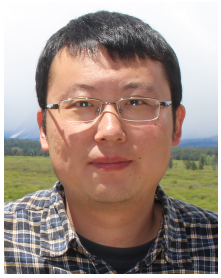
报告题目：面向图模型和深度神经网络的稀疏学习

报告人：袁晓彤

报告人简介：



袁晓彤，现任南京信息工程大学教授，博导，江苏省大数据分析技术重点实验室副主任。主要从事机器学习和计算机视觉方面的研究和教学，研究方向包括稀疏学习、概率图模型、分布式优化、图像识别等。在国内外学术期刊（包括 IEEE-TPAMI, IEEE-TIT, JMLR 等）和会议（包括 NIPS, ICML, ICCV, CVPR 等）上发表论文 70 余篇。曾获得国家自然科学基金优秀青年基金资助，入选江苏省双创人才；获得过 IEEE Transactions on Multimedia 最佳论文提名，ImageNet 国际竞赛图像检测任务第 1 名等。

报告内容：

本报告主要探讨图模型和深度神经网络中的稀疏结构学习及大规模优化问题。报告内容涵盖讲者在高维指数族图模型的自适应稀疏学习方法、稀疏高斯图模型的分布式优化、基于非凸稀疏优化算法的神经网络压缩等方面的研究进展。将重点介绍一类参数可加指数族图模型的稀疏结构估计方法，基于块坐标下降的 Graphical Lasso 分布式优化算法及实现，基于阈值追踪算法的深度神经网络压缩训练等。

报告题目：Parameterless reconstructive discriminant analysis for feature extraction

报告人：黄璞

报告人简介：

黄璞，2014 年 6 月毕业于南京理工大学模式识别与智能系统专业，获工学博士学位，现为南京邮电大学计算机学院讲师。近年来，作为项目负责人，主持了国家自然科学青年基金与中国博士后科学基金，以第一作者在《Information Sciences》、《Neurocomputing》、《Digital Signal Processing》、《Journal of Visual Communication and Image Representation》、《计算机辅助设计与图形学学报》、《中国图象图形学报》、《模式识别与人工智能》等国内外期刊及国际相关会议发表论文十余篇。目前主要的研究方向为：模式识别、机器学习、生物特征识别等。

报告内容：

Dimensionality reduction methods have been widely employed to extract the distinctive features of the original data in pattern recognition tasks. Reconstructive discriminant analysis (RDA) is an effective dimensionality reduction method that can generate an efficient subspace for the linear regression classification (LRC) method. However, the main problem of RDA is that it needs to select the k heterogeneous nearest subspaces of each sample to construct the inter-class reconstruction scatter and it is very difficult to predefine the parameter k in practical applications. In this talk, we introduce an improved version of RDA, namely parameterless reconstructive discriminant analysis (PRDA), for feature extraction. Compared with the existing RDA algorithm, our proposed PRDA method cannot only fit LRC well but also has two important characteristics: (1) the performance of RDA depends on the parameter k that requires manual turning, while ours is parameter-free, and (2) it adaptively estimates the heterogeneous nearest classes for each sample to construct the inter-class reconstruction scatter. We show that PRDA can achieve very competitive results, but is more efficient than RDA for pattern recognition applications.

报告题目：基于高层语义提取的图像识别模型构建

报告人：李群

报告人简介：

李群，南京邮电大学计算机学院、软件学院、网络空间安全学院讲师。2013年于北京邮电大学信息与通信工程学院获得工学博士学位，曾赴美国加州大学河滨分校（University of California，Riverside）计算机视觉和智能系统实验室联合培养，师从美国终身教授Bir Bhanu。受益于该实验室研究领域的多元化特点，开拓了研究思路和眼界。本人一直从事图像识别领域的研究工作，积极跟踪新涌现的计算机视觉技术。近年来，在IEEE Signal Process. Lett.等国内外权威刊物和学术会议上以第一作者发表论文17篇，其中SCI检索论文5篇，EI检索论文11篇。

报告内容：

图像识别是计算机视觉领域的高级操作过程，它将图像数据转化为人们可以理解的语义信息，提供了实现一个真正的实用的计算机视觉系统的可行途径。如何快速而准确地对图像进行识别已经成为人们研究的热点问题，并且图像识别的研究结果可以应用在信息检索的各个领域。在本报告中，将首先介绍如何构建一个图像识别的模型，并重点介绍本人所关注的特征提取模块所展开的研究。随后，将分享对图像识别领域将来讲究的思考和彷徨，并与大家讨论和学习计算机视觉所面临的机遇及挑战。

报告题目：基于超声波的智能手势感知技术

报告人：王炜

报告人简介：

王炜，南京大学计算机科学与技术系副教授。1997 年和 2000 年于南京大学电子科学与工程系分别获得理学学士和理学硕士学位，2008 年于新加坡国立大学电机与电脑工程系获得博士学位。曾在微软亚洲研究院及中兴通讯从事过多年的无线网络研究与标准化工作。主要研究方向为无源动作感知、传感器网络及软件无线电等。在 ACM Mobicom, ACM CCS,NSDI, IEEE/ACM trans. Networking, IEEE trans. Mobile Computing 等会议和期刊上发表过多篇论文。2011 年获江苏省双创人才奖。

报告内容：

近年来涌现的各类智能电子设备，如智能手机、智能手表、VR/AR 设备等都具有通过扬声器和麦克风来收发人耳无法察觉的声波信号的功能。通过测量手指和手掌对自由空间的声波反射，我们可以实现非绑定手势感知和识别。用户不需要在手部佩戴任何设备，即可通过手势对各种智能设备实现实时、精确的操控。在本报告中，我们将首先介绍如何通过测量声波相位来获取精确的手指移动距离，并实现一维和二维的定位。随后，我们将分享我们近年来在超声波手势识别上的思考，讨论超声波手势识别所面临的机遇及挑战。

报告题目：低占空比传感网中的广播调度优化问题研究

报告人：徐力杰

报告人简介：

徐力杰，男，博士，南京邮电大学计算机学院讲师。2014 年毕业于南京大学计算机系计算机软件与理论专业，获工学博士学位。2011 至 2012 年在香港理工大学互联网与移动计算实验室任研究助理。主要研究方向包括传感网/物联网、无线网络、移动与分布式计算、图论算法等。近年来在 ACM Transactions on Sensor Networks、Computer Communications、Wireless Networks、Journal of Computer Science and Technology、Ad Hoc Networks、计算机学报、软件学报等多个知名 SCI/EI 期刊以及 MASS、Globecom、ICPADS、WCNC、ICCCN 等多个重要国际会议上发表论文二十余篇。现作为项目负责人主持包括国家自然科学基金青年项目、中国博士后科学基金面上项目、江苏省博士后科研资助计划、南京大学软件新技术国家重点实验室开放课题等在内的多个科研项目。

报告内容：

无线传感网中的节点普遍采用低占空比的工作模式，该工作模式通过让每个节点周期性地睡眠以适应大多数无线传感网应用所固有的低流量特征，其极大地减少了由于空闲侦听所带来的能量浪费。尽管如此，它也为网络的性能带来了许多新的挑战，尤其是对于广播性能的挑战，这是因为相邻节点之间不同的工作调度会使得无线媒介丧失固有的广播属性，从而导致广播能耗的低效性。对于低占空比传感网而言，如何进行高效的广播是一个重要且具有挑战性的问题。本报告将结合自身工作主要从能耗优化、能量公平性优化以及面向自适应性能需求的权衡优化三个方面来研究和探讨这一问题。

报 告 题 目： Efficient Implementation of Elliptic Curve Cryptography for Resource-Constraint Embedded Processors

报告人：刘哲

报告人简介：

刘哲，南京航空航天大学计算机科学与技术学院教授，博士生导师。曾在法国巴黎高师信息安全组（ISG）和卢森堡大学安全与信任中心（SnT）和加拿大滑铁卢大学量子研究中心和应用密码研究中心从事博士后研究工作。2015 年 11 月于卢森堡大学(University of Luxembourg)算法、密码与安全实验室获得博士学位。博士期间，分别在香港城市大学，比利时（荷兰语）鲁汶大学以及微软总部研究院密码与安全组进行访问。刘哲的博士毕业论文获得卢森堡国家基金委 2016 年评出的唯一杰出博士毕业论文奖(Outstanding Ph.D Thesis Awards)，他也成为了该奖项第一位华人获得者。刘哲已经在国内外密码学术期刊和会议上发表学术论文 60 多篇，其中 20 多篇发表在安全类著名期刊和会议上。刘哲目前担任 4 个著名安全类期刊的编委，10 几个期刊的客座编辑，以及 20 多个安全类国际会议的程序委员会委员。

报告内容：

In this talk, I will present two works related to energy-efficient, high-speed and high-security implementation of elliptic curve scalar multiplication and elliptic curve Diffie-Hellman (ECDH) key exchange on embedded devices. In the first work, we introduce MoTE-ECC, a highly optimized yet scalable ECC library for Memsic's MICAz motes and other sensor nodes equipped with an 8-bit AVR processor. MoTE-ECC supports scalar multiplication on Montgomery and twisted Edwards curves over Optimal Prime Fields (OPFs) of variable size, e.g. 160, 192, 224, and 256 bits without recompilation, which allows for various trade-offs between security and execution time (resp. energy consumption). In the second work, we set new speed records for constant-time elliptic curve scalar multiplication and ECDH key exchange with implementations targeting 8, 16 and 32-bit microcontrollers. For example, our software computes a static ECDH shared secret in 7.2 million cycles (or 0.9 seconds @8MHz) on a low-power 8-bit AVR microcontroller which, compared to the fastest Curve25519 and genus 2 Kummer implementations on the same platform, offers 1.9x and 1.4x speedups, respectively. Similarly, it computes the same operation in 559 thousand cycles on a 32-bit ARM Cortex-M4 microcontroller, achieving a factor-2.5 speedup when compared to the fastest Curve25519 implementation targeting the same platform. These research results demonstrate the potential of deploying MoTE-ECC and FourQ on low-power applications such as protocols for IoTs.

报告题目：物联网和雾计算的安全研究

报告人：王志伟

报告人简介：

2009 年获得北京邮电大学密码学博士学位，现为南京邮电大学计算机学院副教授，硕士生导师，江苏省高校青蓝工程优秀青年骨干教师，香港大学计算机科学系访问学者，还在澳大利亚 Wollongong 大学，南洋理工大学等地从事过学术研究。近几年作为项目负责人获批国家自然科学基金面上项目 2 项，以及多个国家获省部级重点实验室开放课题。近年来以第一作者在国内外权威期刊或会议发表论文 30 多篇，申请专利 6 项，获批 2 项。近年来指导研究生获批江苏省研究生创新工程项目，指导本科生两次获得全国密码技术竞赛优秀指导教师奖。

报告内容：

物联网现已变成最大最重要的计算平台。安全扮演了最重要的角色，因为物联网的各种应用和人们的生活息息相关。雾计算层是物联网三层结构的中间层，相比云中心更加贴近终端，具备多种优势，可以部署各种优化算法与实时服务。报告首先将介绍一个部署在雾计算层的安全架构，用于对付物联网中的各种安全挑战。报告还将介绍雾计算安全应用中密码相关的几个成果，包括智能电网中的身份基数据聚合协议，弱身份终端借助雾设备的认证协议以及改进的抗泄漏 ABE 方案。