基于云计算的混合混沌加密算法研究

田佳鹭
(沈阳师范大学 数学与系统科学学院,辽宁 沈阳 110034)

摘 要:针对云平台环境下数据安全及保密问题,基于MapReduce分布式框架下,综合4种混沌映射系统的优点,提出一种面向云计算的混合混沌加密方法。利用4种混沌映射产生的混沌序列作为密钥,多次使用从混沌系统迭代产生的多重密钥对明文进行加密操作。实验结果证明,该算法的执行效率高,密钥空间足够大,能够有效抵抗暴力破解密钥的攻击。

关键词:混沌加密;云计算;MapReduce;信息安全
中图分类号:TN918;TP391 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.200298

中文引用格式:田佳鹭. 基于云计算的混合混沌加密算法研究[J].电子技术应用,2020,46(10):79-82,87.
英文引用格式:Tian Jialu. Research on hybrid chaotic encryption algorithm based on cloud computing[J]. Application of Electronic Technique,2020,46(10):79-82,87.

Research on hybrid chaotic encryption algorithm based on cloud computing

Tian Jialu
(School of Mathematics and Systems Science,Shenyang Normal University,Shenyang 110034,China)

Absrtact:Aiming at the problem of data security and confidentiality in the cloud platform environment, based on the MapReduce distributed framework, combining the advantages of four chaotic mapping systems, a hybrid chaotic encryption method for cloud computing is proposed. Using the chaotic sequence generated by four chaotic maps as the key, the plaintext is encrypted by using the multiple key generated from the iteration of chaotic system for many times. The experimental results show that the algorithm is efficient and the key space is large enough to effectively resist the attack of brute force key cracking.

Key words:chaos encryption;cloud computing;MapReduce;information safety

0 引言

当前互联网技术已经实现在领域内的普及和应用,网络中的海量数据信息给现阶段应用带来了巨大的挑战。云计算的出现使情况得到了有效的缓解,充分利用现有的技术将所有资源进行整合,按需使用,降低了运营成本。云计算网络在不断推动信息技术发展和社会发展的同时也伴随着数据泄露的危机,数据信息在存储过程中的安全性和可靠性的保障问题引起了人们的广泛关注,急需对此问题进行解决。本文简要分析了云计算、网络安全存储等方面存在的安全隐患,此外为了有效降低数据丢失和泄漏的风险,使用加密技术对传输中的数据进行保护是一种较为有效的措施。本文提出一种运用混合混沌加密的方法对计算机中的数据块进行加密,有效地保障了数据的安全性,更好地防止暴力破解秘钥的攻击。

1 云计算技术分析

“云”是一种高效的虚拟计算资源,可提供计算、通信、存储等多种服务[1]。云计算集中了各种形式的网络资源,通过专门软件减轻了人工的工作量实现机器自动管理,并减轻了一些烦琐的细节,提高效率,有效降低了成本并且对技术进行了一定的创新。专家将云计算定义为:云计算是一种基于网络按照用户需求提供可以动态伸缩的廉价计算服务[2]。对于海量数据分布式存储、云资源管理、虚拟化技术、并行编程计算等是云计算中比较关键的几种应用技术[3]。云计算根据服务类型可分为3种:(1)基础设施即服务(Infrastructure-as-a-Service,IaaS):可提供基础设备按并使用量付费;(2)平台即服务(Platform-as-a-Service,PaaS):可提供便利的运行环境,使用户不必过多注意节点间的协调沟通问题;(3)软件即服务(Software-as-a-Service,SaaS):较前二者则更加稳定成熟,是适应中小型企业的一种工作模式,将某些特定应用软件功能作为主要的服务,便于中小企业工作的完成[4]。

1.1 云计算的特点

(1)规模庞大。

(2)虚拟化技术。“云”作为一种虚拟的形式存在,并不是所谓的固定有形的云实体。它便于用户在各种终

端、任意位置上获取有效服务，充分体现了其虚拟化、便于用户使用的特点。

(3)通用性。同一片“云”可以同时支撑不同的应用运行，为用户带来了极大的便利。

(4)可伸缩性强。“云”本身具有灵活的动态可伸缩性，资源用量的弹性可扩展性，能够更好地满足用户和应用规模的动态增长。

(5)可靠性高。

(6)按需求提供服务。

(7)极其廉价。

1.2 3种云模式

随着云计算的发展，几乎每个企业都在计划或正在使用云计算。针对不同企业的需求，云模式包括3种，分别为：(1)公共云(Public clouds)：主要供第三方提供商用户使用，其优点在于价格低廉，并且在公共开放的网络环境下可以获取更多资源，但其安全性无法很好地保障；(2)私有云(Private Clouds)：主要为独立的公司或企业提供服务，安全性能良好，但价格也相对较高；(3)混合云(Hybrid Cloud)：将公有云和私有云相结合，性能上更加完善，使其在敏捷性和灵活性等方面都有显著提高，应用前景更好[5]。

2 云计算技术在计算机网络中存在的隐患问题

日益强大的计算机网络给人们的生产生活带来了极大的便利，但与此同时一些网络安全问题也相应而生。例如网络信息经常遭受不法之徒与黑客的攻击，造成机密信息的泄露，这对于个人以及企业无论是身心还是经济方面都造成了严重的损失，因此保证云环境中数据存储的安全性是一个十分重要的事情[6]。常见的网络安全隐患包括：网络协议自身带有安全问题，例如协议中明文传输的方式无法保障信息的安全性等；网络硬件设施存在一定缺陷；操作系统存在缺陷，由于日益复杂的网络环境，使得操作系统很容易受到黑客以及不法分子的恶意攻击，从而导致计算机病毒的无限蔓延，给用户的安全和财产都带来了巨大威胁；应用软件存在缺陷；终端用户的不规范使用行为[7]。

人们可以清晰地体会到，现阶段对于网络安全方面的威胁已经相当普遍，无论是个人、企业还是政府机关，都需要面临、考虑如何进行有效的维护网络规范，避免安全威胁产生的负面影响。云计算服务如今面临着许多威胁，专家将它们归结为两类：一类属于云环境的内部威胁，另一类属于云环境的外部威胁[8]。

(1)云环境的内部威胁。云环境内部威胁数据安全的攻击者包括不可信云服务商以及没有查询权限的非法用户，他们会想方设法地利用云环境中的漏洞来窃取用户的隐私数据，对文件进行窃取和破坏。除此之外，在用户共享数据时，由于操作人员的过失操作也会给网络环境的安全性带来一定的威胁。

(2)云环境的外部威胁。云计算技术是各大企业平台和电子服务行业广泛运用的互联网技术，外界的攻击也随之而来。例如在用户将数据文件上传至云端时，网络攻击者就会利用接口入侵用户文件对其进行窃取，或截获数据文件导致文件无法上传成功。此外云平台为用户提供了资源共享的服务，用户在获取便利的同时由于不规范的操作和使用范围的广延性，会导致云环境变得异常混乱，让不法分子有机可乘[9]。

为了针对复杂的网络安全问题，密码学随之而来。通过加密用户的交流信息，来隐藏所传输数据的真实内涵，有效阻止不法分子对用户隐私数据以及网络中重要数据的窃取。

3 混沌加密系统

3.1 混沌学

混沌现象是发生在确定系统中一种貌似随机的不规则运动，即看似有序但实际又无序的伪随机性运动[10]。混沌现象的特征为：

(1)对初值极端敏感依赖：初始条件发生的极小差异都会随着算法演变成巨大的分歧。

(2)长期不可预测和短期预测的可能性。

(3)普适特性：在混沌系统经过迭代过程趋于混沌状态时会出现某类特征保持不变，来代替一般情况中的空间或时间周期性。

(4)有序性：混沌现象的轨迹会呈现出异常的复杂运动形式，但在伪随机运动中却表现出惊人的确定性，长期稳定而局部不稳定。

混沌的密码的体系结构和传统密码算法中对称算法的序列密码最为相似，该算法运用加密过程中多次使用多重密钥的方法来加密明文，即通过多次迭代生成密钥将其与明文异或再同干扰值进行二次异或生成密文。该方法可以使明文实现扩散和置乱的效果，使其具有更好的随机性，并且密钥空间更大，可以有效抵抗恶意破解。方法中选用了两种维数的4种线性混沌映射，分别是二维混沌映射系统：Henon混沌映射、Logistic混沌映射，以及三维非线性混沌系统：Lorenz混沌映射、Wien混沌映射。混沌映射结构的维数越高其随机性和复杂性将更强，使得伪随机序列较难预测，因此加密过程的安全性将得到保障[11]。

3.2 Lyapunov指数

Lyapunov指数又称为李氏指数，是混沌运动判别的一个重要指标，用来判断系统是否处于稳定状态。Lyapunov指数λ为：

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}\ln\left|\frac{\mathrm{d}x_n}{\mathrm{d}x_0}\right| \tag{1}$$

其中，x_0是已知映射初始值，x_n是迭代n次后的点。若指数$\lambda<0$，则系统处于相对稳定状态；若指数$\lambda>0$，则系统的状态不太稳定。

3.3 4种混沌映射介绍

(1)二维 Logistic 混沌映射

二维 Logistic 混沌映射是一种典型的抛物线映射，其描述为：

$$\begin{cases} x_{n+1}=\mu_1 x_n(1-x_n)+\gamma_1 y_n^2 \\ y_{n+1}=\mu_2 y_n(1-y_n)+\gamma_2(x_n^2-x_n y_n) \end{cases} \tag{2}$$

该混沌映射系统中的参数范围在$2.75<\mu_1<3.4$，$2.7<\mu_2<3.45$ 和 $0.15<\gamma_1<0.21$，$0.13<\gamma_2<0.15$，并将参数设为 $\mu_1=2.85$，$\mu_2=3.10$，$\gamma_1=0.180$，$\gamma_2=0.135$。对于生成的混沌序列值 $x,y\in(0,1)$，为了使迭代后的混沌序列(x,y)均值更加符合理想的随机序列，将得到的迭代序列值进行如下处理：

$$x_n=10^6 x_n-\lfloor 10^6 x_n \rfloor \tag{3}$$

$$y_n=10^6 y_n-\lfloor 10^6 y_n \rfloor \tag{4}$$

式中，“$\lfloor\ \rfloor$”为向下取整运算符 Floor。

(2)Lozi 混沌映射

一般形式的 Lozi 系统可描述为：

$$\begin{cases} x_1(n+1)=f_1[x_1(n),x_2(n)]=-a|x_1(n)|+x_2(n)+1 \\ x_2(n+1)=f_2[x_1(n),x_2(n)]=bx_1(n) \end{cases} \tag{5}$$

其中，a、b 是 2 个实值参数，该系统也是一个二维映射系统[12]。

(3)Lorenz 混沌映射

Lorenz 连续混沌映射可以描述为：

$$\begin{cases} \dfrac{dx_1}{dt_1}=p(x_2-x_1) \\ \dfrac{dx_2}{dt_1}=-x_1x_2+rx_1-x_2 \\ \dfrac{dx_3}{dt_1}=x_2x_1-t_1x_3 \end{cases} \tag{6}$$

其中，p、r、t_1 为系统参数。当 $p=10$，$r=28$，$t_1=8/3$ 时该系统处于混沌状态，并具有高迭代性的优点。

(4)Wien 混沌映射

Wien 混沌映射可以描述为下式：

$$\begin{cases} dx(t_2)=-x(t_2)+2.5(y(t_2)-z(t_2)) \\ dy(t_2)=-x(t_2)+1.5y(t_2)-2.5z(t_2) \\ dz(t_2)=5u(y(t_2)-1)z(t_2) \end{cases} \tag{7}$$

其中，t_2 为参数。

3.4 基于 MapReduce 的混合混沌加密方案

本文中的加密方案运用了前面提到的 4 种混沌映射方法，并且将这种混合混沌加密方法与 MapReduce 分布式处理模型相结合对明文进行加密。方法中首先利用 Lorenz 和 Wien 产生混沌序列值作为 Wien 和 2D-Logistic 的迭代初值和干扰值，通过多次迭代生成密钥将其与明文异或再同干扰值进行二次异或生成密文。该方法使得加密效率会随着明文量的增大而逐渐增加，并使密文具有良好的扩散性，尽可能有效地隐藏明文中的每一块信息，使明文、密文和密钥三者的关系尽可能地复杂来保证较高的安全性。加密步骤如下：

(1)明文分块

假设明文的总长度为 L，将明文分割成 n 块，每一块的大小用 $l_i(i\leqslant n)$来表示。首先将前 $n-1$ 块均划分为长度为 $4N$ 的等长数据块，而剩余部分数据则作为第 n 块。即：

$$l_i=\begin{cases} 4N & i<n \\ L-(n-1)4N & i=n \end{cases} \tag{8}$$

(2)生成初值与干扰值

接着对每一块生成拥有不同初始值的迭代序列，先运用三维 Lorenz 混沌映射和 Wien 混沌映射针对每个分块产生相应的初始值和干扰值，每次迭代各产生 3 个随机序列值，2 个随机序列对，则共生成 6 个混沌序列值 $\boldsymbol{\chi}=(x_1,x_2,x_3,x_4,x_5,x_6)$。设 N_0、T_0 为 Lorenz 系统和 Wien 系统的初始迭代次数，获取明文块第一个字节的偏移量 θ_i，则两个系统的迭代次数分别重新定义为 ρ_L、ρ_C：

$$\rho_L=\frac{\theta_i}{N}+N_0 \tag{9}$$

$$\rho_C=\frac{\theta_i}{N}+T_0 \tag{10}$$

对于每个分块产生的混沌序列为：

$$\boldsymbol{\chi}_\rho=(x_1(\rho_L),x_2(\rho_L),x_3(\rho_L),x_4(\rho_C),x_5(\rho_C),x_6(\rho_C)) \tag{11}$$

其中，$x_1(\rho_L)$、$x_2(\rho_L)$、$x_3(\rho_L)$为 Lorenz 系统产生的混沌序列值，$x_4(\rho_C)$、$x_5(\rho_C)$、$x_6(\rho_C)$为 Wien 系统产生的混沌序列值。通过将混沌序列进行异或操作(“$\oplus$”为异或运算符)来消除混沌系统之间存在的互相关性，降低密码攻击的风险，有效提高混沌序列的随机特性。执行的操作如下：

$$x_4(\rho_C)=x_4(\rho_C)\oplus x_1(\rho_L) \tag{12}$$

$$x_5(\rho_C)=x_5(\rho_C)\oplus x_2(\rho_L) \tag{13}$$

$$x_6(\rho_C)=x_6(\rho_C)\oplus x_3(\rho_L) \tag{14}$$

(3)生成加密序列

将混沌序列 $\boldsymbol{\chi}_\rho$ 分为初值序列 $\boldsymbol{\chi}_\rho^{I}$ 和干扰序列 $\boldsymbol{\chi}_\rho^{d}$：

$$\boldsymbol{\chi}_\rho^{I}=(x_1(\rho_L),x_2(\rho_L),x_3(\rho_L),x_4(\rho_C)) \tag{15}$$

$$\boldsymbol{\chi}_\rho^{d}=(x_5(\rho_C),x_6(\rho_C)) \tag{16}$$

Wien 混沌映射和 2D-Logistic 混沌映射的初始值为初值序列 $\boldsymbol{\chi}_\rho^{I}$，并通过两个系统迭代生成加密序列 $\boldsymbol{\alpha}_\rho=(\alpha_1(\rho),\alpha_2(\rho),\alpha_3(\rho),\alpha_4(\rho))$，即密钥，其中 $\alpha_i(\rho)$为加密序列值。接着对混沌序列进行混淆处理，有效保证序列的高可靠性和随机性。执行如下操作：

$$\alpha_3(\rho)=\alpha_1(\rho)\oplus\alpha_3(\rho) \tag{17}$$

$$\alpha_4(\rho)=\alpha_2(\rho)\oplus\alpha_4(\rho) \tag{18}$$

(4)加密前的预处理操作

为了能够与明文进行相应的异或操作，需要将加密序列进行小数点移位、取模等运算转换到相应的的模空间中去。

(5)对明文分块进行加密

加密过程中先取明文中的 4 个字节相应的 ASC Ⅱ

码 T，接着先与加密序列进行一次异或操作实现明文第一次加密。干扰序列的作用在于有效提高加密过程的安全性，因此使用它对密文进行第二次的加密干扰得到密文 C，$K+1$ 代表混合混沌系统的迭代次数。

3.5 基于 MapReduce 的加密实现过程

在 MapReduce 编程模型中，系统中通常包含 M 个Map 操作和 R 个 Reduce 操作，过程分为 3 个步骤：

(1)进行分片，将任务均匀的分配到多个节点机器上面，设集群处理节点数量为 P。

(2)对分片进行加密操作，该混沌方法中对每个数据块的加密计算可以相互独立，使得能够对它们进行充分并行的运算，并且多个 Map 也可同时进行加密。Map 的输入参数是 in_key 和 in_value，它的输出结果是一对 <key，value>。在加密过程中对输入的 value 值中每次取 4 个字节同混沌序列进行加密。

(3)运用 Reduce 操作，对 M 个 Map 操作结果进行合并操作。实际在进行 Reduce 操作之前，系统已经将所有 Map 产生的结果进行了相应的归类处理，因此可以有效简化 Reduce 的归并处理，最后所有 Reduce 产生的处理结果经过简单连接形成了完整的结果集。

4 实验结果与分析

4.1 算法密钥空间分析

在本文提出的加密方案中，密钥可表示为 $\boldsymbol{\chi}(0)=(x_1(0),x_2(0),x_3(0),x_4(0),x_5(0),x_6(0))$，设初始值为 (0.36，0.93，−2.3，1.96，1.29，2.66)，Lorenz 和 Wien 系统的初始迭代次数 N_0=200 和 T_0=300，另外还有两个映射系统的参数分别为 p=10，r=28，t_1=8/3，t_2=1/3。那么存放这些数据需要 344 位的空间大小，则破解密钥的组合数为 2 的 344 次方，可看出该方法的密钥空间足够大，能够有效抵抗暴力破解秘钥的攻击。

4.2 算法执行效率分析

通过分析算法在加密方面的执行效率，可观察出该算法的优势所在。首先表 1 是 RSA 算法、ASE 算法和本文的混合混沌加密算法在相同的硬件和软件环境基础上，对不同大小的文本文件进行加密所需的时间，时间以 ms 为单位。

表 1 RSA 算法、ASE 算法和本文加密算法的加密时间对比

(ms)

算法	文件大小				
	1 KB	1 MB	10 MB	100 MB	1 GB
RSA	525	2 265	10 604	90 101	853 363
ASE	505	1 082	6 531	40 362	423 211
本文加密算法	2	101	722	6 469	79 228

接着实验数据选取大小为 1 GB 的大数据文本文件，并在基于 MapReduce 的并行处理结构的基础上，伴随着集群计算节点个数的增加的情况下，比较本文所设计的算法与采用 RSA 加密算法、AES 加密算法的运行效率，如图 1 所示。

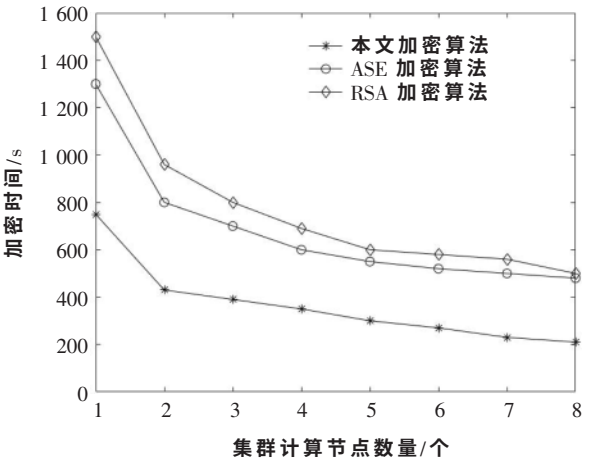

图 1 基于 MapReduce 的执行效率

从图 1 中可以看出，本文的混合混沌加密算法比其他算法的加密效率更高，此外还可以看出随着集群节点个数的增加，本文所提出的算法可以有效提高加密效率，可证明该算法具有良好的并行运行效率。

5 结论

本文针对云计算的平台环境下数据安全及保密问题，综合利用 MapReduce 分布式框架以及 4 种混沌映射系统的优点，提出一种面向云计算的混合混沌加密方法。通过实验结果可以看出，该算法的执行效率较比传统的加密算法有显著的提高。此外，密钥空间的增大可以有效应对恶意破解攻击。由此可见，该算法能够从容应对云计算环境下普遍的数据安全及用户隐私保密的问题，具有一定的应用价值。

参考文献

[1] 崔冉冉.云环境下基于隐私保护的数据安全机制研究[D].济南：山东师范大学，2019.

[2] 陈立朝.基于同态加密的安全多方计算协议及应用[D].西安：西安科技大学，2019.

[3] 王建徽.探讨云计算大数据的安全问题与应对措施[J].网络安全技术与应用，2019(11)：72-73.

[4] 任秋洁，潘刚，白永强，等.基于 FAHP 和攻击树的信息系统安全风险评估[J].电子技术应用，2018，44(8)：113-117.

[5] 拱长青，肖芸，李梦飞，等.云计算安全研究综述[J].沈阳航空航天大学学报，2017，34(4)：1-17.

[6] 姜唐.云计算安全之数据加密[J].计算机与网络，2018，44(18)：52-53.

[7] 李宗育，桂小林，顾迎捷，等.同态加密技术及其在云计算隐私保护中的应用[J].软件学报，2018，29(7)：1830-1851.

[8] PARIKH S，DAVE D，PATEL R，et al.Security and privacy issues in cloud，fog and edge computing[J].Procedia Computer Science，2019，160：734-739.

(下转第 87 页)

图 8 真实模拟康妮数据下投展示模块

3 结论

本文介绍了一款针对大型无人机台风观测能力建设项目进行开发的无人机台风探测实况监控系统。该系统负责实时接收无人机系统地面接收站发送的无人机和气象放舱信息，并实时在三维地图上展示。系统由 CMACast、MICAPS 以及具备地面气象导航规划、飞行器航迹实时气象监视、下投探空标校及后处理子系统等功能的软件子系统组成。完成的实况监控系统运行稳定，模块化清晰，可实现我国综合气象资料与大型无人机监控系统全面结合。该系统是我国首次应用大型无人机与气象产品数据相结合的开发研究，为今后业务化观测台风奠定技术基础。

参考文献

[1] 郭琪，童庆祥.无人机在气象监测中的应用[J].广东气象，2016(6)：64-66.

[2] 马俊.基于 GoogleEarth 的无人机地面站监控系统[D].南京：南京航空航天大学，2011.

[3] 于歌，刘刚，房建成.小型无人机地面监控系统软件设计与实现[J].机械与电子，2007(7)：25-27.

[4] 马杰，孙仁祺.无人机发展的缘起与近期发展的三次浪潮[J].江苏航空，2008(1)：4-5.

[5] 雷小途.无人飞机在台风探测中的应用进展[J].地球科学进展，2015，30(2)：276-283.

[6] 荆平平，刘惠，王厚军，等.基于移动平台的海域无人机监视监测系统集成技术与应用[J].中国科技成果，2018(18)：24-26.

[7] WICK G A，HOCK T F，NEIMAN P J，et al.The NCAR-NOAA global Hawk dropsonde system[J].Journal of Atmospheric and Oceanic Technology，2018，35(8)：1585-1604.

[8] 刘洋，韩泉泉，赵娜.无人机地面综合监控系统设计与实现[J].电子设计工程，2016，24(14)：110-112.

[9] COFFEY J J，WICK G A，HOOD R E，et al.Sensing hazards with operational unmanned technology：NOAA′s application of the global Hawk aircraft for high impact weather forecasting[C].AGU Fall Meeting，2015.

[10] WICK G.NOAA utilization of the global Hawk unmanned aircraft for atmospheric research and forecast improvement[C].AGU Fall Meeting，2014.

(收稿日期：2019-11-25)

作者简介：

张东明(1990-)，男，硕士，工程师，主要研究方向：大气探测、信号处理、软件开发。

张雪芬(1958-)，男，博士，正研级高级工程师，主要研究方向：大气探测。

郭然(1988-)，男，硕士，工程师，主要研究方向：信号探测、信息处理。

(上接第 82 页)

[9] ZHOU Y H，SU K，SHAO L M.A new chaotic hybrid cognitive optimization algorithm[J].Cognitive Systems Research，2018，52：537-542.

[10] 曾珂，禹思敏，胡迎春，等.基于 3D-LSCM 的图像混沌加密算法[J].电子技术应用，2020，46(1)：86-91.

[11] 姚灼琛.用于 Hadoop 平台的大数据混沌加密研究与实现[D].广州：广东工业大学，2019.

[12] WEI S，YU Z，CHONG F，et al.A novel batch image encryption algorithm using parallel computing[J].Information Sciences，2020，518：211-224.

(收稿日期：2020-04-14)

作者简介：

田佳鹭(1996-)，女，硕士研究生，主要研究方向：人工智能与云计算。

版权声明