乱后的语音数据 $\boldsymbol{P}''=[M\times N,1]$。

3.2.3　Lorenz 超混沌语音加密

Lorenz 超混沌语音加密系统主要包括多维混沌序列生成、Arnold 置乱加密和按位异或扩散加密 3 部分组成。具体步骤如下。

（1）多维混沌序列生成。对 Lorenz 超混沌系统输入初始参数 $[c,d,e,f]$ 和密钥 $[K_1,K_2,K_3,K_4]$，并生成置乱用的伪随机序列 $\boldsymbol{XX}''$，长度为 $M\times N$，如式（8）所示；正向扩散用的伪随机序列 $\boldsymbol{S}_1=[1:M\times N]$，如式（9）所示；逆向扩散用的伪随机序列 $\boldsymbol{S}_2=[M\times N+1:2\times M\times N]$，如式（10）所示。

$$\boldsymbol{XX}''=\mathrm{mod}(\mathrm{floor}(\boldsymbol{s}+100)\times10^{10}),10\times\max(M,N)+1 \tag{8}$$

$$\boldsymbol{S}_1=\mathrm{mod}(\mathrm{floor}(\boldsymbol{s}\times\mathrm{pow}2^{16}),256) \tag{9}$$

$$\boldsymbol{S}_2=\mathrm{mod}(\mathrm{floor}(\boldsymbol{s}\times\mathrm{pow}2^{16}),256) \tag{10}$$

（2）Arnold 置乱加密。本次置乱加密是在第 3.2.2 节置乱加密的基础上进行的二次置乱加密。首先将加密后的语音数据 $\boldsymbol{P}''=[M\times N,1]$ 作为输入语音，引入超混沌语音加密系统中，对 $\boldsymbol{P}''$ 中任意位置的语音数据进行 Arnold 变换生成二次置乱后的密文语音 $\boldsymbol{P}'''=[M\times N,1]$。

（3）按位异或扩散加密。使用 Lorenz 超混沌系统生成的伪随机序列 $\boldsymbol{S}_1$ 和 $\boldsymbol{S}_2$，利用式（11）对二次置乱后的语音数据 $\boldsymbol{P}'''$ 先进行正向异或扩散

得到$\boldsymbol{Q}'$，将扩散后的语音数据利用式（12）再进行反向异或扩散得到加密语音$\boldsymbol{Q}''$，其中，C''为异或扩散后的语音采样点。最终，对扩散完成后的语音数据重构获得密文语音 $\boldsymbol{Q}=\{Q(i),1<i<L\}$，完成语音加密。

$$C'(i)=C(i-1)\oplus \boldsymbol{S}_1(i)\oplus C(i) \tag{11}$$

$$C''(i)=C'(i+1)\oplus \boldsymbol{S}_2(i)\oplus C'(i) \tag{12}$$

3.3　双重语音解密算法

本文提出的双重语音解密算法处理流程如图 6 所示。

双重语音解密处理具体步骤如下。

（1）语音预处理。读入密文语音 $\boldsymbol{Q}=\{Q=(i),1<j<L\}$，对密文语音进行分帧，帧长为 256，共计分为$M=L/(256\times 256)$个语音帧。

（2）混沌序列生成。使用与加密相同的密钥对 Lorenz 超混沌系统和改进的 Henon 混沌系统生成混沌序列。

（3）异或解密。使用式（9）和式（10）生成的混沌序列对输入的密文语音 $\boldsymbol{Q}$ 通过式（13）和式（14）分别进行反向扩散解密和正向扩散解密，获得解扩散语音信号 $\boldsymbol{H}$ 。

$$C'(i)=C(i+1)\oplus \boldsymbol{S}_1(i)\oplus C(i) \tag{13}$$

$$C''(i)=C'(i-1)\oplus \boldsymbol{S}_2(i)\oplus C'(i) \tag{14}$$

（4）Arnold 解置乱。首先将解扩散后的语音数据 $\boldsymbol{H}$ 展开为一维的列向量，其次利用式（8）生成的混沌序列对语音数据反向进行 Arnold 置乱，即从$M\times N$到 1 进行解置乱操作生成 Arnold 解置乱语音数据$\boldsymbol{I}=[M\times N,1]$。

（5）Henon 解置乱。利用式（7）生成长度为$M\times N$的 Henon 混沌序列，然后将混沌序列与 Arnold 解置乱语音数据 I 进行解置乱操作，得到解密后的语音 $\boldsymbol{P}_x=\{P_X(i)|1\leqslant i\leqslant L\}$。

（6）解密语音重构。最后将解密后的语音数据重构恢复为时域语音信号 $\boldsymbol{P}_{xx}$，完成语音的解密过程。

3.4　对比论证分析

语音初次加密算法相较于双重语音加密算法在加密、解密性能和安全性等方面均有较大的差异，其具体区别如下。

（1）密钥空间。语音初次加密算法仅有两个密钥控制参数，相较于双重语音加密算法的 6 个密钥控制参数存在密钥空间小、安全性低等问题，不足以抵挡现有的密码学攻击等。

（2）加密时间分析。语音初次加密算法加密时间较快，主要原因是该加密算法结构简单、加密模块单一等。双重语音加密算法加密时间消耗略大，主要因素是该算法加密结构复杂、加密模

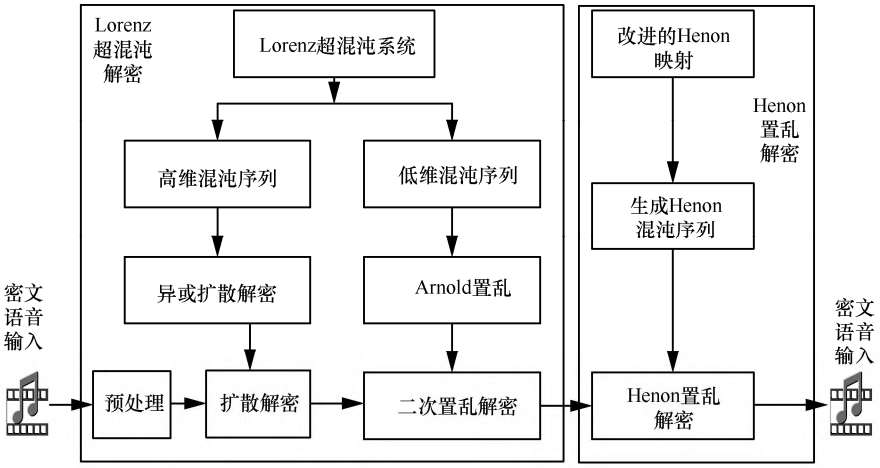

图 6　双重语音解密算法处理流程

块丰富，不仅进行了两次置乱加密且进行了正反向异或扩散加密。

（3）算法安全性分析。语音初次加密算法只针对语音帧的顺序进行了简单置乱操作，无法打乱语音帧相关联的统计特性，不能抵挡统计分析，存在安全性低、加密效果差、敏感信息易泄露等安全隐患。双重语音加密算法因其进行了两次置乱加密和正反向扩散加密，有效地打乱了语音数据相邻信号的统计特征，在保证语音加密数据安全性的同时也有较高的加密效率。

4 实验仿真和性能评估

为了评估本文语音加/解密系统的性能和效率，实验选用清华大学开放的汉语语音数据库THCHS-30[22]中的等长语音作为本次实验的测试语音进行加密、解密，其中，选取不同长度的语音类型各10条作为本次实验数据，见表1。实验硬件平台：Inter(R) Core(TM)i5-10200H CPU，3.17 GHz，内存 16 GB。软件环境：Windows10、MATLAB R2017b 软件实现编程和仿真。

表1 测试语音类型

语音类型	语音长度/s	语音格式
语音1	2	WAV
语音2	4	WAV
语音3	5	WAV
语音4	8	WAV
语音5	9	WAV
语音6	10	WAV

4.1 语音加密算法

4.1.1 密钥空间和密钥敏感度分析

本文提出的语音初次加密算法的密钥空间由改进的Henon映射系统生成，其中，K_1=1、K_2=2，密钥参数均取小数点后 15 位的双精度浮点型数据，密钥空间为$2\times10^{15}\times2\times10^{15}\approx2^{102}$。双重语音加密算法密钥空间由改进的 Henon 映射生成密钥参数$K_1=1.1$、$K_2=2.2$和 Lorenz 超混沌映射生成的密钥参数$K_3=3.3$、$K_4=4.4$、$K_5=5.5$、$K_6=6.6$共同组成。密钥空间可达$2\times10^{15}\times2\times10^{15}\times2\times10^{15}\times2\times10^{15}\times2\times10^{15}\times2\times10^{15}\approx2^{305}$。可以看出，语音初次加密算法的密钥空间与双重语音加密算法相比密钥空间小且存在隐私泄露和易篡改等安全性问题。

以语音4为例生成的原始语音和两种加/解密语音波形图和频谱图如图7所示。混沌系统对密钥高度敏感，只有输入正确的密钥，才能完全解密出密文语音。即使密钥发生微小的变化时，无法正确地解密出原始语音。

图7（i）、图7（j）与图7（k）、图7（l）分别为初次加密和双重加密后对任意密钥小数点后15 位进行改变，以K_1为例，将密钥数据K_1'设置为1.100 000 000 000 001时的错误解密语音波形图和语谱图。从图7（i）、图7（k）可以看出，两种算法均有较好的密钥敏感性，但语音初次加密算法相较于双重语音加密算法的加密性能有待提高。因此双重语音加密算法更适用于现有的语音加密。

4.1.2 直方图分析

直方图[23]因其客观性和可视化被广泛应用于评估语音信号质量的方法之一。本次以语音3为例分析。本文两种加密算法的原始语音和加密语音的幅度直方图如图8所示。

图8（a）和图8（b）均有不规则的统计特征，图8（c）分布较为平稳，无较大的起伏和波动。说明语音初次加密算法无法打破语音数据的统计特征，相关性较高，不足以抵挡统计分析攻击；而双重语音加密算法对语音数据的统计特性具有较好的掩盖效果，相关性较差，统计信息少，足以抵挡统计攻击。

4.1.3 感知质量评估分析

感知语音质量评估（perceptual evaluation of speech quality，PESQ）是国际电信联盟电信标准化部P.862建议的客观平均意见得分（mean opinion

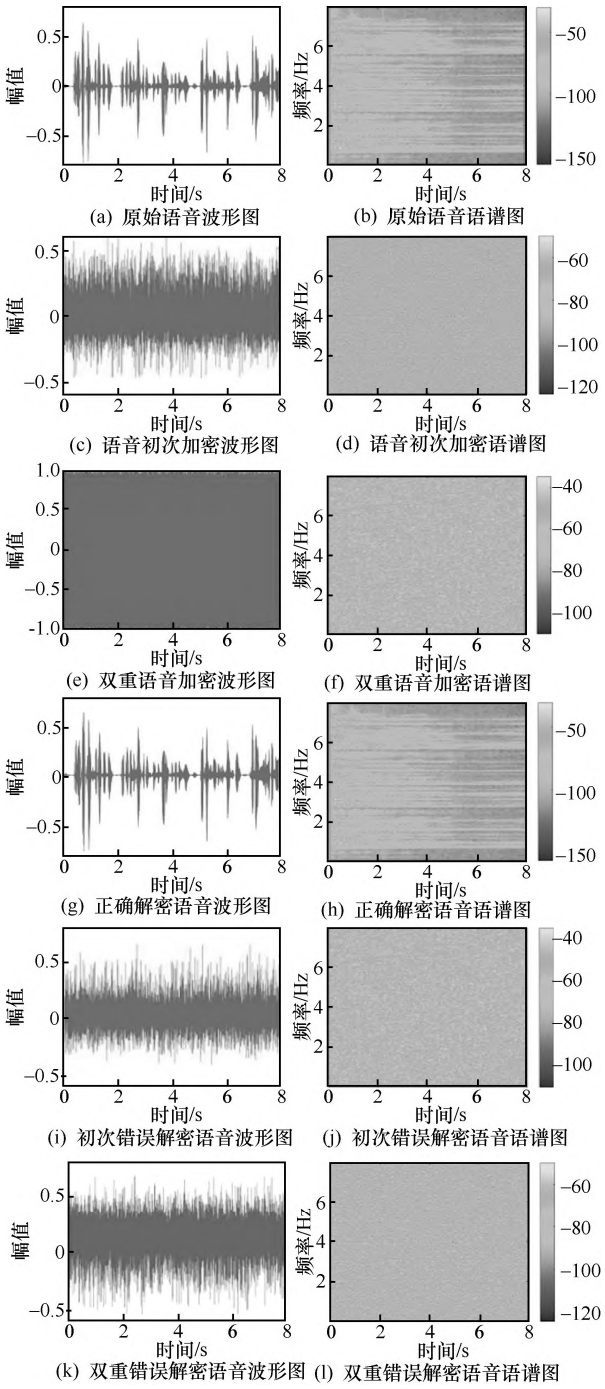

图 7　原始语音和加/解密语音的波形图和语谱图

score，MOS）[24]。通常取值从 1.0（最差）～4.5（最好）的 PESQ-MOS 范围。

各项语音 PESQ 数值见表 2。

由表 2 可知，两种加密算法所得到的加密语音 PESQ 值均在 1 以下，无法获得任何有效信息，而恢复的语音信号均为 4.5，实现了无损恢复。因此，本文提出的两种加密算法均有较好的加密效果和无损解密性能。

4.1.4　信噪比和峰值信噪比分析

信噪比（signal noise ratio，SNR）[25]主要用于测量加密数据中信号的噪声含量和失真程度，被广泛应用于多媒体数据加密中。

信噪比的定义如式（15）所示。

$$\mathrm{SNR}=10\lg\frac{\sum_{n=0}^{l}P^2(n)}{\sum_{n=0}^{l}Q^2(n)} \tag{15}$$

其中，P 为原始语音信号，Q 为加密语音信号。

峰值信噪比（peak signal noise ratio，PSNR）[26]是原始语音信号最大功率与加密语音信号最大功率的比值。PSNR 数值越低代表加密效果越好。峰值信噪比函数定义如式（16）所示。

$$\mathrm{PSNR}=10\times\lg\left(\frac{\max(P_{\mathrm{signal}})}{P_{\mathrm{noise}}}\right) \tag{16}$$

其中，P_{signal} 表示原始语音信号功率，P_{noise} 表示加密信号功率。

两种不同语音加密算法对语音信号的 SNR 和 PSNR 值见表 3。

从表 3 可以看出，语音初次加密算法相较于双重加密算法的 SNR 数值和 PSNR 数值均较高，加密性能有待提高。双重语音加密算法的 SNR 和 PSNR 数值较低，满足语音加密指标要求，说明本文提出的双重语音加密算法具有很强的安全性。

4.1.5　相关分析

相关分析[27]作为一种数据统计方法，被广泛地应用于语音加密算法的性能评估。如果相关系数在+1 或－1 左右，则表明这两个语音信号相关性较强；如果两个语音信号相关系数在 0 左右，则代表这两个语音信号关联性极差。相关系数公式如式（17）～式（19）所示。

$$r_{PQ}=\frac{C(P,Q)}{\sqrt{V(P)}\sqrt{V(Q)}} \tag{17}$$

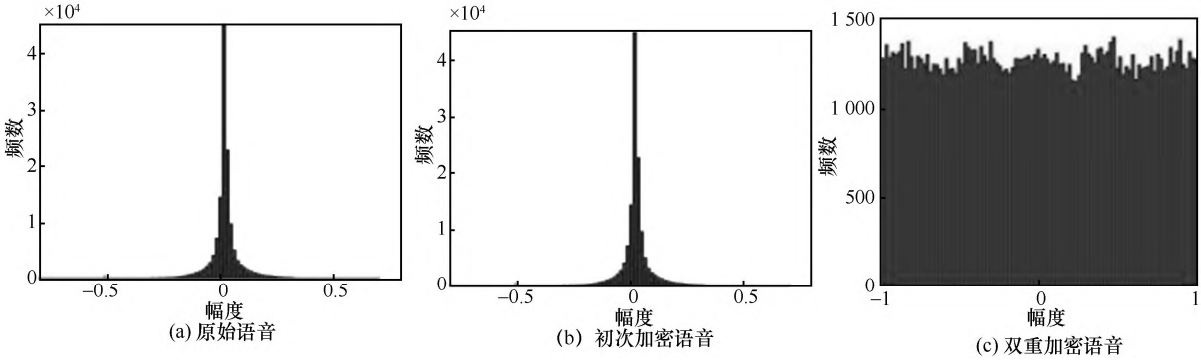

图 8　原始语音和加密语音的幅度直方图

表 2　加密与解密语音的 PESQ-MOS 数值数

语音类型	初次加密 PESQ-MOS	初次解密 PESQ-MOS	双重加密 PESQ-MOS	双重解密 PESQ-MOS
语音 1	0.468 0	4.500 0	0.379 1	4.500 0
语音 2	0.717 6	4.500 0	0.705 6	4.500 0
语音 3	0.743 1	4.500 0	0.834 1	4.500 0
语音 4	0.841 9	4.500 0	0.875 1	4.500 0
语音 5	0.924 1	4.500 0	0.786 3	4.500 0
语音 6	0.903 1	4.500 0	0.817 1	4.500 0
平均值	0.766 3	4.500 0	0.732 9	4.500 0

表 3　加密语音的 SNR 和 PSNR 值

语音类型	初次加密 SNR/dB	初次加密 PSNR/dB	双重加密 SNR/dB	双重加密 PSNR/dB
语音 1	−10.244 1	1.966 9	−40.154 0	0.329 4
语音 2	−18.161 1	1.770 9	−38.488 3	0.001 3
语音 3	−11.645 1	1.610 6	−51.026 1	0.066 9
语音 4	−29.952 2	1.914 7	−47.490 0	0.074 3
语音 5	−26.524 1	1.733 5	−55.538 2	0.139 3
语音 6	−22.541 9	1.467 6	−36.400 2	0.092 4
平均值	−19.844 5	1.744 0	−44.849 5	0.117 3

$$V(P)=\frac{1}{N_s}\sum_{i=1}^{N_s}(P(i)-E(P))^2 \tag{18}$$

$$E(P)=\frac{1}{N_s}\sum_{i=1}^{N_s}P(i) \tag{19}$$

其中，P 为原始语音，Q 为加密语音，r_{PQ} 为 P 和 Q 的相关系数，N_s 表示采样点个数，E（P）为 P 的均值，V（P）和 V（Q）表示 P 和 Q 之间的方差；C（P,Q）为 P 与 Q 的协方差。语音初次加密和双重语音的相关性分析结果见表 4。

从表 4 可以看出，初次加密语音和双重加密语音的相关系数在 0 附近，表示原始语音和加密语音不相关，语音加密性能较好；初次解密语音和双重解密语音的相关系数在 1 附近，表明语音的恢复重构性能较强，可以实现无损恢复。但初

表 4　语音的相关性分析

语音类型	原始语音&初次加密语音	原始语音&初次解密语音	原始语音&双重加密语音	原始语音&双重解密语音
语音 1	0.004 696	1.000 0	0.000 206	1.000 0
语音 2	−0.004 204	1.000 0	−0.002 372	1.000 0
语音 3	0.001 067	1.000 0	0.003 819	1.000 0
语音 4	0.003 373	1.000 0	−0.002 120	1.000 0
语音 5	−0.009 487	1.000 0	−0.000 388	1.000 0
语音 6	−0.000 970	1.000 0	−0.003 338	1.000 0
平均值	0.005 566	1.000 0	0.002 041	1.000 0

次加密语音相较于双重加密语音的相关系数略高，加密性能有待提高。

4.1.6　信息熵分析

信息熵分析主要用于语音加密数据中的错误率，通常信息熵的数值与语音的错误率成正比，加密语音数据的信息熵越高，代表语音加密效果越好，其定义如式（20）所示，如果加密的语音数据信息熵数值接近 16，则表明该语音加密系统加密效率较好、安全性较高。

语音初次加密和双重语音加密的信息熵分析结果见表 5。

$$H=-\sum_{K=0}^{S}P\mathrm{lb}P \tag{20}$$

其中，P 是输入的原始语音数据，S 代表采样点个数。

表 5　语音的信息熵分析

语音类型	原始语音/dB	初次加密/dB	双重加密/dB
语音 1	11.604 1	11.604 1	15.266 9
语音 2	11.750 0	11.750 0	15.418 6
语音 3	12.219 0	12.219 0	15.579 0
语音 4	10.874 5	10.874 5	15.657 8
语音 5	11.092 6	11.092 6	15.418 6
语音 6	11.913 4	11.913 4	15.427 4
平均值	11.575 6	11.575 6	15.461 4

从表 5 可以看出，语音初次加密的信息熵数值并没有改变，说明该加密方案无法抵御熵攻击，存在较高的安全性隐患；双重加密算法的加密语音数据信息熵均接近 16，说明双重语音加密算法具有较高的安全性，足以抵抗熵攻击。

4.1.7　选择明文攻击分析

样本变化率（number of samples change rate，NSCR）[28]是一种选择明文攻击评价指标，它反映了两个语音数据相同位置不相等的数据点所占整个数据点的比例。如果 NSCR 近似等于 100%，则认为加密算法性能较高，能够抵挡各种不同的明文攻击。

语音初次加密和双重语音加密的 NSCR 值见表 6。

表 6　选择明文攻击分析

语音类型	初次加密的 NSCR	双重加密的 NSCR
语音 1	0.999 35	0.999 96
语音 2	0.999 25	0.999 99
语音 3	0.999 68	1.0
语音 4	0.998 47	0.999 98
语音 5	0.998 79	0.999 98
语音 6	0.999 35	0.999 99
平均值	0.999 15	0.999 98

从表 6 可知，本文提出的两种算法得到的 NSCR 数值均接近 100%，表明加密后的语音数据样本点与原始语音截然相反，可以有效地抵挡差

分攻击。语音初次加密算法相较于双重语音加密算法 NSCR 数值较低，说明双重语音加密更适用于语音数据的加密。

4.1.8 加/解密效率分析

语音加密系统的复杂度和语音的加密效率是相互制约的，现有的算法在确保密钥安全性时，往往忽略了语音的加/解密时间，并不能适用于海量的语音加密数据。语音初次加密和双重语音加密对不同语音长度的加/解密时间见表 7。

由表 7 可知，本文对 60 条不同长度语音数据进行测试，实验结果表明语音初次加密算法加密每秒语音所用时间大约在 0.07 s；双重语音加密加/解密每秒语音所需时长大约为 0.11 s。根据语音时长，加密时间呈线性增长。语音初次加密算法相较于双重语音加密算法时间较少的主要原因是：初次加密算法结构单一、加密复杂度低、运算量小等因素，但两种加密算法结合密钥空间、加密安全性、加密效率、算法实时性等综合考虑，本文提出的双重语音加密算法具有较高的安全性和较好的加密效率，更适用于海量语音数据的安全加密。

4.2 与现有加密算法性能对比

本文提出的双重语音加密算法与现有文献[12, 29-33]语音加密算法进行实验结果比较，对本文加密算法进行了客观准确的评价，对比数据均取自各项指标的平均值。本文算法与现有加密算法的性能对比结果见表 8。

表 7 加/解密效率分析

语音类型	初次加密时间/s	初次加密时间/s	双重加密时间/s	双重解密时间/s
语音 1（2 s）	0.139 0	0.136 8	0.224 3	0.213 2
语音 2（4 s）	0.277 6	0.278 3	0.438 2	0.434 3
语音 3（5 s）	0.377 7	0.368 9	0.551 8	0.551 2
语音 4（8 s）	0.556 2	0.553 1	0.887 0	0.894 2
语音 5（9 s）	0.626 0	0.623 3	0.987 2	0.978 6
语音 6（10 s）	0.700 3	0.692 1	1.108 5	1.060 6
加/解密每秒语音	0.070 4	0.069 8	0.110 4	0.108 7

表 8 与现有加密算法的性能对比结果

评价指标	本文算法	文献[12]算法	文献[29]算法	文献[30]算法	文献[31]算法	文献[32]算法	文献[33]算法
密钥空间	2^{305}	2^{298}	—	—	2^{149}	—	2^{192}
SNR/dB	−44.849 5	−133.857 1	—	−29.960 0	−13.115 9	−13.115 9	−5.530 0
PSNR/dB	0.117 3	—	—	—	1.833 7	—	—
R_{PQ}（加密语音）	0.002 0	0.009 4	0.038 6	0.400 0	0.001 4	0.003 5	0.002 7
R_{PP_X}（解密语音）	1.000 0	0.980 7	0.995 8	0.990 0	—	0.865 9	—
PESQ 加密语音	0.732 9	—	0.983 0	0.980 0	—	—	—
PESQ 解密语音	4.500 0	—	—	4.230 0	—	—	—
NSCR	99.998 3%	99.998 9%	99.939 1%	99.930 0%	99.998 4%	99.847 4%	—
加密效率/s	0.110 4	—	—	—	—	0.281 0	—

从表 8 可以看出，本文提出的双重语音加密算法从总体上优于文献[12, 29-33]的算法，主要原因是本文算法将语音数据先进行了一次二维的 Henon 置乱加密，又进行了超混沌加密，在保证良好加密安全性的同时又提高了加密效率。但文献[12]的 SNR、文献[31]的 NSCR、R_{PQ} 性能优于本文。出现微小差值的原因是本文双重加密算法只进行了置乱和扩散加密，没有进行替换，除此之外不同的实验环境也会导致加密效率产生的微小差异等。

5　结束语

本文提出了一种基于改进 Henon 映射和超混沌的双重语音加密算法，并与语音初次加密算法进行性能比较分析，解决了现有语音混沌加密算法密钥空间小、加密效率低等问题。该方法在不改变系统控制参数的前提下，通过扩展控制参数范围，将经典的 Henon 映射控制变量修改为非线性三角函数变量，使得改进后的 Henon 映射具有更大的混沌空间和更高的混沌复杂度；将改进的 Henon 混沌系统与 Lorenz 超混沌系统相结合，并采用改进和优化的广义 Arnold 置乱算法，实现了语音数据的双重加密。实验结果表明，双重语音加密算法可以抵抗暴力攻击、差分攻击、统计攻击、熵攻击等，且具有较低的算法复杂性和较高的安全性，适用于海量语音数据的安全存储和隐私保护。未来的研究方向主要是将语音加密算法应用到数据流的实时传输中。

参考文献：

[1] SHAH D, SHAH T, JAMAL S S. Digital audio signals encryption by Mobius transformation and Hénon map[J]. Multimedia Systems, 2020, 26(2): 235-245.

[2] ZHENG J Y, LIU L F. Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map[J]. IET Image Processing, 2020, 14(11): 2310-2320.

[3] SHI C, WANG H, HU Y, et al. A speech homomorphic encryption scheme with less data expansion in cloud computing[J]. KSII Transactions on Internet and Information Systems, 2019, 13(5): 2588-2609.

[4] ABRO F I, RAUF F, MOBEEN-UR-REHMAN, et al. Towards security of GSM voice communication[J]. Wireless Personal Communications, 2019, 108(3): 1933-1955.

[5] FUERTES W, MENESES F, HIDALGO L, et al. Rsa over-encryption implementation for networking: a proof of concept using mobile devices[J]. Investigacion Operacional, 2020, 41(4): 586-598.

[6] PATEL K. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files[J]. International Journal of Information Technology, 2019, 11(4): 813-819.

[7] KAUR G, SINGH K, GILL H S. Chaos-based joint speech encryption scheme using SHA-1[J]. Multimedia Tools and Applications, 2021, 80(7): 10927-10947.

[8] SUHAIL K M A, SANKAR S. Image compression and encryption combining autoencoder and chaotic logistic map[J]. Iranian Journal of Science and Technology, Transactions A: Science, 2020, 44(4): 1091-1100.

[9] AL-HAZAIMEH O M. A new speech encryption algorithm based on dual shuffling Hénon chaotic map[J]. International Journal of Electrical and Computer Engineering (IJECE), 2021, 11(3): 2203.

[10] AL-HAZAIMEH O M. A new dynamic speech encryption algorithm based on Lorenz chaotic map over Internet protocol[J]. International Journal of Electrical and Computer Engineering (IJECE), 2020, 10(5): 4824.

[11] SAYED W S, TOLBA M F, RADWAN A G, et al. FPGA realization of a speech encryption system based on a generalized modified chaotic transition map and bit permutation[J]. Multimedia Tools and Applications, 2019, 78(12): 16097-16127.

[12] FARSANA F J, DEVI V R, GOPAKUMAR K. An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams[J]. Applied Computing and Informatics, 2020.

[13] HAMDI M, RHOUMA R, BELGHITH S. An appropriate system for securing real-time voice communication based on ADPCM coding and chaotic maps[J]. Multimedia Tools and Applications, 2017, 76(5): 7105-7128.

[14] ZGHAIR H K, MEHDI S A, SADKHAN S B. Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system[J]. Journal of Physics: Conference Series, 2021, 1804(1): 012048.

[15] SHAH D, SHAH T, AHAMAD I, et al. A three-dimensional chaotic map and their applications to digital audio security[J]. Multimedia Tools and Applications, 2021, 80(14): 22251-22273.

[16] IMRAN O A, YOUSIF S F, HAMEED I S, et al. Implementa-

tion of El-Gamal algorithm for speech signals encryption and decryption[J]. Procedia Computer Science, 2020, 167: 1028-1037.

[17] ELSAFTY A H, TOLBA M F, SAID L A, et al. Hardware realization of a secure and enhanced s-box based speech encryption engine[J]. Analog Integrated Circuits and Signal Processing, 2021, 106(2): 385-397.

[18] HÉNON M. A two-dimensional mapping with a strange attractor[J]. Communications in Mathematical Physics, 1976, 50(1): 69-77.

[19] STEWART I. The Lorenz attractor exists[J]. Nature, 2000, 406(6799): 948-949.

[20] 薛伟, 王磊. 一种基于新型混沌的彩色图像加密算法[J]. 光学技术, 2018, 44(3): 263-268.
XUE W, WANG L. A color image encryption algorithm based on novel chaos[J]. Optical Technique, 2018, 44(3): 263-268.

[21] PAN T G, LI D Y. A novel image encryption using Arnold cat[J]. International Journal of Security and Its Applications, 2013, 7(5): 377-386.

[22] WANG D, ZHANG X W. THCHS-30: a free Chinese speech corpus[J]. CoRR, 2015.

[23] NASKAR P K, PAUL S, NANDY D, et al. DNA encoding and channel shuffling for secured encryption of audio data[J]. Multimedia Tools and Applications, 2019, 78(17): 25019-25042.

[24] Perceptual evaluation of speech quality (PESQ): an objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs[EB]. 2001.

[25] BABU N R, KALPANA M, BALASUBRAMANIAM P. A novel audio encryption approach via finite-time synchronization of fractional order hyperchaotic system[J]. Multimedia Tools and Applications, 2021, 80(12): 18043-18067.

[26] SHEELA S J, SURESH K V, TANDUR D. Image encryption based on modified Henon map using hybrid chaotic shift transform[J]. Multimedia Tools and Applications, 2018, 77(19): 25223-25251.

[27] AUGUSTINE N, GEORGE S N, PATTATHIL D P. An audio encryption technique through compressive sensing and Arnold transform[J]. International Journal of Trust Management in Computing and Communications, 2015, 3(1): 74.

[28] BELAZI A, ABD EL-LATIF A A, BELGHITH S. A novel image encryption scheme based on substitution-permutation network and chaos[J]. Signal Processing, 2016, 128: 155-170.

[29] SATHIYAMURTHI P, RAMAKRISHNAN S. Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map[J]. Multimedia Tools and Applications, 2020, 79(25): 17817-17835.

[30] SOLIMAN N F, KHALIL M I, ALGARNI A D, et al. Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication[J]. Multimedia Tools and Applications, 2021, 80(3): 4789-4823.

[31] KORDOV K. A novel audio encryption algorithm with permutation-substitution architecture[J]. Electronics, 2019, 8(5): 530.

[32] KHOIROM M S, LAIPHRAKPAM D S, TUITHUNG T. Audio encryption using ameliorated ElGamal public key encryption over finite field[J]. Wireless Personal Communications, 2021, 117(2): 809-823.

[33] FARSANA F J, GOPAKUMAR K. Private key encryption of speech signal based on three dimensional chaotic map[C]//Proceedings of 2017 International Conference on Communication and Signal Processing (ICCSP). Piscataway: IEEE Press, 2017: 2197-2201.

[作者简介]

张秋余（1966– ），男，兰州理工大学博士生导师，主要研究方向为网络信息安全、智能信息处理与模式识别等。

宋宇杰（1994– ），男，兰州理工大学硕士生，主要研究方向为网络信息安全、密文语音检索等。