计算机网络安全综合评价的神经网络模型

楼文高[1,2],姜 丽[2],孟祥辉[2]
LOU Wen-gao[1,2],JIANG Li[2],MENG Xiang-hui[2]

1.上海理工大学 出版印刷学院,上海 200093
2.上海理工大学 管理学院,上海 200093
1.College of Publishing & Printing,University of Shanghai for Science and Technology,Shanghai 200093,China
2.Business School,University of Shanghai for Science and Technology,Shanghai 200093,China
E-mail:wglou@usst.edu.cn

LOU Wen-gao,JIANG Li,MENG Xiang-hui.Comprehensive evaluation model for computer network security applying artificial neural network.Computer Engineering and Applications,2007,43(32):128-131.

Abstract: Traditional methods such as grey evaluation model and fuzzy theory,determining the subordinate function and weights for each index,are influenced by personal factors.Artificial Neural Network (ANN) is then applied to network security comprehensive evaluation.The training set data,verification set data and testing set data,in agreement with the singular-evaluation index criterion,is randomly generated.The ANN-based model with reliability,effectiveness and comparative for network security is established obeying to the basic principles and steps for establishing ANN-model.The case study shows that the methodology for generating set data and the process for establishing ANN-model are effective and reliable.The phenomenon such as over-training and over-fitting can be effectively escaped and the established model possesses good generalization.The relationship between the network security and the evaluation index is nonlinear and the most important index is network security strategy.
Key words: network security;comprehensive evaluation;Artificial Neural Network(ANN);set data;model

摘 要:灰色评价法、模糊综合评价等需确定隶属函数、各指标权重,明显受人为因素的影响。尝试应用神经网络技术进行网络安全的综合评价,并通过在单指标评价标准范围内随机取值方法,生成建立神经网络模型所需的训练样本、检验样本和测试样本,在遵循BP网络建模基本原则和步骤的情况下,建立了可靠、有效的网络安全综合评价模型。16个实例研究表明:提出的样本生成方法、建模过程是可靠的,并能有效地避免出现"过训练"和"过拟合"现象,建立的BP模型具有较好的泛化能力,不受人为因素的影响,各评价指标与网络安全等级之间存在明显的非线性关系,网络安全策略对网络安全的影响最大。
关键词:网络安全;综合评价;神经网络;样本数据;模型
文章编号:1002-8331(2007)32-0128-03 **文献标识码**:A **中图分类号**:TP183;TP393.08

1 引言

随着计算机网络(以下简称网络)的广泛应用,网络安全问题已成为网络技术发展迫在眉睫、亟待解决的重要前沿研究课题。因此,对网络安全状况进行科学的评价,有助于用户对网络安全进行全面的了解,从而采取相应的防范措施,提高网络的安全性能及其总体效益。

我国网络安全评价理论和方法的研究尚处于初级、分散的状态,没有形成科学体系,目前尚无全面的综合评价指标体系和成型的数学模型。李剑英[1]、申键[2]和许永福等[3-5]首先根据评价系统的完备性、独立性、简要性、准确性和可操作性建立了评价指标体系和单指标评价标准,并应用层次分析法(AHP)、灰色评价法(GE)和模糊理论(FT)神经网络法(ANN)进行网络安全评价的探索性研究,而这些方法明显存在受人为确定隶属函数、各评价指标权重的影响,客观性、可比性和可靠性较差。

另一方面,网络安全综合评价实际上是非线性逼近与模式识别问题。ANN技术具有自学习、自组织能力,尤其适用于非线性、工作机理未知问题的建模[6-8]。但文献[1,2,4,5]在应用ANN技术建模时,训练样本只有12个,文献[1]有12个输入变量,文献[2,4,5]有17个输入变量,隐层取5个节点,训练样本数比网络连接权数少得多,甚至少于输入变量数,又没有检验样本。文献[6-8]认为:训练样本数少于网络连接权数,又没有检验样本,无法判断训练过程是否发生了"过训练"现象,这样建立的ANN模型不可能有好的泛化能力,实用价值很小。为此,在很难获得大量实际网络样本安全性的情况下,如何根据单指标评价标准,生成符合评价标准的足够多的训练样本、检验样本和测试样本,避免训练时发生"过训练"现象,求得全局极小点邻域内的可行解, 建立泛化能力好的ANN模型是网络安全综合评价的核心与关键。

基金项目:上海市重点学科项目资助(No.P0501)。
作者简介:楼文高(1964-),男,教授,博士,研究方向:人工神经网络理论及其应用、综合评价、计算机网络等;姜丽(1979-),女,硕士,研究方向:综合评价理论及其应用;孟祥辉(1982-),男,硕士,研究方向:信息管理。

2　网络安全综合评价指标体系及其评价标准

根据系统应具有完备性、独立性、简要性、准确性和可操作性等，文献[1]建立了由数据加密状况(X_1)、网络安全投入(X_2)、访问控制状况(X_3)、信道加密状况(X_4)、网络隔离状况(X_5)、安全审计(X_6)、系统漏洞检测(X_7)、安全管理策略(X_8)、实时监测(X_9)、路由控制技术(X_{10})、网络安全教育(X_{11})和数字签名技术(X_{12})12个评价指标组成的指标体系和单指标评价标准，将网络安全划分为优(Ⅳ)、良(Ⅲ)、中(Ⅱ)和差(Ⅰ)4个等级，如表1所示。

表1　网络安全评价指标及其4个等级的分级标准

	差	中	良	优
X_1≥	0.00	0.70	0.80	0.90~1.00
X_2≥	0.00	0.70	0.80	0.90~1.00
X_3≥	0.00	0.60	0.75	0.90~1.00
X_4≥	0.00	0.60	0.75	0.90~1.00
X_5≥	0.00	0.70	0.80	0.90~1.00
X_6≥	0.00	0.55	0.70	0.85~1.00
X_7≥	0.00	0.65	0.75	0.85~1.00
X_8≥	0.00	0.70	0.80	0.90~1.00
X_9≥	0.00	0.65	0.80	0.90~1.00
X_{10}≥	0.00	0.60	0.75	0.85~1.00
X_{11}≥	0.00	0.60	0.70	0.90~1.00
X_{12}≥	0.00	0.55	0.75	0.90~1.00

3　BP神经网络建模的基本原则与步骤

ANN技术是20世纪80年代后迅速发展和广泛成功应用于众多学科非线性模拟的技术[7-9]，最常用的BP模型的基本运行机制由信息正向传播和误差反向传播两个过程组成。BP模型具有好的自适应和非线性拟合能力，但也存在易出现“过训练”、“过拟合”、收敛于局部极小点等诸多不足。文献[9]提出了实现BP神经网络从理论到实践的跨越的基本原则和步骤，以确保建立合理的模型和具有较好的泛化能力，其要点为：

(1)将收集到的数据随机分成训练样本和各10%以上的检验样本和测试样本[7]。

(2)一般取一个隐层和尽可能少的隐层节点，在满足精度的前提下，取尽可能紧凑的结构以避免出现“过拟合”现象[8]。合理隐层节点数应综合考虑网络结构复杂程度和误差大小。

(3)对于三层网络，训练样本数必须多于输入层和隐层节点数[6]；一般情况下，训练样本数至少要多于网络连接权值数，通常为2倍~10倍[8]。

(4)用检验样本监控训练过程，在出现“过训练”现象前结束训练或取出现“过训练”现象前的网络连接权值，以消除“过训练”现象的影响。

(5)训练BP模型就是通过不断调整网络权值使网络模型输出值与已知的训练样本输出值之间的误差平方和达到最小或小于某一期望值而建立蕴含训练样本规律的网络模型。必须用检验样本和测试样本(非训练样本)误差的大小评价模型的泛化能力。如果非训练样本误差和训练样本误差一样小或稍大，说明建立的模型已有效逼近样本所蕴含的规律，具有较好的泛化能力，否则，即使训练样本的误差很小，模型仍没有泛化能力，而只是在这些训练样本点上逼近而已。

(6)针对某一网络结构，应通过很多次改变网络初始连接权值，以求得没有发生“过训练”现象的误差较小的全局极小点邻域内的可行解。

(7)随着网络结构的增大，模型的误差一般都随之变小。在增加隐层节点的过程中，训练样本和检验样本的误差表现为：较大的稳定值→迅速减小→较小的稳定值三个阶段，合理隐层节点数应取检验样本迅速减小后趋于基本稳定时的隐层节点数。

合理的BP模型是具有合理隐层及其节点数、训练时没有发生“过训练”现象、求得全局极小点和同时考虑网络结构复杂程度和误差大小的综合结果。

4　实例研究分析

4.1　生成足够多的样本

由表1可知：不同等级的网络安全由各评价指标值的上(下)限值所确定。因此，当X_1≥0.70~0.80、X_2≥0.70~0.80、X_3≥0.60~0.75、X_4≥0.60~0.75、X_5≥0.70~0.80、X_6≥0.55~0.70、X_7≥0.65~0.75、X_8≥0.70~0.80、X_9≥0.65~0.80、X_{10}≥0.60~0.75、X_{11}≥0.60~0.70和X_{12}≥0.55~0.75时，网络安全肯定为中级(Ⅱ)。同理可生成任意多其他网络安全等级的样本。12个评价指标均为正向指标。为了定量、精确地评价和预测网络安全，BP模型输出用连续函数表示，即对应于网络安全等级优、良、中和差，模型理论输出值分别为4、3、2和1。

本文共生成2 676个样本，各随机抽取300个样本(11%左右)的检验样本和测试样本。

4.2　建立网络安全综合评价的BP模型

采用Statsoft公司出品的STATISTICA Neural Networks软件[7]，用拟牛顿法训练模型，结束训练的条件是不发生“过训练”现象，训练样本、检验样本误差基本趋于稳定或训练样本均方根误差(RMSE)小于0.05或迭代达到500次。隐层和输出层均采用Sigmoid转换函数，将输入输出变量的值通过线性变换转化为[0.2，0.8]内的值。取隐层节点数为1、2、3和4时，训练样本的RMSE(检验样本和测试样本基本相似)分别为0.077、0.069、0.068和0.068，取隐层节点数为5~20时，训练样本RMSE均在0.068左右。因此，综合考虑模型的误差大小与结构复杂程度，合理网络结构可取12-4-1。经过500次迭代，不发生“过训练”现象，求得极小点邻域内某一组可行解，其训练样本、检验样本和测试样本的RMSE分别为0.068、0.067和0.071，平均绝对误差(AAE)分别为0.051 3、0.050 1和0.055 3，相关系数分别为0.998 2、998 0、0.997 9。这些指标表明，经上述训练建立的网络模型对训练样本与对检验样本和测试样本具有相似的拟合(或表征)能力，即该网络模型的泛化能力很强，能较好地用于评价未知样本。

4.3　分界样本及其BP模型理论输出值的确定

将表1所示的各项评价指标的分界值输入训练好的BP模型，模型输出值分别为：1.647、2.469和3.547。因此，对应于网络安全Ⅰ~Ⅳ的模型输出值范围分别为：<1.647、≥1.647~2.469、≥2.469~3.547和≥3.547。

4.4　模拟和实际网络的安全等级判定

为了进一步说明本文生成足够多样本和建模方法的可靠性，首先对表2所示网络安全等级明确的6个模拟样本S1~S6进行分析研究：(1)S_1和S_2处于网络安全Ⅰ级与Ⅱ级的分界值两侧，S_1属于Ⅰ级，S_2为Ⅱ级；(2)S_2和S_3同为Ⅱ级，但S_2为Ⅱ级的较差状态，S_3为Ⅱ级的较好状态，接近于Ⅱ级与Ⅲ级的分界情况；(3)S_3和S_4、S_5和S_6的性质同S_1和S_2；(4)S_4和S_5的性

表2 16个网络的各评价指标值、BP模型输出值及其评定结果

序号	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	模型值	评定等级
1	1.00	1.00	1.00	0.98	1.00	0.90	0.96	1.00	1.00	1.00	0.98	1.00	4.256	优
2	0.84	0.82	0.81	0.85	0.86	0.74	0.80	0.84	0.86	0.81	0.82	0.84	2.989	良
3	0.76	0.72	0.72	0.69	0.79	0.56	0.68	0.76	0.74	0.75	0.70	0.71	2.114	中
4	0.61	0.59	0.51	0.53	0.70	0.39	0.64	0.68	0.65	0.60	0.46	0.52	1.425	差
5	0.96	0.94	0.90	0.89	0.90	0.09	0.92	0.94	0.92	0.94	0.92	0.91	3.834	优
6	0.82	0.80	0.80	0.79	0.84	0.80	0.81	0.82	0.81	0.79	0.82	0.86	2.866	良
7	0.74	0.76	0.71	0.72	0.76	0.70	0.72	0.74	0.71	0.69	0.65	0.69	2.096	中
8	0.59	0.50	0.51	0.54	0.70	0.41	0.58	0.60	0.64	0.50	0.44	0.48	1.310	差
9	0.93	0.91	0.96	1.00	0.91	0.89	0.94	0.92	0.93	0.92	1.00	0.94	3.925	优
10	0.87	0.85	0.85	0.87	0.83	0.71	0.80	0.82	0.83	0.82	0.86	0.85	3.033	良
11	0.79	0.77	0.74	0.75	0.72	0.63	0.71	0.76	0.71	0.72	0.70	0.71	2.175	中
12	0.67	0.66	0.52	0.59	0.68	0.44	0.62	0.58	0.59	0.58	0.50	0.44	1.410	差
13	0.92	0.92	0.90	0.91	0.92	1.00	0.91	0.89	0.87	0.85	0.89	0.93	3.701	优
14	0.84	0.81	0.81	0.80	0.81	0.76	0.82	0.81	0.80	0.77	0.80	0.81	2.792	良
15	0.76	0.72	0.71	0.73	0.71	0.58	0.71	0.74	0.74	0.74	0.70	0.74	2.093	中
16	0.67	0.65	0.52	0.56	0.68	0.43	0.60	0.64	0.61	0.56	0.51	0.48	1.426	差

表3 网络安全模糊综合评价的归一化向量及其评价结果

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
差	0.00	0.00	0.15	0.52	0.00	0.00	0.20	0.55	0.00	0.00	0.17	0.52	0.00	0.00	0.23	0.52
中	0.00	0.28	0.43	0.48	0.00	0.34	0.50	0.45	0.00	0.25	0.50	0.48	0.03	0.35	0.50	0.48
良	0.13	0.47	0.42	0.00	0.43	0.50	0.30	0.00	0.37	0.50	0.33	0.00	0.47	0.55	0.27	0.00
优	0.87	0.25	0.00	0.00	0.57	0.30	0.00	0.00	0.63	0.25	0.00	0.00	0.50	0.15	0.00	0.00
结果	优	良	中	差	优	良	中	差	优	良	中	差	优	良	中	差

质同 S_2 和 S_3。针对 S_1~S_6,BP 模型的输出值分别为:1.600、1.695、2.387、2.554、3.460 和 3.633。由 S_1~S_6 的模型输出值和分界样本的输出值可以判定:S_1 为Ⅰ级(差),S_2 和 S_3 同为Ⅱ级(中),而且 S_1 和 S_2 处于Ⅰ级与Ⅱ级的分界值两侧,他们虽然属于不同等级,但差别很小,而 S_2 和 S_3 虽然都属于Ⅱ级,但几乎相差一个等级,即 S_2 处于Ⅱ级的最差情况,S_3 处于Ⅱ级的最好情况。同理,S_3 和 S_4 分别位于Ⅱ级和Ⅲ级的分界值两侧,S_4 和 S_5 分别是Ⅲ级(良)的最差和最好情况,S_5 和 S_6 分别位于Ⅲ级和Ⅳ级的分界值两侧,而且 S_6 属于Ⅳ级(优)的最差情况。BP 模型的计算结果与上述情况完全一致。但是,如果采用 AHP、GE、FT 方法分析,虽然 S_1~S_6 的安全等级与实际情况一致,但不能说明 S_1 和 S_2、S_3 和 S_4、S_5 和 S_6 相差很小,更不能得到 S_2 和 S_3、S_4 和 S_5 几乎相差一个等级的结论,也就是说,这些方法有时表现为“过灵敏”(如对 S_1 和 S_2、S_3 和 S_4、S_5 和 S_6 而言),有时又会表现为“欠灵敏”(如对 S_2 和 S_3、S_4 和 S_5 而言)。

将文献[1]的 12 个训练样本和 4 个测试样本的数据输入到上述建立好的 BP 网络模型,其模型输出值如表 2 所示。对照网络安全Ⅰ~Ⅳ级的模型输出值范围可知:序号 1、5、9、13 的网络安全都为优,而且序号 1 最好,序号 9 次之,随后是序号 13 和 5;同理,序号 2、6、10、14 的网络安全为良,序号 3、7、11、15 的网络安全为中,序号 4、8、12、16 的网络安全为差。BP 模型能精细地评定同一等级内的网络的不同安全程度。

文献[1]用前 12 个为训练样本建模,采用 12–5–4 结构,一方面,显然不符合 BP 模型建模训练样本数要多于网络连接权值数的最基本要求,而且没有检验样本,无法判断训练过程中是否发生了“过训练”现象,如果发生了“过训练”现象,模型的泛化能力得不到保障,模型就没有任何实用价值。另一方面,本文采用 4 个输出节点,不能定量分析同一等级内网络安全的不同程度,也存在同一等级内“欠灵敏”,不同等级之间“过灵敏”的问题。

文献[1]用模糊综合评价方法对上述 16 个网络进行了安全性评价,采用线性隶属函数,综合权重为(0.041,0.141,0.137,0.037,0.139,0.030,0.074,0.098,0.069,0.111,0.098,0.021),综合评价结果如表 3 所示。由表 3 知,在上述隶属函数和权重情况下,网络安全等级评价结果与本文的结果相同,但不能定量分析同一等级内网络(如网络 1、5、9、13)的不同安全程度。再者,如果把归一化向量理解为概率的话,序号 4、12 和 16 属于“差”的概率为 52%,属于“中”的概率为 48%,把它认定为“差”比较勉强。又如序号 13,属于“优”的概率为 50%,属于“良”的概率为 47%,评定为“优”也很勉强。序号 3 属于“差”的概率 15%,属于“中”的概率 43%,属于“良”的概率 42%,最后评定为“中”的说服力不强。事实上,满足随机一致性指标的权重有很多组,如果改变权重,上述结果肯定会发生改变。

4.5 网络安全评价指标的重要性分析

根据每个评价指标对网络安全等级的贡献大小,由软件的变量灵敏度分析功能得:12 项评价指标中,安全管理策略(X_8)的影响最大,其次是路由控制技术(X_{10})、数据加密状况(X_1)、网络安全投入(X_2)、网络隔离状况(X_5)、系统漏洞检测(X_7)、实时监测(X_9)、访问控制状况(X_3)、信道加密状况(X_4)、网络安全教育(X_{11})、数字签名技术(X_{12})和安全审计(X_6)。因此,要提高网络安全程度,首先应从改善网络的安全管理策略着手。对网络安全等级与各评价指标的解析分析表明各评价指标与网络安全等级之间存在明显的非线性关系,如图 1 所示是网络安全策略(X_8)与模型输出值之间的非线性关系(其他指标取中—良等级的分界值)。

5 结束语

网络安全的模糊综合评价方法、灰色评价等传统方法需人为确定指标权重或隶属函数等,隶属函数或权重如果不同,结

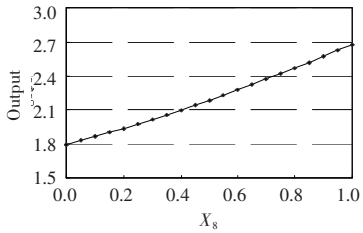

图1　网络安全策略(X_8)与模型输出值之间的非线性关系
（其他指标取中—良等级的分界值）

果就不同，而且，一般只能进行定性分析，评价结果不可避免的在不同等级之间表现为“过灵敏”，在同一等级内表现为“欠灵敏”。

采用BP模型方法，克服了诸如需人为确定权重、隶属函数或只能定性分析等的缺陷，各评价指标的重要度通过训练符合单指标评价标准的样本而得到，具有较好的客观性、可比性和公正性。本文根据单指标评价标准，通过采取在区间内随机生成样本的方法组成足够多的神经网络的训练样本、检验样本和测试样本；遵循训练样本数必须多于网络连接权值数以及必须用检验样本实时监控训练过程以避免发生“过训练”现象等建模基本原则和步骤，采用拟牛顿法训练网络，克服了BP网络建模需要大量训练样本、收敛速度慢、容易出现“过训练”和“过拟合”现象等的缺陷，建立了泛化能力很好的网络安全综合评价神经网络模型。

应用本文建立的网络安全综合评价BP模型对16个网络进行综合评价表明：网络1、5、9、13的安全等级都为优，而且网络1的安全最好，网络9次之，随后是网络13和5；网络2、6、10、14的安全等级为良，网络3、7、11、15的安全等级为中，网络4、8、12、16的安全等级为差。应用神经网络方法可以精细地评定同一等级内的网络的不同安全程度，因此，BP模型能够精细地对进行改造后的网络的安全程度进行再次评价，并据此提出提高网络安全的有效措施。

在网络安全的12项评价指标中，影响最大的是安全管理策略，其次是路由控制技术和数据加密状况等，因此，在进行网络规划时，从网络安全考虑，首先应制定比较好的管理策略和进行较好的数据加密。而且各评价指标与网络安全等级之间存在明显的非线性关系。（收稿日期：2007年4月）

参考文献：

[1] 李剑英.基于人工神经网络与模糊综合评价的计算机网络安评价和安全防范措施的研究[D].兰州大学，2003.
[2] 申健.网络安全综合评价方法的研究及应用[D].兰州大学，2005.
[3] 许福永，申健，李剑英.网络安全综合评价方法的研究及应用[J].计算机工程与设计，2006，27(8)：1398-1400.
[4] 许福永，申健，李剑英.基于AHP和ANN的网络安全综合评价方法研究[J].计算机工程与应用，2005，41(29)：127-129.
[5] 许福永，申健，李剑英.基于Delphi和ANN的网络安全综合评价方法研究[J].微机发展，2005，15(10)：11-14.
[6] 董聪.多层前向网络的逼近与泛化机制[J].控制与决策，1998，13：413-417.
[7] Statsoft.Statistica neural networks[M].Tulsa：Statsoft Inc，1999.
[8] Hagan M T，Demuth H B，Beale M.Neural network design[M].北京：机械工业出版社，中信出版社，2002.
[9] 楼文高.实现BP神经网络从理论到实践的跨越[J].哈尔滨工程大学学报，2006，27：59-63.

（上接127页）

后将每一组密钥的128 bit依次取反得到128段密钥，其中每段包括128 bit与原密钥相差仅一位的新密钥。这样，就可以得到300组密钥，每组包括128段，每段包括128 bit密钥。将这些密钥对明文进行加密，并计算相应密文之间的汉明距离。然后统计每一组中明文-密文对之间的汉明距离为γ的段数HW_γ，根据式(24)和式(25)算出HW_γ的期望值E_r和统计量χ^2。将此值与临界值χ^2_C(自由度为128，显著性水平为0.05)进行比较，检验分组是否满足二项分布$B(n,1/2)$，检验结果表明，300分组中有293组通过明文的敏感性测试，算法具有较好的密钥敏感性测试。

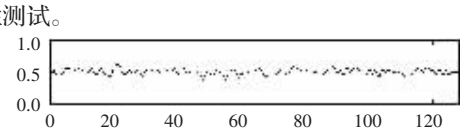

图3　密钥雪崩效应测试结果

6　结论

基于四维混沌猫映射，本文设计了一种新的分组密码，并对其进行了分析。将128 bit二进制数据重新排列成的十进制矩阵，并结合子密钥加密对其随机选取的行和列执行四维混沌猫映射变换，经过8轮运算，算法获得了较好的安全性。统计测试也证实这种新的分组密码具有优良的性能。
（收稿日期：2007年5月）

参考文献：

[1] Jakimoski G，Locarev L.Chaos and cryptography：block Encryption ciphers based on chaotic maps[J].IEEE Transactions on Circuits and System I，2001，48(2)：163-169.
[2] Lu H P，Wang S H，Hu G.Pseudo-random number generator based on coupled map lattices[J].Int J Modern Phys B，2004(18)：17-19.
[3] Liao X F，Li X M，Chen J P G R.A digital secure image communication scheme based on the chaotic Chebyshev map[J].International Journal of Communication Systems，2004(17)：437-455.
[4] Long M，Peng F，Qiu S S，et al.Implementation of a new chaotic encryption system and synchronization[J].Journal of System Engineering and Electronics，2006，17(1)：43-47.
[5] Chen G R，Mao Y B，Chui C K.A symmetric image encryption scheme based on 3D chaotic cat maps[J].Chaos，Solitons and Fractals，2004(21)：749-761.
[6] Lian S G，Shun J S，Wang Z Q.A block cipher based on suitable use of the chaotic standard map[J].Chaos，Solitons and Fractals，2005(26)：117-129.
[7] Locarev L，Jakimoski G.Logistic map as a block encryption algorithm[J].Physics Letters A，2001(289)：199-206.
[8] Yi X，Tan C H，Siew C K.A new block cipher based on chaotic tent maps[J].IEEE Transactions on Circuits and System，2002，49(12)：1826-1829.
[9] Fridrich J.Symmetric ciphers based on two-dimensional chaotic maps[J].Int J Bif Chaos 1998，8(6)：1259-1284.
[10] 冯登国.密码分析学[M].北京：清华大学出版社，2000.
[11] 冯登国，吴文玲.分组密码的设计与分析[M].北京：清华大学出版社，2000.