基于混沌浮点运算的医学图像加密方法与FPGA实现*

庞　宇[1]，魏　东[1]，王俊超[2]
（1.重庆邮电大学 光电信息感测与信息传输实验室 重庆 400065；2.重庆大学 微电子与通信工程学院，重庆 400044）

摘　要： 针对医学图像数据在互联网传输中的高机密性需求，提出一种基于Logistic混沌浮点数运算的加密方法用于医学图像加密。在该加密方法中，结合双精度浮点运算设计了基于Logistic混沌的伪随机数序列发生器（PRNG），并采用硬件描述语言Verilog对PRNG进行了硬件描述。在Altera公司Cyclone IV系列DE2-115开发平台上实现了加密方法综合设计。从密钥敏感性测试、直方图分析、相关性检验、信息熵处理等密码学角度分析了加密算法的安全性。通过将文中提出的图像加密算法与现有的一些图像加密算法进行比较，发现经过该加密算法加密后图像具有对密钥敏感、相关系数小、信息熵高等特点。此外，基于FPGA的硬件加密系统加密稳定性高，实时性好。

关键词： 图像加密；混沌映射；浮点数运算；PRNG；FPGA
中图分类号： TP309　　**文献标志码：** A　　**DOI：** 10.16157/j.issn.0258-7998.222975

中文引用格式： 庞宇，魏东，王俊超. 基于混沌浮点运算的医学图像加密方法与FPGA实现[J]. 电子技术应用，2023，49(1)：135-140.
英文引用格式： Pang Yu，Wei Dong，Wang Junchao. A medical image encryption method based on chaos floating-point operation and its realization by FPGA[J]. Application of Electronic Technique，2023，49(1)：135-140.

A medical image encryption method based on chaos floating-point operation and its realization by FPGA

Pang Yu[1]，Wei Dong[1]，Wang Junchao[2]
(1.Photoelectronic Information Sensing and Transmission Technology Laboratory，Chongqing University of Posts and Telecommunications，Chongqing 400065，China；2.School of Microelectronics and Communication Engineering，Chongqing University，Chongqing 400044，China)

Abstract： Aiming at the high confidentiality requirement of medical image data transmission in the Internet, an encryption method based on Logistic chaotic floating point number operation is proposed for medical image encryption. In this encryption method, PRNG based on Logistic chaos was designed with double-precision floating-point operations and described by the Verilog . The comprehensive design of encryption method is realized on the development platform of Cyclone IV series DE2-115 of Altera Corporation. The security of encryption algorithm is analyzed from the cryptographic perspectives such as key sensitivity test, histogram analysis, correlation test, information entropy processing, etc. By comparing with some existing image encryption algorithms, it is found that the image encrypted by this encryption algorithm has the characteristics of being sensitive to keys, small correlation coefficient and high information entropy. In addition, the FPGA-based hardware encryption system has high encryption stability and good real-time performance.

Key words： image encryption；chaos map；floating point arithmetic；PRNG；FPGA

0　引言

目前，互联网技术的快速发展使电子医疗变得便捷可行和普遍流行。电子医疗提供了一种基于互联网系统的远程、在线就医技术。患者可以联系专家医生进行在线诊断。在线就医过程中，一些涉及患者隐私的医学图像数据需要通过互联网存储和传输，在此过程中可能会面临数据泄露问题。而数据加密是避免医学图像数据泄露、保护隐私的最佳方法。与普通图像相比，医学图像具有的冗余、数据量大、像素相关性大等特点[1-2]，使得类似于AES等传统的加密技术对医学图像这类特殊格式数据的加密效率低下[3]。医学图像加密算法不

* 基金项目：国家自然科学基金（6200010898）

仅需要很高的安全性，还需要可观的加密速度。

基于混沌算法的伪随机数生成器（Pseudo Random Number Generator，PRNG）生成的伪随机序列对初始值极度敏感、周期长、密钥空间大，与其他数据序列相比在安全性上具有明显的优势，用于医学图像加密具有很可观的加密效果[4]。除了算法严格性外，一种有效的加密系统实现技术可保证加密的速度得到提升。而硬件实现的方式在能够满足应用实时性的同时又可以防止运行算法的攻击[5]。现场可编程逻辑器件（Field -Programmable Gate Array，FPGA）以其高并行、可定制、能重构、低成本等特点十分适合于混沌加密算法的硬件实现[6]。

为了防止患者隐私问题的非法泄露，国内外研究者投入了大量的精力研究图像数据的安全性问题。文献[7]将EIGamal算法用于医学图像加密，有效解决了数据扩展问题，但是此类非对称加密算法运行非常耗时。文献[8]提出了基于定点混沌映射的伪随机比特生成方法，构造用于图像加密的随机序列发生器，但是加密精度较低。陈军等人[9]提出一种基于Lorenz映射和Logistic映射的图像分块加密算法，此类混沌级联的方式扩大了混沌密钥空间。文献[10]将患者身份信息水印嵌入到医学图像中，再结合Tent和Lü混沌映射对带水印图像数据进行加密，此种方法提高了医学图像隐秘性。文献[11]、[12]从加密混沌计算公式入手，引入余弦、正弦反馈，构建新的混沌系统并在低成本硬件上实现。文献[13]设计了一种基于超混沌映射的医学图像加密算法。通过超混沌映射Lorenz生成六组密钥序列，增加了算法的复杂性。并将图像数据进行位分解，对高位数据和低位数据分别加密，打破了像素内相关性。文献[14]提出了一种基于量化Logistic混沌映射的无线体域网医学图像加密方案，该方法以定点数为基础，设计了多种量化精度的混沌系统用于不同数据形式加密，做到了低功耗、轻量化加密。

为了解决上述算法在实际医学图像加密应用中存在的问题，本文提出一种基于Logistic映射浮点运算的伪随机序列生成方法用于加密医学图像从而达到提高加密强度的目的。考虑到加密实时性，在FPGA上实现加密系统。混沌映射在有效保证加密随机性的同时，浮点运算能显著提升加密精度，扩大密钥空间。并对硬件加密系统进行稳定性测试，以及对密图数据进行统计分析，验证了算法的有效性以及硬件加密系统的稳定性。

1 密码系统设计

将医学图像数据输入到加密系统中，与PRNG生成的伪随机数异或得到加密图像或原图数据。整个加密系统架构如图1所示，加密的关键在于PRNG的设计。

1.1 引入浮点运算的Logistic混沌系统

本文选择Logistic映射作为混沌序列迭代算法，该算法结构简单，随机性好。方程式定义如式(1)所示：

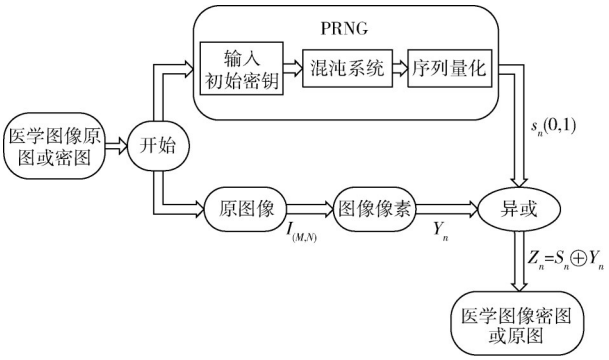


图1 加密系统框架图

$$X_{n+1}=\mu X_n(1-X_n) \tag{1}$$

式中，当控制参数$\mu\in[0,4]$，可保证迭代值$X_n\in[0,1]$。随着μ值增大，系统出现不同的动力学行为，越接近于4[15]，迭代值在[0,1]之内分布越均匀。

数字计算机使用二进制数来表示数字，对于实数，有定点和浮点两种表示格式。浮点格式较之定点格式有更为宽广的动态范围，可以不用考虑数据的溢出和量化问题，因而可以缩短复杂算法的研发周期，与混沌系统结合可扩大混沌序列空间。

IEEE-754标准定义了单精度(FP32)和双精度(FP64)两种浮点格式[16]，并将浮点数划分为符号位S、指数位E和尾数位F三部分，各部分位数如表1所示[17]。

表1 IEEE 754标准浮点格式

类型	符号	指数	尾数
单精度	1	8	23
双精度	1	11	52

在此文中设计了双精度浮点数运算迭代混沌序列可得到更高的精度。十进制μ和X_n用IEEE-754表示：

$$\mu=(-1)^{S_\mu}\times 2^{E_\mu-\mathrm{Bias}}\times(1.f_\mu) \tag{2}$$

$$X_n=(-1)^{S_x}\times 2^{E_x-\mathrm{Bias}}\times(1.f_x) \tag{3}$$

式(2)、式(3)中Bias为指数偏移量，十进制表示为：

$$\mathrm{Bias}=2^{E-1}-1 \tag{4}$$

则双精度指数偏移量为1 023。

混沌迭代过程涉及浮点数的减法和乘法运算模块，运算方程分别如下：

$$\mu-X_n=\begin{cases}(m_\mu-m_x\times 2^{Ex-E\mu})\times 2^{E\mu}, E_\mu>E_x\\(m_\mu\times 2^{E\mu-Ex}\pm m_x)\times 2^{Ex}, E_\mu\leqslant E_x\end{cases} \tag{5}$$

$$\mu\times X_n=(-1)^{s\mu\oplus sx}\times 2^{E\mu+Ex-2\mathrm{Bias}}\times(1.f_\mu\times 1.f_x) \tag{6}$$

其中：$m=(-1)^S\times(1.f)$。

1.2 PRNG

为生成高质量的加密密钥，提出一种基于浮点数的PRNG框架，如图2所示，包括初始密钥输入、浮点混沌系统、随机序列量化三大模块。

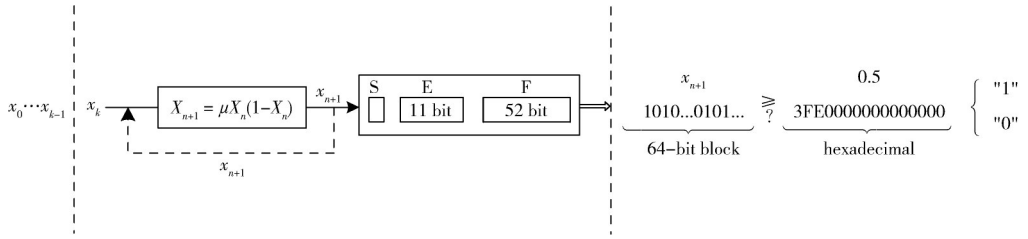


图 2　基于浮点数的 PRNG 框架

初始密钥 X_0 范围在(0,1)之间，双精度浮点格式表示在(0，3FF0000000000000)之间。浮点混沌系统首先接收初始密钥，利用 Logistic 混沌算法结合浮点运算迭代出浮点数格式的混沌伪随机序列 X_n。利用阈值量化法将混沌随机序列 X_n 量化为单比特数据 S_n(0,1)，具体量化方法是指将 X_n 与 3FF0000000000000 比较，若大于此值则将 X_n 量化为 1，否则为 0。这种量化方式可有效继承原有序列的相关特性，并且量化后的输出结果难以推断出最初的混沌序列，可以提高安全性。

2 FPGA 加解密架构

在本文，所提出的基于 FPGA 的加密系统流程如图 3 所示。整个硬件加密系统在 Altera 公司 Cyclone IV EP4CE115F29C7N 开发平台上设计、综合以及验证。加密系统的硬件资源使用情况如表 2 所示。初始密钥以及医学图像数据通过 UART 串口通信模块依次进行传输。使能 Load 以及复位后，初始密钥 key_loaded[63∶0]通过 Uart_rx 端口传输到 PRNG 模块。在 Logistic_Control 控制模块作用下 PRNG 迭代出用于加密的密钥 Xor_byte[7∶0]，再与医学图像数据 Image[7∶0]进行异或加密，得到密图数据 Enc_Image[7∶0]，并通过 Uart_tx 发送出密图数据到 PC。

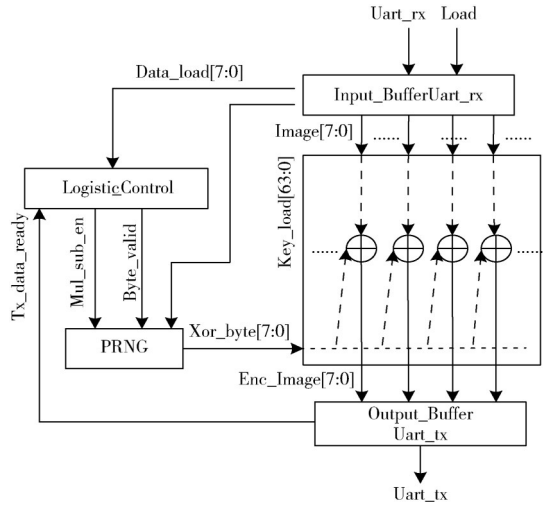


图 3　基于 FPGA 的加密系统流程图

表 2　FPGA 硬件资源使用

参数	值
Total logic elements(LE)	14 867/114 480(13%)
Total combinational function	14 834/114 480(13%)
Dedicated logic registers	431/114 480(<1%)
Embedded Multiplier 9-bit elements	0/532(0%)
Total memory bits	0/3,981,312(0%)
F Max	30.84 MHz

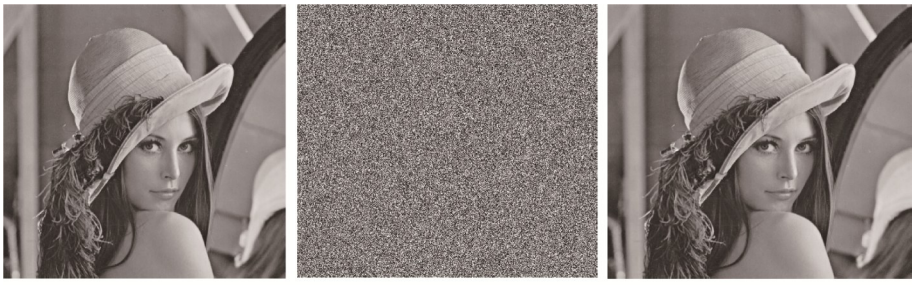
3 加密安全性分析

为了验证加密系统的可行性，用 512×512 的 Lena 灰色图像数据，在 Altera 公司 Cyclone IV EP4CE115F29C7N 开发平台上进行加、解密。设置加密系统参数 μ = 64′h4010000000000000(4.0)，

初始密钥 X_0 = 64′h3FB9999999999999A(0.1)。原图像、加密图像以及解密图像如图 4 所示。结果显示无法从密图中识别出任何原图像信息。解密图像能够恢复明文信息。

3.1 密钥敏感性分析

密钥敏感性表征了密码系统的安全性能。解密时，密钥微小变动便无法解密密文图像。为了检验加密系统的密钥敏感性能，对图像数据进行加密，研究在初始



(a) 明文图像　(b) 密文图像　(c) 解密图像

图 4　基于 FPGA 的 Logistic 混沌浮点加密过程

密钥上翻转一位，进行解密的效果。式(1)数据来源于将式(2)正确初始密钥数据尾数的第1 bit翻转。式(3)将式(2)正确初始密钥数据尾数最后1 bit翻转。分别将式(1)(2)(3)数据作为解密的初始密钥，对密图进行解密。解密效果如图5所示。结果表明密钥仅改变1 bit便不能正确解密，十分敏感。

3.2 统计分析

3.2.1 灰度直方图

图像的灰度直方图可以直观地显示每个灰度像素的统计特征[13]。从原图的灰度直方图可以很清晰看出图像像素值的统计特征。攻击者可以很轻易地从非均匀直方图中获取原图统计信息。而一种安全加密算法能够破坏原图像素值的统计关系，得到均匀分布的直方图，攻击者就难以从密图统计信息中获取原图相关信息。图6测试了几组原始图像以及基于本文算法加密后密图的灰度直方图。经过对比验证了图像经过加密系统加密后灰度值分布无规律可循，加密性能良好。

3.2.2 相邻像素点相关性分析

为了进一步分析图像加密的效果，定性分析了图像原图与经过加密系统加密后的密图的相邻像素值，如图6所示。图6表明原图的两个相邻像素间存在极高的相关性。密图的像素值分布杂乱，相关性较低。也可用相关系数定量分析图像相邻像素的相关性，相关系数的计算过程如下：

图5 初始密钥翻转1位解密过程

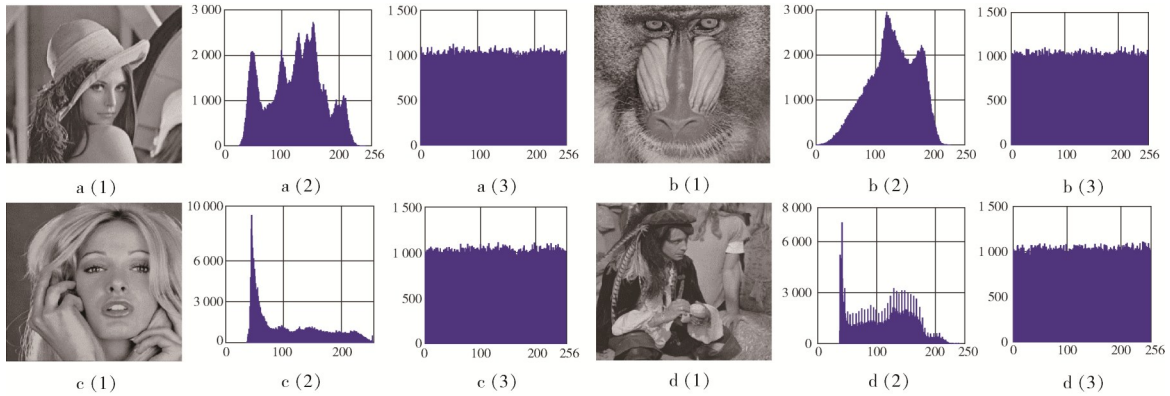


图6 各类图像加密前后灰度直方图

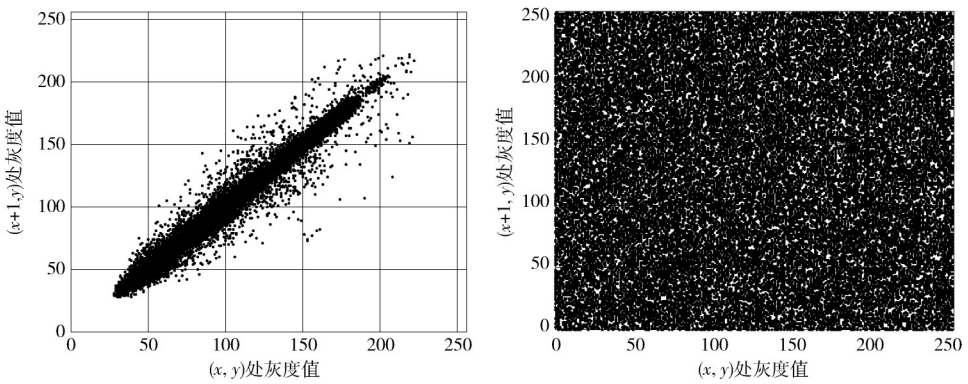


图 7　Lena 图像加密前后相邻像素值分布

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

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{8}$$

$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{9}$$

$$r_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

式中 x、y 是一对相邻像素值，$E(x)$ 是平均值，$D(x)$ 是平均方差，r_{xy} 代表相关系数，其值区间在[-1,1]之间。相关系数绝对值越低，加密效果越好。在表 3 中将 Lena 原始图像和经过本文算法加密后的图像从水平、垂直以及对角线三个方向上进行了相邻像素相关性系数计算，并与当前一些图像加密算法加密后相关系数计算结果进行了比较。可以看出图像加密前相关系数较高，接近于 1，加密后图像相关系数很低，接近于 0。

表 3　图像的相邻像素相关系数

文献	水平	垂直	对角线
本文	−0.009 8	0.004 4	−0.016 7
文献[2]	−0.020 7	−0.017 6	0.016 8
文献[11]	0.000 49	0.000 78	0.000 63
文献[12]	−0.008 2	−0.005 4	0.002 0

3.3 信息熵分析

信息熵反映了信息的不确定性。图像信息熵可以用来衡量加密后的图像的混乱程度，从而判断加密效果。信息熵的计算方法如下。

$$H_1=-\sum_{i=0}^{N-1}p_i\log_2 p_i \tag{11}$$

式中 p_i 表示 i 发生的概率，对于灰度为 256 的图像，信息熵越接近 8，则它越接近随机图像。经过计算，表 4 列出了本文 Lena 密图的信息熵以及一些经过最新的图像加密算法加密后的密图的信息熵的对比。结果表明，基于本文算法计算的信息熵优于其他算法的信息熵。本文算法加密后的图像能有效降低成功攻击的几率。

表 4　不同算法加密 Lena 后的信息熵

本文	文献[2]	文献[12]	文献[20]	文献[21]	文献[22]
7.999 3	7.988 8	7.998 7	7.999 3	7.991 6	7.993 1

4 结论

本文提出了将 Logistic 混沌浮点运算作为基本随机序列迭代算法用于图像加密。在 ED2-115 硬件平台上使用硬件描述语言 Verilog 设计了基于上述算法的图像数据加解密系统，包括双精度浮点数运算。以 Lena 标准测试图为例，对 FPGA 硬件系统加密后的 Lena 密图作安全性分析，实验验证了密图相邻像素相关性极低，信息熵达到 7.999 3，接近于一幅随机图像，优于当前一些加密算法。并且整个 FPGA 密码系统有较好的密钥敏感性以及系统稳定性。

参考文献

[1] CHEN J , CHEN L , ZHANG L Y , et al. Medical image cipher using hierarchical diffusion and non-sequential encryption[J]. Nonlinear Dynamics, 2019 ,96(1):301-322.

[2] NIU Y , ZHANG X , HAN F. Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database[J]. Computational Intelligence and Neuroscience,2017 , 69-77.

[3] 郭翰科, 张彦林, 黄源 . 数据加密技术在网络信息安全中的应用[J]. 计算机与网络, 2021, 47(2):1-8.

[4] 黄伟琦, 陈志刚, 梁涤青,等 . 基于多混沌系统的医学图像加密算法[C]//全国理论计算机科学学术年会, 2012: 261-263,299.

[5] KOTEL S, ZEGHID M, BAGANNE A, et al. FPGA-based real-time implementation of AES algorithm for video encryption, recent advances in telecommunications, informatics and educational technologies[C]// ResearchGate, Berlin, Germany, 2015(3):118-123.

[6] 谢红梅, 夏磊, 朱孟元,等 . 基于 Logistic 混沌映射的图像加密系统及 FPGA 实现[J]. 航空兵器, 2016(2):56-60.

[7] LAIPHRAKPAM D S, KHUMANTHEM M S. Medical

image encryption based on improved EIGamal encryption technique[J]. Optik, 2017, 147: 88 - 102.

[8] HASAN F S . FPGA hardware co-simulation of image encryption using stream cipher based on chaotic maps[J]. Sensing and Imaging An International Journal, 2020, 21(1):117-130.

[9] 陈军, 张向利, 张红梅. 基于Lorenz映射和Logistic映射的图像分块加密算法[J]. 桂林电子科技大学学报, 2019, 39(1): 6-15.

[10] ARUMUGHAM S , RAJAGOPALAN S , RAYAPPAN J , et al. Tamper-resistant secure medical image carrier: an IWT - SVD - Chaos - FPGA combination[J]. Arabian Journal for Science and Engineering, 2019, 44(11):9561-9580.

[11] MERAH L , ADNANE A , ALI-PACHA A , et al. Real-time implementation of a chaos based cryptosystem on low-cost hardware[J]. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 2021: 1-24.

[12] 李春彪, 赵云楠, 李雅宁,等. 基于正弦反馈Logistic混沌映射的图像加密算法及其FPGA实现[J]. 电子与信息学报, 2021, 43(12):9-18.

[13] 王倩. 基于位分解和超混沌映射的医学图像加密研究[J]. 计算机仿真, 2019, 36(1):5-10.

[14] JW A , KH A , SF A , et al. A logistic mapping-based encryption scheme for wireless body area networks[J]. Future Generation Computer Systems, 2020, 110:57-67.

[15] PENG Y X , SUN K H , HE S B. Dynamics analysis of chaotic maps: from the perspective on parameter estimation by meta-heuristic algorithm[J]. Chinese Physics B, 2020, 29(3):12-27.

[16] DAN Z , COWLISHAW M , AIKEN A , et al. IEEE Standard for Floating-Point Arithmetic[S]. IEEE Std 754-2008, 2008:1-70.

[17] 黄兆伟,王连明. 基于FPGA的可配置浮点向量乘法单元设计实现[J]. 计算机应用研究, 2020, 37(9):5-12.

[18] SETOODEH P, HAYKIN S. Robust transmit power control for cognitive radio[J]. Proceedings of the IEEE, 2009, 97(5): 915-939.

[19] FU X , LIU B , XIE Y Y , et al. Image encryption-then-transmission using DNA encryption algorithm and the double chaos[J]. IEEE Photonics Journal, 2018:1-10.

[20] FAN S , LI K , ZHANG Y , et al. A hybrid chaotic encryption scheme for wireless body area networks[J]. IEEE Access, 2020, 8:183411-183429.

[21] LI T , DU B , LIANG X . Image encryption algorithm based on logistic and two-dimensional lorenz[J]. IEEE Access, 2020, PP(99):1-10.

[22] XIANG H , LIU L . A random irregular blocking image encryption algorithm based on improved digital chaotic maps at bit level[J]. International Journal of Bifurcation and Chaos, 2022, 32(04):111-123.

（收稿日期:2022-05-15）

作者简介:

庞宇(1978-),男,博士,教授,主要研究方向:无线通信、集成电路设计数字医疗研究。

魏东(1997-),男,在读硕士,主要研究方向:数字混沌加密。

王俊超(1991-),男,博士,副教授,主要研究方向:集成电路设计数字医疗研究。

扫码下载电子文档

版权声明