动态整数帐篷映射模型及其性能分析

刘建东[1] 张 啸[2] 赵 晨[2] 商 凯[2]
(北京石油化工学院信息工程学院 北京 102617)[1] (北京化工大学信息科学与技术学院 北京 100029)[2]

摘 要 针对整数帐篷映射存在的短周期问题,通过引入动态参量,建立了动态整数帐篷映射模型,证明其具有均匀分布特性,将其与整数化logistic映射进行了比较,并分析了模型的周期性及相关性。该模型弥补了整数帐篷映射的短周期缺陷,并且便于硬件实现。实验及仿真分析表明,该模型具有十分优良的密码学性能,在信息安全领域极具应用价值。

关键词 混沌,密码,整数帐篷映射,动态
中图法分类号 TP301.5 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.11.044

Dynamic Integer Tent Map and its Characteristics Analysis

LIU Jian-dong[1] ZHANG Xiao[2] ZHAO Chen[2] SHANG Kai[2]
(Department of Information Engineering, Beijing Institute of Petrochemical Technology, Beijing 102617, China)[1]
(School of Information Science and Technology, Beijing University of Chemical Technology, Beijing 100029, China)[2]

Abstract Dynamic integer tent map model was established through introduction of dynamic parameters based on integer tent map, which has the problem of short cycle. Its uniform distribution feature was demonstrated and compared with the integer logistic map. Periodicity and interdependency of dynamic integer tent map were analysed. This model eliminates the short-period defects of integer tent map and is easy to be realized in hardware. Experiment and simulation analysis show that this model is featured with excellent cryptography property and possesses high value in cryptographic application.

Keywords Chaos, Ciphers, Integer tent map, Dynamic

1 引言

混沌映射具有不可预测性和伪随机特性,这是确定论混沌系统最具吸引力的特性。近年来,为获得更安全、快速的加密算法,利用混沌映射对变量和参数的变化的敏感特性构造密码算法的研究已取得较大进展[1-5]。基于混沌映射构造的密码算法具有算法简单、实现速度快的优点。目前提出的基于混沌的密码算法与传统的密码算法的一个重要区别就是基于混沌的密码算法界定在实数域上,而传统的密码算法采用的是有限整数的按位操作,在实数域上构造的混沌密码在实际应用中受到很大限制[6]。

将混沌映射在整数集内实现是开展混沌密码学研究的另一条可行途径[6-8]。文献[7]提出基于混沌理论的无线传感器网络加密算法,采用改进的离散logistic运算,即将实数运算转化为整数运算,整数logistic映射与实数域的logistic映射一样,具有不均匀分布特性。帐篷映射也是一种典型的混沌映射,在迭代过程中不断进行拉伸和折叠,其中每次拉伸都会增强系统状态对初始值的敏感性,其折叠特性则可以使拉伸后的状态值回归系统的混沌区间,同时增加了反向推导映射的难度。帐篷映射生成的序列是混沌的,并且具有优良的均匀分布特性,非常适合作为密钥序列的生成算法。在前期研究中,将帐篷映射的实数域运算变为整数集内的运算,进而构造了通过移位、异或及整数加法运算即可实现的密码算法[6,8]。

由于计算机截断误差的存在,在有限精度实现的情况下,数字化混沌系统的动力学特性相对连续系统而言存在严重的退化,这是混沌映射用于密码算法设计的一个致命缺陷。将实数运算转化为整数运算后,这一缺陷更显突出。在整数集中,由于状态空间有限,必然出现短周期行为,为了解决整数帐篷映射的短周期问题,本文在整数帐篷映射中引入动态参量,建立动态整数帐篷映射,使其既具有帐篷映射固有的伸长和折叠的非线性本质及映射不可逆性与均匀分布特性,又打破了整数帐篷映射存在的短周期行为。

2 动态整数帐篷映射模型

2.1 帐篷映射

帐篷映射是极其简单的混沌动力学模型,通过参数 a 对构成帐篷的两条直线进行控制。帐篷映射的表达式如式(1)所示:

$$x_{i+1}=\begin{cases}\dfrac{x_i}{\alpha}, & 0\leqslant x_i\leqslant\alpha\\ \dfrac{1-x_i}{1-\alpha}, & \alpha\leqslant x_i\leqslant 1\end{cases} \tag{1}$$

到稿日期:2015-10-11 返修日期:2016-04-06

刘建东(1966-),男,硕士,教授,主要研究方向为无线传感网络安全、混沌密码、信息隐藏等,E-mail:liujiandong@bipt.edu.cn;张 啸(1990-),男,硕士,主要研究方向为RFID系统安全、混沌密码等;赵 晨(1988-),男,硕士,主要研究方向为无线传感网络安全技术;商 凯(1990-),男,硕士,主要研究方向为无线传感网络安全技术。

a 的大小决定了映射中心点的位置。当 $a=0.5$ 时，其被称为标准帐篷映射。标准帐篷映射的表达式如式(2)所示：

$$x_{i+1}=\begin{cases}2x_i, & 0\leqslant x_i\leqslant 0.5\\ 2(1-x_i), & 0.5\leqslant x_i\leqslant 1\end{cases} \tag{2}$$

帐篷映射的优异特性之一是其具有均匀的分布函数。帐篷映射由于具有高遍历性、类随机、初始值敏感性等特点，能够满足密码算法对扩散特性的要求。

2.2 整数帐篷映射

将标准帐篷映射(式(2))由实数域运算等价转化为整数运算(设整数的二进制位数为 n)：

$$F_a: x_{i+1}=\begin{cases}2x_i+1, & x_i\in[0,2^{n-1})\\ 2(2^n-1-x_i), & x_i\in[2^{n-1},2^n-1)\end{cases} \tag{3}$$

式(3)即为整数帐篷映射，映射 F_a 仍可由折线表示，并服从$[0,2^n-1]$上的均匀分布。整数帐篷映射保持了实数域帐篷映射的伸长和折叠特性，其伸长特性导致相邻点指数分离，其折叠特性保持生成序列有界，且引起映射不可逆。

下文的分析均取 $n=8$，即在整数集$\{0,1,2,\cdots,2^8-1\}$内进行。

由于映射 F_a 定义在有限域内，由此生成的迭代序列必然进入周期态(如图 1(a)，$x_1=1$，周期为 8)，甚至出现一些周期长度很小的周期点(如图 1(b)，$x_1=227$，周期为 3)。

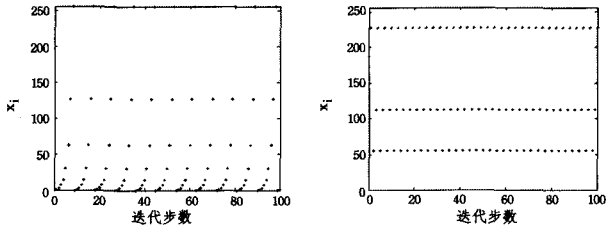

图 1 整数帐篷映射时间序列

2.3 动态整数帐篷映射及其均匀分布特性

为了避免整数帐篷映射出现短周期，将帐篷映射与取模运算相结合，对整数帐篷映射进行动态扩展，得到新的映射模型——动态整数帐篷映射模型。

$$F_\beta: x_{i+1}=\begin{cases}2g_i+1, & g_i\in[0,2^{n-1})\\ 2(2^n-1-g_i), & g_i\in[2^{n-1},2^n-1]\end{cases} \tag{4}$$

其中，

$$g_i=(x_i+k_i)\bmod 2^n \tag{5}$$

F_β 映射中(见图 2)，由动态参量 k_i 控制“帐篷”水平移动(k_i 表示“帐篷”沿横轴移动的距离)。

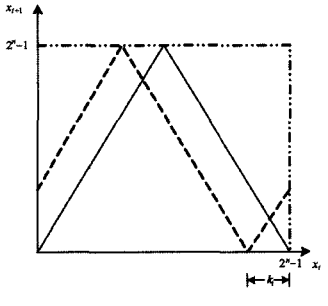

图 2 动态整数帐篷映射

迭代运算中，随着迭代步数 i 的变化，k_i 取不同的值。每次迭代运算，图 2 中的“帐篷”都是移动变化的，因而称其为动态整数帐篷映射。动态整数帐篷映射的定义域仍为$[0,2^n-1]$。

定义 1 若离散型随机变量 X 的所有可能取值为 $0,1,\cdots,2^n-1$，且它的分布为：

$$p_k=P(X=k)=\frac{1}{2^n}$$

其中，$k\in\{0,1,\cdots,2^n-1\}$，则称随机变量 X 服从整数集$\{0,1,\cdots,2^n-1\}$上的均匀分布。

定义 2 若离散型随机变量 X 的所有可能取值为 $0,1,\cdots,2^n-1$，且它的分布为：

$$p_k=P(X<k)=\frac{k}{2^n}$$

其中，$k\in\{0,1,\cdots,2^n\}$，则称随机变量 X 服从整数集$\{0,1,\cdots,2^n-1\}$上的均匀分布。

通常情况下，定义 2 中随机变量的分布表示方法是针对连续型随机变量的。下面证明过程中为了表达方便，在离散型随机变量的分布中也采用这种表示方法。

引理 1 若离散型随机变量 X 服从整数集$\{0,1,\cdots,2^n-1\}$上的均匀分布，则对于任意满足 $0\leqslant a<b\leqslant 2^n$ 的非负整数 a，b，有

$$\begin{aligned}P(a\leqslant x<b)&=P(x<b)-P(x<a)\\&=\frac{b}{2^n}-\frac{a}{2^n}=\frac{b-a}{2^n}\end{aligned}$$

引理 2 映射 F_a(式(3))服从整数集$[0,2^n-1]$上的均匀分布。

定理 映射 F_β(式(4)、式(5))服从整数集$[0,2^n-1]$上的均匀分布。

证明：令 $k=p*2^n+q$，其中 p,q 为非负整数，且 $q\in[0,2^n-1]$，则

$$\begin{aligned}y&=(x+k)\bmod 2^n\\&=(x+q+p*2^n)\bmod 2^n\\&=(x+q)\bmod 2^n\end{aligned}$$

现取 $\varepsilon\in[0,2^n-1]$，由引理 1、引理 2 有：

(1)当 $\varepsilon\leqslant q$ 时，

$$\begin{aligned}P(y<\varepsilon)&=P((x+q)\bmod 2^n<\varepsilon, x+q>\varepsilon)\\&=P(2^n\leqslant x+q<2^n+\varepsilon)\\&=P(2^n-q\leqslant x<2^n+\varepsilon-q)\\&=P(x<2^n+\varepsilon-q)-P(x<2^n-q)\\&=\frac{\varepsilon}{2^n}\end{aligned}$$

(2)当 $\varepsilon>q$ 时，

$$\begin{aligned}P(y<\varepsilon)&=P((x+q)\bmod 2^n<\varepsilon)\\&=P((x+q)\bmod 2^n<\varepsilon, x+q\leqslant\varepsilon)+P((x+q)\\&\quad\bmod 2^n<\varepsilon, x+q>\varepsilon)\\&=P(x+q<\varepsilon, x+q\leqslant\varepsilon)+P(2^n\leqslant x+q<2^n+q)\\&=\frac{\varepsilon-q}{2^n}+\frac{q}{2^n}\\&=\frac{\varepsilon}{2^n}\end{aligned}$$

所以，映射 F_β(式(4)、式(5))服从整数集$[0,2^n-1]$上的均匀分布。

证毕。

3 动态整数帐篷映射性能分析

3.1 动态整数帐篷映射生成的时间序列

图 3 给出了动态整数帐篷映射的时间序列分布，迭代初

值 $x_1=1$，每次迭代的动态参量 k_i 取 $4*i \bmod 2^{32}$（i 为当前迭代步数，对 2^{32} 取余数是为了防止当迭代步数过多时由于 k_i 过大而导致数据溢出）。对比图 1(a)可以发现，加入了动态参量的整数帐篷映射的性能有了极大改善，不再存在短周期现象。

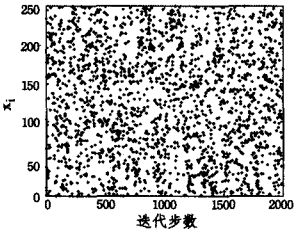

图 3　动态帐篷映射生成的时间序列

3.2　动态整数帐篷映射时间序列频数分布

密码学中，理想的伪随机序列的状态值应服从均匀分布，即每个状态值出现的概率相等。用统计频数的方法估计序列的分布情况，具体做法是：

(1)选取 m 个不同的初值，对每个初值均迭代 n 步，得到 m 组迭代序列；

(2)对于每组迭代序列，分别统计其状态值等于其值域内各离散点的值的频数；

(3)将同一离散点对应的 m 个频数累加，再除以 m，以其平均值作为最终此离散点的频数。

图 4 为动态整数帐篷映射的序列频数分布，图 5 为文献[7]给出的整数 Logistic 映射的序列频数分布。通过对比可以看出，动态整数帐篷映射的序列在值域内服从均匀分布，而整数 Logistic 映射的序列呈现出两边取值概率大、中间取值概率小的不均匀分布特性。

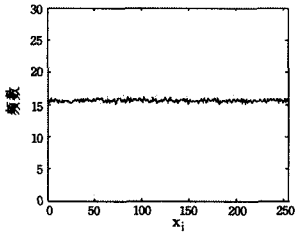

图 4　动态整数帐篷映射的时间序列频数分布

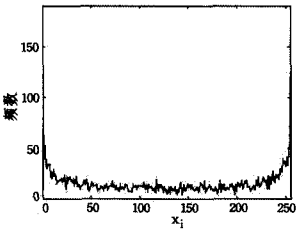

图 5　整数 Logistic 映射的时间序列频数分布

3.3　动态整数帐篷映射周期性分析

由于帐篷映射通过离散化被定义在有限域内，削弱了实数域帐篷映射模型的各态历经性，帐篷映射生成序列的状态值必然存在周期现象，甚至出现短周期及不动点。针对动态整数帐篷映射的周期性测试是评判改进模型优劣的重要因素。

对于整数帐篷映射(式(3))，一个迭代周期的完整表述为：初始值 x_0 经过迭代后，迭代值 x_i 回归初始值完成的最短迭代轮数，即 $x_0=x_i$（$i>0$ 且取最小值）。

取式(3)中的状态变量 x 为字长为 8bit 的整型变量，对取值范围[0,255]内的所有初始值进行 255 轮 F_a 映射迭代，统计各初值在 F_a 映射迭代中的最小周期的最大值、最小值、平均值，统计结果如表 1 所列。

表 1　8bit 整数帐篷映射周期统计

最大值	最小值	平均值
9	1	8.898438

对于整数帐篷映射(式(3))，在计算字长为 8bit 的情况下，绝大部分初值产生的迭代结果周期为 9，当初始值为 56，113，227 时出现周期为 3 的短周期，并且当初始值为 170 时出现了不动点现象。

对于动态整数帐篷映射(式(4))，由于引入动态参量 k，迭代周期的判定不再只遵循状态变量 x，还与动态参量 k 有关。在 k 值固定的情况下，一个迭代周期的完整表述为：经过 m 轮迭代后，$x_m=x_0$，同时 k_1 到 k_m 的累加和能够被 2^n 整除。

取式(4)中的状态变量 x 为字长为 8bit 的整型变量，取动态参量 $k=1$，对取值范围[0,255]内的所有初始值进行 255 轮 F_β 映射迭代，统计各初值在 F_β 映射迭代中的最小周期的最大值、最小值、平均值，统计结果如表 2 所列。

表 2　8bit 动态整数帐篷映射周期统计

最大值	最小值	平均值
>100000	256	>10000

可以看出，动态整数帐篷映射消除了整数帐篷映射存在的不动点，映射周期得到大幅度增大。

3.4　动态整数帐篷映射相关性分析

归一化后整数序列的自相关函数定义为：

$$c_{ii}(\tau)=\hat{C}_{ii}(\tau)/\hat{C}_{ii}(0) \tag{6}$$

其中，

$$\hat{C}_{ii}(\tau)=\frac{1}{N}\sum_{n=1}^{N}(x_i^{(n)}-\bar{x}_i)(x_i^{(n+|\tau|)}-\bar{x}_i)$$

归一化后整数序列的互相关函数定义为：

$$C_{ij}(\tau)=\hat{C}_{ij}(\tau)/\sqrt{\hat{C}_{ii}(0)\hat{C}_{jj}(0)} \tag{7}$$

其中，

$$\hat{C}_{ij}(\tau)\frac{1}{N}\sum_{n=1}^{N}(x_i^{(n)}-\bar{x}_i)(x_j^{(n+|\tau|)}-\bar{x}_j)$$

序列自相关或互相关旁瓣的均方根表示混沌序列码间干扰的大小，越小表明系统抗干扰性能越好，如式(8)和式(9)所示：

$$\sigma_{C_{ii}}=\sqrt{\frac{1}{N}\sum_{n=1}^{N}[C_{ii}(\tau)]^2} \tag{8}$$

$$\sigma_{C_{ij}}=\sqrt{\frac{1}{2N+1}\sum_{\tau=-N}^{N}[C_{ii}(\tau)]^2} \tag{9}$$

取动态参量 $k=1$，字长 $n=32$，比较整数帐篷映射序列和动态整数帐篷映射序列自相关和互相关旁瓣的均方根值，结果如表 3 所列。

表 3　整数帐篷映射序列和动态整数帐篷映射序列相关性比较

N	自相关旁瓣均方根		互相关旁瓣均方根	
	整数帐篷映射	动态整数帐篷映射	整数帐篷映射	动态整数帐篷映射
2048	0.2887	0.0546	0.0172	0.0451
8192	0.2494	0.0213	0.0086	0.0183
32768	0.2944	0.0105	0.0042	0.0083

在相关间隔范围 N 为有限长度的条件下，动态整数帐篷映射的自相关特性比整数帐篷映射具有显著优势；随着序列长度逐渐增加，二者的互相关特性趋同。

结束语　混沌映射由于特有的拉伸与折叠效应，势必具有极好的扩散与混淆特性，同时还具有算法代码量小、运算速度快、存储容量小的特点。本文将混沌帐篷映射在整数集内实现，并引入动态机制，构建了动态整数帐篷映射模型，克服了整数帐篷映射所存在的短周期缺陷，涉及的运算极易由软

硬件实现，适用于硬件资源有限且对安全性有一定要求的系统。将其作为密码系统的一个非线性部件，用于设计加密及认证算法，可满足低功耗无线传感器网络对密码算法的基本要求。

无线传感器网络节点配备的能源少，单节点计算能力低，存储资源有限，无线通信距离短，节点数目多，成本低，体积小。在这样的条件下，安全密码算法的可实现性就成为一个关键问题，传统密码算法很难满足其要求。提高无线传感器网络的安全性，必然要求提高传感器节点的计算能力，扩大存储容量，以实现安全性高的复杂密码算法，这必将提高无线传感器网络节点的成本；反之，要求无线传感器网络节点廉价，必然采用低成本的处理器和小容量的存储器，这又会降低运算能力，从而影响安全性高的复杂算法的实现；再者，由于无线传感器网络与应用密切相关，因此无线传感器网络的安全问题应该与实际运算处理能力结合，实现安全与成本的均衡考虑。动态整数帐篷映射用于保障无线传感器网络安全领域，有望解决无线传感器网络面临的信息安全问题。

参 考 文 献

[1] Akhshani A, Mobaraki A, et al. Pseudo random number generator based on quantum chaotic map[J]. Communication in Nonlinear Science and Numerical Simulation, 2014, 19(1): 101-111

[2] Cicek I, Pusane A E, Dundar G. A novel design method for discrete time chaos based true random number generators[J]. Integration , the VLSI journal, 2014, 47(1): 38-47

[3] Cheng Yan-yun, Song Yu-rong. Hash function Construction Based on Chaotic System of Coupled Map Lattice[J]. Journal of Applied Sciences, 2010, 28(1): 44-48(in Chinese)
程艳云，宋玉蓉. 基于耦合映象格子混沌系统的 Hash 函数构造[J]. 应用科学学报，2010，28(1)：44-48

[4] Radwan A G, Abd-El-Hafiz S K. Image encryption using generalized tent map[C]// 2013 IEEE 20th International Conference on Electronics, Circuits, and Systems(ICECS). IEEE, 2013: 653-656

[5] Ghebleh M, Kanso A, Noura H. An image encryption scheme based on irregularly decimated chaotic maps[J]. Signal Processing: Image Communication, 2014, 29(5): 29: 618-627

[6] Liu Jian-dong. One-way Hash Function based on Integer Coupled Tent Maps and Its Performance Analysis[J]. Journal of Computer Research and Development, 2008(3): 563-569(in Chinese)
刘建东. 基于整数耦合帐篷映射的单向 Hash 函数及其性能分析[J]. 计算机研究与发展，2008(3)：563-569

[7] Chen Shuai. Research on Chaos Encryption Theory and Key Technology for Wireless Micro-Sensor Network[D]. Chongqing: Chongqing University, 2006(in Chinese)
陈帅. 无线微传感器网络混沌加密理论及其关键技术研究[D]. 重庆：重庆大学，2006

[8] Liu Jian-dong. Extended integer tent maps and dynamic hash function[J]. Journal on Communications, 2010(4): 51-59(in Chinese)
刘建东. 扩展整数帐篷映射与动态散列函数[J]. 通信学报，2010(4)：51-59

(上接第 199 页)

[2] Feiler P H. Model-based validation of safety-critical embedded systems[C]// Proceedings of the Aerospace Conference. 2010 IEEE, 2010: 1-10

[3] Shokry H, Hinchey M. Model-Based Verification of Embedded Software[J]. Computer, 2009, 42(4): 53-59

[4] Battueux M, Prosvirnova T, Rauzy A, et al. The AltaRica 3. 0 project for model-based safety assessment[C]// 2013 11th IEEE International Conference on Proceedings of the Industrial Informatics(INDIN). 2013: 127-132

[5] Humbert S, Seguin C, Castel C, et al. Deriving Safety Software Requirements from an AltaRica System Model[M]// Computer Safety, Reliability, and Security. Springer Berlin Heidelberg, 2008: 320-331

[6] Li S, Su D. A Practicable MBSA Modeling Process Using Altarica[M]// Model-Based Safety and Assessment. Springer International Publishing, 2014: 1-13

[7] Patcas L M, Lawford M, Maibaum T. From System Requirements to Software Requirements in the Four-Variable Model[J/OL]. http://core. al. uk/display/23645454

[8] Patcas L M, Lawford M, Maibaum T. Implementability of requirements in the four-variable model[J]. Science of Computer Programming, 2015, 111(P2): 339-362

[9] Miller S P, Tribble A C. Extending the four-variable model to bridge the system-software gap [J]. Digital Avionics Systems dascconference, 2001: 4E5/1-4E5/11

[10] Farkas H, Noszticzius Z. Analytical investigation of a four-variable model of the BZ reaction[J]. Reaction Kinetics & Catalysis Letters, 1987, 33(1): 93-98

[11] Heitmeyer C L, Jeffords R D, Labaw B G. Automated Consistency Checking of Requirements Specifications[J]. Automated Consistency Checking of Requirements Specifications, 1996, 5(3): 231-261

[12] Point G, Rauzy A. AltaRica: Constraint automata as a description language [J/OL]. http://altarica. labri. fr/pub/publications/PR996. pdf

[13] Bieber P, Bougnol C, Castel C, et al. Safety Assessment with Altarica[J]. Journal of the American College of Cardiology, 2004, 53(11): 982-991

[14] Joshi A, Miller S P, Whalen M, et al. A proposal for model-based safety analysis[C]// Proceedings of the Digital Avionics Systems Conference, 2005(DASC 2005). 2005

[15] Cassez F, Pagetti C, Roux O. A Timed Extension for ALTARICA[J]. Fundamenta Informaticae, 2004, 62(3/4): 291-332

[16] Bozzano M, Cimatti A, Lisagor O, et al. Symbolic Model Checking and Safety Assessment of Altarica models[J/OL]. http://journal. ub. tu-berlin. de/eceasst/article/view/697

[17] Bieber P, Castel C, Seguin C. Combination of Fault Tree Analysis and Model Checking for Safety Assessment of Complex System[M]// Dependable Computing EDCC-4. Springer Berlin Heidelberg, 2002: 19-31

[18] Lee W S, Grosh D L, Tillman F A, et al. Fault Tree Analysis, Methods, and Applications ? A Review[J]. IEEE Transactions on Reliability, 1985, 34(3): 194-203

[19] Boulanger J L. Safety Analysis of the Embedded Systems with the AltaRica Approach[M]. Industrial Use of Formal Methods: Formal Verification. John Wiley & Sons, Inc. , 2013: 83-121