文章编号:1671-4598(2021)05-0204-05 DOI:10.16526/j.cnki.11—4762/tp.2021.05.041 中图分类号:TP309 文献标识码:A

大数据加密算法在数据安全保护中的应用研究

张晓敏
(中共陕西省委党校(陕西行政学院)文化与科技教研部,西安 710075)

摘要:针对大数据加密算法安全性不高,计算效率低等问题,本研究采用双混沌系统结合改进AES加密算法设计出一个混合加密算法,改进AES算是利用仿射变换对(A7、6F)生成新的S盒,采用的双四维超混沌系统是从两个三维混沌系统进行改造而成,然后利用改造后的超混沌系统生成混沌序列,设计出一个分组加密方案,在Hadoop大数据平台上,将双超混沌加密方案和改进的AES算法进行合并;试验表明,本研究的大数据加密算法安全性能高、密钥长度达688 bit,加密解密效率提高2倍以上。

关键词:大数据加密算法;混沌系统;AES算法;超混沌;大数据

Research on Application of Big Data Encryption Algorithm in Protection of Data Security

Zhang Xiaomin
(Party School of the Shaanxi Provincial Committee of CPC, Xi'an 710075, China)

Abstract: Aiming at the problems of low security of big data encryption algorithm and low computational efficiency, this study uses a double chaos system combined with an improved AES encryption algorithm to design a hybrid encryption algorithm. The improved AES can be regarded as using affine transformation pairs (A7, 6F) to generate new S-box, the dual four-dimensional hyperchaotic system adopted is transformed from two three-dimensional chaotic systems, and then the transformed hyperchaotic system is used to generate a chaotic sequence, and a block encryption scheme is designed. On the Hadoop big data platform, the double hyperchaotic encryption scheme and the improved AES algorithm are combined. Experiments show that the big data encryption algorithm in this study has high security performance, the key length is 688 bit, and the encryption and decryption efficiency is increased by more than 2 times.

Keywords: big data eneryption algorithm; chao system; AES algorithm; hyperchaotic system; big data

0 引言

大数据是指数据规模较大,无法使用现有技术进行存储和处理的数据集,用户的隐私和数据安全问题一直是大数据领域研究的重点。随着大数据技术的逐渐成熟,大数据技术被广泛的运用到各个领域,大数据加密算法和方案的研究受到广泛关注。

在现有研究中,文献[1]采用超混沌分组加密和AES混合加密方案,虽然提高了算法的执行效率,但是忽视了AES加密算法的S盒迭代循环周期短的问题,文献[2]采用双混沌系统设计出一个数据加密模型,虽然也能够提高数据加密的效率和安全性,但是没有考虑到AES算法。本研究基于以上内容,对两组三倍混沌进行改进和AES算法进行改造生成两个新的四维混沌系统和新的AES算法,采用两个四维混沌系统设计出一个分组加密方案,最后在Hadoop平台上与改进AES算法融合成一个加密算法。

1 Hadoop大数据平台

Hadoop是一个分布式大数据平台,主要由HDFS和MapReduce两个核心组件组成,HDFS主要负责数据的分布式存储,MapReduce主要负责数据的分布式计算[3]。

MapReduce会将从HDFS传输过来的数据集分成若干个独立部分,然后由Map任务对这些独立的部分分别进行并行运算来完成对它们的处理,运算的结果则会传输给Reduce任务[4]。一般情况下,中间过程的运算结果会存储在本地磁盘中,只有最终的输出结果和输入会存储在HDFS中。

2 两个改进超混沌系统

超混沌系统相比混沌系统在加密领域具有更高的应用价值,因为其具有更为复杂的动力学行为[5]。

2.1 改进超混沌系统1

文献[6]提出了一种三维连续自治的混沌系统,其状态方程为:

收稿日期:2020-10-24; **修回日期**:2020-11-05。
作者简介:张晓敏(1981-),女,汉,甘肃白银人,硕士,讲师,主要从事应用数学与信息安全方向的研究。
引用格式:张晓敏.大数据加密算法在数据安全保护中的应用研究[J].计算机测量与控制,2021,29(5):204-5.

$$\begin{cases}\dot{x}=-ax+yz\\ \dot{y}=-x+cy\\ \dot{z}=dy^2-bz\end{cases}\tag{1}$$

式（1）中，a,b,c,d 为该三维系统的实际参数，x,y,z 为该三维系统的状态变量。该系统在 $a=20,b=5,c=10,d=7$ 时会产生混沌吸引子，此时该系统会变成超混沌状态，产生 3 个 Lyapunov 指数，分别为 $LE_1=1.237\ 1,LE_2=-0.029\ 1,LE_3=-16.448\ 4$。

将式（1）中的 $\dot{z}=dy^2-bz$ 项中的 dy^2 改成 dxy，能够得到一个新的三维连续自治混沌系统：

$$\begin{cases}\dot{x}=-ax+yz\\ \dot{y}=-x+cy\\ \dot{z}=dxy-bz\end{cases}\tag{2}$$

经过计算和分析，该系统在 $a=20,b=5,c=10,d=2$ 时的 3 个 Lyapunov 指数为 $LE_1=2.051\ 8,LE_2=-0.017\ 2,LE_3=-17.406\ 1$，相比文献[6]中提出的混沌系统，可以很明显看出本研究的混沌系统的 3 个 Lyapunov 指数远大于文献[6]的混沌系统 Lyapunov 指数，因此本研究的混沌系统具有比文献[6]混沌系统更复杂的动力学特性，比文献[6]中的混沌系统更非常适合用于大数据加密研究。

但是，该系统存在计算资源消耗高和结构复杂等问题，为此，采用状态反馈控制法，引入一个第四维的状态变量 w[7]，并将状态变量 w 引入到式（2）中的的第二个方程中，能够得到一个新的四维混沌系统：

$$\begin{cases}\dot{x}=-ax+yz\\ \dot{y}=-x+cy+w\\ \dot{z}=dxy-bz\\ \dot{w}=-ey\end{cases}\tag{3}$$

该系统相比传统的超混沌系统，只有两个非线性项，结构更加简单，除此之外，在相同的计算资源下，能够产生比文献[6]更长的混沌序列，因此比文献[6]的混沌系统更适用于大数据加密。

2.2　改进超混沌系统 2

文献[8]提出一个三维 Bao 混沌系统，其数学模型为：

$$\begin{cases}\dot{x}=a(x-y)\\ \dot{y}=xz-cy\\ \dot{z}=x^2-bz\end{cases}\tag{4}$$

该系统中包含两个非线性项的连续自治微分方程，式（4）中，a,b,c 为该三维系统的实际参数，x,y,z 为该三维系统的状态变量。该系统在 $a=20,b=4,c=32$ 时会产生混沌吸引子，此时该系统会呈超混沌状态，产生 3 个 Lyapunov 指数，分别为 $LE_1=2.887\ 3,LE_2=-0.011\ 5,LE_3=-18.904\ 9$。

同样的，将式（4）中的 $\dot{z}=x^2-bz$ 项中的 x^2 项改为 xy，可以得到一个新的三维混沌系统：

$$\begin{cases}\dot{x}=a(x-y)\\ \dot{y}=xz-cy\\ \dot{z}=xy-bz\end{cases}\tag{5}$$

经过计算和分析，该系统在 $a=20,b=8,c=32,d=3,e=5.7$ 时，的 3 个 Lyapunov 指数为 $LE_1=4.294\ 2,LE_2=-0.006\ 2,LE_3=-24.335\ 9$，相比文献[8]中提出的混沌系统，可以很明显的看出改进后的混沌系统的 3 个 Lyapunov 指数远大于文献[8]的混沌系统 Lyapunov 指数，因此改进后的混沌系统的动力学特性比文献[8]更复杂，比文献[8]更适合用于大数据加密研究。

同样的在式（5）的基础上引入一个第四维的状态变量 w 和一个控制参数 d，然后将反馈控制项添加到式（5）的第一项中，能够得到一个四维超混沌系统：

$$\begin{cases}\dot{x}=a(x-y)+ew\\ \dot{y}=xz-cy\\ \dot{z}=xy-bz\\ \dot{w}=-dx\end{cases}\tag{6}$$

该系统在 $a=20,b=8,c=32,d=3,e=5.7$ 时会产生超混沌吸引子，在系统结构、计算资源消耗上比文献[8]的混沌系统更有优势。

3　改进 AES 加密算法

S 盒是 AES 算法的重要组成部分之一，而传统的 S 盒迭代周期短，导致加密的安全性不高，存在被破解的可能，因此本研究对 AES 的 S 盒进行改进[9]。

3.1　S 盒的结构和原理

在 AES 算法中，S 盒运算是一种作用于状态字节的可逆的非线性变换运算，其定义为：

$$BS(a_{i,j})=\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}a_{i,j}{}^{-1}+\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix}\tag{7}$$

式（7）中，$a_{i,j}{}^{-1}$ 为 $a_{i,j}$ 在 $GF(2^8)$ 域中的乘法域：

$$a_{i,j}{}^{-1}=\begin{cases}(a_{i,j})^{254},a_{i,j}\neq 0\\ 0,a_{i,j}=0\end{cases}\tag{8}$$

因为有关运算是在 $GF(2^8)$ 域上进行，所以运算产生的计算结果也会在 $GF(2^8)$ 域上，最终产生的 S 盒是由 16×16 个字节组成的矩阵，并且最终的结果具有非线性度，因为计算的过程使用了乘法逆[10]。

3.2　改进 S 盒方案

提高 S 盒的迭代周期方法有采用不同的仿射变换对、改变 S 盒的计算顺序等方式[11]。因此本研究采用文献[12]中的新仿射变换对（$A7,6F$）对传统的 S 盒进行改进，改进的方法是采用新的仿射变换对（A7、6F）进行两次仿射变化，两次变换之间要求乘法逆。

4 大数据加密算法设计

4.1 两组超混沌加密方案

在设计混沌密码的过程中，当加密算法选择的是连续时间混沌系统时，需要注意连续混沌序列离散化、密钥参数选取对算法性能的影响[13]，除此之外，还要保证算法的安全性和实用性。基于以上内容，本研究的大数据加密方案如下：

(1) 选取密钥参数。选取密钥参数的前提是混沌系统处于超混沌态，通过试验和计算系统达到超混沌系统时的参数，保持参数不变，选取的密钥参数为上述两个超混沌系统的 8 个初始值，这样能够保证算法具有足够大的密钥空间[14]。

(2) 对混沌序列进行预处理。第一步对混沌系统进行离散化处理，本研究采用的是四阶 RungeKutta 法，第二部舍弃迭代序列的前 100 个值，舍弃前 100 个值的原因是为了让生成的混沌序列的随机性高[15]，第三步对混沌序列进行相关运算，使得混沌序列能够适应于字节加密，计算方法为：

$$\begin{cases} p_x^{(i)}(k) = \mathrm{mod}((x_i(k) - \lfloor x_i(k) \rfloor) \times 10^5, 256) \\ p_y^{(i)}(k) = \mathrm{mod}((y_i(k) - \lfloor y_i(k) \rfloor) \times 10^5, 256) \\ p_z^{(i)}(k) = \mathrm{mod}((z_i(k) - \lfloor z_i(k) \rfloor) \times 10^5, 256) \\ p_w^{(i)}(k) = \mathrm{mod}((z_i(k) - \lfloor z_i(k) \rfloor) \times 10^5, 256) \end{cases} \tag{9}$$

式 (9) 中，mod 为模去余数运算，$i = 1,2$，$\lfloor \rfloor$为向下取整运算，$p_x^{(i)}(k)$，$p_y^{(i)}(k)$，$p_z^{(i)}(k)$，$p_w^{(i)}(k)$ 为经过计算得到的 8 个混沌序列，它们的取值范围为 [0，256]。

(3) 混淆处理。超混沌系统生成的状态变量会存在一定的关联性，在被攻击时，这些关联性会为攻击者提供一定的信息，会提高被攻破的概率，为了提高算法的性能，减少被攻破的概率[16]，本研究对生成的两组混沌序列进行混淆处理，混淆处理的方法为：

$$\begin{cases} p_1(k) = p_x^{(1)}(k) \oplus p_x^{(2)}(k) \\ p_2(k) = p_y^{(1)}(k) \oplus p_y^{(2)}(k) \\ p_3(k) = p_z^{(1)}(k) \oplus p_z^{(2)}(k) \\ p_4(k) = p_w^{(1)}(k) \oplus p_w^{(2)}(k) \end{cases} \tag{10}$$

式 (10) 中，$\oplus$ 为异或运算符号，$p_i(k)$，$i = 1,2,3,4$ 为经过运算后得到的可以用于大数据加密的超混沌序列，最终得到的这些序列之间的关联性全部被破坏，从而提高了算法的安全性[17]。

(4) 分组加密。将步骤 (3) 中得到的 4 个序列对数据进行加密，加密方法是将数据按字节分组，每 4 个字节为一组进行加密，具体的加密过程为：

$$\begin{cases} C(4(k-1)+1) = M(4(k-1)+1) \oplus p_1(k) \\ C(4(k-1)+2) = M(4(k-1)+2) \oplus p_2(k) \\ C(4(k-1)+3) = M(4(k-1)+3) \oplus p_3(k) \\ C(4(k-1)+4) = M(4(k-1)+4) \oplus p_4(k) \end{cases} \tag{11}$$

式 (11) 中，M 为需要进行加密处理的数据明文，C 为经过超混沌分组加密后得到的密文。加密方案如图 1 所示。

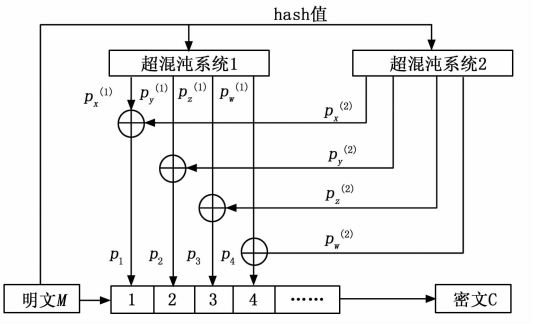

图 1 超混沌系统加密方案

4.2 基于 MapReduce 的超混沌系统和改进 AES 的混合加密算法

本研究的加密算法是在 Hadoop 大数据平台上实现的，采用 Hadoop 平台中的 MapReduce 编程模块对加密算法进行编程，MapReduce 由 Map 和 Reduce 两个函数组成，其中 Map 函数负责将上述超混沌数据加密和改进 AES 算法进行融合[18]，Reduce 函数负责在数据加密完成后的将所有的数据合并。具体步骤为：

(1) 对大数据集进行分片处理，将存储在 HDFS 上的大数据集按照 Hadoop2.0 的默认大小进行分块，每块 128 MB。

(2) Mep 将超混沌系统和改进 AES 算法进行混合，首先 Mep 函数要对分片处理后的数据集进行读取，采用键值对方式进行读取[19]，$< key_{in}^M, value_{in}^M >$ 代表输入键值对，$< key_{out}^M, value_{out}^M >$ 代表输出键值对。第一步选取密钥参数，这里需求上述两个超混沌系统的初始值，第二步按照图 1 的方案进行加密，第三步使用改进 AES 算法再进行数据加密。混合加密算法的伪代码为：

Input：K_{CHAOS}，K_{AES}，$< key_{in}^M, value_{in}^M >$

Output：

call farctional－hyperchaos－Ⅰ(K_{CHAOS})

call farctional－hyperchaos－Ⅱ(K_{CHAOS})

M(k)← $value_{in}^M$

$C(4(k-1)+1) = M(4(k-1)+1) \oplus p_1(k)$

$C(4(k-1)+2) = M(4(k-1)+2) \oplus p_2(k)$

$C(4(k-1)+3) = M(4(k-1)+3) \oplus p_3(k)$

$C(4(k-1)+4) = M(4(k-1)+4) \oplus p_4(k)$

$value_{out}^M$ ←C(k)

call AES－encrypt(K_{AES})

return $< key_{out}^M, value_{out}^M >$

其中：K_{CHAOS} 为超混沌系统密钥，K_{AES} 为改进 AES 算法密钥。

(3) 数据合并，数据合并采用的是 Reduce 函数来实现的，合并的对象是 Map 输出的经过加密算法加密后的数据

块，数据块在进行加密之前还需要采用 Shuffle 进行排序[20]。$<key_{in}^{R}, value_{in}^{R}>$ 为 Reduce 函数的输入，$<key_{out}^{R}, value_{out}^{R}>$ 为 Reduce 函数的输出。

（4）数据合并完成后，会存储在 HDFS 上，存储完成后即完成整个加密过程。

同样的解密算法的设计基本与加密算法相同，唯一不同的是解密算法中的 Map 函数进行的是解密操作而不是加密，只有当解密密钥和加密密钥完全匹配时，才会得到原始的明文数据，如果不能完全匹配，则不能得到明文数据[21]。因为采用了具有更加复杂动力学的超混沌系统和迭代周期长的 AES 算法，使得本研究的加密算法的安全性得到了很大的提高。

5　试验结果与分析

选择在实验室内采用高性能计算机对本研究的算法进行验证，计算机的硬件配置 CPU 为，inter corei7－9700H，运行内存为 3 200 MHz 8 G×2，硬盘大小为 512 G 固态。首先需要部署多个虚拟机，虚拟机的布置采用的是 VMware workstation 12 软件，虚拟机的配置为单核 CPU 和 1 GB 的运行内存，然后再虚拟机上部署 Hadoop 大数据平台，Hadoop 的版本为 2.7.3，算法的编程采用的是 JAVA，JAVA 版本为 Jdk8，IDE 的开发环境为 Eclips3.8。试验所用的数据为大小为 1 GB 和 2 GB 的大数据集，采用 Map 对其进行默认分块，每块的大小为 128 MB。

首先对本研究算法的密钥长度进行验证，验证方法为对比验证，对比的对象为文献[1]、文献[2]、文献[6]和文献[8]中的加密算法，本研究的加密算法的密钥长度为超混沌系统的长度和改进 AES 算法长度之和，本研究将两个超混沌系统的初始值作为超混沌系统密钥参数，密钥空间可以表示为：

$$K_{CHAOS} \in \{x_1^{(0)}, y_1^{(0)}, z_1^{(0)}, w_1^{(0)}, x_2^{(0)} y_2^{(0)}, z_2^{(0)}, w_2^{(0)}\}$$

这里设置密钥的精度为 10^{-15}，然后选取双精度的密钥参数，通过计算可以得到超混沌系统的密钥长度为 432 bit，在再加上改进 AES 算法的 256 bit，一共为 688 bit。将本研究算法的密钥长度与其他文献算法的密钥长度进行对比，可以得到表 1 数据。

表 1　密钥长度对比

算法	本文	文献[1]	文献[2]	文献[6]	文献[8]
密钥长度/bit	688	628	256	344	192

从表中数据可以看出，本文算法的密钥长度明显高于其他算法，密钥长度能够影响密文被破译的难度，密钥的长度越长，则被破译的可能性就越低，算法的安全性就越高。

然后对本文算法的效率进行验证，将本文算法中的超混沌加密方案和改进 AES 算法的效率分别进行验证，采用两种算法对上述 1 GB 和 2 GB 大小的数据集分别进行加密，逐步增加计算节点，统计不同节点下的加密时间，可以得到图 2 的加密时间对比图。

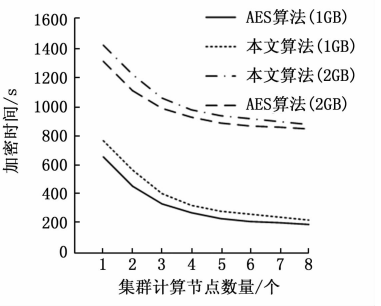

图 2　加密时间对比图

从图 2 中可以看出，虽然本研究的算法计算时间略微高于 AES 算法，但是随着计算节点的增加，本研究算法的计算效率显著提高。

最后对算法密钥的敏感性和统计性进行分析，密钥的敏感性决定算法的安全性，试验结果表明，只有当密钥完全匹配时，才会得到明文数据。当密钥的参数误差为 10^{-15} 时会产生雪崩效应，无法获取明文数据，并且会生成跟明文数据具有较大差异的密文，此时的密钥参数解密数据直方图如图 3 所示。

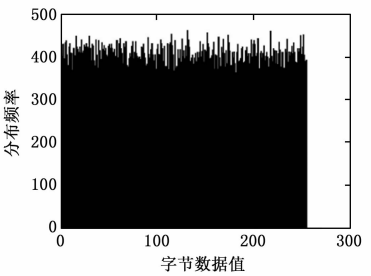

图 3　微小误差下的密钥参数解密数据直方图

从图中可以看出本研究算法的密钥敏感性优秀，在达到临界值后能够产生雪崩效应，使得破译的难度增大。

加密前后的数据字节数据值对比如图 4 所示。

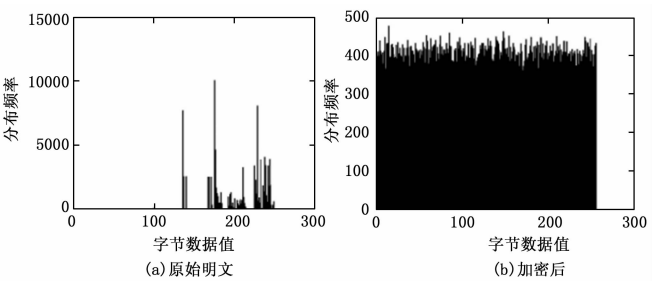

图 4　加密前后的文本数据统计图

从图中可以看出，原始具有一定规律分布的明文数据经过本研究算法的加密之后呈无相关性的随机分布状态。

综上所述，本研究的大数据加密算法性能优秀。

6 结束语

本研究将利用 MapReduce 将双超混沌加密算法与改进 AES 算法合并生成一个新的加密算法，通过试验证明了算法的可行性，并得出以下结论：

1）数据加密中密钥的空间大小会影响加密算法的安全性，本研究将两个三维混沌系统进行改造生成了两个四维混沌系统，提高了混动加密方案的密钥长度。

2）传统的 AES 加密算法的迭代周期短，可能会存在被破译的风险，本研究采用新的仿射变换对生成一个新的 S 盒序列，提高了 AES 算法的迭代周期。

3）混沌系统具有非常复杂的动力学特性，不仅能够用于数据加密，还能用于其他类型文件的加密，系统的维数越高，动力学特性越复杂，加密效果越好。

实验结果表明，本研究的数据加密算法具有密钥空间大、安全性能高，加密效率高等优势，在网络数据安全保护方面具有一定的研究价值，但是由于人为疏忽，难免会存在一些问题，在后续的研究中需要进行相应的改进和完善。

参考文献：

[1] 温贺平，陈俞强. 面向大数据的超混沌和 AES 混合加密方法研究 [J]. 计算机应用与软件，2018，35 (5)：318 - 322.

[2] 司红伟，钟国韵. 基于双混沌系统的大数据环境并行加密算法设计 [J]. 计算机测量与控制，2015，23 (7)：2475 - 2477.

[3] 冯 凯. 基于 Hadoop 的大数据平台风险监测系统研究 [J]. 自动化技术与应用，2020，39 (9)：135 - 138.

[4] 闫 鹏，张 林. 基于 Hadoop 平台的交通大数据智能特征分析研究 [J]. 华北理工大学学报（自然科学版），2020，42 (3)：80 - 88.

[5] 王 勇，朱 光，王 瑛. 细胞神经网络与改进 AES 的超混沌图像加密方案 [J]. 计算机工程与应用，2018，54 (21)：194 - 200.

[6] 卢辉斌，薛 瑶，赵 玲，等. 一个新型四维混沌系统的构造与应用 [J]. 燕山大学学报，2019，43 (1)：25 - 33.

[7] 洪玲玲，杨启贵. 新四维超混沌系统的复杂动力学研究 [J]. 广西师范大学学报（自然科学版），2019，37 (3)：96 - 105.

[8] Bao Bochen，Liu Zhong，Xu Jianping. New chaotic system and its hyperchaos generation [J]. Journal of Systems Engineering and Electronics. 2009，20 (6)：1179 - 1187.

[9] 刘海峰，陶建萍. 基于改进 AES 的一次一密加密算法的实现 [J]. 科学技术与工程，2019，19 (13)：146 - 150.

[10] 何 丰，王耀灯. AES 密钥扩展算法的研究 [J]. 微电子学与计算机. 2017，34 (10)：68 - 71.

[11] 卢 军，张国辉，李国强. 一种基于数据分解的 AES 优化算法设计 [J]. 单片机与嵌入式系统应用，2019，19 (4)：15 - 18.

[12] 孙爱娟. 基于 AES 加密算法的改进及其 MATLAB 实现 [D]. 哈尔滨：哈尔滨理工大学，2009.

[13] 魏 慧，李国东，许向亮. 基于改进的复合混沌系统的图像加密算法 [J]. 微电子学与计算机，2020，37 (4)：19 - 25.

[14] 王 勇，杨 锦，王 瑛. 改进 Henon 超混沌系统与 AES 结合的图像加密算法 [J]. 计算机工程与应用，2019，55 (22)：180 - 186.

[15] 谢国波，陈志伟. 基于改进的 CAT 置乱与 Henon _ Kent 混沌系统的彩色图像自适应加密算法 [J]. 计算机应用研究，2019，36 (11)：3369 - 3372.

[16] 王 倩. 改进 Arnold 算法和超混沌系统的医学图像加密研究 [J]. 计算机时代，2018 (2)：43 - 47.

[17] 汪 彦，涂 立. 基于改进 Lorenz 混沌系统的图像加密新算法 [J]. 中南大学学报（自然科学版），2017，48 (10)：2678 - 2685.

[18] 温贺平，禹思敏，吕金虎. 基于 Hadoop 大数据平台和无简并高维离散超混沌系统的加密算法 [J]. 物理学报，2017，66 (23)：76 - 89.

[19] 王 勇，方小强，王 瑛. 超混沌系统和 AES 结合的图像加密算法 [J]. 计算机工程与应用，2019，55 (8)：164 - 170.

[20] 林 愿，陈爱萍. 基于超混沌和 AES 的混合图像加密算法 [J]. 湖南工程学院学报（自然科学版），2016，26 (2)：6 - 9.

[21] 谢国波，姚灼琛. 用于 Hadoop 平台的混沌加密研究与实现 [J]. 计算机应用研究，2019，36 (11)：3378 - 3381.

（上接第 203 页）

[8] Bologna G，Benoit Deville，Pun T，et al. Identifying Major Components of Pictures by Audio Encoding of Colours [A]. International Work－conference on Nature Inspired Problem－solving Methods in Knowledge Engineering：Interplay Between Natural & Artificial Computation [C]. Springer － Verlag，2007.

[9] 许伯恩. 基于 Kinect 的盲人室内环境防碰撞辅助系统 [D]. 嘉义：台湾国立中正大学，2013.

[10] 张晓静. 基于数字图像处理的导盲系统设计 [D]. 石家庄：河北科技大学，2016.

[11] Li X，Li X. Filling the holes of 3D body scan line point cloud [A]. Advanced Computer Control (ICACC)，2010 2nd International Conference on [C]. IEEE，2010，334 - 338.

[12] 王 冲，李锻能，邓君裕，等. 改进法线方向的点云实时分割提取平面方法研究 [J]. 计算机测量与控制，2018，26 (5)：210 - 213.

[13] 林 怡，季昊巍，叶 勤. 基于 LiDAR 点云的单棵树木提取方法研究 [J]. 计算机测量与控制，2017，25 (6)：142 - 147.

[14] 陈 朋，谭晔汶，李 亮. 地面三维激光扫描建筑物点云特征线提取 [J]. 激光杂志，2016，37 (3)：9 - 11.

[15] 姚明海，隆学斌. 基于改进的卷积神经网络的道路井盖缺陷检测研究 [J]. 计算机测量与控制，2020，28 (1)：66 - 70.