DOI:10.11721/cqnuj20240507

累加正弦化混沌系统模型的性能分析*

李忠洪[1], 王 蕊[1], 王 洁[1], 李国楠[1], 罗海军[1,2]
(1.重庆师范大学 物理与电子工程学院; 2.重庆师范大学 国家应用数学中心, 重庆 401331)

摘要:为进一步提高现有的混沌系统的复杂度,提出了累加正弦化混沌系统的增强型模型(additive sinusoidal chaotic system model,ASCSM)。该模型通过将 3 个一维正弦化的传统混沌映射(Logistic、Sine 和 Fraction 映射)两两结合来增强混沌系统的复杂程度。首先,通过理论分析证明了 ASCSM 的性能,并根据复杂度指标(Lyaponuv 指数、谱熵和 C_0 复杂度)仿真分析了增强后的混沌映射的动态特性,结果表明增强后的混沌映射较种子混沌映射性能更好。其次,基于数字信号处理器平台,利用 ASCSM 产生随机序列验证了该模型在硬件系统上实现的可行性。最后,为了与传统混沌映射在图像加密中的应用能力相比较,将这些模型作为加密算法的异或序列生成器,通过各种加密评估指标证明了新模型在加密应用中具有更高的保密性。

关键词:混沌模型;Lyaponuv 指数;谱熵;硬件实现;混沌加密
中图分类号:TN911.7 **文献标志码**:A **文章编号**:1672-6693(2024)05-0095-11

随着信息技术的飞速发展以及信息安全威胁的增加,保密通信[1]已经成为各国研究的热点。混沌理论研究的是确定但不可预测的动力学系统,后来发展为非线性科学的一个分支[2]。混沌系统的初值敏感性、长期不可预测性、遍历性等特征让它在通信领域被广泛研究和应用[3]。目前,混沌安全通信[4]、多媒体保密通信[5]、混沌密码学[6]和混沌图像加密[7]已经成为国际电子通信研究的热点。利用混沌系统产生的序列可以作为加密算法运行的密钥[8],而且这种加密方法非常安全——除非已知系统的初始状态,否则系统的动态特性无法被预测。然而,现有的混沌系统仍待改进:首先,有些混沌系统复杂度较低,通过识别初始状态或预估混沌轨道就可以破解;其次,有些混沌只能在某些区域内表现出微弱的混沌行为;另外,由于有限域模拟的精度不够,对混沌行为进行无限域模拟分析时会出现混沌退化现象[9]。这些潜在的问题削弱了混沌系统的应用,因此需要寻找复杂度更高的增强型混沌。

为解决上述问题,研究人员探索了各种方法去改善混沌的性能。2019 年,Hua 等人[10]提出一种正弦化的混沌模型,由此不仅增强了原有混沌的复杂度,而且可以在更大的范围内获得较好的混沌性能。Liu 等人[11]提出了一个由 Lorenz 混沌映射和四阶 Rossler 超混沌映射组成的双混沌系统,生成 3 组用于扩散运算的混沌序列;该方法补偿了 2 类混沌映射的伪随机性,使得混沌序列更难预测。Ye 等人[12]提出采用粒子群算法提高控制系统的动态性能,从而提高系统的混沌复杂度。Spitz 等人[13]发现量子级联激光器能够发射出确定性混沌模式,当使用光注入代替传统的光反馈时,混沌特性则得到了改善。

受 Wu[14]提出的级联-正弦混沌化模型(cascade-sine chaotification model,CSCM)的启发,本文提出了累加正弦化混沌系统的增强型模型(additive sinusoidal chaotic system model,ASCSM),通过累加 2 个正弦化混沌映射达到进一步增强混沌性能的目的,再由理论推导验证了该模型的复杂度。同时,将该模型运用到常见的一维映射中,利用 Lyaponuv 指数(E_L)、谱熵(E_S)和 C_0 复杂度分析了增强后的混沌映射的动态特性。其次在 TI 公司的数字信号处理器(digital signal processor,DSP)平台搭建增强混沌映射的实验系统,并通过示波器观察到动态行为,从而验证了该混沌模型硬件实现的可行性。不仅如此,ASCSM 生成的混沌序列还被用作加密算法的异

* **收稿日期**:2024-03-11 **修回日期**:2024-06-11 **网络出版时间**:2024-11-11T09:35
资助项目:国家自然基金青年科学基金项目(No. 51507023);重庆市自然科学基金面上项目(No. cstc2020jcyj-msxmX0726);重庆市教育委员会科技项目重点项目(No. KJZD-K202100506);重庆市高校与中国科学院附属机构合作项目(No. HZ2021007)
第一作者简介:李忠洪,女,研究方向为混沌系统及其应用,E-mail:2022110511026@stu.cqnu.edu.cn;**通信作者**:罗海军,男,教授,博士,E-mail:luohaijun@cqnu.edu.cn
网络出版地址:https://link.cnki.net/urlid/50.1165.n.20241108.1649.002

或序列,可以进一步有效加强图像保密性,与普通的一维混沌序列相比,提出的新混沌序列在图像加密中具有更突出的信息隐藏能力。

1 混沌模型

1.1 ASCSM 定义

ASCSM 将传统的一维混沌映射和正弦变换系统级联,并通过累加来改善种子混沌映射的动态特性,模型结构如图 1 所示。

ASCSM 的数学表达式为:

$$x_{i+1}=\Lambda(x_i)=\sin(\pi f(a,x_i))+\sin(\pi g(b,x_i)),$$

其中:$f(a,x_i)$和 $g(b,x_i)$是传统的一维混沌映射,a 和 b 是对应一维混沌映射的控制变量,x_i 作为系统模型的输入,在经过正弦非线性变化后相加得到输出,并作为下一次迭代的输入,可以选取传统的一维混沌映射代替上式中的 $f(a,x_i)$和 $g(b,x_i)$。Hua[10] 已经证明正弦化混沌系统可以获得比之前更复杂的动态特征,在这里将 2 个已经正弦化的混沌映射线性相加从而获得更强的混沌复杂度。此外,该模型不仅可以累加 2 个正弦化混沌系统,也适用于累加多个正弦化混沌系统,尽管经累加正弦化之后模型仍然具有正弦的特征,但复杂性会随着嵌入的一维混沌映射的不同而改变。如图 2 所示,选择多个不同的混沌映射可以获得更加随机和复杂的动态特征。

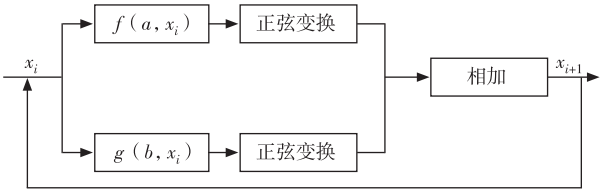


图 1 ASCSM 结构

Fig. 1 ASCSM structure

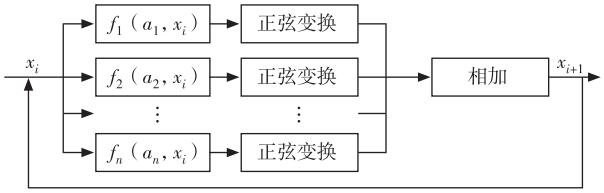


图 2 n 个混沌映射的增强型模型结构

Fig. 2 Structure of the augmented model with n chaotic mappings

1.2 传统种子混沌模型

为了增进混沌模型的复杂度,常常将传统的混沌模型作为改进型混沌模型的组成成分,英文统称为 seed map,翻译为种子图[15]。为了验证 ASCSM 的性能,将它应用到 3 个不同的一维混沌映射中去,分别是 Logistic 映射、Sine 映射和 Fraction 映射。本文首先对这些传统映射进行介绍,再分析 3 个增强后的混沌映射动态特征。

Logistic 映射来源于人口统计学,是为了模拟人口增长的模型[16]。目前运用最广泛的是非线性离散混沌模型,数学表达式为:

$$x_{i+1}=L(x_i)=4\mu x_i(1-x_i), \tag{1}$$

其中:控制参数 $\mu\in[0,1]$,当 $\mu>0.892$ 时,系统处于混沌状态,映射的分岔图见图 3a。

Sine 映射是由正弦函数推导出来的,它的映射方程为:

$$x_{i+1}=S(x_i)=\mu\sin(\pi x_i), \tag{2}$$

其中:控制参数 $\mu\in[0,1]$,映射的分岔图如图 3b 所示。

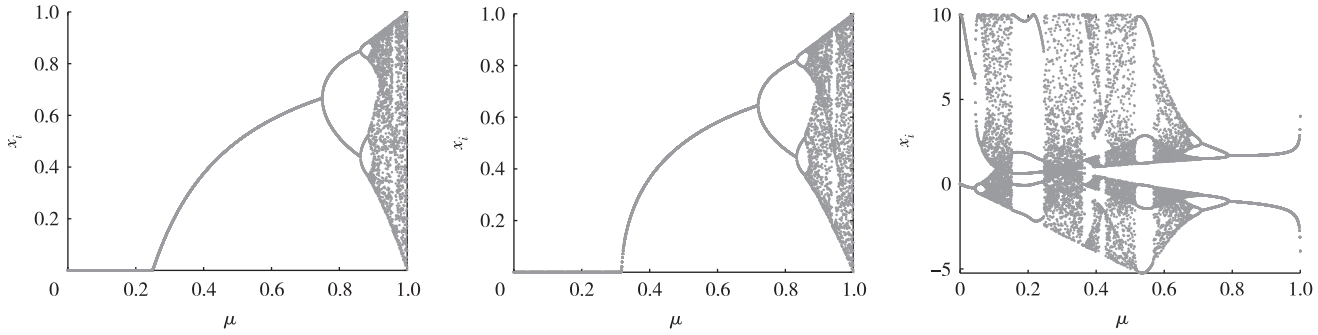
Fraction 映射[17] 是用来描述生物进化中遗传的随机性,它的混沌映射是:

$$x_{i+1}=F(x_i)=\frac{1}{x_i^2+0.1}-\mu x_i,$$

其中:控制参数 $\mu\in[0,1]$,映射的分岔图如图 3c 所示。

2 混沌复杂度理论分析

为定量表明混沌系统对初始值的敏感度时,利用 E_L 作为标准,它可以定量描述混沌系统在局部范围里系统轨道间的分离程度。如果 $E_L>0$,那么运动轨道的局部不稳定,相邻点的轨道按指数方式分离,在此作用下反复折叠,形成混沌吸引子,称系统进入混沌。反之如果 $E_L<0$,则系统的状态会趋于稳定且对系统的初始状态不敏感。



a　Logistic 映射的分岔图　　b　Sine 映射的分岔图　　c　Fraction 映射的分岔图

图 3　3 种传统种子映射分岔图

Fig. 3　Three traditional seed mapping bifurcation diagrams

函数 $\Lambda(x_i)=x_{i+1}$ 的 E_L 可计算为：

$$\lambda_{\Lambda(x)}=\lim_{n\to\infty}\left\{\frac{1}{n}\ln|\Lambda'(x_i)|\right\}。$$

定义：

$$\lambda_F=\lim_{n\to\infty}\left\{\frac{1}{n}\ln|F'(a,x_i)|\right\},$$

$$\lambda_G=\lim_{n\to\infty}\left\{\frac{1}{n}\ln|G'(b,x_i)|\right\}=\lim_{n\to\infty}\left\{\frac{1}{n}\ln|S'(g(b,x_i))g'(b,x_i)|\right\}=$$

$$\lim_{n\to\infty}\left\{\frac{1}{n}\ln|S'(g(b,x_i))|\right\}+\lim_{n\to\infty}\left\{\frac{1}{n}\ln|g'(b,x_i)|\right\}=\lambda_{S_g}+\lambda_g,\tag{3}$$

$$\lambda_{\Lambda(x_i)}=\lim_{n\to\infty}\left\{\frac{1}{n}\ln|[F(a,x_i)+G(b,x_i)]'|\right\}=\lim_{n\to\infty}\left\{\frac{1}{n}\ln|F'(a,x_i)+G'(b,x_i)|\right\}=$$

$$\lim_{n\to\infty}\left\{\frac{1}{n}\ln|F'(a,x_i)|+\frac{1}{n}\ln\left|1+\frac{G'(b,x_i)}{F'(a,x_i)}\right|\right\}=\lim_{n\to\infty}\left\{\frac{1}{n}\ln|F'(a,x_i)|\right\}+\lim_{n\to\infty}\left\{\frac{1}{n}\ln\left|1+\frac{G'(b,x_i)}{F'(a,x_i)}\right|\right\}>$$

$$\lim_{n\to\infty}\left\{\frac{1}{n}\ln|F'(a,x_i)|\right\}+\lim_{n\to\infty}\left\{\frac{1}{n}\ln\left|\frac{G'(b,x_i)}{F'(a,x_i)}\right|\right\}>\lambda_F+\lambda_G-\lambda_F=\lambda_G,\tag{4}$$

其中：λ_F 表示 $F(a,x_i)$ 的 E_L，λ_G 表示 $G(b,x_i)$ 的 E_L，$F(a,x_i)$ 表示正弦化的 $f(a,x_i)$，$G(b,x_i)$ 表示正弦化的 $g(b,x_i)$，即 $F(a,x_i)=S(f(a,x_i))$，$G(b,x_i)=S(g(b,x_i))$，并用 $S(x)$ 来表示正弦混沌映射控制参数 a，$b=1$ 时的混沌映射，同时 $F'(a,x_i)$ 和 $G'(b,x_i)$ 满足正负相同，且 $F'(a,x_i)\neq 0$，λ_{S_g} 表示正弦化 $g(b,x_i)$ 某一点的 E_L，λ_g 表示 $g(b,x_i)$ 的 E_L。

由式(3)、(4)得 $\lambda_{\Lambda(x)}>\lambda_{S_g}+\lambda_g$。

从图 3b 可知当 a，$b=1$ 时，正弦混沌映射处于混沌状态，即 $\lambda_{S_g}>0$。以下讨论 $g(b,x_i)$ 在不同情况下的结果：

1) 假设 $g(b,x_i)$ 是混沌映射，则 $\lambda_g>0$，即 $\lambda_{\Lambda(x_i)}>0$，表明通过 ASCSM 之后的现有混沌模型具有更好的混沌性能；

2) 假设 $g(b,x_i)$ 不是混沌映射。如果 $\lambda_g+\lambda_{S_g}>0$，尽管 $g(b,x_i)$ 不是混沌的，依旧可以通过 ASCSM 获得一个正的 E_L 值，这表明非混沌映射通过该模型转换后存在混沌的可能性。

3) 假设 $g(b,x_i)$ 不是混沌映射且 $\lambda_g+\lambda_{S_g}<0$，该系统将不再混沌。

综上所述，现有的混沌系统通过 ASCSM 会获得更大的 E_L，而最初的非混沌序列在通过模型之后可能仍然会变成混沌，这意味着它们在更广的参数范围内具有更好的混沌性能。

3　增强型混沌映射

为了证明 ASCSM 的高效性，将 Logistic、Sine 和 Fraction 这 3 种传统映射两两结合，利用 ASCSM 生成 3 种

新的混沌映射,分别是增强的 Logistic-Sine 映射(LS 映射)、增强的 Sine-Fraction 映射(SF 映射)和增强的 Logistic-Fraction 映射(LF 映射),为了简化分析讨论,将控制参数都设为 α。

3.1 增强的 LS 映射

LS 映射是将式(1)的 Logistic 映射代入到 $f(a,x_i)$,式(2)中的 Sine 映射代入到 $g(b,x_i)$,同时把控制参数都设为 α,则 LS 的表达式为:

$$x_{i+1}=\sin(\pi L(\alpha,x_i))+\sin(\pi S(\alpha,x_i)),$$

其中:$\alpha\in[0,+\infty]$。

2 个种子映射(Logistic、Sine)的分岔图如图 3a、b 所示,图中显示 Logistic 映射在(0.89,1)中处于混沌状态,Sine 映射在(0.85,1)中处于混沌状态。如图 4a 所示,当控制参数 $\alpha\in[0,10\ 000]$时,LS 映射的分岔图输出随机分布在$[-2,2]$,这些输出分布几乎遍布在整个数据范围内。换句话说,LS 映射在更大范围内获得了更优的复杂动态特性。

3.2 增强的 SF 映射

利用 ASCSM 系统结构,改变 $f(a,x_i)$为 Sine 映射,改变 $g(b,x_i)$为 Fraction 映射,构成新的混沌映射 SF 映射,表达式为:

$$x_{i+1}=\sin(\pi S(\alpha,x_i))+\sin(\pi F(\alpha,x_i)),$$

其中:$\alpha\in[0,+\infty]$。

如图 3c 所示,Fraction 映射在$[0,1]$中的某些时间段处于混沌状态。而增强后的 SF 映射在控制参数 $\alpha\in[0,10\ 000]$时,分岔图如图 4b,输出数据在$[-2,2]$范围内随机遍布,该图像表明 SF 映射在更广泛参数范围处于混沌状态,复杂性更好。

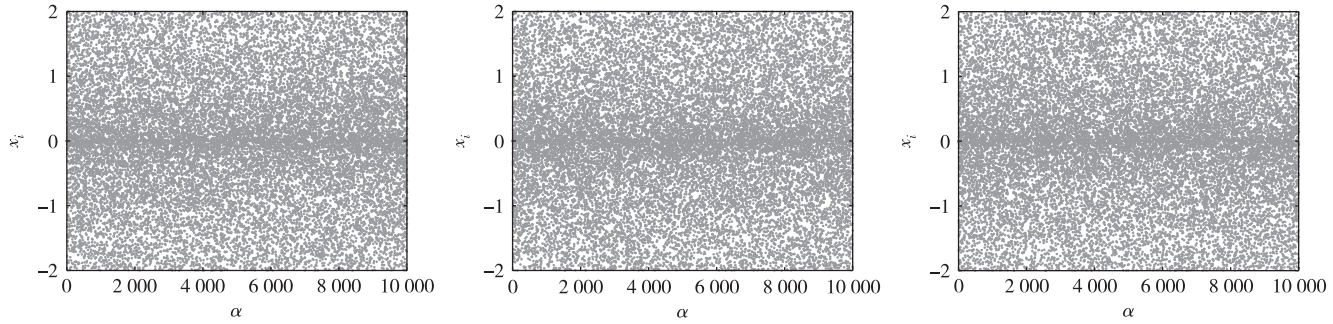
3.3 增强的 FL 映射

另外一种增强映射利用 Fraction 映射替代 $f(a,x_i)$,Logistic 映射替代 $g(b,x_i)$,得到新的 LF 混沌映射,表达式为:

$$x_{i+1}=\sin(\pi F(\alpha,x_i))+\sin(\pi L(\alpha,x_i)),$$

其中:$\alpha\in[0,+\infty]$。

图 4c 是当控制参数 $\alpha\in[0,10\ 000]$时 LF 映射的分岔图,输出随机分布在$[-2,2]$范围内,相较于 Logistic、Fraction 分岔图,LF 映射动态特征更好,复杂度更高。



a LS 映射的分岔图　　b SF 映射的分岔图　　c LF 映射的分岔图

图 4 3 种 ASCSM 映射分岔图

Fig. 4 Three ASCSM mapping bifurcation diagrams

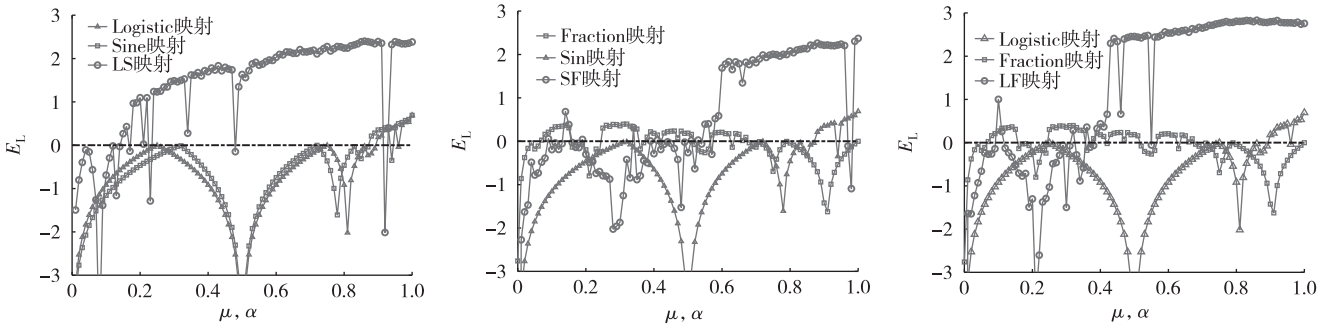
4 性能评估

ASCSM 可以很好地改善现有混沌系统的复杂度。为了证明 ASCSM 的性能,使用 E_{L}、E_{S} 和 C_0 复杂度分析对比增强的 LS、SF、LF 映射和传统 Logistic、Sine、Fraction 映射的复杂程度。

4.1 E_{L}

E_{L} 表示相空间相邻轨迹的平均指数发散率的数值特征[18]。对于非线性系统,如果 E_{L} 为负,则动力系统是

稳定的，并在相空间中收缩。而正 E_L 则表示系统的相体积在一个方向上连续扩展和折叠，即系统是混沌的。为了可视化地比较传统种子映射和新生成的 ASCSM 映射，本文将新生成的混沌映射的 α 参数范围设置为(0，1)，传统混沌映射 μ 参数的范围也设置为(0，1)。其中图 5a 展示了增强 LS 映射和 2 种种子(Logistic、Sine)映射的 E_L，LS 映射的 E_L 在 $\alpha=0.2$ 左右就开始进入混沌；图 5b 展示了增强 SF 映射和 2 种种子(Sine、Fraction)映射的 E_L，根据增强 SF 映射的图像，可以看出在 $\alpha=0.6$ 左右就开始进入混沌；图 5c 展示了增强 LF 映射和 2 种种子(Logistic、Fraction)映射的 E_L，增强 LF 映射的 E_L 在 $\alpha=0.4$ 左右就开始进入混沌。结果表明增强映射的混沌范围比种子映射的范围更宽，并且增强映射的 E_L 幅度比种子映射的 E_L 强很多，即增强的 ASCSM 混沌系统获得了更复杂的动态特性。



a　LS、Logistic 和 Sine 映射的 E_L　　b　SF、Fraction 和 Sine 映射的 E_L　　c　LF、Fraction 和 Logistic 映射的 E_L

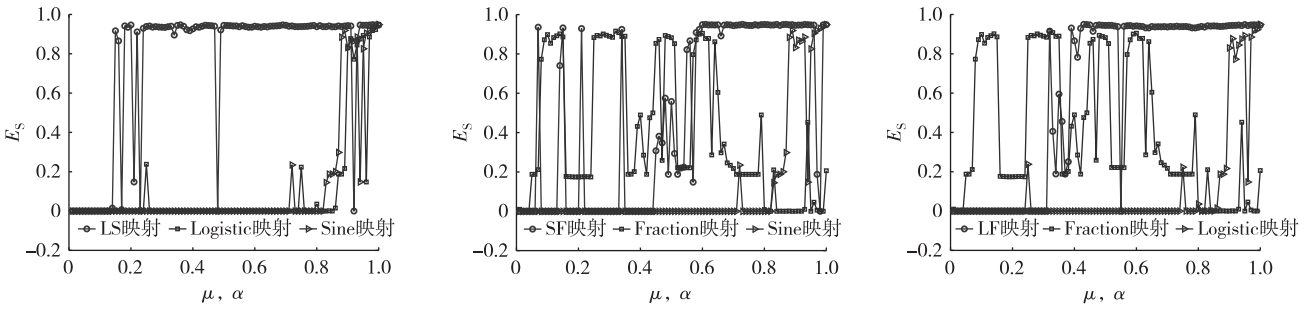
图 5　ASCSM 和传统一维映射的 E_L 对比

Fig. 5　Comparison of E_L for ASCSM and conventional 1D mappings

4.2　E_S

E_S 是通过变换域中的频率不变特性和能谱特性来分析序列的复杂性[19]。当使用 E_S 评估动力系统的复杂性时，E_S 值越大，则系统的输出时间序列可以达到较低的正则度，并进一步表明动力系统具有较高的复杂性。

图 6 绘制了 ASCSM 生成 LS、SF 和 LF 混沌映射及它们 Logistic、Sine 和 Fraction 种子映射的 E_S，其中图 6a 展示了增强 LS 映射和 2 种种子(Logistic、Sine)映射的 E_S；图 6b 展示了增强 SF 映射和 2 种种子(Sine、Fraction)映射的 E_S；图 6c 展示了增强 LF 映射和 2 种种子(Logistic、Fraction)映射的 E_S。比较 E_S 的结果得到，利用 ASCSM 结构生成的增强映射的 E_S 比原来种子映射大很多，范围也比种子映射宽，即 ASCSM 增强的混沌映射可以生成正则度远低于传统种子映射正则度的时间序列。



a　LS、Logistic 和 Sine 映射的 E_S　　b　SF、Fraction 和 Sine 映射的 E_S　　c　LF、Fraction 和 Logistic 映射的 E_S

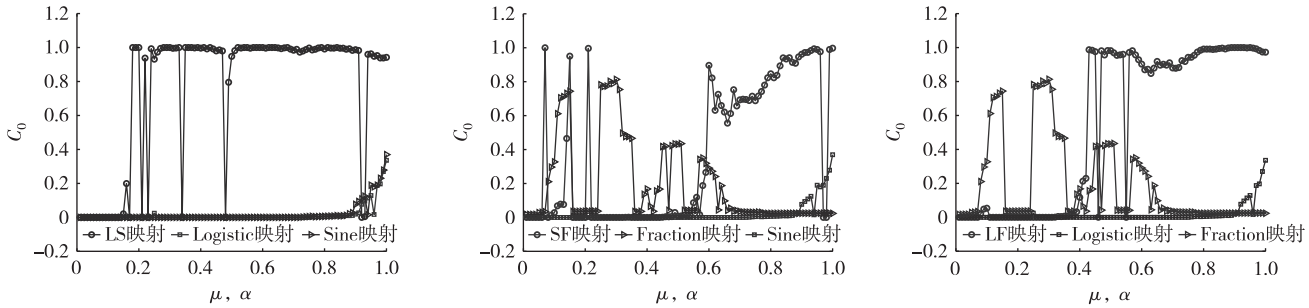
图 6　ASCSM 和传统一维映射的 E_S 复杂度对比

Fig. 6　Complexity comparison of ASCSM and conventional one-dimensional mappings

4.3　C_0 复杂度分析

C_0 复杂度算法主要通过分解规则部分和不规则部分[20]。它的值是指不规则部分占整个序列的比例。序列中不规则部分所占比例越大，对应的时域信号与随机序列越接近，复杂度越大，也就是 C_0 值越大。正如图 7 所示，增强的 LS、SF 和 LF 在更广的范围获得了更大的 C_0 值，也就是经过 ASCSM 的混沌系统拥有更大比例的不

规则部分。种子映射只在很小的范围内有较小的 C_0 值,且以规则部分为主。



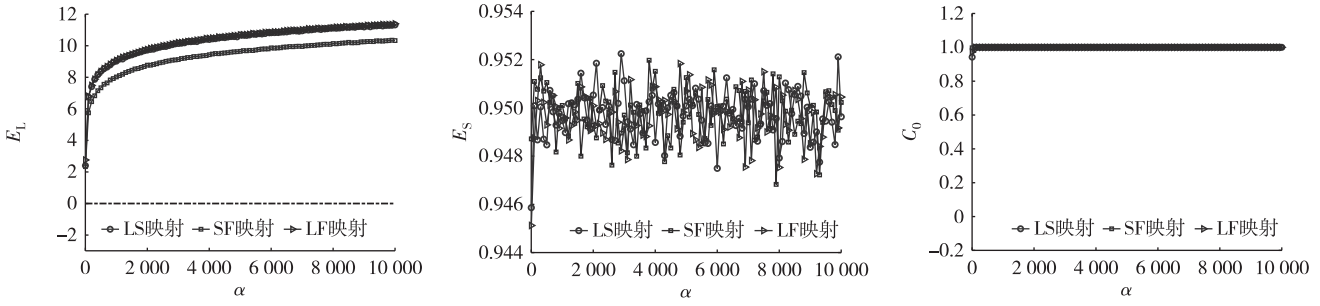
a LS、Logistic 和 Sine 映射的 C_0　　b SF、Fraction 和 Sine 映射的 C_0　　c LF、Fraction 和 Logistic 映射的 C_0

图 7 ASCSM 和传统一维映射的 C_0 复杂度对比

Fig. 7 Comparison of the C_0 complexity of ASCSM and traditional one-dimensional mapping

4.4 大范围控制参数复杂度分析

前面章节对比了增强映射和种子映射的 E_L、E_S 和 C_0 复杂度,控制参数范围均设为(0,1)。为了研究控制参数更大范围内的复杂度,将控制参数 α 范围设置为[1,10 000],分别计算了 3 种增强映射的 E_L、E_S 和 C_0 复杂度。如图 8a 所示,LS、SF 和 LF 映射在 $\alpha\in[1,10\ 000]$范围内的 E_L 曲线,$E_L>0$,且随着控制参数增加,E_L 的值还在进一步增大;如图 8b 所示,在 $\alpha\in[1,10\ 000]$范围内的 E_S 主要集中在 0.95 附近;如图 8c 所示,LS、SF 和 LF 映射在 $\alpha\in[1,10\ 000]$范围内的 C_0 趋近 1,表明增强映射很大参数范围内都呈现混沌状态,且复杂度很高。



a LS、SF 和 LF 映射的 E_L　　b LS、SF 和 LF 映射的 E_S　　c LS、SF 和 LF 映射的 C_0

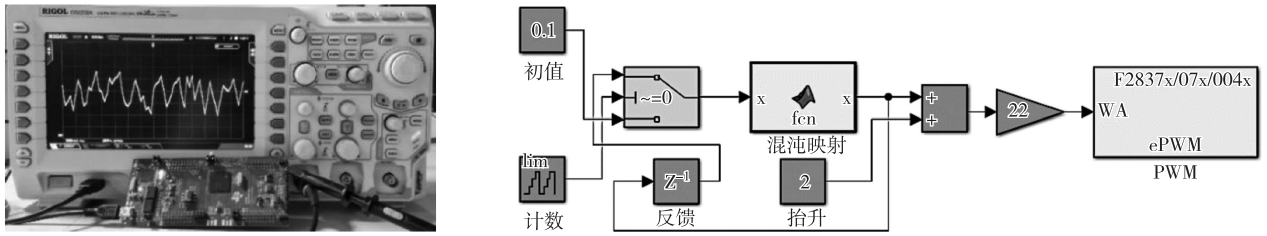
图 8 大范围控制参数下 ASCSM 映射的 E_L、E_S 和 C_0 复杂度分析

Fig. 8 Complexity analysis of E_L, E_S and for ASCSM mapping under a wide range of control parameters

5 硬件实现

前面在理论上推导了 ASCSM 映射的混沌性能,通过 E_L、E_S 和 C_0 评估了新的增强映射的复杂度。利用 TI 公司 DSP 平台,将 3 种新增的 ASCSM 映射通过硬件产生随机序列,由示波器观测到的随机序列验证了 ASCSM 可以在硬件系统上实现。如图 9a 所示,硬件平台是德州仪器公司的 LAUNCHXL-F28379D,该平台利用 PWM 模块和低通模块实现数模转化(digital to analog converter,DAC)功能。如图 9b 展现了增强的 LS 混沌系统在硬件实现的结构框图,该系统主要由混沌函数映射模块、计时器、延迟反馈和 PWM 模块 4 部分组成。混沌函数映射模块主要构成 LS 映射方程,延迟反馈保持当前 x_i 为下次计算的输入值,每次产生的随机数控制 PWM 模块的占空比,通过低通滤波器得到一个模拟电压输出。每次不同随机数值都将得到一个模拟电压值,通过示波器可以直观地观察混沌系统产生的随机序列。图 10 展示了通过示波器观测到的 LS、SF 和 LF 映射硬件产生的随机序列,可以看出新增的 ASCSM 通过 DSP 硬件系统应用到实际中。同时该模型可以通过软件仿真实现,将图 10 中的 ePWM 硬件模块转为可被随机序列控制占空比的 PWM 波和低通滤波器的软件模块,同样可将数字信号转为无规则的模拟电压信号序列。若软件仿真设置与硬件系统相同的低通滤波器、相同占空比的 PWM 波以及初始值等,可以得到与硬件系统产生的一致的序列。由于示波器一直在运行,每次截取到的电压信号图片

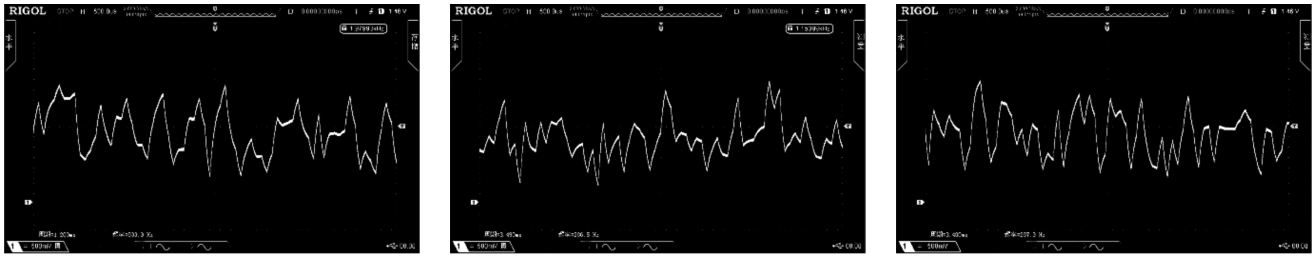
因保存时间的不同而有所改变，故本文不展示软件仿真图片。



a　硬件系统实物图　　b　LS 映射的硬件实现结构框图

图 9　LS 映射的硬件实现

Fig. 9　Hardware implementation of the LS model



a　LS 映射的硬件产生随机序列　　b　SF 映射的硬件产生随机序列　　c　LF 映射的硬件产生随机序列

图 10　增强的 LS、SF 和 LF 映射的硬件实现随机序列

Fig. 10　Enhanced hardware implementation of LS, SF and LF mapping for random sequences

6　ASCSM 在图像加密中的应用

基于混沌系统所具有的独特性质：对初值极端的敏感性和高度的随机性，混沌理论已经被广泛应用于各种加密中[21]。现将传统的一维种子混沌模型和新建的 ASCSM 应用到图像加密上，通过实际应用来体现 ASCSM 的优势。

为了不受算法的影响，每个模型嵌入的算法均为最简单的同一种算法，具体代码如算法 1。首先，通过加密同一张图片对比各个模型由算法生成的加密图像的隐蔽性；其次，为避免肉眼观测加密效果的主观性，因此更客观地通过对比加密图像的直方图来判断不同模型产生的序列的随机性；最后，采用熟悉的加密评估指标，如图像相邻像素相关性分析、信息熵分析等，在加密应用的效果上对一维种子模型和本文提出的模型进行更全面的评估。

算法 1　加密算法

输入：图像大小为 $M\times N$ 的灰度图。

输出：图像大小为 $M\times N$ 的加密灰度图。

读取图片数据，保存在矩阵 $\boldsymbol{Y}$ 内；

各个模型的控制参数均初始化为 0.99，初始值(x_0,y_0)设为(0.291 5,0.506 0)；

for $i=1$: M do

　for $j=1$: N do

　将 $\boldsymbol{Y}(i,j)$像素值作为模型的 x_i，通过模型计算 x_{i+1} 得到新的像素值 $\boldsymbol{Y}'(i,j)$，用 $\boldsymbol{Y}'(i,j)$替换 $\boldsymbol{Y}(i,j)$的像素值；

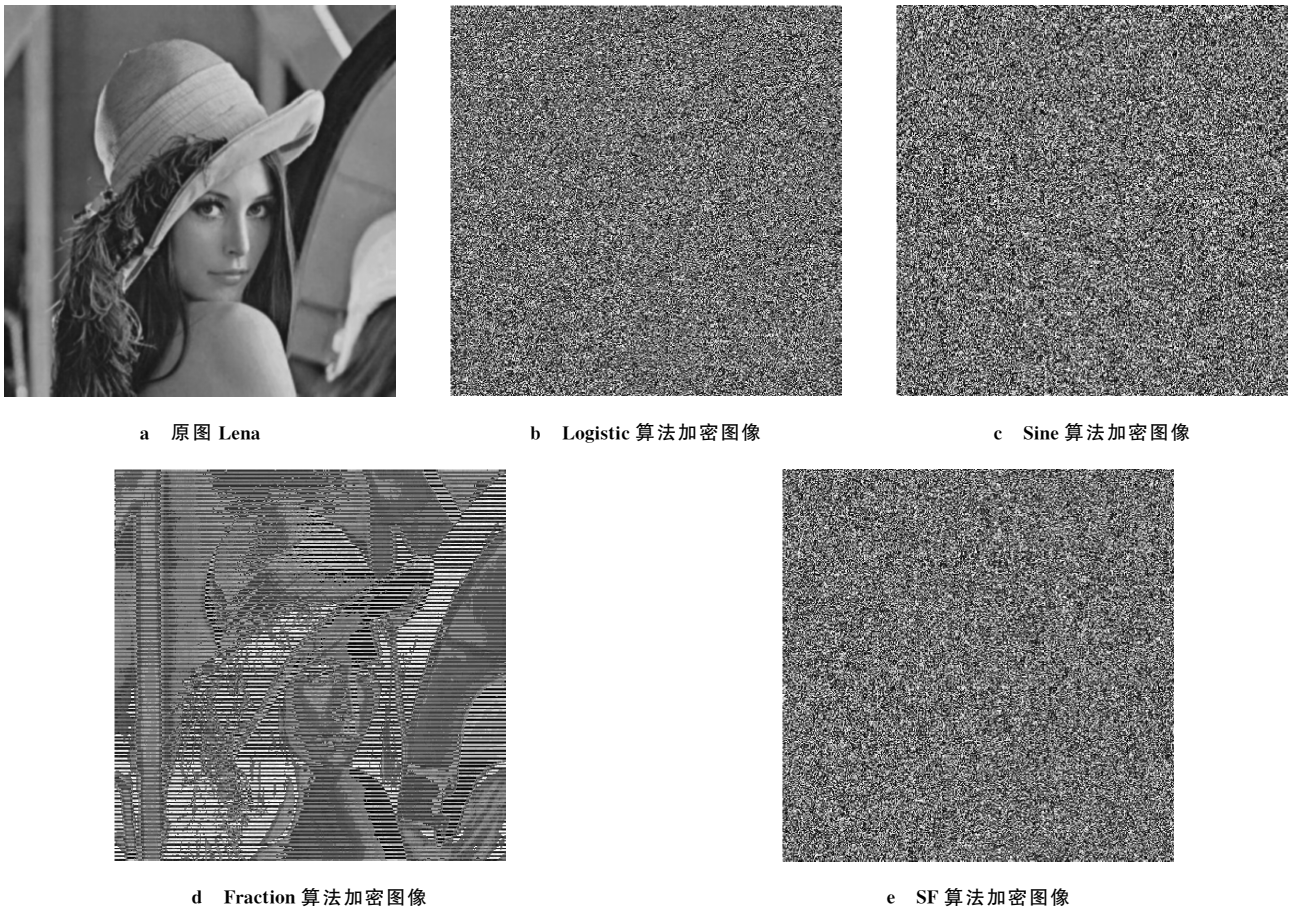
　end for

end for

6.1　不同模型加密效果对比

图 11 展示了原始明文图像以及通过各种模型嵌入加密后的图像。这里采用 Sine 和 Faction 模型组合成 SF

模型作为ASCSM的示例,不难看出除了Fraction模型嵌入的算法加密的图像还能够看出原始图像以外,其他加密图像信息则均能被完好隐藏。



a 原图Lena　b Logistic算法加密图像　c Sine算法加密图像

d Fraction算法加密图像　e SF算法加密图像

图11 不同模型算法加密图像对比

Fig. 11 Comparison of encrypted images with different modeling algorithms

6.2 不同模型加密直方图对比

图像直方图以图像像素值数据组成的总值作为直方图的横坐标,以每个值出现的次数或比例作为纵坐标,利用图像直方图可以确定图像的信息特征。从图12可以看出,SF模型嵌入算法生成的加密图像的直方图的像素值分布更为均匀,从而反映出ASCSM生成的序列随机性更强。

6.3 图像相邻像素相关性分析

相关性分析是指对2个或多个具备相关性的变量元素进行分析,从而衡量变量之间的相关密切程度。加密图像的目标之一就是减小相邻像素相关性,主要包括水平像素、垂直像素和对角线像素之间的关联度。关联度越小,则说明加密效果越好,安全性越高。相关系数的计算公式如下:

$$R_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

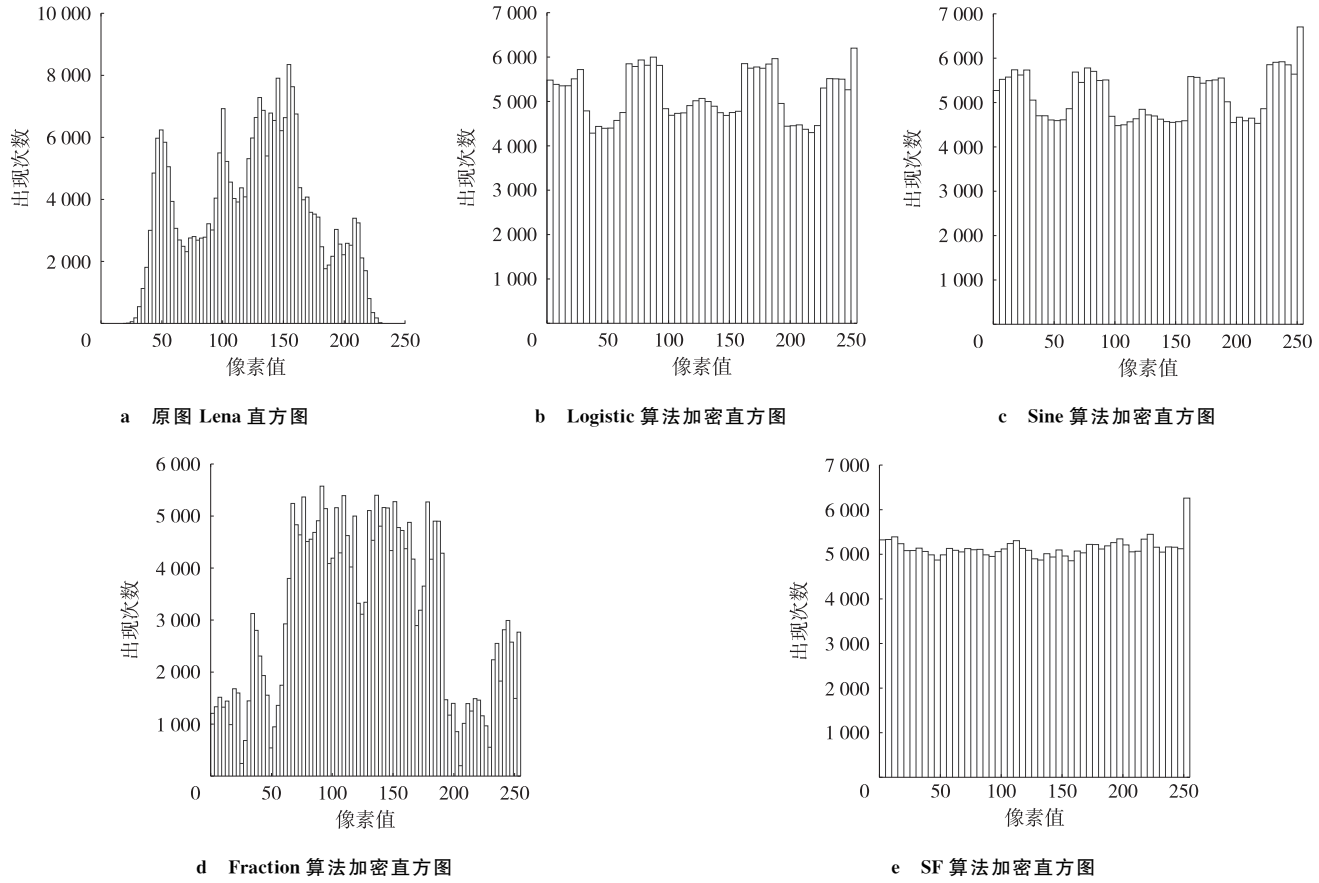
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i,$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2,$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)),$$

其中:y为x的相邻像素,N为图像中像素点的总数,R_{xy}即为两相邻像素的相关性,$\operatorname{cov}(x,y)$是x和y这2个像素点处的协方差,$\sqrt{D(x)}$是标准差,$D(x)$是方差,$E(x)$是均值。通常,明文图像相邻像素的R_{xy}接近1,而密

文图像相邻像素的 R_{xy} 应该接近 0。



a　原图 Lena 直方图　　b　Logistic 算法加密直方图　　c　Sine 算法加密直方图

d　Fraction 算法加密直方图　　e　SF 算法加密直方图

图 12　不同模型算法加密直方图对比

Fig. 12　Comparison of encryption histograms of different modeling algorithms

表 1 展示的是采用不同模型算法加密之后的图像相邻像素相关性分析，第 1 列为相邻像素的方向坐标，依次为水平、垂直、左斜、右斜方向。因为原始坐标的选取本身具有随机性，所以在此直接展示第 1 次运行的结果。除 Fraction 加密图像以外，可以看出加密后的图像的像素相关性几乎为 0，并且由 SF 模型加密之后的像素相关性整体而言最接近于 0，说明 ASCSM 在图像加密中性能更好。

表 1　不同混沌映射加密图像相邻像素相关性

Tab. 1　Neighboring pixel correlation of encrypted images with different chaotic mappings

方向	原图	Logistic	Fraction	Sine	SF
水平像素相关性	0.988 1	−0.045 9	−0.892 3	0.045 7	−0.015 3
垂直像素相关性	0.976 5	−0.003 6	0.947 7	0.016 0	0.006 6
左斜像素相关性	0.961 4	0.007 2	−0.880 7	−0.028 2	−0.001 6
右斜像素相关性	0.971 4	−0.029 8	−0.886 9	−0.022 1	0.003 3

6.4　信息熵分析

信息熵是一个衡量不确定度的量，若信息熵为 0，则说明一切都是确定的。信息熵计算公式为：

$$H(x)=-\sum_{i=1}^{L}P(x_i)\log_2 P(x_i),$$

其中：L 代表像素点的总数，$P(x_i)$代表每个像素值 x_i 的概率。信息熵越接近 8，表示图像所含信息量越小，随机性越强[22]。本文分别通过普通一维混沌映射和 SF 映射算法对图像进行加密，可以从表 2 看出，ASCSM 的信

息熵高于一维映射产生的信息熵。

表2 不同混沌映射加密图像信息熵对比

Tab. 2 Comparison of information entropy of encrypted images with different chaotic mappings

混沌映射	密文图像信息熵	混沌映射	密文图像信息熵
Logistic 映射	7.982 9	Fraction 映射	7.745 9
Sine 映射	7.983 2	ASCSM-SF 映射	7.990 8

7 结论

本文针对现有混沌系统复杂度低的情况,提出通过 ASCSM 来进一步提高复杂度,并通过以下方法进行了验证:基于 Lyapunov 指数定律从理论及实际仿真这两方面分析了 ASCSM 的性能,表明将传统的混沌系统植入 ASCSM 将获得更大的 E_L;对比仿真了 3 种增强映射和 3 种种子映射的 E_S、C_0 复杂度,结果表明增强的混沌映射比种子映射在更广的参数范围内具有更好的混沌性能;采用 DSP 平台实现增强混沌映射系统,通过示波器可以直观地观察混沌系统产生的随机序列,验证了 ASCSM 系统可以利用硬件实现,在随机信号产生、通信保密、图像加密等方面具有较好的应用前景;最后将 ASCSM 应用于图像加密,通过直方图、相邻像素相关性、信息熵分析验证了该模型加密的图像保密性比传统的种子映射更高。

参考文献:

[1] ZHOU G,PAN C,REN H,et al. Secure wireless communication in RIS-aided MISO system with hardware impairments[J]. IEEE Wireless Communications Letters,2021,10(6):1309-1313.

[2] YERRAPRAGADA A K, EISMAN T, KELLEY B. Physical layer security for beyond 5G: ultra secure low latency communications[J]. IEEE Open Journal of the Communications Society,2021,2:2232-2242.

[3] 张茜,刘光斌,郭金库,等. 基于混沌时间序列建模的频谱状态持续时长预测[J]. 电子与信息学报,2015,37(4):868-873.
ZHANG Q,LIU G B,GUO J K,et al. Prediction of spectrum state duration based on chaotic time series modelling[J]. Journal of Electronics and Information Technology,2015,37(4):868-873.

[4] SHAO W, FU Y, CHENG M, et al. Chaos synchronization based on hybrid entropy sources and applications to secure communication[J]. IEEE Photonics Technology Letters,2021,33(18):1038-1041.

[5] 禹思敏,吕金虎,李澄清. 混沌密码及其在多媒体保密通信中应用的进展[J]. 电子与信息学报,2016,38(3):735-752.
YU S M,LÜ J H,LI C Q. Some progresses of chaotic cipher and its applications in multimedia secure communications[J]. Journal of Electronics and Information Technology,2016,38(3):735-752.

[6] ABDELFATAH R I. Secure image transmission using chaotic-enhanced elliptic curve cryptography[J]. IEEE Access,2020,8:3875-3890.

[7] 刘泉,李佩玥,章明朝,等. 基于可 Markov 分割混沌系统的图像加密算法[J]. 电子与信息学报,2014,36(6):1271-1277.
LIU Q,LI P Y,ZHANG M C,et al. Image encryption algorithm based on chaos system having Markov portion[J]. Journal of Electronics and Information Technology,2014,36(6):1271-1277.

[8] NGUYEN N,PHAM-NGUYEN L,NGUYEN M B,et al. A low power circuit design for chaos-key based data encryption[J]. IEEE Access,2020,8:104432-104444.

[9] 赵亮. 抗退化混沌序列密码研究[D]. 西安:西安电子科技大学,2021.
ZHAO L. Compressed sampling technology and its application[D]. Xi'an:Xidian University,2021.

[10] HUA Z, ZHOU B, ZHOU Y. Sine chaotification model for enhancing chaos and its hardware implementation[J]. IEEE Transactions on Industrial Electronics,2019,66(2):1273-1284.

[11] LIU Q,LIU L. Color image encryption algorithm based on DNA coding and double chaos system[J]. IEEE Access,2020,8:83596-83610.

[12] YE J,YANG J,XIE D,et al. Strong robust and optimal chaos control for permanent magnet linear synchronous motor[J]. IEEE Access,2019,7:57907-57916.

[13] SPITZ O,HERDT A,CARRAS M,et al. Enhanced chaotic performance with optically injected quantum cascade lasers[C]// 2019 IEEE Photonics Society Summer Topical Meeting Series (SUM),July 8-10,2019,Ft. Lauderdale,FL,USA. Piscataway:

IEEE,2019.
[14] WU Q. Cascade-sine chaotification model for producing chaos[J]. Nonlinear Dynamics,2021,106(3):2607-2620.
[15] ZHOU Z,XU X,JIANG Z,et al. Multiple-image encryption scheme based on an n-dimensional chaotic modular model and overlapping block permutation-diffusion using newly defined operation[J]. Mathematics,2023,11(15):3373.
[16] MAY R M. Simple mathematical models with very complicated dynamics[J]. Nature,1976,261(5560):459-467.
[17] LU J,WU X,LÜ J,et al. A new discrete chaotic system with rational fraction and its dynamical behaviors[J]. Chaos,Solitons & Fractals,2004,22(2):311-319.
[18] CARPINTERO D D,MUZZIO J C. The Lyapunov exponents and the neighbourhood of periodic orbits[J]. Monthly Notices of the Royal Astronomical Society,2020,495(2):1608-1612.
[19] 孙克辉,贺少波,何毅,等. 混沌伪随机序列的谱熵复杂性分析[J]. 物理学报,2013,62(1):35-42.
SUN K H,HE S B,HE Y,et al. Complexity analysis of chaotic pseudo-random sequences based on spectral entropy algorithm [J]. Acta Physica Sinica,2013,62(1):35-42.
[20] 叶晓林,牟俊,王智森,等. 基于 SE 和 C_0 算法的连续混沌系统复杂度分析[J]. 大连工业大学学报,2018,37(1):67-72.
YE X L,MOU J,WANG Z S,et al. Complexity analysis of continuous chaotic systems based on SE and C_0 algorithms[J]. Journal of Dalian Polytechnic University,2018,37(1):67-72.
[21] 张红,周尚波. 混沌理论在密码学中的应用[J]. 重庆大学学报,2004,27(4):39-43.
ZHANG H,ZHOU S B. Applications of chaos theory in cryptography[J]. Journal of Chongqing University,2004,27(4):39-43.
[22] 韦丞婧. 基于高维超混沌系统的伪随机序列发生器设计及应用[D]. 桂林:桂林电子科技大学,2023.
WEI C J. Design and application of pseudo-random sequence generator based on high-dimensional hyperchaotic system[D]. Guilin:Guilin University of Electronic Science and Technology,2023.

Performance Analysis of Additive Sinusoidal Chaotic System Model

LI Zhonghong[1], WANG Rui[1], WANG Jie[1], LI Guonan[1], LUO Haijun[1,2]
(1. College of Physics and Electronic Engineering, Chongqing Normal University;
2. National Center for Applied Mathematics, Chongqing Normal University, Chongqing 401331, China)

Abstract: To further increase the complexity of existing chaotic systems, the work proposes the Additive Sinusoidal Chaotic System Model (ASCSM), which adds two one-dimensional sinusoidalized conventional chaotic mappings (Logistic, Sine, Fraction) to enhance the complexity of chaotic systems. First, the performance of ASCSM is proved by theoretical analysis, and the dynamic characteristics of the enhanced chaotic mapping are simulated and analyzed according to the complexity metrics (Lyapunov exponent, spectral entropy, complexity), and the results show that the enhanced chaotic mappings performs better compared to the seed chaotic mappings. Secondly, based on the digital signal processor (DSP) platform, the feasibility of implementing the model on a hardware system is verified by generating random sequences using ASCSM. Finally, in order to compare its capability with traditional chaotic mappings in image encryption using these models as XOR sequence generators for encryption algorithms. Various cryptographic evaluation metrics demonstrate that the new model has higher confidentiality in cryptographic application.

Keywords: chaotic model; Lyapunov exponent; spectral entropy; hardware implementation; chaotic encryption

(责任编辑 黄 颖)