基于正弦反馈Logistic混沌映射的图像加密算法及其FPGA实现

李春彪* 赵云楠 李雅宁 孔思晓
(南京信息工程大学电子与信息工程学院 南京 210044)

摘 要：基于混沌的数字图像加密算法因具有较大的密钥空间和较高的密钥敏感特性等而被广泛地应用。该文在经典Logistic映射中引入正弦反馈，构成新的映射关系，并分析该映射的混沌行为。利用混沌映射导出离散混沌加密序列，并对加密序列进行放大取整，增强其伪随机性；利用NIST随机性测试方法测试了加密序列的伪随机性；将伪随机序列与原始图像进行异或运算，实现图像加密。数值仿真结果表明所提加密算法具有较好的加密效果，其密钥也具有较好的敏感性和伪随机性，最后基于FPGA平台的硬件加密实现了本算法。

关键词：图像加密；Logistic混沌映射；正弦反馈；FPGA；NIST
中图分类号：TN911.73; TN918.4 **文献标识码**：A **文章编号**：1009-5896(2021)12-3766-09
DOI: 10.11999/JEIT200575

An Image Encryption Algorithm Based on Logistic Chaotic Mapping with Sinusoidal Feedback and Its FPGA Implementation

LI Chunbiao ZHAO Yunnan LI Yaning KONG Sixiao
(*School of Electronic & Information Engineering, Nanjing University of Information Science & Technology, Nanjing* 210044, *China*)

Abstract: Digital image encryption algorithm based on chaos is widely used because of its large key space and high key sensitivity. The sinusoidal feedback is introduced into the classical Logistic mapping to form a new discrete mapping, and the chaotic behavior of the mapping is analyzed. The chaotic mapping is used to derive the discrete chaotic encryption sequence, and the encryption sequence is enlarged and rounded to enhance its pseudo-randomness. The pseudo-randomness of encrypted sequences is tested by NIST (National Institute of Standards and Technology) test method. The pseudo-random sequence is XOR (Exclusive OR) with the original image to realize image encryption. Numerical simulation results show that the new encryption algorithm has better encryption effect, and its key shows better sensitivity and pseudo-randomness. Finally, hardware encryption for this algorithm is realized based on FPGA (Field Programmable Gate Array) platform.

Key words: Image encryption; Logistic chaotic map; Sinusoidal feedback; Field Programmable Gate Array (FPGA); National Institute of Standards and Technology (NIST)

1 引言

数字图像的安全传输和隐私保护在网络空间中易受挑战，而传统分组加密算法容易遭受穷举法的攻击。由于图像数据具有特殊格式，图像加密对加密效率有更高的要求。分组加密算法对图像的加密具有一定的局限性，故而常用于文字符号等信息的加密。大量的图像加密方案也将明文图像视为文本数据来处理[1]，这使得传统分组加密算法的效率不够高。目前，先进的拍摄设备使数字图像具有大数据量和高冗余的特点，加之数字图像本身的相邻像素相关性高[2]，分组加密算法难以削弱相邻像素相关性。

随着混沌理论的发展，人们将混沌理论引入密码学形成新的数字图像加密算法[3]。混沌具有遍历性、随机性和初值敏感性等特点，其混合和随机性类似于密码学的置换和扩散。混沌加密算法使得加密安全性更高、密钥空间更大、密钥敏感性更强，比传统加密方法更有潜力[4]。然而数字图像的混沌加密算法也面临着安全性能方面的挑战。基于混沌系统的伪随机序列发生器存在一定的弱随机性[1]。

收稿日期：2020-07-13；改回日期：2021-03-28；网络出版：2021-06-02
*通信作者： 李春彪 goontry@126.com; chunbiaolee@nuist.edu.cn
基金项目：国家自然科学基金 (61871230)，江苏省自然科学基金 (BK20181410)
Foundation Items: The National Natural Science Foundation of China (61871230), The Nature Science Foundation of Jiangsu Province (BK20181410)

典型的Logistic映射的数学表达式简单但动力学特性复杂。文献[5]从离散序列和相对熵的理论中分析了Logistic映射的时间不可逆性、初值敏感性、混沌状态程度等特性，因而可以采用Logistic映射或者改进Logistic映射来加密数字图像。文献[6]采用了典型的Logistic映射进行数字图像加密，该方法能够实现良好的加密效果，但密文图像的灰度直方图不平坦，加密效果欠佳；文献[7]改进Logistic映射并基于初始值与控制参数之间存在的关系对变量域进行分段处理，扩大了混沌域；陶红[8]试着将典型的Logistic映射与其他加密方式相结合来改善加密效果。上述加密方式均基于单一混沌映射进行数字图像加密。

本文在经典Logistic映射中引入正弦反馈，构成新的映射关系，并对生成的伪随机序列进行预处理，增强其伪随机性，削弱伪随机序列发生器的弱随机性造成的弊端。使用NIST随机数测试法测得加密序列的伪随机性较好。FPGA系统稳定性高，可用电路直观表达逻辑，且成本较低[9]。利用FPGA进行加密处理，数据稳定性更强，逻辑更清晰。本文使用FPGA平台，实现本文提出加密方案，加密效果较好。

2　引入正弦反馈的Logistic映射

2.1　映射数学模型

基于Logistic映射[10]，引入正弦函数，构建出新的1维混沌映射，其函数如式(1)所示

$$x_{n+1} = k \times x_n \times [1 - \sin x_n] \tag{1}$$

其中，k为系统数且$k \neq 0$。

2.2　一次映射不动点稳定性分析

已知新的混沌映射函数式(1)，存在不动点x_{f}，x_{f}满足方程

$$k \times x_{\mathrm{f}} \times [1 - \sin x_{\mathrm{f}}] - x_{\mathrm{f}} = 0 \tag{2}$$

解得

$$x_{\mathrm{f}_1} = 0,\ x_{\mathrm{f}_2} = \arcsin\left(1 - \frac{1}{k}\right) \tag{3}$$

$$\frac{\partial f(x,k)}{\partial x}|_{x=x_{\mathrm{f}}} = k \times (1 - \sin x_{\mathrm{f}} - x \times \cos x_{\mathrm{f}}) \tag{4}$$

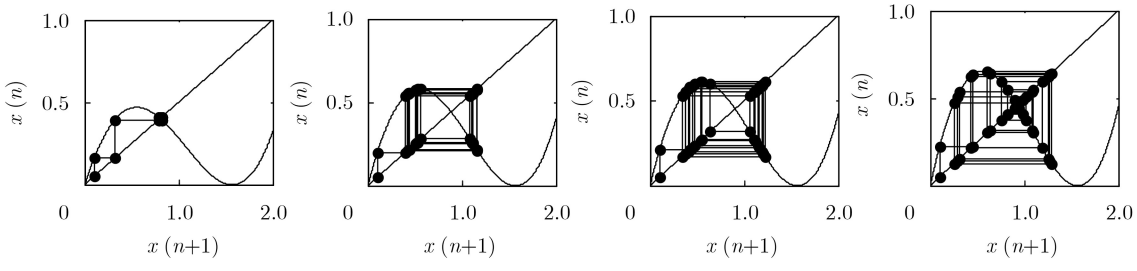
由式(4)和式(3)可以得出式(5)

$$\frac{\partial f(x,k)}{\partial x}|_{x=x_{\mathrm{f}_1}} = k,\ \frac{\partial f(x,k)}{\partial x}|_{x=x_{\mathrm{f}_2}} = k \times \left\{\frac{1}{k} - \arcsin\left(1 - \frac{1}{k}\right) \times \cos\left[\arcsin\left(1 - \frac{1}{k}\right)\right]\right\} \tag{5}$$

将Lyapunov指数为0时的k值代入式(5)，$\dfrac{\partial f(x,k)}{\partial x}$在$x = x_{\mathrm{f}_1}$条件下的值均小于等于1，在$x = x_{\mathrm{f}_2}$条件下的值均大于1。可知该混沌映射具有不稳定不动点x_{f_1}和稳定不动点x_{f_2}[11]。利用蛛网结构进一步探究1维迭代映射的过程[12]。给定一个输入值k，画一条垂线直到与图像P相交，高度为输出值$x(n+1)$。迭代中令$x(n+1)$为新的输入值，再画一条水平直线与45°对角线相交，重复过程。结果如图1所示。该蛛网说明不动点是不稳定的，观察曲线与对角线的交线，$x(n)$不动点的偏差在每一次的迭代中被一个恒定的常数乘子驱使而缩紧。从物理意义上讲，不管初始条件如何，整个混沌系统总是会进入相同的受迫振荡中。

2.3　分岔图与Lyapunov指数分析

在初值为$x_0 = 0.1$的情况下，计算状态量$x(n)$的分岔图和Lyapunov指数谱，如图2所示。从图中可以看出引入非线性正弦因子的Logistic混沌系统的混沌区域大，使用该混沌系统能得到更宽的加密区间。Lyapunov指数表征了一个系统的混沌属性[13]。比较分岔图与Lyapunov指数谱，可以看出分岔图在最大Lyapunov指数为零时便会进入新的分岔。可以看出引入正弦因子的Logistic混沌系统的Lyapunov指数大于零的范围很宽，总的密钥空间也较大。当$k = 3.584$时，混沌分岔图开始分岔，从周期1进入周期2；当$k = 4.428$时，从周期2进入周期4，当$k = 4.627$时，从周期4进入周期8，并继而进入混沌态。



(a) k=3.84, $x(0)$=0.1　(b) k=4.428, $x(0)$=0.1　(c) k=4.627, $x(0)$=0.1　(d) k=5, $x(0)$=0.1

图 1 蛛网结构图

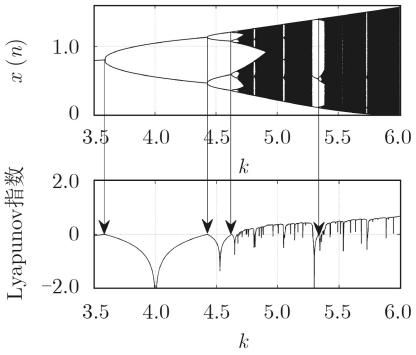


图 2 分岔图和Lyapunov指数谱图

2.4 敏感性分析

密钥敏感性表征了密码系统的安全性能[14]。敏感性高表明了密钥微小的扰动便无法解密密文图像。引入非线性正弦因子的Logistic混沌系统的敏感性如图3所示。根据新混沌系统的系统方程，设初值$x_0=0.1$，系统参数$k=4.9$，改变初值为$0.1+10^{-4}$, $0.1+10^{-8}$, $0.1+10^{-12}$，迭代计算100次；设初值$x_0=0.1$，系统参数$k=4.9$，改变系统参数为$4.9+10^{-4}$, $4.9+10^{-8}$, $4.9+10^{-12}$，迭代计算100次。仿真得出的波形如图3所示。从图3中可以看出，密钥一旦发生微小变化，迭代次数n增加后，密钥序列变得完全不同，在图中表现为两条曲线的重合度。可见，密钥敏感级别可达到10^{-12}甚至更高的级别。

3 加密性能测试

引入非线性正弦因子的Logistic混沌系统产生一个范围在[0, 1.6]的加密序列。该序列中可能存在大量相似数据。所以先对该加密序列进行预处理，增强该加密序列的伪随机性，增强过程如式(6)所示。

$$C_i=\mathrm{mod}\left\{\mathrm{round}[1000\times|100\times C_i-\mathrm{round}\left(100\times C_i\right)|],256\right\} \tag{6}$$

其中，mod()和round()分别为取余和取整运算。该运算先将加密序列扩大取整，再取余计算，得到一组在[0, 255]内的加密序列[15]。该预处理将加密序列放大取整，避免小数过多影响加密效果，并增强伪随机性。加密/解密流程如图4所示。密文图像呈现噪声样式，无法解读有效信息。解密图像可以恢复明文信息。

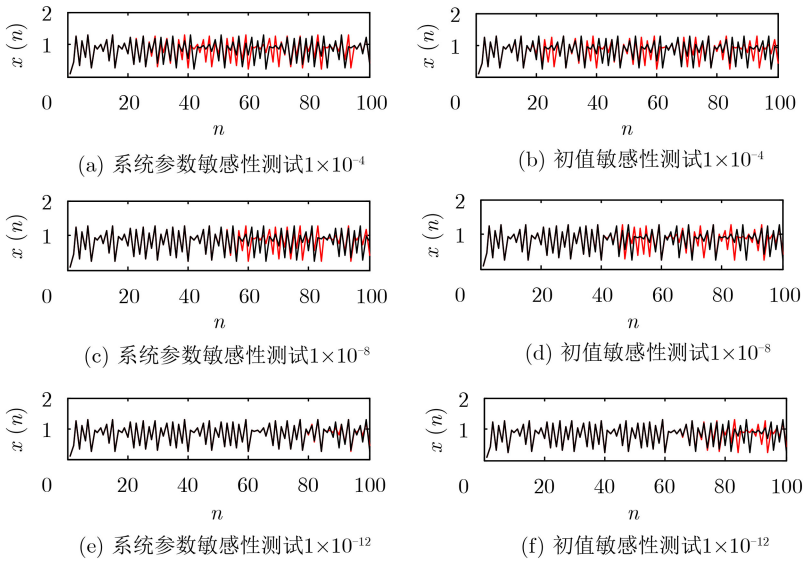
3.1 伪随机性能测试

NIST发布的“随机数和伪随机数发生器统计测试组件”能全面地分析伪随机序列的性能，具有频率测试等15个测试的维度[16]，测试样本为二进制。NIST对每个测试项都会生成P_value，当P_value > 0.01时，则该测试通过；当P_value ≤ 0.01时，则该测试不通过[17]。本文采用NIST推出的STS 2.1.2 (Statistical Test Suite 2.1.2)版本进行测试。

控制引入非线性正弦因子的Logistic混沌系统生成一组有262144个十进制数的伪随机加密序列，为保证混沌效果，取后131072个数据并转化成二进制文本。在STS界面设置100个大小为10000的数据块，进行标准1-13的测试。再控制该混沌系统生成一组含有37500000个十进制整数的伪随机加密序列，取后18750000个十进制数，二进转化后进行标准14-15的测试。NIST测试结果如表1所示。被测伪随机加密序列通过了15项NIST测试，且通过率均在97%以上，这表明该伪随机加密序列具有较好的伪随机性能。

3.2 密钥空间大小

本文所提出的引入非线性正弦因子的Logistic

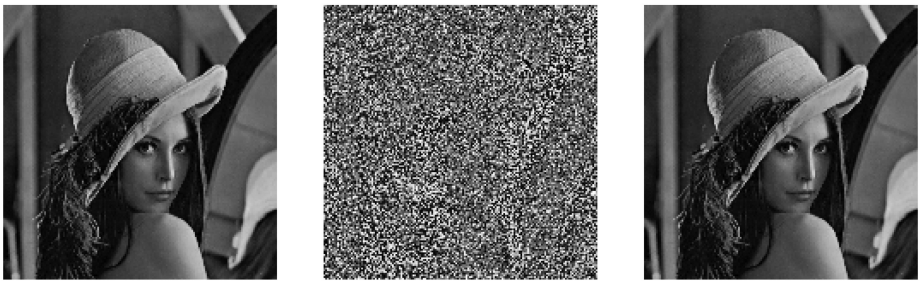


(a) 系统参数敏感性测试1×10^{-4}　(b) 初值敏感性测试1×10^{-4}

(c) 系统参数敏感性测试1×10^{-8}　(d) 初值敏感性测试1×10^{-8}

(e) 系统参数敏感性测试1×10^{-12}　(f) 初值敏感性测试1×10^{-12}

图 3 敏感性测试



(a) 原始图像　　(b) 密文图像　　(c) 解密图像

图 4 引入正弦因子的Logistic加密解密过程

表 1　NIST标准伪随机测试结果

测试编号	测试名称	P_value	测试通过率(%)
1	频率(单比特)测试	0.964290	99
2	块内频数测试	0.181557	100
3	游程测试	0.401199	99
4	块内最大游程测试	0.779188	100
5	二元矩阵秩测试	0.004981	100
6	频谱测试	0.304126	100
7	非重叠字匹配测试	0.534146	97
8	重叠字匹配测试	0.213390	99
9	Maurer通用统计检测	0.178278	100
10	线性复杂度测试	0.262249	98
11	系列测试	0.058984	99
12	近似熵测试	0.178876	100
13	累积和测试	0.816537	98
14	随机游程测试	0.535328	所有数据为一个数据块，大小为30 MB，不计通过率
15	随机游程变量测试	0.532553	

混沌加密系统的密钥为$K=\{x_0,k\}$。在敏感性初值测试中，系统敏感性可达到10^{-17}，密钥的步进大小为10^{-18}，每个密钥由两个参数构成，计算可得该密钥空间大小为$10^{34}\approx 2^{114}$。由于$2^{120}>2^{100}$，可以判断，该密钥空间对穷举法攻击具有足够的防御性[18]。

3.3　信息熵测试

热力学采用熵值来表征物质状态的无序性。类比热力学，信息源信息的不确定度可由信息熵表示。信息源的熵值越大、紊乱程度越高，可接受信息越少。理论上，256灰度级完全随机图像的信息熵H为8。信息熵的计算公式如式(7)所示。式中K表示突出的灰度级个数，$f(i)$表示灰度i在所有灰度中出现的概率[19]。

$$H=-\sum_{i=0}^{K}[f(i)\times\log_2 f(i)] \tag{7}$$

本文采用密钥$K=\{0.1,5\}$，以一副256灰度级的Lena图像为例，计算其明文和其密文的信息熵，其计算结果列于表2中。由表2可知，密文图像的信息熵为7.9987。引入正弦因子且对伪随机序列进行预处理之后再加密，密文图像具有较高的信息熵，图像加密性能更加优越。

3.4　密文统计特性测试

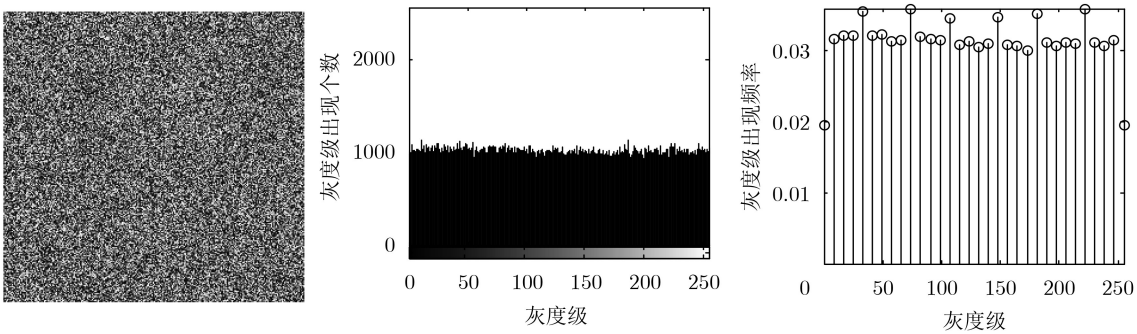
选取密钥$K=\{0.1,5\}$，利用引入非线性正弦因子的Logistic混沌加密系统和典型的Logistic混沌加密系统对图像进行加密，绘制出密文图像的灰度直方图，如图5和图6所示。和典型Logistic混沌加密系统相比，引入非线性正弦因子的Logistic混沌加密系统得到的加密图像的直方图更加平滑，加密性能更优越。

3.5　根据相邻像素相关性分析

图像的相邻两个像素主要分散于水平、垂直和

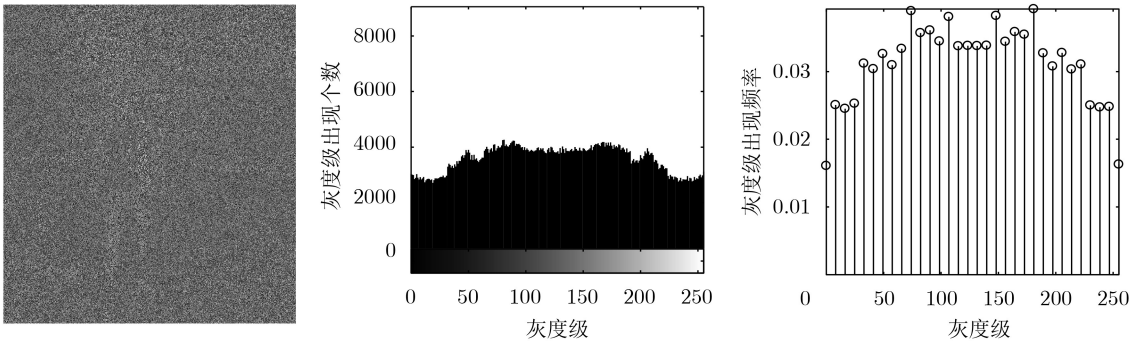
表 2　信息熵实验结果

明文	密文
7.6005	7.9987



(a) 新混沌加密系统密文图像 (b) 新混沌加密系统灰度直方图 (c) 新混沌系统归一化直方图

图 5 新混沌加密系统统计特性



(a) 典型Logistic混沌加密系统密文图像 (b) 典型Logistic混沌加密系统灰度直方图 (c) 典型Logistic混沌加密系统归一化直方图

图 6 典型Logistic混沌加密系统统计特性

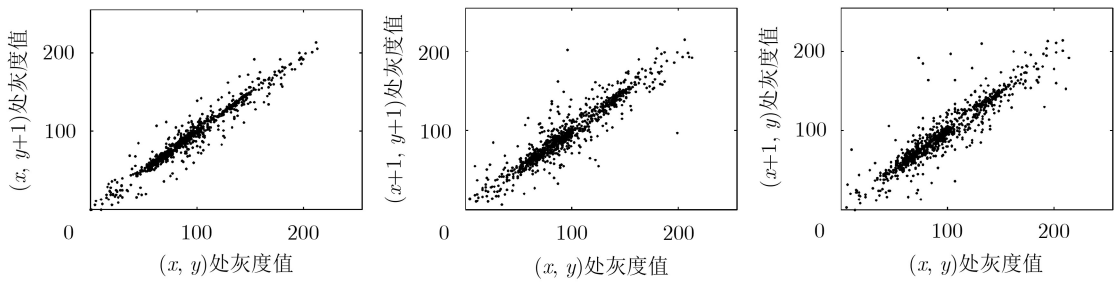
对角线方向。加密后的图像相关性小才能掩盖原信息以防止信息泄露。计算公式如式(8)所示，从图像矩阵中随意抽选N对相邻像素点的像素值，分别记为x_i和y_i[20]。

$$C=\frac{\sum_{i=1}^{N}\left[\left(x_i-\frac{1}{N}\times\sum_{i=1}^{N}x_i\right)\times\left(y_i-\frac{1}{N}\times\sum_{i=1}^{N}y_i\right)\right]}{\sqrt{\sum_{i=1}^{N}\left(x_i-\frac{1}{N}\times\sum_{i=1}^{N}x_i\right)^2\times\sum_{i=1}^{N}\left(y_i-\frac{1}{N}\times\sum_{i=1}^{N}y_i\right)^2}} \tag{8}$$

挑选8000对不同位置的相邻像素点，计算相邻像素相关系数并进行可视化处理。结果如图7、图8和表3所示。明文图像的相邻像素值呈现线性关系，相关性强；密文图像的相邻像素值均匀分布，相关性差。

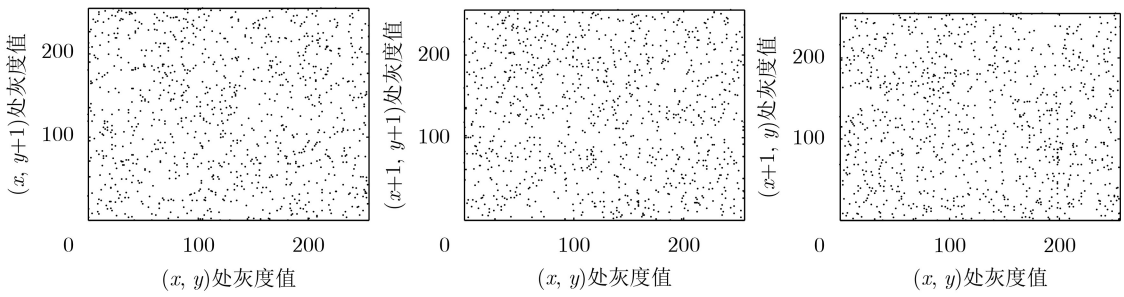
3.6 密钥敏感性测试

上文的敏感性分析已表明引入非线性正弦因子的Logistic混沌加密系统具有密钥敏感性。本节通过改变密钥初值x_0来测试密钥敏感性。以密钥$K=\{0.1,0.4\}$进行加密。则密钥$x_0=1.0+10^{-15}$无法解密，密钥$x_0=1.0+10^{-17}$解密成功。这表明密钥出现微弱扰动便无法解密图像，十分敏感。如图9与图10所示。



(a) 明文垂直相邻像素相关性 (b) 明文对角相邻像素相关性 (c) 明文水平相邻像素相关性

图 7 明文各方向相关系数

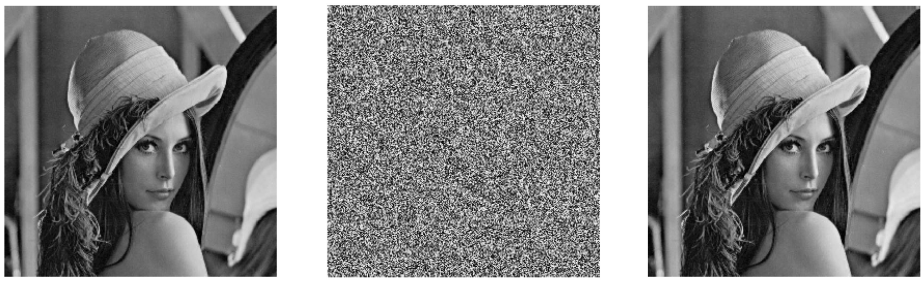


(a) 密文垂直相邻像素相关性　(b) 密文对角相邻像素相关性　(c) 密文水平相邻像素相关性

图 8 密文各方向相关系数

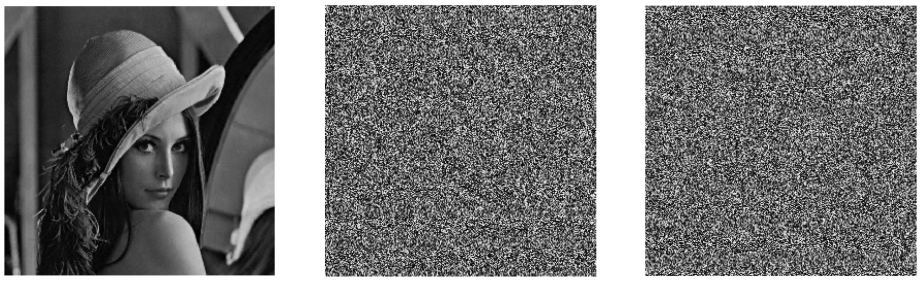
表 3　图像的相邻像素相关性

图像		水平	垂直	对角线
Lena	明文	0.9765	0.9597	0.9420
	密文	–0.0082	–0.0054	0.0020



(a) 明文图像　(b) 密文图像　(c) 解密图像

图 9 密钥为$x_0 = 1.0 + 10^{-17}$时的解密过程



(a) 明文图像　(b) 密文图像　(c) 解密图像

图 10 密钥为$x_0 = 1.0 + 10^{-15}$时的解密过程

4　FPGA加密和解密实现

4.1　硬件平台介绍

本文采用的FPGA硬件实现平台为Altera的以Cyclone IV EP4CE15F17C8N为核心的开发平台。其开发环境为Quartus II 13.1。该FPGA配置了EPCS4芯片。其VGA接口驱动采用了专用的ADV7123转换DA芯片。

4.2　加密/解密结构介绍

该加密/解密系统采用FPGA开发板的VGA显示驱动、ROM存储、JTGA下载功能。整个框架包含混沌加密序列发生模块、图像存储控制模块、程序下载模块和VGA显示模块。通过JTGA接口将程序固化进FPGA的Flash。加密时，从ROM中读取图像数据和混沌加密序列，进行异或运算并通过VGA接口，将原图、密文图像和解密图像依次显示在显示屏上。该混沌加密系统的结构框图如图11所示，解密系统结构框图如图12所示。

加密系统的RTL如图13所示。其中clk为50 MB系统时钟；rst_n为复位信号；vga_vs和vga_hs是VGA显示器的行场扫描信号；vga_rgb (lcd_data)为输出的加密图像信号；image_data为原始图像的信号；8位的信号pixel_data经过8到

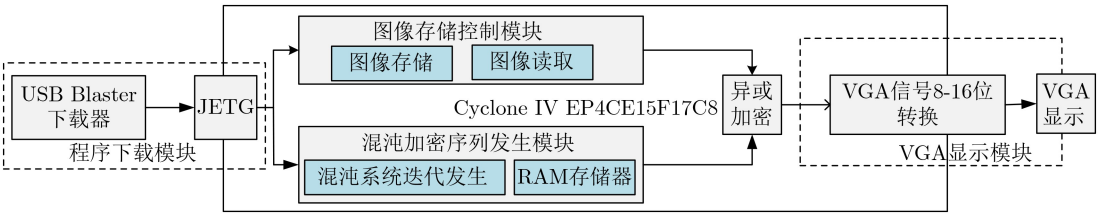


图 11 系统加密结构框图

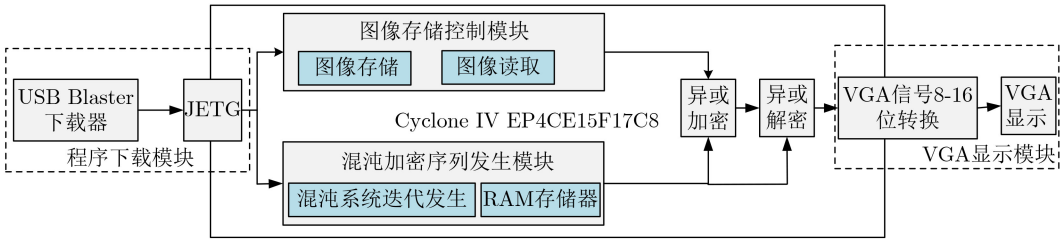


图 12 系统解密结构框图

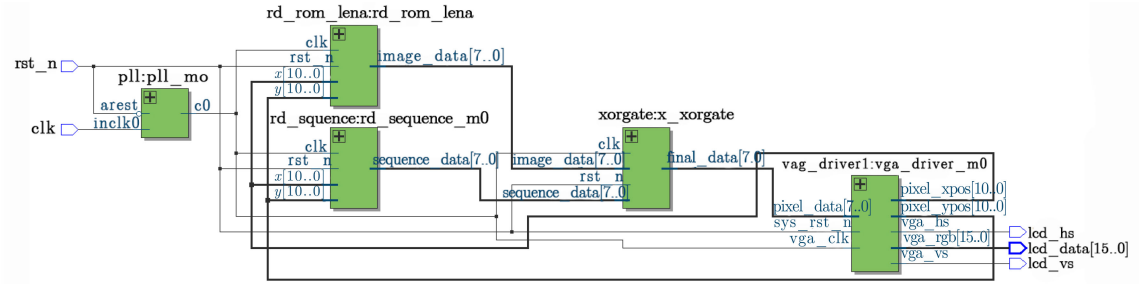


图 13 加密系统RTL图

16位VGA信号转换得到16位的vga_rgb信号输出。

解密系统的RTL图与加密系统RTL图类似，如图14所示，在加密系统RTL图中增加一次异或运算得出解密信号。图14中的pixel_data为解密图像信号。

4.3 硬件实现加密时序图分析

Quartus II具有嵌入式逻辑分析仪(signal tap)，它能方便地抓取模块中的信号，方便开发者对各个信号的时序进行查看。本加密系统的Signal Tap图由图15所示。图中a信号为原始图像信号，b为密文图像信号，c为解密后图像信号。从图15中可以看出，原始图像信号和解密图像信号完全相同，较好地实现了加密的效果。

4.4 FPGA加密结果

基于FPGA的混沌加密结果如图16所示。图16

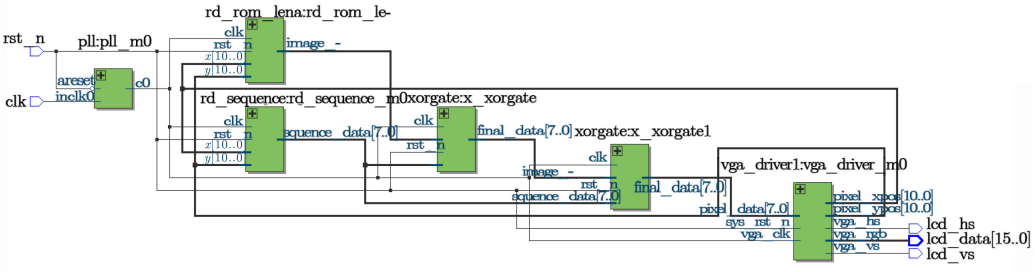


图 14 解密系统RTL图

图 15 Signal Tap时序图

(a) 明文图像VGA显示　(b) 密文图像VGA显示　(c) 解密图像VGA显示

图 16 FPGA实验结果VGA显示图

所展示的为完整加密过程的FPGA实验结果及VGA显示图。从图中可以看出FPGA硬件实现的图像结果与上文理论仿真一致，从而表明本文所提出的加密方案实际可行。

5　结束语

本文在经典的Logistic映射基础上，引入非线性正弦反馈从而构建得到一种新的混沌系统。基于新的混沌映射，产生混沌加密序列，并对混沌加密序列先进行处理增强其伪随机性，再进行数字图像的加密运算。利用NIST测试组件对混沌加密序列的伪随机性进行测试。数值仿真结果可见，本文所提出的新的数字图像加密算法能够较好地实现数字图像加密，具有密钥空间大、加密安全性高、计算简单等特点。在FPGA中，该加密方法也能得到较好的实现。

参 考 文 献

[1] LI Chengqing, ZHANG Yun, Xie E Y. When an attacker meets a cipher-image in 2018: A year in review[J]. *Journal of Information Security and Applications*, 2019, 48: 102361. doi: 10.1016/j.jisa.2019.102361.

[2] 张慧奔. 基于混沌图像加密算法的研究[D]. [硕士论文], 电子科技大学, 2015.
ZHANG Huiben. Chaotic image encryption algorithm research[D]. [Master dissertation], University of Electronic Science and Technology of China, 2015.

[3] YOON J W and KIM H. An image encryption scheme with a pseudorandom permutation based on chaotic maps[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2010, 15(12): 3998–4006. doi: 10.1016/j.cnsns.2010.01.041.

[4] PENG Yuexi, SUN Kehui, and HE Shaobo. Dynamics analysis of chaotic maps: From perspective on parameter estimation by meta-heuristic algorithm[J]. *Chinese Physics B*, 2020, 29(3): 030502. doi: 10.1088/1674-1056/ab695c.

[5] 徐红梅, 郭树旭. 基于符号相对熵的Logistic混沌系统时间不可逆性分析[J]. 电子与信息学报, 2014, 36(5): 1242–1246. doi: 10.3724/SP.J.1146.2013.01262.
XU Hongmei and GUO Shuxu. Time irreversibility analysis of logistic chaos system based on symbolic relative entropy[J]. *Journal of Electronics & Information Technology*, 2014, 36(5): 1242–1246. doi: 10.3724/SP.J.1146.2013.01262.

[6] 郑继明, 汤智睿, 邓建秀, 等. 基于Logistic混沌映射的数字图像加密算法[J]. 科技与创新, 2018(18): 8–11. doi: 10.15913/j.cnki.kjycx.2018.18.008.
ZHEN Jiming, TANG Zhirui, DENG Jianxiu, *et al*. Digital image encryption algorithm based on Logistic chaotic map[J]. *Science and Technology & Innovation*, 2018(18): 8–11. doi: 10.15913/j.cnki.kjycx.2018.18.008.

[7] 陈志刚, 梁涤青, 邓小鸿, 等. Logistic混沌映射性能分析与改进[J]. 电子与信息学报, 2016, 38(6): 1547–1551. doi: 10.11999/JEIT151039.
CHEN Zhigang, LIANG Diqing, DENG Xiaohong, *et al*. Performance analysis and improvement of Logistic chaotic mapping[J]. *Journal of Electronics & Information Technology*, 2016, 38(6): 1547–1551. doi: 10.11999/JEIT151039.

[8] 陶红. 基于Logistic混沌序列的图像加密设计[D]. [硕士论文], 东南大学, 2018.
TAO Hong. Design of image encryption algorithm based on Logistic chaotic sequence[D]. [Master dissertation], Southeast University, 2018.

[9] 齐红涛, 苏涛. 基于FPGA的高速AD采样设计[J]. 航空兵器, 2010(1): 35–39. doi: 10.19297/j.cnki.41-1228/tj.2010.01.009.
QI Hongtao and SU Tao. Design of high AD sampling based on FPGA[J]. *AERO Weaponry*, 2010(1): 35–39. doi: 10.19297/j.cnki.41-1228/tj.2010.01.009.

[10] MAY R M. Simple mathematical models with very complicated dynamics[J]. *Nature*, 1976, 261(5560): 459–467. doi: 10.1038/261459a0.

[11] 高智中, 李会芳. Logistic的混沌分析及其控制[J]. 运城学院学报, 2006, 24(2): 12–14. doi: 10.15967/j.cnki.cn14-1316/g4.2006.02.006.
GAO Zhizhong and LI Huifang. Chaos analysis and chaos controlling of Logistic map[J]. *Journal of Yuncheng University*, 2006, 24(2): 12–14. doi: 10.15967/j.cnki.cn14-1316/g4.2006.02.006.

[12] 张双红. Logistic模型的Matlab计算与可视化[J]. 吉林师范大

学学报: 自然科学版, 2009, 30(3): 97–99. doi: 10.16862/j.cnki.issn1674-3873.2009.03.024.

ZHANG Shuanghong. Calculation and visualization of Logistic model by using Matlab[J]. *Jilin Normal University Journal: Natural Science Edition*, 2009, 30(3): 97–99. doi: 10.16862/j.cnki.issn1674-3873.2009.03.024.

[13] 罗利军, 李银山, 李彤, 等. 李雅普诺夫指数谱的研究与仿真[J]. 计算机仿真, 2005, 22(12): 285–288. doi: 10.3969/j.issn.1006-9348.2005.12.080.

LUO Lijun, LI Yinshan, LI Tong, *et al*. Research and simulation of Lyapunov's exponents[J]. *Computer Simulation*, 2005, 22(12): 285–288. doi: 10.3969/j.issn.1006-9348.2005.12.080.

[14] 毛骁骁, 孙克辉, 刘文浩. 基于分数阶统一混沌系统的图像加密算法[J]. 传感器与微系统, 2017, 36(6): 138–141. doi: 10.13873/j.1000-9787(2017)06-0138-04.

MAO Xiaoxiao, SUN Kehui, and LIU Wenhao. Image encryption algorithm based on fractional order unified chaotic system[J]. *Transducer and Microsystem Technologies*, 2017, 36(6): 138–141. doi: 10.13873/j.1000-9787(2017)06-0138-04.

[15] 李付鹏, 刘敬彪, 王光义, 等. 基于混沌集的图像加密算法[J]. 电子与信息学报, 2020, 42(4): 981–987. doi: 10.11999/JEIT190344.

LI Fupeng, LIU Jingbiao, WANG Guangyi, *et al*. An image encryption algorithm based on chaos set[J]. *Journal of Electronics & Information Technology*, 2020, 42(4): 981–987. doi: 10.11999/JEIT190344.

[16] 马上, 刘剑锋, 杨泽国, 等. 基于余数系统与置换多项式的高速长周期伪随机序列生成方法[J]. 电子与信息学报, 2018, 40(1): 42–49. doi: 10.11999/JEIT170421.

MA Shang, LIU Jianfeng, YANG Zeguo, *et al*. A method of generating high speed and long period pseudo-random sequence based on residue number system and permutation polynomial[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 42–49. doi: 10.11999/JEIT170421.

[17] 肖成龙, 孙颖, 林邦姜, 等. 基于神经网络与复合离散混沌系统的双重加密方法[J]. 电子与信息学报, 2020, 42(3): 687–694. doi: 10.11999/JEIT190213.

XIAO Chenglong, SUN Ying, LIN Bangjiang, *et al*. Double encryption method based on neural network and composite discrete chaotic system[J]. *Journal of Electronics & Information Technology*, 2020, 42(3): 687–694. doi: 10.11999/JEIT190213.

[18] 郭媛, 周艳艳, 敬世伟. 基于图像重组和比特置乱的多图像加密[J]. 光子学报, 2020, 49(4): 0410002. doi: 10.3788/gzxb20204904.0410002.

GUO Yuan, ZHOU Yanyan, and JING Shiwei. Multiple-image encryption based on image recombination and bit scrambling[J]. *Acta Photonica Sinica*, 2020, 49(4): 0410002. doi: 10.3788/gzxb20204904.0410002.

[19] 刘旭. 基于深度学习对一类混沌图像加密算法进行安全性分析[D]. [硕士论文], 南京邮电大学, 2019.

LIU Xu. Security analysis of a class of chaotic image encryption algorithm based on deep learning[D]. [Master dissertation], Nanjing University of Posts and Telecommunications, 2019.

[20] 向滔. 基于混沌的数字图像加密算法的分析与设计[D]. [硕士论文], 重庆大学, 2014.

XIANG Tao. Analysis and designs of digital image encryption algorithm based on chaos[D]. [Master dissertation], Chongqing University, 2014.

李春彪：男，1971年生，教授，研究方向为非线性电路与系统及其应用.

孔思晓：男，1996年生，硕士生，研究方向为电子与通信工程.

责任编辑：马秀强