بسمه تعالی زمان نصب در تابلوی اعلانات:

☐ دفاع از رساله دکتری ☐ سمینار عمومی (Colloquium)

✓ دفاع از پایان‌نامه کارشناسی‌ارشد ☐ سمینار تخصصی (Seminar)

☐ سمینار تخصصی و مشورتی (Informal Seminar)

عنوان: بررسی آسیب‌پذیری‌های ناشی از حملات فعّال در سامانه‌های خودکار تصدیق گویندهٔ مقاوم در برابر حملات بازپخش

سخنران: عرفان تیداک

چکیده:

در سری چالش‌های ASVspoof، سامانه‌های مقابله با جعل تصدیق خودکار گوینده پیشنهاد می‌شود. موضوع سامانه‌های تصدیق گفتار در مقابل حملات فعّال (حملات جعبه سفید، سیاه و خاکستری)، در تحقیقات کمی بررسی شده است. در تحقیق پیش‌رو، به‌منظور ارتقاء عملکرد سامانه‌های شناسایی جعل، از شبکه‌های عصبی عمیق استفاده شده است. ابتدا یک شبکه عصبی عمیق برای تمایز بین سیگنال‌های گفتار اصلی و جعلی آموزش داده شده است و از ضرایب کپسترال فرکانس مل دلتا به همراه دلتای دوگانه، تبدیل موجک پیوسته و ویژگی تبدیل بسته موجک-مل به‌عنوان ورودی شبکه عصبی عمیق استفاده می‌شود. سپس برای هر ویژگی، ویژگی‌های تنگنا با استفاده از شبکه عصبی عمیق آموزش‌دیده، ایجاد شده است. یک دسته‌بند استاندارد مدل مخلوط گوسی برای شناسایی جعل با ویژگی‌های سطح آکوستیک و ویژگی‌های تنگنا، به وجود آمده است. دو مدل مخلوط گوسی برای کلاس واقعی و جعلی با استفاده از مجموعهٔ آموزش پایگاه دادهٔ چالش جعل ASVSpoof 2017 آموزش دیده‌اند. در مجموعهٔ توسعهٔ این چالش، سامانه‌های ضرایب کپسترال فرکانس مل-تنگنا، تبدیل موجک پیوسته-تنگنا و سامانه تبدیل بستهٔ موجک-مل-تنگنا، به ترتیب، به نرخ خطای معادل ۶/۲۷٪، ۶/۰۹٪ و ۵/۸۳٪ و در مجموعهٔ ارزیابی، به نرخ خطای معادل ۱۲/۶۳٪، ۱۱/۸۱٪ و ۱۰/۵۷٪ دست یافتند. همچنین، این سامانهٔ مقابله با جعل، تحت حملات جعبه سفید FGSM و جعبه سیاه NES مورد ارزیابی قرار گرفته است.

زمان برگزاری: چهارشنبه ۳۰ شهریور ۱۴۰۱، ساعت ۱۰ صبح

مکان برگزاری: اتاق دفاع دانشکده برق