文章编号:1671-4598(2018)07-0153-04 DOI:10.16526/j.cnki.11—4762/tp.2018.07.033 中图分类号:TP309 文献标识码:A

基于云计算的混合超混沌分组密码方案研究

温贺平，柯居鑫，陈俞强
(东莞职业技术学院 信息与教育技术中心，广东 东莞 523808)

摘要：针对云计算环境中的数据安全问题，提出了一种基于云计算的混合超混沌加密算法；首先，选取三个超混沌系统的初始值作为密钥参数，利用超混沌系统更加复杂的动力学行为产生随机特性良好的混沌序列；接着，对三个超混沌系统进行预处理后，进而设计一个混合超混沌分组加密方案；最后，基于 MapReduce 的云计算分布式编程模型，设计并行超混沌加密算法；实验结果和分析表明，算法具有执行效率高，密钥空间大及密钥敏感性良好的特性。

关键词：混沌密码；超混沌；云计算；MapReduce

Research on Hybrid Hyperchaotic Block Cipher Scheme Based on Cloud Computing

Wen Heping, Ke Juxin, Chen Yuqiang
(Dongguan Polytechnic, Dongguan 523808, China)

Abstract: Aiming at the problem of data security in cloud computing environment, a hybrid hyper chaotic encryption algorithm based on cloud computing is proposed. Firstly, the initial values of three hyperchaotic systems are chosen as the key parameters, and the chaotic sequences with good random characteristics are generated by the more complex dynamical behavior of hyperchaotic systems; Then, three hyperchaotic systems are pre—processed, and then a mixed hyperchaotic block encryption scheme is designed; Finally, a parallel hyper chaotic encryption algorithm is designed based on the distributed programming model of cloud computing in MapReduce. Experimental results and analysis show that the algorithm has the characteristics of high efficiency, large key space and good key sensitivity.

Keywords: chaotic cryptography; hyperchaos; cloud computing; MapReduce

0 引言

云计算是以计算机网络、服务器虚拟化、大规模数据处理等技术为基础，具备按需分配、资源共享、分布式处理等特点，是一种能够适应于当今网络通信环境的主流计算模式[1]。随着计算机网络、移动互联网、物联网等技术的发展，全球入网的终端和用户激增，云计算技术在工业、金融、政府、医疗、教育等各个行业和领域得到了广泛的应用。但是，由于云计算安全架构尚存在不够完善的地方，伴随着云计算技术的普及和推广，在云计算环境中的各种安全问题逐渐显露出来，引起了各界人士的广泛关注[2]。

密码技术作为一种传统的安全防护手段，具有悠久的发展历史。在云计算环境中，密码技术作为数据安全防护的一种基本的手段和方法，被许多专家和学者广泛讨论，且已经取得了一定的研究成果[3-5]。文献[3]针对云计算环境中数据存储安全问题，提出了一种基于 HDFS 的数据安全防护方案，在传输和存储环节，采用 AES 和 RSA 加密的方法提高云数据的安全性；文献[4]提出了一种面向云计算环境的并行 AES 加密算法，利用云计算 MapReduce 框架，采用并行数据处理模式，提高了加密算法的执行效率；最近，文献[5]在文献[4]的基础上，对密码算法进行改进和优化，混合三维连续混沌系统和二维离散混沌系统，提出了一种基于云计算 MapReduce 并行架构的混沌密码方案，进一步减少了密码方案的运行时间。然而，现有的基于云计算的密码方案仍然存在一些不足之处：一是随着量子计算机等新兴技术的发展，密钥空间的安全性问题将面临更加严峻的考验[6]；二是现有的混沌密码算法中均采用低维混沌系统，容易被黑客采用系统重构等方法攻击和破解，安全性还有待提高[7]。为了进一步提高云计算环境中的数据安全性，融合现有的研究方法的优良特性，进而改善和提高密码方案的安全性、可靠性和可行性，本文对一种基于云计算的混合超混沌密码方案进行分析和研究。首

收稿日期:2018-10-23； **修回日期**:2017-12-21。
基金项目:广东省教育厅青年创新人才自然科学类项目(2017GkQNCX114)；东莞市社会科技发展(一般)项目(20185071561239)；广东省科技计划项目(2014A010103002)；东莞职业技术学院科研基金资助项目(政 2017014，政 201703)；东莞职业技术学院科研项目(2017C22)。
作者简介:温贺平(1984-)，男，广东梅州人，CCF 会员，博士研究生，高级工程师，主要从事混沌密码与网络大数据安全方向的研究。

先，选取三个超混沌系统的初始值作为密钥参数，利用超混沌系统更加复杂的动力学行为产生随机特性良好的混沌序列；然后，对三个超混沌系统进行预处理后，进而设计一个混合超混沌分组加密方案；最后，基于云计算分布式编程模型 MapReduce，设计并实现了混合超混沌分组密码方案，并对其安全性和运行效率进行分析。

1 Hadoop 云计算平台

Hadoop 是 Apache 基金会一个开源的分布式计算平台，包括两个核心组件：HDFS 和 MapReduce。HDFS 为海量数据提供存储，MapReduce 则为海量数据提供计算[8]。Hadoop 在存储和处理大量数据时效率很高，并且与其他平台相比更经济。

1.1 云存储 HDFS

HDFS 是 Hadoop 中的分布式文件系统（Hadoop Distributed File System）的缩写，具有着高容错性的特点，通常部署在低廉的硬件上。它提供高传输率来访问应用程序的数据，适合那些有着超大数据集的应用程序。HDFS 采用主从架构，由两个基本基本组件构成：名称节点 NameNode 和数据节点 DataNode。

1.2 云计算框架 MapReduce

MapReduce 是一种专门面向云计算的编程模型和实现框架，具有简单、高效、易伸缩以及高容错性等特点。它是与 HDFS 相应的数据处理部分，提供最基本的数据批处理机制。与 HDFS 类似，MapReduce 也是采用主从架构，包括两个主要部分：主节点 JobTracker 和从节点 TaskTracker。MapReduce 将作业分解成顺序执行的 Map 阶段和 Reduce 阶段，Map/Reduce 任务的实例部署到 Map/Reduce 节点并行执行。

2 超混沌系统及其密码方案设计

2.1 超混沌系统

自从 1963 年气象学家洛伦兹发现第一个混沌系统以来，混沌理论方面的研究得到了深入而广泛的推进。超混沌系统及其在混沌密码中的应用是近年来混沌领域研究的热门方向之一。超混沌系统是指具有两个或两个以上的正 Lyapunov 指数，具有比一般的混沌系统更为复杂的动力学行为[9-11]。在此引进入三个经典的四维超混沌系统：Lorenz、Chen 和 Lü 超混沌系统。为方便叙述，分别将 Lorenz 超混沌系统[9]、Chen 超混沌系统[10]和 Lü 超混沌系统[11]简记为超混沌系统Ⅰ、Ⅱ和Ⅲ，其数学模型分别为：

$$\begin{cases}\dot{x}_1 = a_1(y_1 - x_1) + w_1,\\ \dot{y}_1 = -c_1x_1 - x_1z_1 - y_1,\\ \dot{z}_1 = -b_1z_1 + x_1y_1,\\ \dot{w}_1 = -y_1z_1 + d_1w_1\end{cases}$$

$$\begin{cases}\dot{x}_2 = -a_2(y_2 - x_2) + w_2,\\ \dot{y}_2 = d_2x_2 - x_2z_2 + c_2y_2,\\ \dot{z}_2 = x_2y_2 - b_2z_2,\\ \dot{w}_2 = y_2z_2 + e_2w_2.\end{cases}$$

$$\begin{cases}\dot{x}_3 = a_3(y_3 - x_3) + w_3,\\ \dot{y}_3 = -x_3z_3 + c_3y_3,\\ \dot{z}_3 = x_3y_3 - b_3z_3,\\ \dot{w}_3 = x_3z_3 + d_3w_3.\end{cases}$$

其中：$x_i, y_i, z_i, w_i, i = 1,2,3$ 是三个超混沌系统的状态变量，a_i, b_i, c_i, d_i, e_i 是系统的控制参数。当系统Ⅰ、Ⅱ和Ⅲ为参数要求分别满足：

$$\begin{cases}(a_1, b_1, c_1, d_1) = (10, 8/3, 28, -1),\\ (a_2, b_2, c_2, d_2, e_2) = (35, 3, 4, 12, 7, 0.58),\\ (a_3, b_3, c_3, d_3) = (36, 3, 20, 1).\end{cases}$$

则系统Ⅰ、Ⅱ和Ⅲ处于超混沌态。三个超混沌系统的的吸引子相图及时域波形图如图 1 所示。可以看出，三个超系统具有复杂的动力学行为，并且所产生的混沌伪随机序列具有长期不可预测性、周期点稠密、对初始和参数高度敏感等混沌特性，与密码学中的混淆和扩散等特性具有许多相似之处，非常适合应用于数据加密中。

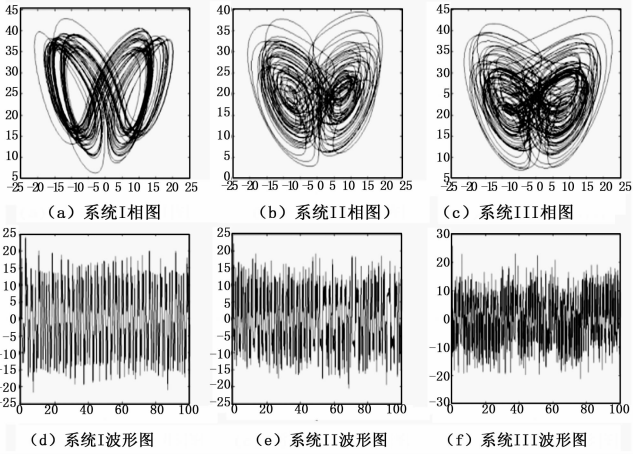

图 1 三个超混沌系统的吸引子相图及时域波形图

2.2 混合超混沌分组密码方案设计

对称混沌密码包括流密码和分组密码两种，为了融合多个超混沌系统所产生的混沌序列的随机特性，提高算法的安全性，本文所设计的密码方案采用分组密码。值得指出的是，超混沌系统产生的各个状态变量之间存在一定的关联性，这种关联性导致产生的混沌序列之间可能存在一定的互相关性，在密码攻击中存在容易被辨识或预估的风险。为了解决这个问题，对三个超混沌系统的状态变量混合异或的方法进行混淆，从而进一步提高混沌序列的随机特性。混合超混沌分组加密方案的具体步骤如下：

1）对连续混沌系统产生混沌序列预处理。首先，采用四阶 Runge－Kutta 法对连续时间超混沌系统进行离散化处理，丢弃前面 $l = 200$ 个迭代序列的值，得到 12 个混沌序列：$x_i(n), y_i(n), z_i(n), w_i(n), i = 1,2,3$；接着，对混沌序列进行小数点移位、取模等运算，处理为适合于按照字节加密的混沌序列，处理方法为：

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

其中：$p_x^{(i)}(k), p_y^{(i)}(k), p_z^{(i)}(k), p_w^{(i)}(k), i = 1,2,3$ 为经过预处理的混沌序列，$\lfloor \rfloor$ 为向下取整运算，mod 为模取余数运算。

2）混淆三个超混沌系统产生的随机序列。将经过预处理的三个超混沌系统产生的混沌序列按照状态变量进行对应的异或操作，从而使得各混沌序列之间的互关联性降低。

3）超混沌序列数据加密操作。将这 4 个混沌序列按照每 4 个字节为一组进行分组数据加密。超混沌分组加密方案如图 2 所示。

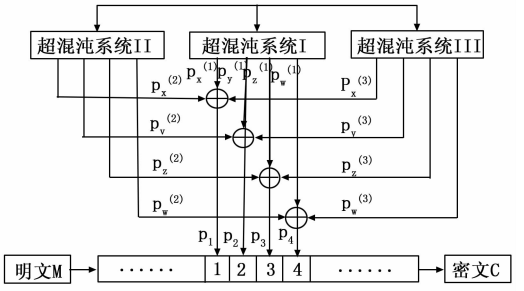

图 2　混合超混沌分组加密方案

其中，“⊕”表示按位异或运算，经过混合超混沌分组加密后的明文 M 将变成密文 C。

3　基于云计算的混沌加密算法设计

基于云计算的混沌加密算法是基于云存储 HDFS 和云计算模型 MapReduce 共同实现的。其中 MapReduce 函数的设计是混沌加密算法实现的关键步骤。首先，从 HDFS 读取数据，并对数据进行分片处理；接着，设计 MapReduce 函数，Map 函数实现分片数据块的混合超混沌分组加密操作，Reduce 函数完成加密后的数据块的合并；最后，将加密后的数据存储到 HDFS 上。加密算法的具体步骤如下：

1）从 HDFS 读取数据。

读取存储在 HDFS 上数据，并进行分片处理，为 MapReduce 并行处理做准备。值得注意的是，在 HDFS 的分片操作是由 Hadoop 根据系统参数设置自动完成的逻辑数据分块，并不需要设计额外的算法及编程代码进行实现。在 Hadoop2.0 中，数据块的大小默认设置为 128MB。

2）MapReduce 函数程序设计。

Map 函数的输入以键值对 $<key, value>$ 的形式表示。为方便叙述，输入以 $<k_{in}^{Map}, v_{in}^{Map}>$ 表示，输出则以 $<k_{out}^{Map}, v_{out}^{Map}>$ 表示，分别代表明文分片数据块和混沌加密后的密文数据块。$K_{CHAOS}^{(e)}$ 是超混沌分组密码方案的加密密钥，代表 3 个超混沌系统的密钥参数的集合，用于产生混沌序列密码 $p^{(e)}(k)$。Map 函数输入的分片明文数据按照图 2 分组加密的方法并行执行加密操作，输出各个密文数据块并就近存储到本地的磁盘上。各个 Map 子任务并行执行数据块的加密操作，利用云计算分布式并行处理的优势，可有效提高加密数据处理的运行效率。经过并行 Map 数据块加密之后，对应的 Reduce 函数读取各个密文数据块进行合并操作。Reduce 函数的输入和输出分别以键值对 $<k_{in}^{Reduce}, v_{in}^{Reduce}>$ 和 $<k_{out}^{Reduce}, v_{out}^{Reduce}>$ 进行表示，分别代表合并前后的密文数据。

3）将加密后的数据写入到 HDFS 中，将经过 Reduce 合并后的分片密文大数据存储在 HDFS 上。这样，即完成整个加密的过程。

解密算法的设计思想和加密算法基本一致，也是基于 MapReduce 函数来实现。所不同的是，解密算法中的 Map 函数对分片的密文数据块实现分布式并行解密操作，而 Reduce 函数同样是对分片数据块进行合并。

4　实验结果与分析

4.1　云计算实验环境

云计算实验环境采用一台高性能 PC 服务器，安装虚拟机软件 VMware workstation 12，部署 1 至 8 个集群计算节点数，每个计算节点均配置为单核 CPU 和 1 G 内存，云计算软件平台采用 Hadoop2.7.3 版本。实验数据集采用两个大小分别为 1 GB 和 2 GB 的文本数据文件。根据 Hadoop2.7.3 的默认设置，Map 分块数大小根据默认设置为 dfs.block.size=128MB。

4.2　加密算法执行效率

执行效率是衡量密码算法优劣的一个重要指标，也是算法是否具有实用价值的必要条件。文中算法与 AES 算法执行效率比较情况如图 3 所示。实验结果表明，基于云计算的混沌密码算法具有较好的并行度，随着集群计算节点的增加，加密时间逐渐减少；此外，在相同的云计算环境中，文中算法具有比 AES 加密算法更快的执行速度，验证了本文所提算法的有效性。

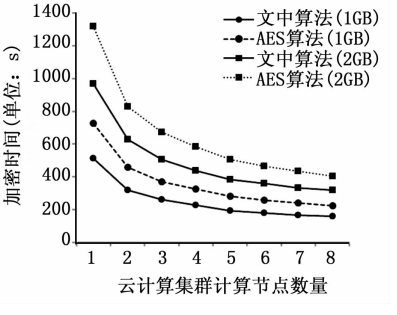

图 3　算法效率比较

4.3　密钥空间

本文算法选取三个超混沌系统的初始值作为密钥参数，

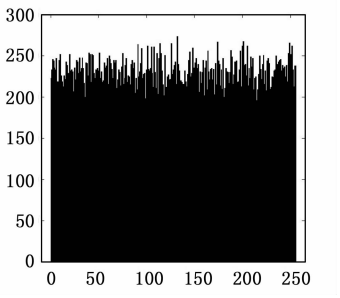

图 4 密钥失配直方图

因此算法密钥空间可以表示为：$K_{CHAOS} \in \{x_i^{(0)}, y_i^{(0)}, z_i^{(0)}, w_i^{(0)}\}, i=1,2,3$，总共 12 个密钥参数。密钥参数均选取双精度数据类型，假定精度为 10^{-14}，则算法的密钥空间大小为 $10^{14\times12}=10^{168}\approx2^{558}$，密钥长度大约为 558bit。本文算法所设计的密钥长度与相关文献的对比情况如表 1 所示。

表 1 几种加密算法密钥空间对比

加密算法	文中算法	文献[3]	文献[4]	文献[5]
密钥长度(bit)	558	256	192	344

可以看出，本文算法的密钥空间显著大于其他同类方法。如果将超混沌系统的控制参数也作为密钥参数，密钥长度还有扩容的可能。因此，本文所提的算法具有充分大的密钥空间，足以抵御暴力攻击。

4.4 密钥敏感性分析

选取其中一个超混沌系统的初始值作为密钥参数，当解密密钥参数失配 10^{-14} 时，密文的文本统计直方图如图 4 所示。从实验结果可知，仅仅是微小的密钥失配，仍然无法正确还原原始明文，且产生与明文差距巨大的密文，说明密钥对解密密文具有雪崩效应，验证了算法具有良好的密钥敏感性，可抵御差分攻击。

5 结论

针对当今云计算环境中存在的数据安全问题，综合利用云计算 MapReduce 的并行编程架构及混沌密码算法的优点，提出了一种基于 Hadoop 云计算平台的混合超混沌分组密码方案。实验结果和数据分析表明，在运行效率方面，本文所设计的密码算法具有优于同样实验环境下的 AES 算法。在安全性方面，密钥空间显著增大，足以对抗暴力攻击；密钥参数对密文具有雪崩效应，可有效抵抗差分攻击。此外，本文所提的密码方案是基于云计算环境进行开发和设计，因此，能够很好地适应于当前的网络通讯环境，对于应当和解决移动互联网、网络大数据下的数据安全及隐私保护等问题具有潜在的应用价值。

参考文献：

[1] 张玉清，王晓菲，刘雪峰，等．云计算环境安全综述［J］．软件学报，2016，27（6）：1328－1348.

[2] 林 闯，苏文博，孟 坤，等．云计算安全_架构、机制与模型评价［J］．计算机学报，2013，36（9）：1765－1784.

[3] 余 琦，凌 捷．基于 HDFS 的云存储安全技术研究［J］．计算机工程与设计，2013，34（8）：2700－2705.

[4] 付雅丹，杨 庚，胡 持，等．基于 MapReduce 的并行 AES 加密算法［J］．计算机应用，2015，35（11）：3079－3082.

[5] 王欣宇，杨 庚，闵兆娥．基于 MapReduce 的并行混合混沌加密方案［J］．计算机应用研究，2015，32（6）：1757－1760.

[6] 刘红军．混沌理论在一次一密图像加密及保密通信系统中的应用研究［D］．大连：大连理工大学，2014.

[7] 李 玲，王伟男，李津杰，等．基于 Logistic 映射和超混沌的自适应图像加密算法［J］．微电子学与计算机，2012，29（1）：42－46.

[8] 罗军舟，金嘉晖，宋爱波，等．云计算_体系架构与关键技术［J］．通信学报，2011，32（7）：3－21.

[9] Wang X，Wang M. A hyperchaos generated from Lorenz system［J］. Physica A Statistical Mechanics & Its Applications，2008，387（14）：3751－3758.

[10] Li Yuxia，Wallace K. S. Tang，Chen Guanrong. Generating Hyperchaos via Statf Feedback Control［J］. International Journal of Bifurcation & Chaos，2005，15（10）：3367－3375.

[11] Chen A，Lu J，Lü J，et al. Generating hyperchaotic Lü attractor via state feedback control［J］. Physica A Statistical Mechanics & Its Applications，2006，364：103－110.

（上接第 152 页）

[17] 刘海波，杨 杰，吴正平，等．基于暗通道先验和 Retinex 理论的快速单幅图像去雾方法［J］．自动化学报，2015，41（7）：1264－1273.

[18] 陈炳权，刘宏立．基于全变分 Retinex 及梯度域的雾天图像增强算法［J］．通信学报，2014，35（6）：139－147.

[19] Lin S C F，Wong C Y，Rahman M A，et al. Image enhancement using the averaging histogram equalization（AVHEQ）approach for contrast improvement and brightness preservation［J］. Computers & Electrical Engineering，2015，46：356－370.

[20] Rahman Z，Jobson D J，Woodell G A. Retinex processing for automatic image enhancement［J］. Journal of Electronic Imaging，2004，13（1）：100－110.

[21] 胡韦伟，汪荣贵，方 帅，等．基于双边滤波的 Retinex 图像增强算法［J］．工程图学学报，2010（2）：104－109.