doi:10.3969/j.issn.1001-4616.2022.02.012

基于微控制单元的彩色图像加密无线通信方案

贾晓霞[1],邢进生[2]

(1.太原学院计算机科学与技术系,山西 太原 030000)
(2.山西师范大学数学与计算机科学学院,山西 临汾 041081)

[摘要] 为解决无线信道中的彩色图像通信安全问题,提出了一种基于微控制单元(micro controller units,MCU)的彩色图像实时加密通信方案. 利用所提密码系统提高混沌序列的随机性,通过基于混沌映射的伪随机数生成器(pseudo random number generator,PRNG)和 XOR 操作进行图像加密,并通过 RS-232 端口发送嵌入式加密系统的输出. 在 PIC 16F873A 微控制器上实施了提出的方案,并在无线链路上进行了实验. 结果表明,与其他优秀加密方法相比,所提方案提供了更高的安全性,可抵御各种已知攻击. 此外,使用双浮点精度的 PRNG 的处理速度为 13.52 Mbit/s,能够满足现实应用的实时通信要求.

[关键词] 混沌映射,伪随机数字生成器,微控制单元,芯片上系统,机器到机器
[中图分类号]TN918;TP391　[文献标志码]A　[文章编号]1001-4616(2022)02-0098-08

A MCU-Based Color Image Encryption and Communication Scheme for Wireless Channel

Jia Xiaoxia[1],Xing Jinsheng[2]

(1.Department of Computer Science and Technology,Taiyuan University,Taiyuan 030000,China)
(2.College of Mathematics and Computer Science,Shanxi Normal University,Linfen 041081,China)

Abstract:In order to solve the security problem of color image communication in wireless channel,a real-time encryption and communication scheme for color images based on micro controller units(MCU) is proposed. The proposed cryptographic system is used to improve the randomness of the chaotic sequence,the image is encrypted through a pseudo-random number generator(PRNG) based on chaotic mapping and XOR operation,and the output of the embedded encryption system is sent through the RS-232 port. The proposed scheme was implemented on the PIC 16F873A microcontroller,and experiments were carried out on the wireless link. The results show that the proposed encryption scheme provides a high degree of security,can resist various known attacks,and has better security performance than classic encryption algorithms. In addition,the processing speed of the proposed PRNG with double floating point precision is 13.52 Mbit/s,which can meet the real-time communication requirements of practical applications.

Key words:chaotic map,PRNG,MCU,system on chip,machine to machine

随着智能化设备、通信技术和互联网协议的技术进步,使用电子设备或嵌入系统 ES,通过公共信道交换私密信息的服务和应用也呈指数增长[1]. 预计到 2025 年,使用嵌入系统的物联网(internet of things,IoT)设备全球数量将达到 1 000 亿台. 然而,威胁通信系统信息安全的攻击手段也在不断进化,必须确保信息传输的安全性[2]. 经典加密方案,例如数据加密标准(data encryption standard,DES),高级加密标准(advanced encryption standard,AES),国际数据加密算法(international data encryption algorithm,IDEA)等,在文本加密时性能较强,但由于数字图像加密中要区分的特征涉及的数据容量大,原始像素冗余性高,邻近像素关联性强,这些经典方案在数字图像加密中不能提供令人满意的安全性[3]. 且计算时间长,能耗高,不适用于数字图像的快速通信或实时加密[4].

混沌加密被视为保护机密信息的最安全方法之一,有着许多优秀属性,包括对初始条件的高敏感性和依

收稿日期:2021-08-20.
基金项目:山西省软科学基金资助项目(2011041033-03)、山西省高等学校教学改革创新项目(J2021779)、山西省教育科学“十四五”规划课题(GH-21403).
通讯作者:贾晓霞,讲师,研究方向:图像加密与通信. E-mail:jiaxiaoxia@tyu.edu.cn

赖性、行为不可预测性、遍历性、随机性、拓扑复杂性、对安全通信的高度适应性等[5]. 混沌映射已被广泛应用到数字图像加密中,与连续时间混沌系统相比,其运算量很小,需要的硬件资源也更少[6]. 经典混沌映射方法包括 Henon、Tinkerbell、Chen 和 Logistic 映射等. 当前,随着入侵手段越来越成熟,安全问题也逐渐复杂,这些方法的安全性已经不能满足通信要求[7]. 有必要开发新的嵌入式加密系统,提高安全性和效率[8].

文献[9]提出了基于 Josephus 问题和过滤扩散的图像加密方案,但其中至少需要两个加密轮,造成加密效率较低. 文献[10]提出了用于实时图像加密的一维混沌映射方案,该方案加密速度较快,能够满足实时处理要求,但该加密方案的随机性不足,容易被破解. 文献[11]提出了基于混沌 logsitic 映射,结合 Haar 小波变换和 AES 的图像加密方法. 文献[12]提出了基于 DNA 编码和超混沌算法的图像加密方案,利用 SHA-3 算法计算明文图像哈希值作为超混沌系统初始值并进行 DNA 序列运算,然后利用超混沌系统进行图像置乱. 文献[13]提出了超混沌系统与 AES 结合的图像加密算法,通过混沌序列产生每轮加密中的 S 盒和轮密钥,改善了密钥随机性. 文献[14]提出的图像加密技术中结合了 4 种不同加密算法(DNA-RSA-DES-Chebyshev,DRDC). 但对于嵌入式系统或 MCU 来说,这些算法的计算负荷过大.

本文针对无线链路上的图像传输安全问题,设计了适用于低功耗设备的图像加密方案,使用 MCU 构建基于混沌映射的 PRNG,加强了输入混沌序列的随机性,仅利用单个混沌映射算法就能够确保彩色图像的传输安全性,显著提高了处理速度. 大量安全分析证明所提方案具有密钥空间大,加密图像的像素相关性低,传输过程中保密信息无损失的优点,且处理速度显著优于 AES 等经典加密方法.

1 基于混沌映射的密码系统

所提密码系统基于简单的对称密钥流编码[15],通过加密运算,利用密文字符串 $S=\{s_1,s_2,\cdots,s_n\}$ 对包含 n 个元素的消息 $M=\{m_1,m_2,\cdots,m_n\}$ 进行加密. 为提高加密方法安全性,S 编码的序列中必须包含唯一随机元素,利用混沌映射,设计了混沌发生器,以生成用于密文序列的伪随机序列 $X,Y,\cdots,Z$. 本文实施的伪随机序列生成器如图 1 所示.

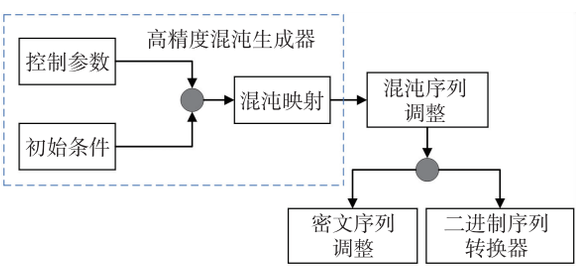


图 1 伪随机序列生成器

Fig. 1 Pseudo random sequence generator

1.1 系统实施

在 SOC Raspberry Pi 3 上实施伪随机序列生成系统,其中包含 3 个基本实体:控制参数,初始条件和混沌映射. 混沌映射相关的每个状态 $X=\{x_0,x_1,\cdots,x_n\},\cdots,Z=\{z_0,z_1,\cdots,z_n\}$,对应于一个浮点元素的伪随机序列.

混沌映射的动态行为具有离散性和复杂性,适合在加密算法中实施. 本文在所提密码系统中测试了 3 个经典混沌算法,即 Henon、Tinkerbell 和 Chen 混沌映射[16].

Henon 混沌映射可表示为:

$$\begin{aligned} x_{n+1}&=y_n+1-ax_n^2,\\ y_{n+1}&=bx_n, \end{aligned} \tag{1}$$

其动态性取决于两个参数,$x_0=0.10$,$y_0=0.15$.

Tinkerbell 混沌映射可表示为:

$$\begin{aligned} x_{n+1}&=x_n^2-y_n^2+ax_n+bx_n,\\ y_{n+1}&=2x_ny_n+cx_n+dy_n, \end{aligned} \tag{2}$$

式中,$a=0.9$,$b=-0.6013$,$c=2$,$d=0.5$.

Chen 超混沌映射可表示为:

$$\begin{aligned} x_{n+1}&=1-a(x_n^2+y_n^2),\\ y_{n+1}&=2-abx_ny_n, \end{aligned} \tag{3}$$

式中,$a=1.95$,$b=1$,初始条件 $x_0=0.025$,$y_0=0.025$.

1.2　位伪随机序列生成器

基于图 1,且仅考虑混沌映射的输出状态 X,通过所提高精度混沌发生器实体生成预定义数值精度的元素,其后通过"混沌序列调整"得到整数元素序列 $D=\{d_0,d_1,\cdots,d_{k-1}\}$. 将得到的 D 序列输入二进制序列转换器,得到序列 $B=\{\{b_{0,0},b_{0,1},\cdots,b_{0,nb}\},\{b_{1,0},b_{1,1},\cdots,b_{1,nb}\},\cdots,\{b_{k-1,0},b_{k-1,1},\cdots,b_{k-1,nb}\}\}$,如图 2 所示. 将 nd 定义为每个元素 d_n 包含的位数(通过将元素转换为位序列得到),将高精度混沌序列的每个 x_n 数据与 1×10^{np} 相乘,以得到整数 dn,代表最大 $nd=np+1$ 的整数位数. 子实体"二进制序列转换器"中的每个元素得出的位序列的最大长度为 $nb=\log_2(1\times10^{nd})+1$(包括符号位),其中 n 为十进制整数.

1.3　数字图像加密

使用所提密码系统进行数字图像加密的程序如图 3 所示. 针对数字图像加密,遵循 IEEE 754 标准,利用 32 位浮点计算得到混沌序列,再将其映射为 8 位二进制序列. 所提加密程序中,将混沌序列与常数 1×10^6 相乘,以得到 32 位整数,其后使用 mod 255 函数将其转换为 8 位格式的二进制序列. 使用二进制序列,通过 XOR 操作对数字图像进行加密,由此提升混沌信号的随机性.

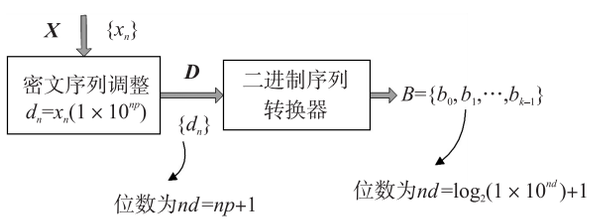


图 2　生成位伪随机序列的程序

Fig. 2　Program for generating bit pseudo-random sequence

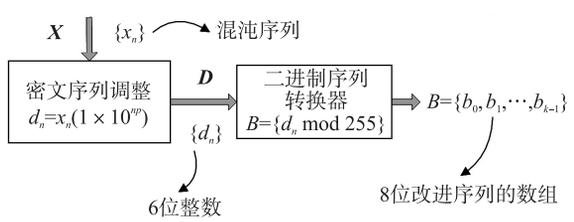


图 3　混沌序列改进方法

Fig. 3　Improved method of chaotic sequence

1.4　基于 MCU 的 PRNG

基于 MCU PIC 16F873A 的电路区块方案如图 4 所示,以生成混沌序列. MCU 执行混沌映射以生成伪随机数(PRNG). 为观察并验证生成混沌序列的行为,通过 DAC MCP4929 对序列进行数模转换.

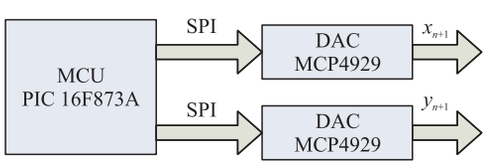


图 4　PRNG 框图

Fig. 4　Block diagram of PRNG

2　加密图像的无线通信方案

当前的芯片系统(SOC)通常包含作为实时中央处理单元的微处理器或微控制器,RAM 和 FLASH 存储器,以及一些通信端口,例如 RS-232、USB、蓝牙,WiFi 等. 其中嵌入了时钟振荡器,用于内部操作和能量子系统的同步化. 为保障运行和信息管理,应使用通信协议防火墙,通过无线信道(例如 Zigbee,Wifi 等)发送信息. 所提方案的功能模块如图 5 所示.

使用 RF 发射器(例如 ZigBee 或 Wifi 模块),通过 RS-232 端口发送嵌入式加密系统的输出. 在接收器中执行与加密相反的操作. 通过 Zigbee 标准将 3 个 MCU PIC16F877A 连接在一起,分别代表 M2M 方案中的发射器、接收器和入侵者. 使用 XCTU 软件完成 Zigbee 发射器的设置. 无线通信参数配置为:Baud = 115200,FlowControl = NONE,DataBits = 8,Parity = NONE,StopBits = 1. 调制解调器参数配置为:PAN ID, Destination Address High, Destination Address Low(Serial Number Low). 假设入侵者可连接到 Zigbee 信道,并尝试提取保密信息. 要加密数字图像时,通过 MCU 的 RS-232/USB 串口接收. 在接收器侧,执行与加密相反程序,恢复通过 RS-232/USB 串口发送到 PC 的保密信息.

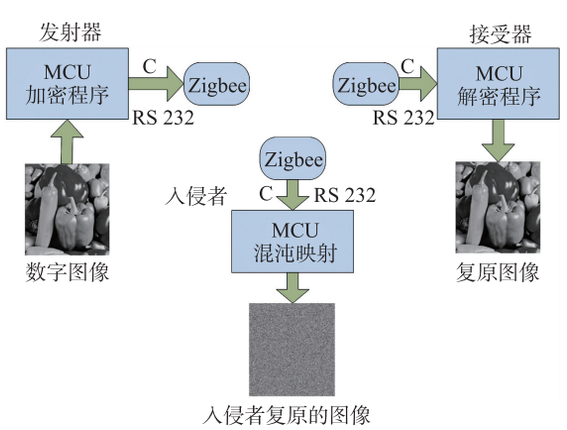


图 5　本文方案的各个模块

Fig. 5　Each module of this scheme

为实施所提方案,使用以 C 语言编码的中央设备 MCU PIC 16F873A,执行混沌映射,生成 PRNG. 其

后,MCU 使用本文所提密码系统,通过 XOR 操作对数字图像进行加密.

本文图像加密程序中,将混沌序列与常数 1×10^6 相乘,以得到 32 位整数,其后使用 mod 255 函数将其转换为 8 位格式的二进制序列. 使用二进制序列,通过 XOR 操作对数字图像进行加密,由此提升混沌信号的随机性. 如下算法给出了通过 MCU 对保密信息进行加密和传输的主要过程. 在接收器中执行相反操作.

算法:本文无线通信中的图像加密算法

输入:混沌映射的条件、变量,以及无线通信参数和调制解调器参数;

输出:Zigbee 信道发送出的加密信息;

1 初始化 混沌映射的条件和变量(针对不同的混沌映射会有不同的条件初始化,见式(1)、式(2)、式(3);

2 初始化 参数(无线通信参数和调制解调器参数配置);

3 计算混沌序列;

4 通过(1×10^6)调整混沌序列,得到 x_{adj};

5 使用 mod(x_{adj},255)改进混沌数据,并转换为二进制;

6 读取数字图像;

7 在混沌二进制数据和数字图像的每个像素之间执行 XOR 操作;

8 通过 Zigbee 信道发送加密结果.

3 实验结果与分析

本节将通过安全分析,检验所提方案的稳健性、统计特征和安全性等.

3.1 密钥空间

密钥空间是在加密或解密程序中使用的不同密钥总数量. 有效安全的密码系统的密钥空间应足够大,以抵御蛮力攻击. 所提密码系统的密钥包含两部分:(1)初始条件;(2)混沌映射参数. PRNG 的密钥必须包含超过 2 100 个可能密钥,以抵御穷举攻击. 本文使用 IEEE 754 标准的单精度和双精度浮点数计算分别实施了 3 个混沌映射,将混沌序列临时保存在 32 位和 64 位存储寄存器中. 所提嵌入式密码系统使用不同混沌映射时的密钥空间如表 1 所示. 从中可发现,所有混沌映射均满足最小密钥空间标准,证明本文方案可以抵御蛮力攻击.

表 1 密钥空间大小

Table 1 Space size of key

混沌映射	单精度	双精度
改进 Henon	2^{128}	2^{256}
改进 Tinkerbell	2^{192}	2^{384}
改进 Chen	2^{128}	2^{256}

3.2 统计检验

利用 NIST SP800-22 统计检验套件,应用到不同混沌映射生成的二进制序列的比较结果如表 2 所示. 所有测试中,序列流包含 100 个序列,序列流长度为 1 000 000 位. 测试中,使用的决策规则为 1%水平,即 $\alpha=0.01$. 若计算出的 P 值大于等于 α,则可认为该序列是随机的,且置信度为 99%. 否则,可认为该序列是非随机的,置信度为 99%. 此外,若成功率大于 0.96,则可认为该序列通过了 NIST 检验,证明该序列是随机序列. 表 2 中可发现,除了块内最长连续“1”测试之外,应用本文方案的混沌序列成功通过其他 NIST 测试.

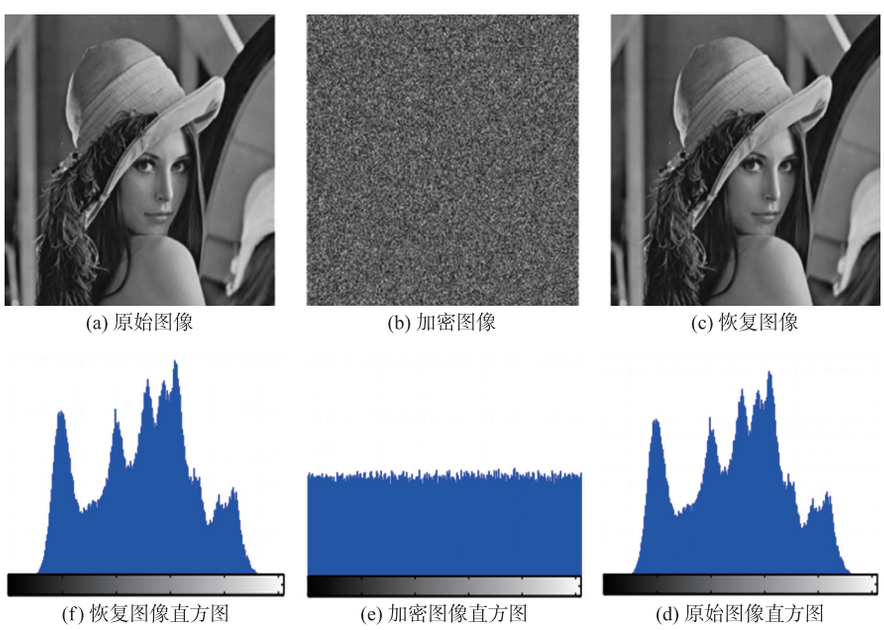
3.3 直方图分析

为执行数字图像直方图上的统计分析测试,使用 Lena 512×512 灰度图像. 选择改进 Tinkerbell 混沌映射的 x_1 状态执行信息加密,并给出直方图分析. 图 6(a)是原始图像,相应直方图如图 6(d)所示. 加密图像如图 6(b)所示,可发现该图像对于入侵者毫无价值. 图 6(e)给出了加密图像的相应直方图,从中可发现信息在 0 到 255 灰度等级的整个范围上分布,即以随机数据的形式均匀分布,由此证明所提密码系统可以很好地抵御统计攻击. Lena 的恢复图像如图 6(c)所示,可发现与原始图像相同,证明在加密和无线通信过程中没有信息损失. 最后,恢复图像的直方图如图 6(f)所示,从中可发现与图 6(d)的原始图像直方图基本相同,这证明了没有保密信息损失.

表 2　所提方案的 NIST 统计分析结果

Table 2　NIST statistical analysis results of the proposed scheme

统计检验	成功率					
	改进 Tinkerbell		改进 Chen		改进 Henon	
频率	0.98	0.98	0.99	0.99	0.99	0.99
块内频率	0.99	0.99	0.99	0.99	0.99	1.00
累积和-前向	0.98	0.99	0.98	0.98	0.98	1.00
累积和-逆向	0.99	0.98	0.99	0.99	0.98	1.00
游程	0.99	0.98	0.97	0.98	0.95	0.96
块内最长连续“1”	0.94	0.94	0.96	0.96	0.94	0.90
二元矩阵秩	0.99	0.97	0.99	1.00	1.00	0.98
离散傅里叶变换	0.99	0.98	0.98	0.98	0.98	0.99
非重叠模板匹配	1.00	0.98	0.97	0.99	0.98	0.99
重叠模板匹配	0.98	0.99	0.98	0.98	0.97	0.97
全局通用	0.96	0.99	1.00	0.98	0.96	1.00
近似熵	0.96	0.97	0.99	0.96	0.96	0.96
随机偏移	0.97	0.99	0.99	0.97	0.97	0.98
随机偏移变量	0.98	0.98	0.97	0.98	0.99	0.99
线性复杂度	0.99	1.00	0.99	0.98	0.98	0.99
串行(2m∇)	0.98	0.99	0.98	0.99	0.97	0.96
均值	0.98	0.98	0.98	0.98	0.98	0.97



(a) 原始图像　(b) 加密图像　(c) 恢复图像

(f) 恢复图像直方图　(e) 加密图像直方图　(d) 原始图像直方图

图 6　加密数字图像 Lena 的直方图分析

Fig. 6　Histogram analysis of encrypted digital image lena

3.4　相邻像素相关性分析

通过加密图像中相邻像素的相关性检验[17],分析加密程序设计的扩散和混淆性能. 随机选择要分析的数字图像(原始或加密)的 5 000 对像素(x_i,y_i),然后计算相应的相关系数 r_{xy}:

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{4}$$

式中,

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)), \tag{5}$$

式中,$\operatorname{cov}(x,y)$为协方差,$D(x)$为方差,x 和 y 表示数字图像中灰度等级的标度值. 使用以下离散形式:

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i, \tag{6}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x)),\tag{7}$$

式中,$E(x)$为像素平均灰度等级.

原始 Lena 图像和通过改进 Henon 混沌映射的 x_1 状态进行加密的图像的 5 000 对相邻像素在水平、垂直和对角方向的相关性分布如图 7 所示. 其中,图 7(a)是原始图像的相邻像素相关性分布图,可发现相邻像素是高度相关的,像素值与邻近像素值接近,且大多集中在对角线两边的区域. 图 7(b)给出了加密图像的像素相关性,可发现邻近像素的相关性完全不同,无明显像素堆积情况或明显的空白区域,平面上可观察到非常大的离散性.

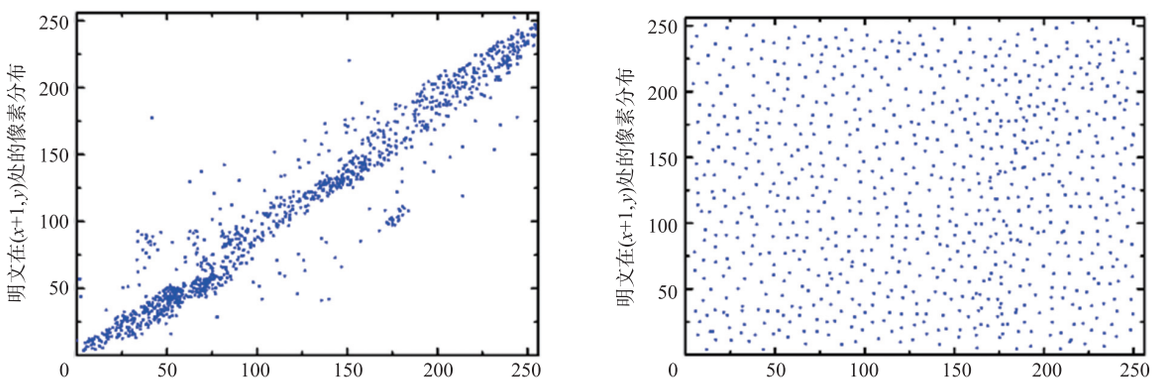


图 7　原始图像和加密图像中的邻近像素相关性

Fig. 7　Correlation between adjacent pixels in original image and encrypted image

相关系数 r_{xy} 值如表 3 所示,可发现原始图像相关系数接近 1,即相邻像素非常相似. 加密图像的理想相关系数应等于 0,可发现大部分情况下相关系数接近 0. S-box、AES 和 DRDC 与 0 差距较大,证明这些方法不能很好地完成图像加密.

表 3　邻近像素的相关系数

Table 3　Correlation cofficient of adjacent pixels

混沌映射	原始图像 256×256	加密图像 256×256	原始图像 512×512	加密图像 512×512	混沌映射	原始图像 256×256	加密图像 256×256	原始图像 512×512	加密图像 512×512
	0.9252	0.0195	0.9766	−0.0017		0.9252	0.3210	0.9766	0.2601
改进 Henon	0.9679	0.0110	0.9833	0.0222	S-box	0.9679	0.1984	0.9833	0.1725
	0.9047	−0.0189	0.9974	0.0038		0.9047	0.2920	0.9974	0.2666
	0.9252	0.0022	0.9766	−0.0029		0.9252	0.5177	0.9766	0.4835
改进 Tinkerbell	0.9679	−0.0097	0.9833	−0.0399	AES	0.9679	0.4922	0.9833	0.4765
	0.9047	−0.0171	0.9974	−0.0071		0.9047	0.3849	0.9974	0.3325
	0.9252	−0.0222	0.9766	0.0081		0.9252	0.1800	0.9766	0.1394
改进 Chen	0.9679	−0.0177	0.9833	−0.0059	DRDC	0.9679	0.2937	0.9833	0.2108
	0.9047	0.0201	0.9974	−0.0088		0.9047	0.3757	0.9974	0.1877

原始图像和加密图像之间得到的相关系数 r 如表 4 所示. 可发现大部分情况下,相关系数 r 非常接近 0,表明原始图像和加密图像之间不相似. 这也表明所提方法适用于任何图像大小.

表 4　相关系数 r

Table 4　Correlation coefficient r

混沌映射	Lena 256×256	Lena512×512
改进 Henon	−0.0027	−0.0008
改进 Tinkerbell	0.0035	0.0023
改进 Chen	0.0011	0.0042

3.5　信息熵分析

信息熵是测量数据随机性的指标[18],也用于评估加密安全性,计算如下:

$$H(s)=\sum_{i=0}^{2^{N-1}}P(s_i)\cdot\log_2\left(\frac{1}{P(s_i)}\right)\text{bit},\tag{8}$$

式中,$P(s_i)$表示 s_i 符号的概率. 对于以相同概率给出 $2N$ 个符号的纯随机源,熵 $H(s)=N$,即对于完全随机像素组成的 8 位图像,熵的理想值为 $H(s)=8$ bit. 对于数字图像加密,理想熵值为 8. 加密系统发出的符号(密文)的熵值低于 8,则存在一定程度的可预测性,存在安全隐患. 使用 8 位格式 Lena 图像,使用的 5 个混沌映射与其他方法得出的熵值比较如表 5 所示. 从中可发现,熵值不受图像大小影响,且各方法性能接近. 此外,经典加密算法 AES 的熵值与 8 差距较大,有一定程度可预测性,存在风险. 证明其不适用于图像加密.

表 5　密文图像的熵值比较

Table 5　Entropy comparison of ciphertext images

混沌映射	256×256	512×512
改进 Henon	7.998 0	7.999 1
改进 Tinkerbell	7.997 2	7.999 3
改进 Chen	7.998 0	7.998 2
S-box	7.983 2	7.956 7
DRDC	7.997 3	7.982 0
AES	7.795 0	7.858 0

3.6　NPCR 差分攻击

为执行差分攻击,使用两个常用指标,NPCR 和 UACI. 其用于测量整个加密布局中像素变化的影响. 使用 512×512 的 Lena 灰度图像,接收器的加密密钥 x_1 有着 1^{-10}的差异,得到两个有着细微差异的密文 C_1 和 C_2. NPCR 检验结果如表 6 所示,从中可发现,所提方案在使用 3 种混沌映射时,均通过了 NPCR 差分攻击检验. 经典 S 盒和 AES 加密算法通过了 NPCR 检验,但 DRDC 加密算法未通过检验. 证明本文方案有效改善了输入混沌序列的随机性,提高了加密图像的安全性. 使用双浮点精度 PRNG 的处理速度为 13.52 Mbit/s,如表 7 所示,结果证明所提方案适用于现实应用和电信设备.

表 6　NPCR 检验结果

Table 6　Test results of NPCR

加密图像大小 512×512		NPCR 关键值		
方法	NPCR/%	$N_{0.05}=99.589\ 3\%$	$N_{0.01}=99.581\ 0\%$	$N_{0.001}=99.571\ 7\%$
改进 Henon	99.812 3	通过	通过	通过
改进 Tinkerbell	99.783 5	通过	通过	通过
改进 Chen	99.807 5	通过	通过	通过
S-box	99.664 7	通过	通过	通过
AES	99.659 0	通过	通过	通过
DRDC	98.591 5	未通过	未通过	未通过

表 7　处理速度(Mbit/s)比较

Table 7　Comparison of processing speed(Mbit/s)

方法	CPU 频率	软件	双精度
改进 Henon	2.7	Python 3.5.2	13.520 0
改进 Tinkerbell	2.7	Python 3.5.2	9.180 8
改进 Chen	2.7	Python 3.5.2	12.776 7
DES	2.8	Crypto+Library	6.448 5
AES(192 位密钥)	2.8	Crypto+Library	11.687 9
AES(256 位密钥)	2.8	Crypto+Library	10.258 8

4　结论

本文提出了无线链路上彩色图像实时加密传输方案,其中通过在 MCU 上实施的 PRNG,提高了输入混沌序列的随机性,增强了无线信道上传输的彩色图像的安全性. 使用单个混沌映射方法和 XOR 操作完成图像加密,显著降低了计算量和处理时间,支持彩色图像在 M2M 链路上的实时通信. 在 PIC 微控制器上的仿真和实验结果表明,所提方案在使用不同的混沌映射算法时,均能够提供彩色图像加密所需的安全性,抵御各种已知攻击,顺利通过了 NPCR 和 UACI 差分攻击检验,且处理速度能够满足 M2M 和 IoT 环境中低功耗设备的加密图像实时传输要求.

[参考文献]

[1] MORABITO R,PETROLO R,LOSCRI V,et al. LEGIoT:A lightweight edge gateway for the Internet of Things[J]. Future generation computer systems,2018,81(1):1-15.

[2] ELHOSENY M,SHANKAR K,LAKSHMANAPRABU S K,et al. Hybrid optimization with cryptography encryption for medical image security in Internet of Things[J]. Neural computing and applications,2020,32(15):10979-10993.
[3] 宫帅,霍橙,谢冬. 基于压缩感知和 DNA 编码的图像加密算法[J]. 南京师范大学学报(工程技术版),2021,21(1):8-14.
[4] SHAH A A,PARAH S A,RASHID M,et al. Efficient image encryption scheme based on generalized logistic map for real time image processing[J]. Journal of real-time image processing,2020,17(6):2139-2151.
[5] 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.
[6] 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.
[7] ÖZKAYNAK F. Brief review on application of nonlinear dynamics in image encryption[J]. Nonlinear dynamics,2018,92(2):305-313.
[8] RAJAGOPALAN S,JANAKIRAMAN S,RENGARAJAN A. Medical image encryption:microcontroller and fpga perspective[M]. Medical Data Security for Bioengineers. IGI Global,Hershey,Pennsylvania,USA,2019:278-304.
[9] HUA Z,XU B,JIN F,et al. Image encryption using Josephus problem and filtering diffusion[J]. IEEE access,2019,7(1):8660-8674.
[10] TALHAOUI M Z,WANG X,TALHAOUI A. A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme[J]. The visual computer,2021,37(7):1757-1768.
[11] SHAKIR H R. An image encryption method based on selective AES coding of wavelet transform and chaotic pixel shuffling[J]. Multimedia tools and applications,2019,78(18):26073-26087.
[12] 张勋才,刘奕杉,崔光照. 基于 DNA 编码和超混沌系统的图像加密算法[J]. 计算机应用研究,2019,36(4):1139-1143.
[13] 王勇,方小强,王瑛. 超混沌系统和 AES 结合的图像加密算法[J]. 计算机工程与应用,2019,55(8):164-170.
[14] MANIYATH S R,THANIKAISELVAN V. A novel efficient multiple encryption algorithm for real time images[J]. International journal of electrical and computer engineering,2020,10(2):1327-1336.
[15] SIDDAVAATAM P,SEDAGHAT R. A novel architecture with scalable security having expandable computational complexity for stream ciphers[J]. Facta universitatis,series:electronics and energetics,2017,30(4):459-475.
[16] De la FRAGA L G,MANCILLAS L C,TLELO C E. Designing an authenticated Hash function with a 2D chaotic map[J]. Nonlinear dynamics,2021,104(1):4569-4580.
[17] INZUNZA G E,CRUZ HC. Double hyperchaotic encryption for security in biometric systems[J]. Nonlinear dynamics and systems theory,2013,13(1):55-68.
[18] 屈凌峰,陈帆,和红杰,等. 基于位平面-块置乱的图像加密算法安全性分析[J]. 应用科学学报,2019,37(5):631-642.

[责任编辑:陆炳新]