به نام خدا

دانشگاه تهران

دانشکدگان فنی

دانشکده مهندسی برق و کامپیوتر

یادگیری ماشین

گزارش اول پروژه

اعضای گروه :

حسین سیفی ۸۱۰۱۰۰۳۸۶

محمدجواد کامیاب ۸۱۰۱۰۰۴۵۷

فروردین ۱۴۰۲

فهرست

دسته‌بندی تصاویر واقعی و مصنوعی

طبقه‌بندی تصویر مصنوعی و واقعی فرآیندی برای تعیین این است که یک تصویر صحنه‌ای واقعی را به تصویر می‌کشد یا به صورت مصنوعی تولید شده است و می‌تواند شامل هر یک از تجزیه و تحلیل جنبه‌های مختلف تصویر، مانند محتوای بصری، ویژگی‌های آماری، و فراداده[1] یا ترکیبی از آن‌ها باشد. تصاویر مصنوعی تصاویری هستند که توسط انسان یا کامپیوتر تولید می‌شوند و صحنه یا شی غیر واقعی را نشان می دهند. این تصاویر را می‌توان از طریق روش های مختلفی مانند استفاده از نرم‌افزار مدل‌سازی سه بعدی یا الگوریتم های یادگیری ماشین تولید کرد. از سوی دیگر، تصاویر واقعی، تصاویری هستند که نشان‌دهنده یک صحنه یا شی در دنیای واقعی هستند. هدف از طبقه‌بندی تصاویر مصنوعی و واقعی، تمایز دقیق بین تصاویری است که صحنه‌های واقعی را از تصاویری که صحنه‌های مصنوعی تولید شده را به تصویر می‌کشند و می‌تواند در زمینه‌های مختلف مانند گرافیک کامپیوتری، بینایی کامپیوتر و واقعیت افزوده مفید باشد.

کاربردها

یکی از کاربردهای اصلی در حوزه بینایی ماشین و تشخیص تصویر است که در آن تشخیص تصاویر واقعی و جعلی برای کارهای مختلف اهمیت بالایی دارد. به‌عنوان مثال، در بازارهای آنلاین یا وب‌سایت‌های تجارت الکترونیک، مهم است که اطمینان حاصل شود که تصاویر محصول به‌طور مصنوعی تولید یا تغییر نمی‌کنند تا از تقلب و فریب جلوگیری شود. به‌طور مشابه، در برنامه‌های امنیتی و نظارتی، برای جلوگیری از حملات جعلی، تمایز بین تصاویر واقعی و جعلی مهم است.

کاربرد دیگر این مسئله طبقه بندی در حوزه سنتز تصویر و مدل‌های مولد است. با آموزش یک طبقه‌بند برای تشخیص تصاویر واقعی و جعلی، می‌توان عملکرد مدل‌های تولیدی را ارزیابی کرد و زمینه‌های بهبود را شناسایی کرد. این می‌تواند منجر به توسعه مدل‌های مولد بهتری شود که قادر به تولید تصاویر واقعی‌تر و باورپذیرتر هستند.

علاوه بر این، این مشکل طبقه بندی می تواند در حوزه پایش و حفاظت از محیط زیست مورد استفاده قرار گیرد. با تجزیه و تحلیل تصاویر واقعی از جنگل‌ها، دریاها و کوه‌ها می‌توان تغییرات محیطی مانند جنگل زدایی یا فرسایش سواحل را شناسایی و رصد کرد. این می‌تواند به اطلاع رسانی تلاش‌های حفاظتی و بهبود درک ما از تأثیر فعالیت‌های انسانی بر محیط طبیعی کمک کند.

به‌طور خلاصه، استفاده از مسئله طبقه‌بندی برای سه گروه جنگل، دریا و کوه با تصاویر جمع‌آوری‌شده به دو صورت - یکی با استفاده از دوربین و ثبت مناظر واقعی و دیگری ایجاد شده با استفاده از هوش‌مصنوعی - کاربردهای عملی متعددی در

---

[1] Metadata

حوزه‌ها دارد. بینایی کامپیوتر، سنتز تصویر و نظارت بر محیط. با تمایز بین تصاویر واقعی و جعلی، می‌توان از تقلب و فریب جلوگیری کرد، عملکرد مدل‌های تولیدی را بهبود بخشید و تغییرات محیط طبیعی را رصد کرد.

تکنیک‌ها

چندین تکنیک در طبقه بندی تصاویر مصنوعی و واقعی مورد استفاده قرار می‌گیرند. سه مورد از بهترین تکنیک‌ها در ادامه مورد بررسی قرار می‌گیرند:

تحلیل فراداده‌ها

تجزیه و تحلیل فراداده‌ها شامل بررسی داده‌هایی مانند تاریخ، زمان، مکان، تنظیمات دوربین و سایر اطلاعات است که با یک فایل تصویری مرتبط هستند. از این اطلاعات می توان برای تعیین اینکه آیا تصویر با صحنه‌های دنیای واقعی مطابقت دارد یا به طور مصنوعی ایجاد شده است، استفاده کرد.
به عنوان مثال، اگر تصویری ادعا می کند که در یک مکان و زمان خاص گرفته شده است، می توان از تجزیه و تحلیل ابرداده برای تایید اینکه آیا تصویر با شرایط نوری مورد انتظار، الگوهای آب و هوا و سایر عوامل محیطی در آن مکان و زمان مطابقت دارد، استفاده کرد. تجزیه و تحلیل ابرداده همچنین می تواند برای تشخیص علائم دستکاری، مانند تغییر در وضوح تصویر، تنظیمات فشرده سازی، یا سایر داده هایی که ممکن است نشان دهنده تغییر تصویر باشد، استفاده شود.
برخی از تکنیک های رایج مورد استفاده در تجزیه و تحلیل ابرداده عبارتند از:

۱. تحلیل داده‌های Exif: داده‌های Exif فراداده‌هایی هستند که توسط دوربین یا دستگاهی که آن را ضبط کرده در یک فایل تصویری جاسازی می‌شوند. داده‌های Exif می‌تواند شامل اطلاعاتی درباره تنظیمات دوربین، مانند زمان نوردهی، دیافراگم، و ISO، و همچنین مکان و زمان عکس باشد. از این اطلاعات می توان برای تایید صحت تصویر و واقعی بودن آن استفاده کرد.
۲. تحلیل موقعیت جغرافیایی: تجزیه و تحلیل موقعیت جغرافیایی شامل تجزیه و تحلیل داده‌های مکان مرتبط با تصویر برای تعیین اینکه آیا با مکان ادعا شده مطابقت دارد یا خیر است. این تکنیک می تواند شامل مقایسه داده‌های مکان با پایگاه داده‌ای از مکان‌های شناخته شده برای تایید صحت آن باشد.

۳. تحلیل فایل تصویری: تجزیه و تحلیل فایل تصویری شامل بررسی ساختار و قالب فایل تصویری برای تشخیص علائم دستکاری است. این تکنیک می‌تواند شامل تجزیه و تحلیل هدر فایل، تنظیمات فشرده سازی و سایر داده‌ها برای تایید اینکه آیا تصویر با منشاء ادعا شده مطابقت دارد یا خیر باشد.

تحلیل آماری

تجزیه و تحلیل آماری تکنیکی است که در تشخیص تصاویر مصنوعی و واقعی به منظور شناسایی ناهنجاری‌ها یا الگوهایی در یک تصویر استفاده می‌شود که ممکن است نشان‌دهنده این باشند که تصویر به صورت مصنوعی تولید شده است. تجزیه و تحلیل آماری شامل تجزیه و تحلیل ویژگی های آماری مختلف تصویر، مانند توزیع شدت پیکسل، هیستوگرام رنگ، و ویژگی های بافت، برای شناسایی سازگاری آنها با دنیای واقعی است. تجزیه و تحلیل آماری ابزاری قدرتمند برای تشخیص مصنوعی یا واقعی بودن یک تصویر است، با این حال، توجه به این نکته مهم است که تجزیه و تحلیل آماری به تنهایی ممکن است برای تعیین صحت یک تصویر کافی نباشد.
تکنیک های تجزیه و تحلیل آماری بسته به کاربرد خاص و نوع تصویر مورد تجزیه و تحلیل می‌تواند متفاوت باشد. برخی از تکنیک‌های آماری رایج مورد استفاده در طبقه‌بندی تصاویر عبارتند از:

۱. تحلیل فوریه: تحلیل فوریه تکنیکی است که برای تجزیه یک تصویر به اجزای فرکانسی آن استفاده می‌شود. این تکنیک می‌تواند در شناسایی تصاویر مصنوعی مفید باشد زیرا ممکن است الگوها یا نظم‌هایی در تصاویر مصنوعی وجود داشته باشند که در دنیای واقعی رخ نمی‌دهند.
۲. مدل‌سازی مارکوف: مدل‌سازی مارکوف شامل مدل‌سازی وابستگی‌های آماری بین پیکسل‌های همسایه در یک تصویر است. این تکنیک می تواند در تشخیص اینکه آیا یک تصویر به طور مصنوعی تولید شده است مفید باشد زیرا تصاویر مصنوعی ممکن است شامل الگوهایی باشند که از وابستگی‌های آماری پیروی نکنند.
۳. فیلترهای گابور: از فیلترهای گابور برای شناسایی الگوها یا لبه‌های یک تصویر استفاده می‌شود. این فیلترها می‌توانند در شناسایی تصاویر مصنوعی مفید باشند زیرا ممکن است لبه‌ها یا الگوهایی در این تصاویر وجود داشته باشند که در صحنه های دنیای واقعی دیده نمی‌شوند.

تحلیل محتوای بصری

تحلیل محتوای بصری یک تکنیک مهم است که در طبقه بندی تصاویر مصنوعی و واقعی یک تصویر بر اساس محتوای بصری آن استفاده می شود. این تکنیک شامل تجزیه و تحلیل ویژگی‌های بصری یک تصویر، مانند رنگ‌ها، بافت‌ها، شکل‌ها و ساختارها می‌شود تا مشخص شود که آیا آنها با صحنه‌های دنیای واقعی سازگار هستند یا خیر. تجزیه و تحلیل

محتوای بصری را می توان با استفاده از تکنیک‌های مختلفی از جمله درک انسان، استخراج ویژگی و الگوریتم‌های یادگیری ماشین انجام داد. برخی از تکنیک‌های رایج مورد استفاده در تحلیل محتوای بصری عبارتند از:

۱. ادراک انسانی: ادراک انسانی شامل تجزیه و تحلیل تصویر با استفاده از تخصص بصری کارشناسان آموزش دیده برای شناسایی نشانه‌های بصری است که ممکن است نشان دهنده جعلی بودن تصویر باشد. این تکنیک می‌تواند شامل شناسایی جزئیات یا مصنوعات ظریفی باشد که تشخیص آن‌ها برای الگوریتم‌های یادگیری ماشین دشوار است.
۲. استخراج ویژگی: استخراج ویژگی شامل شناسایی و استخراج ویژگی‌های بصری از یک تصویر، مانند لبه‌ها، رنگ‌ها، بافت‌ها و اشکال است. سپس می توان از این ویژگی‌ها برای مقایسه یک تصویر با پایگاه داده‌ای از صحنه های شناخته شده در دنیای واقعی استفاده کرد تا مشخص شود که آیا تصویر با واقعیت مطابقت دارد یا خیر.
۳. الگوریتم‌های یادگیری ماشین: الگوریتم‌های یادگیری ماشین را می توان برای تجزیه و تحلیل محتوای بصری یک تصویر و طبقه بندی آن به عنوان واقعی یا جعلی بر اساس مجموعه‌ای از معیارهای از پیش تعریف شده آموزش داد. این الگوریتم‌ها را می توان با استفاده از مجموعه داده‌های بزرگی از تصاویر واقعی و جعلی آموزش داد تا الگوهای بصری و ویژگی‌هایی را که صحنه‌های دنیای واقعی را از صحنه‌های ساخته شده مصنوعی متمایز می‌کند، یاد بگیرند.

چالش‌ها

چالش‌های پیش‌پردازش

پیش پردازش یک مرحله مهم در تجزیه و تحلیل داده‌ها و یادگیری ماشین است و شامل تبدیل داده‌های خام به قالبی مناسب برای تجزیه و تحلیل است. برخی از چالش‌های مرتبط با پیش‌پردازش عبارتند از:

پاک‌سازی داده‌ها: داده‌های خام اغلب حاوی خطاها، ناسازگاری‌ها و مقادیر گم شده هستند. پاک‌سازی داده‌ها شامل شناسایی و رسیدگی به این مسائل است تا اطمینان حاصل شود که داده‌ها دقیق و کامل هستند. با این حال، این فرآیند می‌تواند زمان‌بر و چالش‌برانگیز باشد، به‌خصوص زمانی که با مجموعه داده‌های بزرگ سروکار داریم.

انتخاب ویژگی: انتخاب ویژگی شامل شناسایی مرتبط‌ترین ویژگی‌ها برای مشکل موجود است. این مهم است زیرا گنجاندن ویژگی‌های نامربوط می‌تواند منجر به برازش بیش از حد و کاهش دقت مدل شود. با این حال، انتخاب ویژگی‌های مناسب می‌تواند چالش‌برانگیز باشد، زیرا به دانش دامنه و درک مشکل نیاز دارد.

تبدیل داده‌ها: تبدیل داده‌ها به قالبی مناسب برای تجزیه و تحلیل می‌تواند چالش‌برانگیز باشد، به‌ویژه زمانی که با ساختارهای داده پیچیده سروکار داریم. برای مثال، داده‌های متنی ممکن است به تکنیک‌های پیش‌پردازش مانند نشانه ساز، ریشه‌یابی و واژه‌سازی نیاز داشته‌باشند که پیاده‌سازی آن‌ها ممکن است دشوار باشد.

مدیریت مقادیر از دست رفته: مقادیر از دست رفته ممکن است به‌دلایل مختلفی رخ دهد، مانند خطاهای ورود داده یا داده‌هایی که در دسترس نیستند. مدیریت مقادیر از دست رفته می‌تواند چالش‌برانگیز باشد، زیرا مستلزم تصمیم گیری در مورد استراتژی مقابله با آنها است، مانند انتساب یا حذف.

مقیاس بندی داده‌ها: مقیاس بندی فرآیند عادی سازی داده‌ها است تا اطمینان حاصل شود که همه ویژگی‌ها در یک مقیاس هستند. این مهم است زیرا برخی از الگوریتم‌های یادگیری ماشین به مقیاس داده‌ها حساس هستند. با این حال، انتخاب روش مقیاس بندی مناسب می‌تواند چالش‌برانگیز باشد، زیرا به توزیع داده‌ها بستگی دارد.

به‌طور کلی، پیش پردازش می‌تواند چالش‌برانگیز باشد و نیازمند بررسی دقیق داده‌های موجود و مشکل موجود است. پرداختن به این چالش‌ها ضروری است تا اطمینان حاصل شود که داده‌ها برای تجزیه و تحلیل مناسب هستند و مدل حاصل دقیق و قابل‌اعتماد است.

چالش‌های طبقه‌بندی

عدم تعادل داده‌ها: در برخی موارد، مجموعه داده ممکن است تعداد نمونه‌های مساوی برای همه کلاس‌ها نداشته‌باشد، که می‌تواند منجر به نامتعادل شدن داده‌ها شود. این می‌تواند پیش بینی دقیق طبقات اقلیت را برای طبقه بندی کننده دشوار کند. که البته این مسئله برای مجموعه‌ی داده‌ی ما مطرح نیست چرا که نمونه‌های هر کلاس برابر است.

برازش بیش از حد: برازش بیش از حد زمانی اتفاق می‌افتد که یک مدل بیش از حد پیچیده باشد و خیلی نزدیک به داده‌های آموزشی تناسب داشته‌باشد که منجر به عملکرد تعمیم ضعیف در داده‌های جدید و دیده نشده می‌شود. در مواردی که مجموعه داده کوچک یا نویزی است، این می‌تواند یک چالش باشد.

مهندسی ویژگی: انتخاب مجموعه مناسبی از ویژگی‌ها که اطلاعات مربوطه را جمع‌آوری می‌کند، می‌تواند چالش برانگیز باشد، به‌ویژه در مواردی که داده‌ها ابعاد بالایی دارند.

انتخاب الگوریتم مناسب: انواع مختلفی از الگوریتم‌های طبقه بندی وجود دارد که هر کدام نقاط قوت و ضعف خود را دارند. انتخاب الگوریتم مناسب برای مشکل موجود می تواند چالش برانگیز باشد.

پیچیدگی مدل: پیچیدگی مدل می تواند بر عملکرد آن تأثیر بگذارد. مدلی که خیلی ساده است ممکن است پیچیدگی زیربنایی داده‌ها را نشان ندهد، در حالی که مدلی که خیلی پیچیده است ممکن است بیش از حد با داده‌های آموزشی مطابقت داشته‌باشد.

چالش‌های خوشه‌بندی

انتخاب تعداد مناسب خوشه: تصمیم گیری در مورد تعداد مناسب خوشه‌ها می‌تواند چالش‌برانگیز باشد، زیرا به دانش دامنه و درک مسئله نیاز دارد.

مقیاس بندی داده‌ها: الگوریتم‌های خوشه بندی می‌توانند به مقیاس داده‌ها حساس باشند که می‌تواند بر کیفیت خوشه‌های حاصل تأثیر بگذارند.

مدیریت نقاط پرت: نقاط پرت می‌توانند به‌طور قابل توجهی بر عملکرد خوشه بندی تأثیر بگذارند، زیرا ممکن است خوشه خود را تشکیل دهند یا بر خوشه بندی سایر نقاط داده تأثیر بگذارند.

حساسیت الگوریتم: الگوریتم‌های مختلف خوشه‌بندی حساسیت‌های متفاوتی نسبت به توزیع داده‌ها، نویز و نقاط پرت دارند. انتخاب الگوریتم مناسب برای مشکل موجود می تواند چالش برانگیز باشد.

تفسیر نتایج: تفسیر نتایج خوشه‌بندی می‌تواند چالش‌برانگیز باشد، به‌ویژه زمانی که با داده‌های با ابعاد بالا سروکار داریم. این نیاز به درک ساختار زیربنایی داده‌ها و دانش دامنه دارد تا خوشه‌های حاصل را درک کند.

چالش‌های مختص فرآیند تشخیص تصویر واقعی از ساخته‌گی

کیفیت تصویر: کیفیت تصاویر گرفته شده توسط دوربین ممکن است به دلیل عواملی مانند شرایط نور، تنظیمات دوربین و عوامل محیطی متفاوت باشد. به‌طور مشابه، کیفیت تصاویر تولید شده مصنوعی ممکن است بسته به الگوریتم مورد استفاده و پارامترهای تنظیم شده متفاوت باشد. کیفیت تصاویر می تواند بر دقت مدل طبقه بندی تأثیر بگذارند. به همین دلیل باید در گام پیش‌پردازش اندازه‌ی تمامی تصاویر را یکسان می‌کنیم

استخراج ویژگی: برای طبقه‌بندی یک تصویر به عنوان واقعی یا جعلی، مدل نیاز به شناسایی ویژگی‌های مرتبط دارد که بتواند بین آنها تمایز قائل شود. با این حال، تمایز بین تصاویر واقعی و جعلی نیاز به تجزیه و تحلیل عمیق تری از تصاویر دارد و شناسایی ویژگی‌های خاص می‌تواند دشوار باشد.

برازش بیش از حد: برازش بیش از حد زمانی اتفاق می‌افتد که یک مدل بیش از حد پیچیده باشد و خیلی نزدیک به داده‌های آموزشی تناسب داشته‌باشد، و وقتی روی داده‌های جدید و دیده نشده اعمال می‌شود دقت آن کمتر می‌شود. با این مشکل، مدل می‌تواند بر روی مجموعه داده‌های موجود آموزش داده شود و عملکرد خوبی را در آن مجموعه داده نشان دهد، اما ممکن است به‌خوبی به تصاویر جدید تعمیم ندهد.

کمبود داده: مجموعه داده موجود ممکن است تصاویر واقعی و جعلی کافی برای آموزش یک مدل دقیق نداشته‌باشد. همچنین ممکن است ایجاد یک مجموعه داده بزرگ به‌اندازه کافی از تصاویر جعلی که واقعی هستند و ویژگی‌های مشابه تصاویر واقعی دارند چالش برانگیز باشد.