****

**دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **نام استاد راهنما: جناب اقای دکتر محسن ابراهیمی مقدم** | | | **نام دانشجو: مهسا سلیمانی** | |
| **مقطع: ارشد** | **گرایش: هوش مصنوعی، رباتیکز و رایانش شناختی** | | | **رشته: مهندسی کامپیوتر** |
| **تاریخ: 22/12/1400** | | | **نوع دفاع:**   * **دفاع پروپوزال □** * **دفاع پایان نامه** * **دفاع رساله دکترا □** | |
| **ساعت: 08:00 تا 10:00** | | |
| **مکان: http://194.225.24.96/defa-computer-4** | | |
| **عنوان: تشخیص تصاویر چهره‌ی واقعی از جعلی مبتنی بر وصله در حضور انسداد** | | | | |
| **داوران داخلی: جناب اقای دکتر علیرضا طالب پور** | | **داوران خارجی: جناب اقای دکتر منصور جم زاد** | | |
| **چکیده:**  جعل عمیق به معنی به‌کارگیری یادگیری عمیق و تکنیک‌های هوش مصنوعی برای تولید یا تغییر محتوای ویدیویی و تصاویر می‌باشد. با توجه به اینکه امروزه جعل عمیق توسط برخی برنامه‌ها حتی برای کاربرانی که مهارت خاصی در رابطه با جعل عمیق ندارند می‌تواند انجام شود، زمینه و انگیزه‌ی تحقیق برای کشف و تشخیص این نوع دست‌کاری شدت گرفته است. تشخیص جعلی یا واقعی بودن تصاویر می‌تواند در بهبود عملکرد دستگاه تشخیص چهره و احراز هویت تصاویر و ویدیوهای غیراخلاقی منتشرشده از بازیگران یا محتوای منتشرشده‌ی دروغین از سیاستمداران و به‌طور کلی سوء‌استفاده از این زمینه، کاربرد داشته باشد. هم‌چنین سازمان فتا، صداوسیما، دادگاه‌ها و خبرگزاری‌ها می‌توانند از سامانه‌ی تشخیص جعل جهت اطمینان از صحت تصاویر و ویدیوها استفاده نمایند. به‌طورکلی سه دسته‌بندی برای روش‌های تشخیص تصاویر تولیدشده توسط شبکه‌های مخالف مولد وجود دارد که شامل روش‌های آماری ویژگی‌های ذاتی، تحلیل سیگنال فیزیولوژیکی و روش‌های مبتنی بر یادگیری عمیق است که رویکرد ارائه‌شده در این پژوهش مبتنی بر یادگیری عمیق می‌باشد. چالش‌های موجود در این زمینه عبارتند از تشخیص جعل تصاویر نویزی، تشخیص جعل تصاویر فشرده، تشخیص جعل تصاویر تار، تشخیص جعل تصاویر دارای انسداد، تشخیص جعل تصاویر نیم‌رخ و تشخیص تصاویر جعلی تولیدی از شبکه‌ی مخالف مولد که در مجموعه‌ی آموزشی نباشند و در مجموعه‌ی آزمایش ظاهرشده باشند. هدف از این پژوهش، ارائه‌ی یک رویکرد پیشنهادی جدید مبتنی بر وصله برای تشخیص تصاویر واقعی از جعلی و بهبود روند تشخیص با در نظر گرفتن چالش انسداد می‌باشد. هم‌چنین، از میان انواع دست‌کاری های ایجاد‌شده توسط شبکه‌های مخالف‌مولد، سنتز تمام‌چهره مورد بررسی این رساله می‌باشد. مجموعه تصاویر مورد استفاده‌ی ما شامل تصاویر جعلی و واقعی است که تصاویر جعلی شامل تصاویر تولید شده توسط شبکه های StyleGan و StyleGan2 با آموزش توسط تصاویر واقعی FFHQ و تصاویر تولیدشده توسط StarGan و PGGAN با آموزش توسط تصاویر واقعی CelebA می‌باشند و از تصاویر مجموعه داده‌های CelebA و FFHQ به عنوان تصاویر واقعی استفاده کرده‌ایم. در این پژوهش نشان داده شده است که استفاده از چند روش تشخیص، استفاده از وصله‌های چهره و حذف انسداد برای تصاویر دارای انسداد منجر به بهبود در تشخیص تصاویر جعلی از واقعی می‌شود و باعث می‌شود که رویکرد پیشنهادی در گام‌های اول پردازش نتایج بهتری را نسبت به دیگر پژوهش ها ارائه دهد. ما در مجموعه‌داده‌های اول و دوم صحت برابر با 100 درصد و در مجموعه‌داده‌ی سوم، صحت برابر با 99.7 را به دست آورده‌ایم که از بهترین مرجع 0.3 بهبود داشته‌است، در مجموعه‌داده‌ی چهارم، صحت برابر با 84 درصد را به ‌دست آورده‌ایم که نسبت به بهترین مرجع 4 درصد بهبود داشته است و در مجموعه‌داده‌ی پنجم صحت برابر با 90 درصد را به دست آورده‌ایم که نسبت به بهترین مرجع 8 درصد بهبود داشته است. | | | | |