基于混沌系统的伪随机数发生器设计

蔚艳文[1],李 震[1,2],李良荣[1]
(1.贵州大学 大数据与信息工程学院,贵州 贵阳 550025;2.贵州省公共大数据重点实验室,贵州 贵阳 550025)

摘 要:伪随机数发生器广泛应用于信息安全领域,基于超混沌 Lorenz 系统和斜帐篷映射提出一种伪随机数发生器。首先利用超混沌 Lorenz 系统迭代产生 4 路伪随机序列{S_1,S_2,S_3,S_4},并以每 8 位为一个分组;然后利用斜帐篷映射迭代产生 1 个伪随机序列 Ss 用于数据选择;最后通过 Ss 序列值选择{S_1,S_2,S_3,S_4}序列中的一个为该 8 位的输出,继而产生伪随机序列输出。设计方案的输出结果通过了 NIST 的 SP800-22 rev1a 的全部随机性检验,并用图像加密测试证明其具有良好的随机性。

关键词:伪随机数发生器;超混沌 Lorenz 系统;斜帐篷映射;NIST SP800-22 检测
中图分类号:TN918 **文献标识码**:A DOI:10.16157/j.issn.0258-7998.200596

中文引用格式:蔚艳文,李震,李良荣. 基于混沌系统的伪随机数发生器设计[J].电子技术应用,2020,46(10):114-117,122.
英文引用格式:Wei Yanwen,Li Zhen,Li Liangrong. Design of pseudo-random number generator based on chaotic system[J]. Application of Electronic Technique,2020,46(10):114-117,122.

Design of pseudo-random number generator based on chaotic system

Wei Yanwen[1],Li Zhen[1,2],Li Liangrong[1]
(1.College of Big Data and Information Engineering,Guizhou University,Guiyang 550025,China;
2.Guizhou Province Key Laboratory of Public Big Data,Guiyang 550025,China)

Abstract:Pseudo-random number generator is widely used in the field of information security. This paper proposes a pseudo-random number generator based on hyper-chaotic Lorenz system and skew tent mapping. In this scheme, four pseudo-random sequences{S_1,S_2,S_3,S_4} are generated iteratively by using the hyper-chaotic Lorenz system, and each 8 bits are grouped into groups. Then a pseudo-random sequence Ss is generated iteratively by skew tent mapping for data selection. Finally, one of the{S_1,S_2,S_3,S_4} sequences is selected by Ss sequence value, and then the pseudo-random sequence output is generated. The output result of this paper has passed all randomness test of SP800-22 rev1a of NIST, and it is proved to have good randomness by image encryption test.

Key words:pseudo-random number generator;hyper-chaotic Lorenz system;skew tent mapping;NIST SP800-22 testing

0 引言

伪随机数发生器作为理想信息源,有良好的统计特性和随机特性,广泛应用于信息安全领域。根据香农的一次一密理论[1],采用随机序列作为密钥加密信息是绝对安全,不可破译的。众所周知,真正随机序列在信息系统应用是不可能的,故而在密码学研究中常采用循环周期长且能通过随机数检验的伪随机数来代替真正的随机数。伪随机数发生器(PRNGs)统计检测标准由美国国家标准与技术研究院(NIST)公布,包括 FIPS140 检测、DIEHARD 检测和 SP800-22 检测等。

混沌[2]是动力学系统产生的一种及其复杂的类似噪声的运动行为,是确定的非线性系统中出现的内在随机性现象,表现出对系统初值和控制参数的高度敏感性和类随机行为。它具有如下特性:运动的遍历性、对初始状态和系统参数的高度敏感、正的 Lyapunov 指数、自相似性、运动轨道的长期不可预测性以及有界性等。ALIPOUR M C 等人[3]采用 Logistic 混沌映射用于生成 PRNGs 和两个突变阶段的种子值,以及用于扩散操作的 PRNGs。CHUGUNKOV I V 等人[4]提出了一类由非线性反馈移位寄存器组成的新序列。MURILLO-ESCOBAR M A 等人[5]利用提高的 Logistic 映射构造伪随机数发生器。Zhu Congxu 等人[6]提出了基于一维复合离散混沌系统 Logistic-Tent 映射的伪随机数发生器(PRNG)设计新方案。CHEN E 等人[7]通过构造了一个 8 维 DCSLE GCS 系统用于混沌伪随机数发生器的设计。TAHA M A 等人[8]设计和构建基于视网膜的伪随机数发生器,用于安全应用。Zhao Yi 等人[9]提出了一种基于超混沌系统的自扰伪随机序列发生器。曹艳艳等人[10]利用可变扰动参数迭代对 Logistic 混沌映射进行扰动随机动态分组。魏连锁等人[11]提出一种将云模型与广义三阶 Fibonacci 相结合

的混沌系统。朱淑芹等人[12]利用反正弦函数变换使构造的二次多项式混沌映射服从均匀分布设计出伪随机数发生器。朱和贵等人[13]提出一种复合一维 Sine 和 Tent 混沌映射的二维超混沌图像加密算法。陈飞等人[14]将一维整数动态帐篷映射模型拓展为二维整数动态帐篷映射模型，克服了一维模型均匀性较差的缺陷，其迭代生成序列具有良好的均匀分布特性及相互独立性，其密码学特性更加完善。曾珂等人[15]设计一种基于三维 Logistic-Sine 级联映射的图像混沌加密算法。李春虎等人[16]基于斜帐篷混沌映射和 Arnold 变换提出一种新的图像加密算法。汪彦等人[17]利用图像加密新算法来提高图像加密算法的加密安全性和抗攻击能力，在 Lorenz 混沌系统下进行了分析。RSSLER Q E[18]给出的超混沌方程是简单的四维(变量)振荡器模型，其系统能产生具有两个方向上双曲不稳定的超混沌吸引子。本文通过采用超混沌 Lorenz 系统对初值进行干扰并加以处理，将所生成的四组混沌序列通过数据选择器的选取，最终输出的即为较高性能的伪随机数。通过对混沌伪随机数生成器的性能分析，测试结果显示该伪随机数发生器符合设计要求。

1 相关混沌映射

1.1 Skew Tent 混沌映射

Skew Tent 映射是被广泛研究及应用的混沌映射，其产生混沌的非线性因素是二分段线性，迭代方程简单、序列发生器易于实现。

Skew Tent 映射的数学表达式[19]为：

$$t_{n+1}=\begin{cases}t_n/p, & t_n\in(0,p)\\(1-t_n)(1-p), & t_n\in[p,1)\end{cases} \tag{1}$$

其中 p 是斜帐篷系统的参数。当 $p\in(0,0.5)\cup(0.5,1)$，该系统可以产生混沌序列 $t_n\in(0,1)$。

1.2 超混沌 Lorenz 系统

美国气象学家 LORENZ E N 在研究对流实验的过程中发现了一个高维的动力学系统，并经傅里叶分解、简化后，得到一个三维非线性方程组，这一系统被称为 Lorenz 系统[20]。产生超混沌吸引子的必要条件：耗散结构，方程维数不少于四维，系统至少有两个增强不稳定因素方程且其至少有一个含非线性项。在该系统方程中引入非线性控制器 w，设 w 的变化率为 $\dot{w}=-yz+rw$，则产生的新系统[21]为：

$$\begin{cases}\dot{x}=a(y-x)\\\dot{y}=cx-x-xz\\\dot{z}=xy-bz\\\dot{w}=-yz+rw\end{cases} \tag{2}$$

应用计算微分方程组 Lyaponov 指数[22]谱的方法，得到当 $r=-1$ 时，系统(2)产生超混沌运动，对应的吸引子在各平面上的投影如图 1 所示。

2 伪随机数生成方式

伪随机数生成的流程图如图 2 所示。

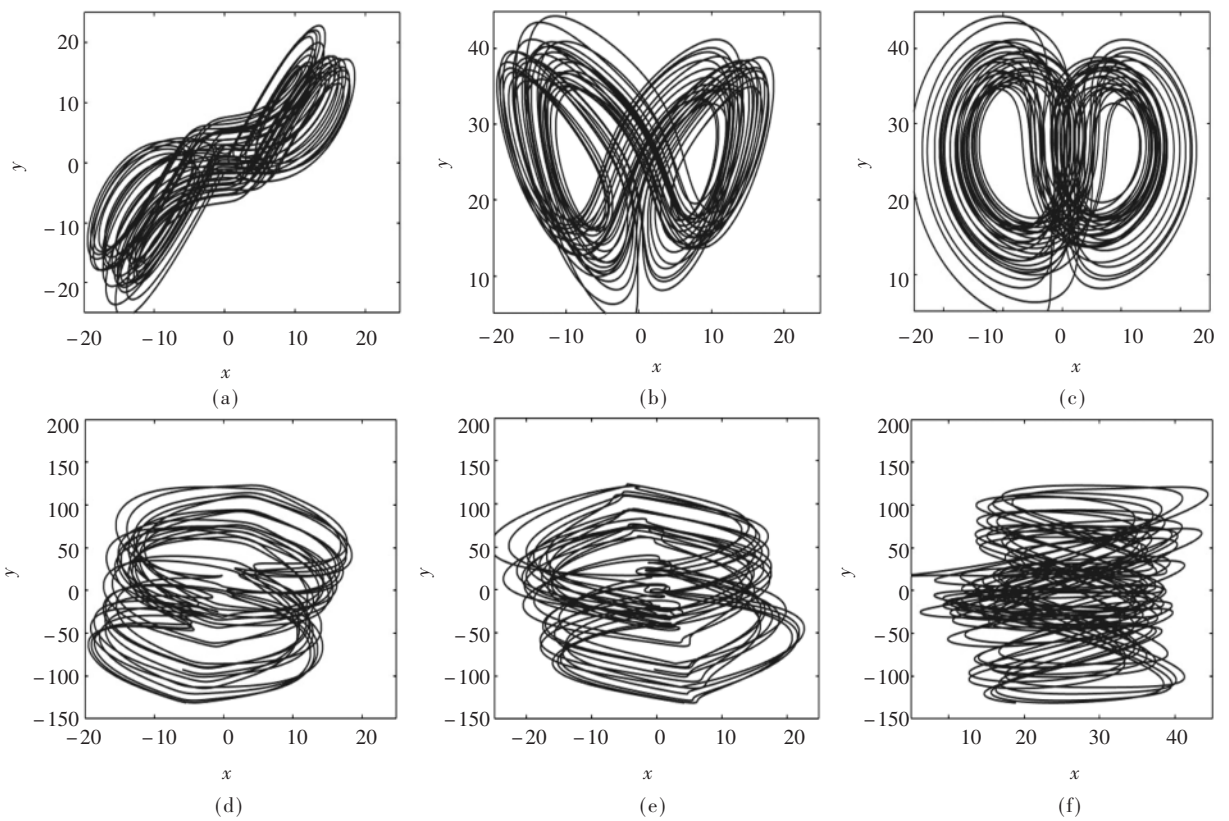


图 1 $r=-1$ 时，系统(2)的超混沌吸引子在各平面上的投影

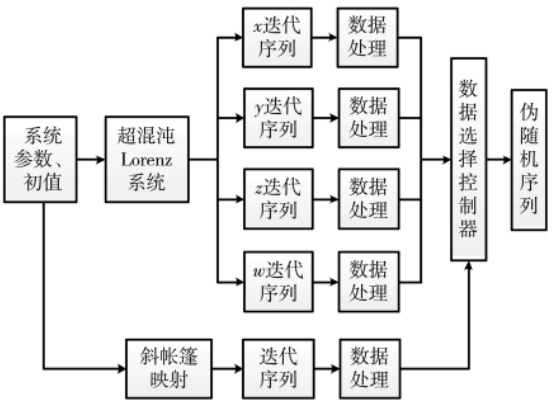


图 2 伪随机数生成的流程图

伪随机数生成步骤：

(1)对超混沌 Lorenz 映射采用四阶龙格-库塔算法[23]分别同时进行迭代，迭代 200 次后，依次得出 4 路迭代序列$\{S_1, S_2, S_3, S_4\}$；

(2)根据式(3)~式(6)：

$$S_{1_2}=\mathrm{mod}(\mathrm{floor}(S_{1_1}+100)\times 2^{16}, 256) \tag{3}$$

$$S_{2_2}=\mathrm{mod}(\mathrm{floor}(S_{2_1}+100)\times 2^{16}, 256) \tag{4}$$

$$S_{3_2}=\mathrm{mod}(\mathrm{floor}(S_{3_1}+100)\times 2^{16}, 256) \tag{5}$$

$$S_{4_2}=\mathrm{mod}(\mathrm{floor}(S_{4_1}+100)\times 2^{16}, 256) \tag{6}$$

经过相同的处理，以每 8 位为一个分组，得到处理后的 4 路序列；

(3)利用斜帐篷映射 Skew Tent 映射迭代 200 次，产生 1 个伪随机序列 S_s；

(4)将(3)中产生的迭代序列进行处理：

$$S_{s_2}=\mathrm{mod}(\mathrm{fix}(S_{s_1}\times 8^8), 4) \tag{7}$$

(5)通过(4)产生的序列值选择(2)序列中的一个为该 8 位的输出，继而产生伪随机序列输出。

3 混沌伪随机数发生器的性能分析

3.1 NIST 随机性检测

关于伪随机序列的检测，现有几种代表性检测标准，如美国国家标准技术研究所(National Institute of Standards and Technology，NIST)制定的 FIPS 140-2 标准和 SP800-22 标准[24]，Marsaglia 的 Diehard Battery 检测等。本文采用 SP800-22 标准进行伪随机序列的检测。SP800-22 从多角度检验是否满足随机序列的性能，包含 15 个大项，188 个小项测试。每个二进制序列测试指标都会给出一个测试结果 P-value 值，设定阈值 α，如果 P-value 大于 α，表明测试序列随机性可信度为 $1-\alpha$，序列通过了该项检测指标的随机性测试；反之，说明没有通过测试。对所获得的伪随机序列进行 NIST SP800-22 测试($\alpha=0.01$)，得到如表 1 所示的 NIST SP800-22 测试结果表。

表 1 NIST SP800-22 测试结果表

测试项	P-value	测试结果
单比特	0.255 96	通过
块内频率	0.550 6	通过
游程	0.106 37	通过
最长游程	0.022 709	通过
二进制矩阵秩	0.040 77	通过
离散傅里叶谱	0.039 365	通过
非重叠模板匹配	0.888 41	通过
重叠模板匹配	0.417 66	通过
Maurer 通用统计	0.274 05	通过
线性复杂度	0.992 29	通过
序列 *	0.357 871	通过
近似熵	0.528 91	通过
累加和	左游程 0.684 84 右游程 0.904 6	通过
随机旅行 *	0.704 096 6	通过
随机旅行变种 *	0.436 643 9	通过

注：用 * 标记的结果是平均值。

3.2 图像加密分析

由于混沌映射所具有的遍历性、随机性和对初值以及参数敏感等性质能够使得所生成的混沌序列具有良好的密码学性质，故利用所产生的伪随机数对图像进行加密。香农所提出的信息熵[25]是用于表征信源的不确定性程度，系统越有序，信息熵就越低；系统越混乱，信息熵就越高。即熵值越大，图像的随机性越强。8 bit 灰度图作为信源，可发出 2^8 种相同概率的不同状态，熵定义下 8 bit 灰度图的理想熵值为 8。为了验证上述算法的合理性以及有效性，图 3 中，图(a)是用于明文图像的标准8 bit 灰度图 Lena，图(b)是随机数与明文像素值进行异或后生成的密文图像，图(c)是原图像的直方图，图(d)是加密后图像的直方图。明文加密变换为具有均匀直方图的密文，原图像的统计规律被破坏，攻击者很难对原始图像进行恢复，这表明加密算法具有不错的密码学特性。本方案生成的随机数用于图像加密后，信息熵为 7.999 3，非常接近 8，表明该图像具有良好的随机性。

4 结论

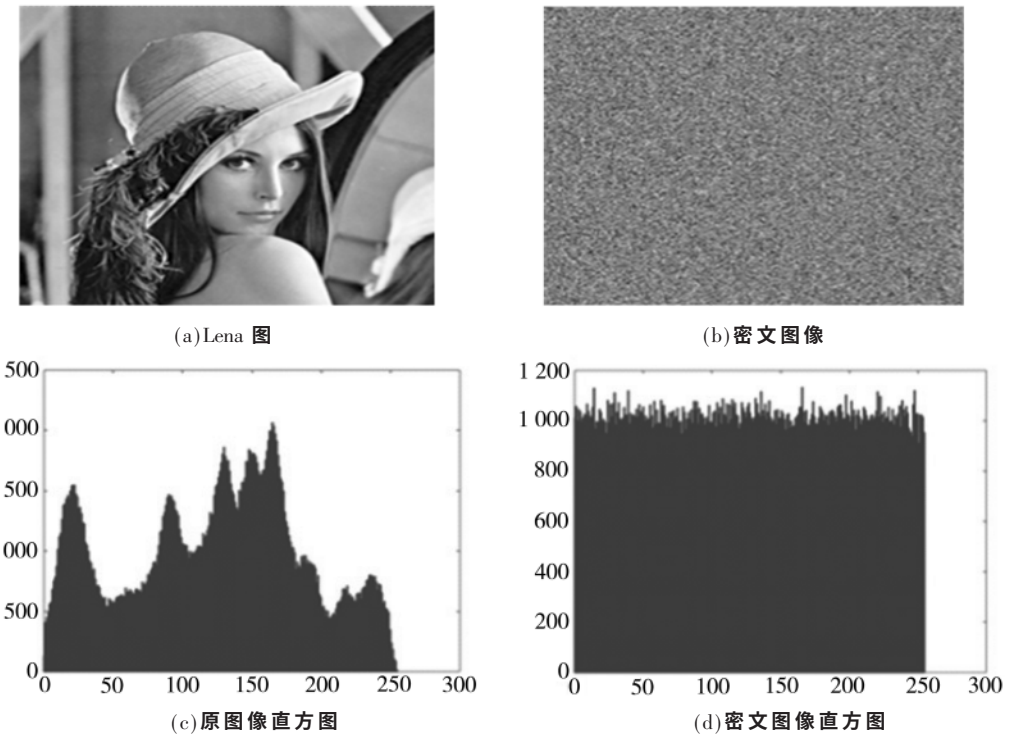
本文基于超混沌 Lorenz 系统和斜帐篷映射提出一种伪随机数发生器。本方案首先利用超混沌 Lorenz 系统迭代产生 4 路伪随机序列$\{S_1, S_2, S_3, S_4\}$，并以每 8 位为一个分组；然后利用斜帐篷映射迭代产生 1 个伪随机序列 S_s 用于数据选择；最后通过 Ss 序列值选择$\{S_1, S_2, S_3, S_4\}$序列中的一个为该 8 位的输出，继而产生伪随机序列输出。本文设计方案的输出结果通过了 NIST 的 SP800-22 rev1a 的全部随机性检验，并用图像加密测试证明其具有良好的随机性。

参考文献

[1] SHANNON C E.Communication theory of secrecy systems[J]. The Bell System Technical Journal，1949，28(4)：656-715.

[2] 陈奉苏.混沌学及其应用[M].北京：中国电力出版社，1998.

[3] ALIPOUR M C，GERARDO B D，MEDINA R P.A secure image encryption architecture based on pseudorandom number generator and chaotic logistic map[C].2019 Association for Computing Machinery，2019.



(a)Lena 图　(b)密文图像

(c)原图像直方图　(d)密文图像直方图

图 3　图像及其直方图

[4] CHUGUNKOV I V,KLIUCHNIKOVA,ETAL B V,IVANOV M A. New class of pseudorandom number generators for logic encryption realization[C].2020 IEEE Conference of Russian Young Researchers in Electronic Engineering,2020.

[5] MURILLO-ESCOBAR M A,CRUZ-HERNÁNDEZ C,CARDOZA-AVENDAÑO L,et al.A novel pseudorandom number generator based on pseudorandomly enhanced logistic map[J].Nonlinear Dynamics,2017,87(1):407-425.

[6] Zhu Congxu,Li Shuai,Lu Qin.Pseudo-random number sequence generator based on chaotic logistic-tent system[C].2019 IEEE 2nd International Conference on Automation,Electronics and Electrical Engineering,2019.

[7] CHEN E,Min Lequan.Discrete chaotic systems with one-line equilibria and their application to image encryption[J].International Journal of Bifurcation and Chaos,2017,27(3):1-17.

[8] TAHA M A,HASAN T M,SAHIB N M.Retina random number generator for security applications[C].2019 2nd International Conference on Engineering Technology and its Application (IICETA),2019.

[9] Zhao Yi,Liu Jie.A self-perturbed pseudo-random sequence generator based on hyperchaos[J].Chaos,Solitons & Fractals:X4(2020).doi:Http://doi.org/10.1016/j.csfx.2020.

[10] 曹艳艳,杨波.动态分组混沌伪随机数发生器[J].计算机应用研究,2019,36(8).

[11] 魏连锁,胡现成,郭媛,等.基于云模型与 Fibonacci 的混沌伪随机序列发生器设计[J].实验室研究与探索,2019,38(8):57-61.

[12] 朱淑芹,王文宏,李俊青.一类二次多项式混沌及其随机数生成器设计[J].计算机工程与应用,2018,54(9):84-88.

[13] 朱和贵,蒲宝明,朱志良,等.二维 Sine-Tent 超混沌映射及其在图像加密中的应用[J].小型微型计算机系统,2019,40(7):1510-1518.

[14] 陈飞,刘建东,胡辉辉,等.二维整数帐篷映射模型设计及安全性仿真分析[J].计算机工程与应用,2019,55(1):103-108,173.

[15] 曾珂,禹思敏,胡迎春,等.基于 3D-LSCM 的图像混沌加密算法[J].电子技术应用,2020,46(1):86-91.

[16] 李春虎,罗光春,李春豹.基于斜帐篷混沌映射和 Arnold 变换的图像加密方案[J].计算机应用研究,2018,35(11):3424-3427.

[17] 汪彦,涂立.基于改进 Lorenz 混沌系统的图像加密新算法[J].中南大学学报(自然科学版),2017,48(10):2678-2685.

[18] RSSLER O E.An equation for continuous chaos[J].Physics Letters A,1976,57(5):397-398.

[19] HASLER M,MAISTRENKO Y L.An introduction to the synchronization of chaotic systems:Coupled skew tent maps[J].IEEE Transactions on Circuits and Systems-I,1997,44(10):856-866.

[20] LORENZ E N.Deterministic non-periodic flow[J].Journal of the Atmospheric Sciences,1963,20(2):130-141.

[21] Wang Xingyuan,Wang Mingjun.A hyperchaos generated from Lorenz system[J].Physics A:Statistical Mechanics and Its Applications,2008,387(14):3751-3758.

[22] KALMAN R E.Lyapunov functions for the problem of

(下转第 122 页)

先下降(放电状态),之后电压急速上升,然后进入恒压充电模式,由于超级电容内阻存在,充电结束后其电压呈现一定程度的下降。实验结果与系统工作状态预期一致。同时如图 9 所示,示波器显示值为 200 ms/格,即 300 ms 激励时间下,系统回电时间约为 600 ms,故一个工作周期约为 1 s, 可满足实际中持续加热的需要。此外 H 桥70 V 工作电压下,采用普源公司 RP1005C 电流探头测得RLC 回路电流有效值约为 21.2 A,功率输出约为 1.48 kW。

4.2 实际检测实验

采用实验样机对 45# 凹槽裂纹进行检测,输出功率 1.5 kW、激励频率 40 kHz、激励时间 300 ms,采用对应的图像处理算法进行处理,检测结果如图 10 所示。

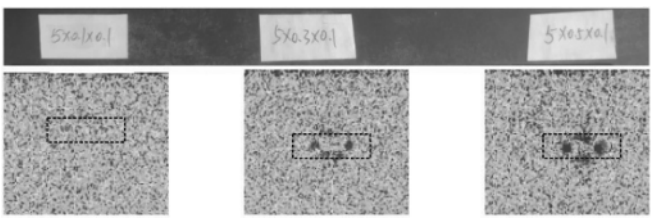


图 10 45# 凹槽检测效果图

如图 10 所示,5 mm×0.1 mm×0.1 mm 分别代表裂纹的长×深×宽,黑色边框标记的地方即为热成像图中的裂纹所在。由于激励频率较小,而第一条裂纹深度较小,导致检测效果较差,其余两条均能明显观察到“尖端效应”反映的裂纹存在。

5 结论

本文介绍了一种便携式脉冲涡流热成像电源系统方案,搭建了便携式脉冲涡流热成像电源系统样机。经实验表明,该样机体积重量小、易携,具有较好的实用性,同时其输出功率、检测能力满足脉冲涡流热成像对电源的需求。该电源系统设计可初步满足脉冲涡流热成像技术应用于现场检测的需求。

参考文献

[1] 闫会朋,杨正伟,田干,等.涡流热成像裂纹检测中的形状大小影响分析[J].仪器仪表学报,2016,37(7):1610-1617.

[2] 王晓娜,杨沛,侯德鑫,等.脉冲涡流热成像的自适应异常提取算法[J].仪器仪表学报,2016,37(8):1818-1824.

[3] TIAN G Y,GAO Y L,LI K J,et al.Eddy current pulsed thermography with different excitation configurations for metallic material and defect characterization[J].Sensors,2016,16(6).

[4] 唐波,方旭,侯德鑫,等.面向脉冲涡流热成像的激励电源特性研究[J].仪器仪表学报,2018,39(1):208-215.

[5] 王晓娜,方旭,唐波,等.脉冲式感应加热电源频率跟踪技术的研究与实现[J].电工技术学报,2018,33(18):4357-4364.

[6] 戴军军,唐波,侯德鑫,等.面向涡流热成像的双路正交激励电源系统[J].仪表技术与传感器,2017(3):68-72,77.

[7] 王同辉,王晓娜,侯德鑫,等.高频感应热成像电源的全数字频率跟踪技术[J].电力电子技术,2019,53(6):39-41,98.

[8] 晏勇.现代便携式设备电源技术研究与应用[J].四川兵工学报,2014,35(2):116-119.

[9] VRANA J,GOLDAMMER M,BAUMANN J,et al.Mechanisms and models for crack detection with induction thermography[J].Aip Conference Proceedings,2008.

[10] WILSON J,TIAN G Y,MUKRIZ I,et al.PEC thermography for imaging multiple cracks from rolling contact fatigue[J].NDT and E International,2011,44(6).

[11] PENG J P,TIAN G Y,WANG L,et al.Investigation into eddy current pulsed thermography for rollingcontact fatigue detection and characterization[J].NDT & E International:Independent Nondestructive Testing and Evaluation,2015,74:72-80.

[12] 林苗.超级电容与锂电池混合动力系统能量控制研究及实现[D].武汉:武汉理工大学,2014.

(收稿日期:2020-06-16)

作者简介:

张廷尧(1996-),男,硕士研究生,主要研究方向:无损评价技术与设备。

王晓娜(1975-),女,硕士,副教授,主要研究方向:几何量精密测量和光电检测技术。

叶树亮(1973-),通信作者,男,博士,教授,主要研究方向:化工安全及工艺安全测试技术与仪器、零部件无损检测设备与仪器、光栅信号处理、齿轮精密测量,E-mail:itmt_paper@126.com。

(上接第 117 页)

Lur'e in automatic control[C].Proceedings of the National Academy of Science of the USA,1963,49(2):201-205.

[23] 李庆扬.数值分析[M].北京:清华大学出版社,2001.

[24] NIST special publication SP 800-22 Rev[EB/OL].(2010-04-15).http://csrc.nist.gov/publications/nist-pubs/800-22-rev1a/SP800-22 rev1a.Pdf.

[25] SHANNON C E.A mathematical theory of communication[J].Bell Labs Technical Journal,1948,27(4):379-423.

(收稿日期:2020-06-30)

作者简介:

蔚艳文(1995-),女,硕士研究生,主要研究方向:电路与系统。

李震(1987-),男,硕士,实验师,主要研究方向:混沌密码学、信息安全与隐私保护。

李良荣(1963-),通信作者,男,本科,教授,主要研究方向:电路与系统、EDA 技术。

版权声明