دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: **فاطمه ترقی**		**نام استاد راهنما:** **جناب آقای دکتر محسن ابراهیمی‌مقدم**
مقطع: کارشناسی ارشد	**رشته: مهندسی کامپیوتر**	**گرایش: هوش مصنوعی، رباتیک و رایانش شناختی**
نوع دفاع: • **دفاع پروپوزال** □ • **دفاع پایان نامه** ☑ • **دفاع رساله دکترا** □		**تاریخ: ۱۴۰۳/۱۱/۲۸** **ساعت:** **مکان: دانشکده مهندسی کامپیوتر**
عنوان : تشخیص حملات ارائه چهره‌پردازی فریبنده مبتنی بر رویکردهای یادگیری عمیق		
داوران خارجی:جناب آقای دکتر محمد شهرام معین		**داوران داخلی: جناب آقای دکتر حامد ملک**

چکیده:

علی‌رغم پیشرفت‌های چشمگیر سیستم‌های تشخیص چهره و محبوبیت‌شان، این سیستم‌ها در معرض حملاتی موسوم به حملات ارائه چهره قرار دارند. یکی از چالش‌برانگیزترین حملات ارائه، تغییر چهره با آرایش است که می‌تواند ویژگی‌های ظاهری فرد را تغییر داده و سیستم‌های تشخیص چهره را گمراه کند. در این حوزه نوعی از حملات وجود دارند که می‌توان از آن‌ها به عنوان چهره‌پردازی یا گریم نام برد و با وجود اهمیت بسیار بالایشان، در ادبیات موضوع به آن‌ها کمتر پرداخته شده است و مجموعه داده‌ی مناسبی نیز در این زمینه وجود ندارد. این دسته از حملات بسیار طبیعی و واقع‌گرایانه‌اند و چهره افراد را به‌گونه‌ای تغییر می‌دهند که هویت اصلی آن‌ها مشخص نباشد. حملات چهره پردازی (گریم) با ابزارهای آرایشی پیشرفته، تکه‌سازی و پروتزهایی با ظاهری طبیعی انجام می‌شوند و حتی ممکن است انسان‌ها نیز قادر به تشخیص آن‌ها نباشند. از این‌روی نیاز به توسعه سیستمی خودکار با کارایی مناسب جهت تشخیص این دسته از حملات می‌باشد. با توجه به تنوع تکنیک‌های گریم و نمونه‌های ناشناخته، مدل‌سازی این حملات چالش‌برانگیز است و سیستم‌های تشخیص، نیازمند الگوریتم‌های تعمیم‌پذیر برای شناسایی انواع مختلف گریم هستند. در این پژوهش، ابتدا مجموعه داده‌ای مطابق با شرایط دنیای واقعی جمع‌آوری گردیده است. در ادامه سیستمی مبتنی بر وصله‌های چهره طراحی شده است که با بهره‌گیری از هدایت مدل مبتنی بر کل چهره و رویکرد یادگیری متریک و تعمیم دامنه، عملکردی مناسب در جهت تشخیص حملات گریم ارائه داده است؛ به‌طوری‌که ACER آن روی مجموعه‌داده‌ی گریم جمع‌آوری شده برابر با ۷.۸۲٪ شد و EER آن به مقدار ۸.۹٪ رسید. هم‌چنین ACER معماری پیشنهادی روی حمله‌ی Obfuscation و Impersonation مجموعه‌داده‌ی SiW-Mv2 برابر با ۰٪ شد و برروی حمله‌ی Cosmetics از مجموعه‌داده‌ی مذکور به مقدار ۱.۳۴٪ رسید.