DOI:10.19651/j.cnki.emt.2106855

应用机器学习对超晶格信号随机性的研究和评估*

李振曜 宋贺伦 应杰攀
(中国科学院 苏州纳米技术与纳米仿生研究所 苏州 215123)

摘 要:本研究由对超晶格随机数发生器的信号随机性检测为出发点展开。通过使用人工智能方法对发生器产生的随机信号进行检测和评估。针对这种新随机信号采用了几种常见的机器学习方法,来预处理一部分信号并试图训练聚类或网络模型,然后对随机数其他部分进行测试并判断随机性优劣。将此方法运用于比较正态分布随机数与超晶格发生器随机数,结论为超晶格随机数具有更好更明显的随机性,且各类机器学习方法在随机数性能检验中有价值,可以展望使用机器学习方法研究随机数及其相关的密码安全性的可能前景。

关键词:随机数;随机数检测;机器学习;非监督学习;K-means;神经网络;长短程记忆网络;超晶格
中图分类号:TP2 **文献标识码**:A **国家标准学科分类代码**:510.1050

Brief research of machine learning cryptanalysis for superlattice device

Li Zhenyao Song Helun Ying Jiepan
(Suzhou Institute of Nano-Tech and Nano-Bionics(SINANO),Chinese Academic of Science,Suzhou 215123, China)

Abstract: This article expands from the research of randomness testing of signal generated by superlattice random number generator (SRNG). The thesis tests the generated random signal for this new random signal using some common machine learning methods to preprocess one part of random signal and try to train clustering or network model, and then testing other part of random number to judge the quality of randomness. These methods are used on normal distributed random number and SRNG signals, comparison of which shows better performance of SRNG signals. The thesis shows value of randomness testing using machine learning, and possible future of cryptology security research using machine learning.

Keywords: random number; random number testing; machine learning; unsupervised learning; K-means; neuron network; LSTM; superlattice device

0 引 言

密码学是信息安全领域的基石,对密码的攻击与保护,对加密解密手段的评价,一直是密码学的研究重点,并形成了各种认证标准。随机数的生成是密码学中的重要环节,在密码学中有举足轻重的地位。传统的验证随机数优劣的标准,如美国 NIST、我国 GMT0005-2012 标准等,多基于假设检验,属于证伪过程,覆盖的范围较小,数据的组合形式较为单一。近年在机器学习思想影响下,通过机器学习的训练结果最大限度的尝试发现随机数串中是否有规律性,从而判断其是否可以作为优质密钥使用这一方式,得到了不少重视,并在各种机器学习方法下都取得了初步的进展[1]。

本文探究的是一种由材料混沌现象生成的物理密码器—超晶格自震荡混沌密码器[1]所产生的随机数信号,该随机信号器件由中科院苏州纳米所张耀辉团队研发并生产[2],密码源使用了 GaAs 等材料[3],在直流偏压或交流驱动中,会出现动态电场畴和混沌现象,是一种基于半导体材料新物理特性的全新的随机信号技术。它具有优秀的不可预测性和孪生不可克隆性,这种密码的成本比量子密码低,可以期待会有相应的应用场景。

对随机数的基本要求有:1)随机性;2)不可预测性;3)不可重现性。仅可满足前两类要求的属伪随机数,只有满足不可重现性的随机数才是真随机数。虽然,伪随机数已可满足社会的大多数需求,但对于涉及国家安全的重大技术、经济、军事活动中的信息保管、交换、传递等,仍必须

收稿日期:2021-06-03
*基金项目:中国科学院科技服务网络计划(KFJ-STS-QYZX-061)、纳米真空互联试验站(2018-000052-73-01-000356)、"十三五"国家密码发展基金(MMJJ20180112)项目资助

应用真随机数进行通信加密、信息认证、数字签名及密钥管理。软件只能生成伪随机数。真随机数是从温度、声音、核裂变、粒子运动等不可重现的物理现象中产生的。能够从这些物理现象中获取不可重现性随机数信息的就是物理随机数发生器，即真随机数发生器(true random number generator，TRNG)。

密码学与神经网络的交叉学科已经成为当下的重点[4]，近期的研究如 Li 等[5]设计的一种基于两层混沌神经网络的单向新型哈希函数，其在统计特性、密钥敏感性、抗攻击能力等指标上均有突出表现，因此在相关研究中被广泛讨论。而文献[6-7]开创了将神经相互学习的同步性质用于密钥协商的先河，为后续研究提供重要的理论支撑和实践基础等。1990 年，日本学者 Aihara 等创造性地提出了混沌神经网络的概念－基于生物神经元的混沌特性，将神经网络与混沌理论相结合，使其具有更复杂和更丰富的非线性动力学特性。这些性质与密码学有着更紧密关联，其可源于 1949 年 Shannon 的经典著作，使得神经网络与密码学建立了更紧密的联系。在其中，针对密码中密钥本身，即随机数串本身的性质的机器学习讨论也有了一定的研究。

近年在对热门课题量子密码中居于主要地位的单个光子的量子不可预测性的研究已开始有使用机器学习的方法，2018 年悉尼大学 Truong 等[8]的研究就使用了神经网络方法用于量子密码随机数，研究了其面对不同噪音干扰时的可靠性。在本文的实验中，除了使用神经网络方法，也引入非监督学习的 K-means 方法[9-10]，而使用非监督学习方法对随机数的研究尚无先例。该方法通过在规定分配方式的向量空间中，随机数形成的向量的在最终迭代产生的 k 个聚类中心周围的分布情况来判定随机数基本的分布性质。本文的实验用这几种方法处理超晶格随机数的同时，将其与遵循特定分布的伪随机数在同样处理条件下进行对比。机器学习方法预期可以拥有更高的覆盖面，能够比传统方法有更高的可信度，在对伪随机数的检测方面会明显优于传统方法，而对真随机数则传统方法与机器学习方法结论一致。

1　监督学习与非监督学习

尽管 Truong 等[8]对量子密码的研究采用了设定标签的神经网络，本文也会实验此方法并进行拓展，但对于纯随机数串，直观上没有任何的先验指标，也没有适合的用于形成机器学习分析元素的条件形式，更理想的分析是采用非监督学习(unsupervised learning)方法。表 1 所示是监督学习与非监督学习较为直接的对比。

当直接对随机数信号本身进行检验时，如果使用监督学习，需要指定数串-标签(类型名)的映射，则需要在不借助其他数据材料的情况下在随机数信号中自行取得标签，即要用一定的方法将随机数串分为输入-输出两个部分。在非监督学习方法下，需要检验的随机数串可以看做一个整体，随机数串每个部分为具有同等地位的研究对象。在随机数信号作为整体的情况下，均匀分成单个的用于学习的元素，形成向量形式，使用 K-means、DBSCAN 这类方法找到聚类中心，或是定义高/低维度的映射用以进行主成分分析(principal component analyse，PCA)。相应的，在有已知的明文-密文映射的情况下，则使用监督学习有着更明显的意义。

表 1　机器学习分类

	监督学习	非监督学习
训练对象	存在输入-输出映射	无输出
训练目标	对于输出数据 X 能预测变量 Y	自行观察数据 X 的特征
优化方向	标记数据	分类、聚类
常用算法	K-近邻、决策树、朴素贝叶斯	K-means、主成分分析(PCA)、DBSCAN

2　用机器学习方法进行随机数实验

对于随机数串进行机器学习的形式，最直观的方法是按序列形成向量。在本次实验中，对于 0/1 随机信号序列，首先按照一定的位数作为初始元素的范围(m 位代表 2^m 范围内的数)，然后选取 n 作为向量的维度，每连续的 n 个数(或者也可以不连续，按照其他的定义)形成一个向量。对于 K-means 方法，随机数仅需要分成向量，其标签会自动随序列生成，本质也是一个映射。而对于其他需要给定初始标签的监督学习方法，包括本文中后续提到的神经网络方法，则可以在每个向量之后选取一个数(或者用其他形式取数)作为标签。结构如图 1 所示。

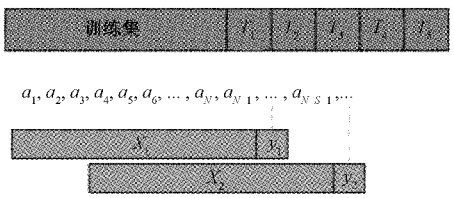

图 1　随机数形成向量标签

在本次实验中，真随机数由超晶格随机数生成器给出，伪随机数在 MATLAB 环境下有 rand、randi、randn 等几个命令可以实现，在 Pytorch 环境中也有 torch.randn 命令可以实现，以命令 randn 生成的 10^6 个，以 k 位一组作为向量，本实验中 $k=5$ 时取得较明显的对比效果。randn 的结果是以 0 点为中心的正态分布随机数，而超晶格随机数取自 0/1 串，通过将 randn 的结果平移到全正数，缩放到[0，2^n]范围，然后取整(如用 round)将其转化为与 0/1 串格式一致的对比实验组。

2.1　K-means 方法

K-means 是一种对中心分布的判断，以此方法判定随机数在给定的向量空间中是否分布均匀，K-means 的分析

对象为一组向量，以 k 个随机初始中心为基础，经过迭代后确立 k 个正式的聚类中心，在训练集训练完毕后导入测试集，观测其他向量在该 k-中心空间中的分布是否均匀。K-means 是最基础的非监督学习方法之一，用于把向量空间中间隔较近的自动归为一类，其元素的标签是 k 个初始聚类中心的序号，由序列自动生成。将由 0/1 组成的随机数串用 m 位一个数，n 个数一组的分组方式形成 n 维向量，然后对这些向量使用 K-means 进行聚类分组，在 MATLAB 中有直接的函数调用语句 idx=kmeans(X,k)，其中 X 即为输入的整个随机数串，输出 idx 是向量，是每个向量最后迭代得到的组号。K-means 算法过程如下所示。

算法 1　K-means 算法

输入：向量集 N，初始聚类中心数 k
输出：对 N 中的每个向量输出一个聚类中心标签 l
While True **do**：
　for int $i=0$；$i<n$；$i++$ **do**
　　for int $j=0$；$j<k$；$j++$ **do**；
　　设置随机的初始聚类中心；
　　end
　　计算点 i 到类 j 的距离；
　　找出所有属于自己这一类的所有数据点；
　　把自己的修改为这些数据点的中心点坐标；
　end
end

2.2　神经网络

神经网络本质上是对一个函数的多层次不断的拟合，并且由自己规定的网络层数决定中间运算节点多少，并计算出这些节点的系数。该方法需要指定分析对象的标签，则使用一长串随机数中的靠前的部分。该类设计网络的研究对象为内容一标签的映射，反映在随机数中，以一定量的作为目标特征向量形式(pattern)，然后选取几位数作为标签(例如选取 4 位二进制数，则标签总共 2^4 种)，这是一种比较直观地粗糙的随机数分析，但即便如此在这种规则下依然有很多参数调整空间，例如特征向量和标签各自的长度，选取间隔，迭代学习过程中的遗忘率，另外当然还包括训练集、测试集的比例等。在此基础上，取大量元素作为训练集，验证集和测试集(在某些模型中仅有训练集和测试集)。在通常的神经网络训练中需要训练集的量远大于测试集，依据经验设定本实验选取 5∶1∶1。神经网络结构如图 2 所示。

如今，代表性的机器学习方法为卷积神经网络(convolution neural network，CNN)[11-12]，在图像识别和预测领域中有着很好的适应性，同时，回归神经网络(recurrent neural network，RNN)，由于同时具有正反双向

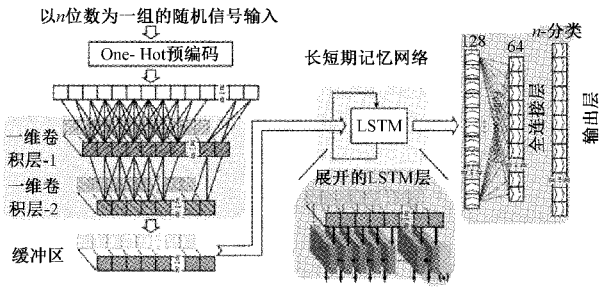

图 2　神经网络

的数据来源，稳定性有很高的保证。最常见的 RNN 方法是被称为长短程记忆网络的(long-short term memory，LSTM)，它可以对网络形成过程中一些前驱或后驱的输入，进行有针对性的取舍。本次实验中，借助 MATLAB 中的 trainNetwork 和 Pytorch 模块做了两组相关实验，并使用含 128 个隐藏层的双向长短程记忆网络(BiLSTM)，然后由 16 个全连接层进行拟合演算。

在 MATLAB 中形成的标准神经网络训练层如下：

5x1 Layer array with layers：

1" Sequence Input 输入层

2" BiLSTM 128 隐藏单位的双向 LSTM

3" Fully Connected 16 全连接层(层数由标签的总量决定)

4" Softmax Softmax 回归模型

5" Classification Output 分类输出

具体算法流程如算法 2 所示。

算法 2　LSTM 过程

输入：神经网络初始参数
输出：迭代后的神经网络参数
lstm=rnn(回归神经网络).基础 LSTM 核(size)
state=zeros(batchsize,lstm.state.size)
loss=0.0
for 每个目前数据库中位于 batch 中的元素 **do**：
　输出状态=lstm(当前 batch 状态)
　logits=matmul(softmax 输出)+softmax_b
　概率=nn.softmax(logits)
　loss+=lossfunction(目标概率)
end

这类算法在 NLP 等众多领域中间的步骤表示每次处理一批后更新状态值，之后的输出用于预测下一次状态。

2.3　在 Pytorch 中用 NLP 的思路进行实验

在包含预测阶段的训练中，引入自然语言处理(NLP)中序列对序列(sequence to sequence learning)方法对随机数进行映射[13-14]，将随机数串代入语库的位置，将较长的序列和用于标签的 N 位二进制数分别作为句子和索引，然后

引入 PPL 作为衡量训练好坏的标准，PPL 是用在自然语言处理领域(NLP)中，衡量语言模型好坏的指标。它主要是根据每个词来估计一句话出现的概率，并用句子长度作 normalize，公式为：

$$PPS = P(\omega_1\omega_2\cdots\omega_N)^{\frac{1}{N}} = \sqrt[N]{\frac{1}{P(\omega_1\omega_2\cdots\omega_N)}} = \sqrt[N]{\prod_{i=1}^{N}\frac{1}{p(\omega_i \mid \omega_1\omega_2\cdots\omega_{i-1})}} \tag{1}$$

S 在 NLP 中代表句子，在随机数中即代表随机数串。N 为随机数串长度，$p(\omega_i)$ 代表第 i 个词(随机数串中标签)的概率。在 NLP 的模型中，通常先把句子变成向量，而词则相当于向量中的元素。这个式子可以这样理解，PPL 越小，$p(\omega_i)$ 则越大，期望的序列出现的概率就越高。那么对于随机数而言则意味着则是随机性更差。

3　机器学习实验结果

K-means 方法的结果是对随机数从分布角度做基本的分布判断，将超晶格产生的物理信号随机数与正态分布伪随机数作对比，得到如图 3 所示的聚类中心最终分布对比，图中横坐标为聚类中心编号，纵坐标为最终聚类中心密度。正态分布低维向量随机数在几个聚类中心附近有明显的聚拢。这代表正态分布随机数据有明显的集性。

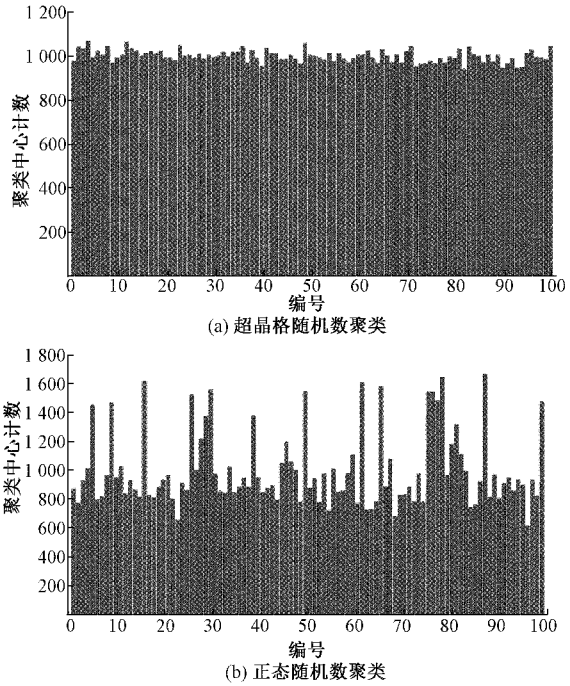

图 3　使用 K-means 聚类分别对超晶格随机数和对正态分布伪随机数的向量聚类中心密度对比

其中，图 3(a)为超晶格随机数分布，图 3(b)为 2^n 正态随机数分布。横轴为标签，纵轴为统计数。

MATLAB 默认的神经网络训练过程中可以显示精确度和误差曲线，训练过程平滑。当使用 MATLAB 读取 4 位二进制位作为标签的时候，训练的神经网络可以达到接近满精确度，如图 4 所示(图 4(a)，横坐标为迭代次数，纵坐标上图为模型准确率，下图为网络误差)，可见在漫长的迭代后，由训练集产生的拟合神经网络比较勉强的达到了自身精确。

但用测试集检测后没有任何效果，准确率为标准 4 位二进制数下的 1/16，无法做任何有效预测，这个层面上说明随机性能的保障。而当改变一些参数，诸如在读取开始阶段以 8 位二进制为标准，(此时相应需要 2^8 层全连接层)，则神经网络无法完成训练(如图 4(b)所示)，无法在训练集取得自洽准确性的情况下，验证集准确度便无法生效。

对于正态分布随机数采用类似的结果，训练结果更加顺利(如图 4(c)所示)，使用测试集检验后精确度达到 0.066，比 1/16 即 0.062 5 还是明显高的。而当将伪随机数数量增加到 10^5 之后，伪随机数的训练也无法随着迭代层数提高精确度。

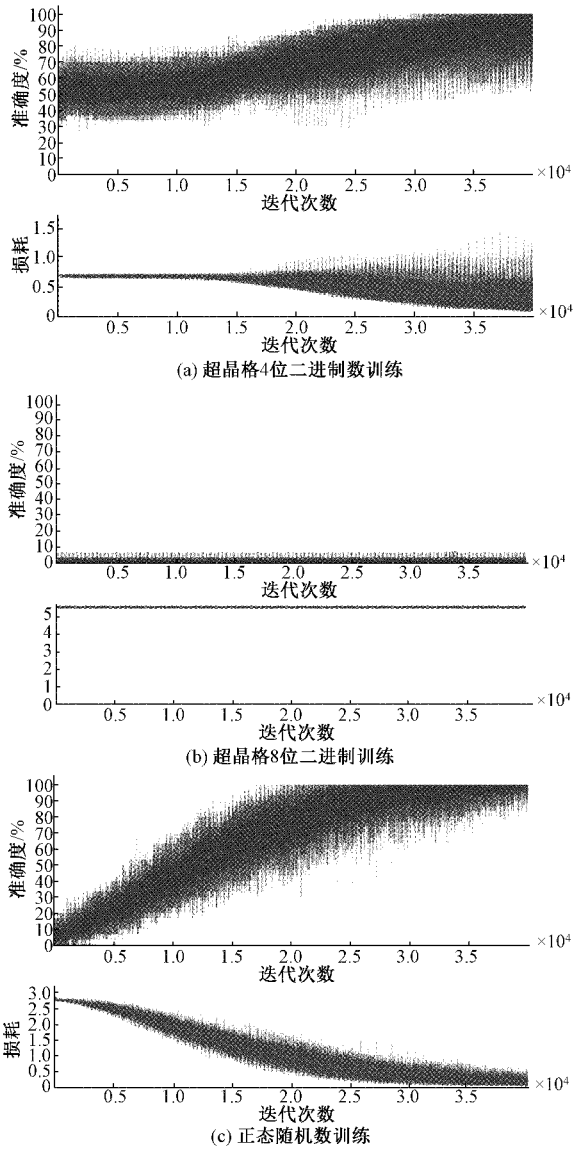

图 4　神经网络训练误差对比

使用 Pytorch 中的序列对序列训练-NLP 方法，控制迭代次数，神经网络层数，遗忘率（丢包率），以有效误差和 PPL 作为神经网络好坏参数，得到如表 2 所示的结果。

表 2 Pytorch 神经网络训练结果

随机数类型	迭代次数	神经网络层数	遗忘率	有效误差	有效 PPL
超晶格	10	2	0.1	5.54	255.91
	20	2	0.2	5.54	255.92
	20	3	0.2	5.56	255.95
正态随机数	10	2	0.1	4.51	91.28
	20	2	0.2	4.51	91.11
	20	3	0.2	4.51	91.53

该结果显示了在以 PPL 作为参考的基础上超晶格随机数对比正态分布的混沌性和优越性。

4 结 论

本文使用了两种机器学习方法，分别对应监督学习与非监督学习，对由超晶格随机数发生器产生的随机数 0-1 信号进行训练分析，并使用这样的方法与 2^n 取整正态分布随机数进行对比，两种机器学习方法都能得到超晶格随机数对比机器正态分布随机数的有明显更优秀的随机性能的结论，且非监督学习方法在随机数研究中价值更高。机器学习参数的改变对实验结果的影响，对随机性优秀的真随机数测试影响微乎其微，对伪随机数则有较大影响。

今后的工作，由于机器学习方法诸多，初始化数据结构和训练方法诸多，在各种具体的方法中参数也诸多，而机器学习过程中所计算出的权值、系数等在现实层面并无直接意义对应，所以使用机器学习研究随机数的实验还可以有很大的讨论和拓展空间[15 16]。本文所涉及的方法及相应变量控制的也仅仅是庞大的机器学习体系中的一小部分，今后如果此方向的研究能继续进行，则需要进行更多组实验，且应以确定哪个机器学习参数拥有更明显的影响效果为目标。同时还需要对这种方法本身加以更广泛地讨论，能更有说服力地确定超晶格或其他真随机数密码的性能优劣，并且探讨及开发使用其他机器学习方法，尤其是非监督学习方法的可能性，讨论一个基于特定机器学习方法的，可能辅助或替代现有随机数检验标准的新标准，使得随机数测试更加主动和全面。

参考文献

[1] 童新海，陈小明，徐述. 超晶格密码的研究进展[J]. 科学通报，2020，65(Z1)：108-116.

[2] LI W，REIDLER I，AVIAD Y，et al. Fast physical random-number generation based on room-temperature chaotic oscillations in weakly coupled superlattices[J]. Physical Review Letters，2013，111(4)：044102.

[3] HUANG Y Y，LI W，MA W Q，et al. Spontaneous quasi-periodic current self-oscillations in a weakly coupled GaAs/(Al，Ga)As superlattice at room temperature[J]. Appl. Phys. Lett.，2013，DOI：10.1063/1.4811358.

[4] 葛钊成，胡汉平. 神经网络与密码学的交叉研究[J]. 密码学报，2021，8(2)：215-231.

[5] LI Y T，DENG S J，XIAO D. A novel hash alorithm construction based on chaotic neural network[J]. Neural Computing & Applications，2011，20(1)：133-141.

[6] KINZEL W，KANTER I. Neural cryptography[C]. Proceedings of 9th International Conference on Neural Inrofming Processing，IEEE，2002：1351-1354.

[7] KANTER I，KINZEL W，KANTER E. Secure exchange of information by synchronization of neural networks[J]. Europhysics Letters，2002，57(1)：141-147.

[8] TRUONG N D，HAW J Y，ASSAD S M，et al. Machine learning cryptanalysis of a quantum random number generator[J]. IEEE Transactions on Information Forensics and Security Feb，2019：403-414.

[9] 杨俊闯，赵超. K-Means 聚类算法研究综述[J]. 计算机工程与应用，2019，55(23)：7-14.

[10] 王艳娥，梁艳，司海峰，等. 基于 K-means 算法的最佳聚类数研究[J]. 电子设计工程，2020，28(24)：52-56.

[11] 惠文珊，李会军，陈萌，等. 基于 CNN-LSTM 的机器人触觉识别与自适应抓取控制[J]. 仪器仪表学报，2019，40(1)：211-218.

[12] 金鹭，张寿明. 基于神经网络的语谱图情感分类算法[J]. 电子测量技术，2020，43(24)：57-63.

[13] 宋鹏，葛洪伟. 最近邻的密度峰值聚类标签传播算法[J/OL]. 计算机科学与探索，2021：1-13[2021-07-28].

[14] LANI M M. Testing randomness in ciphertext of block-ciphers using dichard tests[J]. International Journal of Computer Science and Network Security，2010，10(1)：53-57.

[15] QU Z，SU L，WANG X，et al. A unsupervised learning method of anomaly detection using GRU[C]. IEEE International Conference on Big Data & Smart Computing，2018，DOI：10.1109/BigComp.2018.00126.

[16] MADRY M，BO L，KRAGIC D，et al. ST-HMP：Unsupervised spatio-temporal feature learning for tactile data[C]. International Conference on Robotics and Automation，2014：2262-2269.

作者简介

李振曜，硕士，研究实习员，主要研究方向为密码及机器学习应用。

E-mail：zyli2019@sinano.ac.cn

宋贺伦（通信作者），博士，研究员，主要研究方向为半导体器件集成化应用。

E-mail：hlsong2008@sinano.ac.cn

应杰攀，硕士研究生，主要研究方向为半导体器件集成化应用。

E-mail：jpy2018@mail.ustc.edu.cn