فن‌آوری تشخیص کپچا براساس یادگیری عمیق

چکیده

آزمون تورینگ عمومی کاملا خودکار برای تمایز بین انسان وماشین برای وب سایت است تا از حمله برنامه مخرب خودکار جلوگیری کند. مطالعات تشخیص کپچا می‌توانند شکاف‌های امنیتی در کپچا پیدا کنند، تکنولوژی کپچا را بهبود بخشند، همچنین می‌توانند فن‌آوری‌های تشخیص پلاک خودرو و تشخیص دست نویسی را ارتقا دهند. این مقاله یک روش مبتنی بر مدل شبکه عصبی کانولوشن (‏سی ان ان)‏برای شناسایی کپچا و جلوگیری از فن‌آوری سنتی پردازش تصویر مانند مکان و تقسیم‌بندی ارائه کرده‌است. نرخ یادگیری تطبیقی برای سرعت بخشیدن به نرخ هم‌گرایی مدل معرفی شده‌است و مشکل بیش از حد تناسب و راه‌حل بهینه محلی حل شده‌است. مدل آموزشی مشترک چندوظیفه‌ای برای بهبود دقت و قابلیت تعمیم تشخیص مدل استفاده می‌شود. نتایج تجربی نشان می‌دهد که این مدل اثر تشخیص خوبی بر کپچا با نویز پس‌زمینه و اعوجاج چسبندگی کاراکتر دارد.

کلمات کلیدی: شبکه عصبی کانولوشن ، کپچا ، نرخ یادگیری انطباقی آموزش مشترک چند وظیفه

مقدمه

با توسعه سریع صنعت اینترنت، مسائل امنیتی شبکه بیشتر و بیشتری اتفاق می‌افتد. فن‌آوری کپچا [‏ ۱ ]‏ طیف گسترده‌ای از کاربردها را در حفاظت از شبکه و امنیت اطلاعات دارد. کپچا مخفف آزمون تورینگ عمومی کاملا خودکار برای تشخیص بین کامپیوتر و انسان است. به عنوان یک استراتژی امنیت شبکه، عمدتا برای وب سایت‌ها استفاده می‌شود تا از حملات خودکار برنامه‌های مخرب مانند ثبت‌نام خودکار ،رای‌گیری خودکار اسپم و غیره جلوگیری شود.. برای انسان‌ها، دقت تشخیص کپچا های موثر حداقل ۸۰ % است، اما برای کامپیوترها باید کم‌تر از ۰.۰۱ % باشد. تحقیق شناسایی کپچا می‌تواند نقایص کپچا را در زمان پیدا کند، و پیشنهاد بهبود برای برنامه تولید کد ارائه دهدتا امنیت کپچا را افزایش دهد، در عین حال، به عنوان نوعی آزمون تورینگ، کپچا شناخت نتایج تحقیق پردازش تصویر و حوزه هوش مصنوعی را ترکیب می‌کند، و نقش مثبتی در توسعه فن‌آوری هوش مصنوعی، مانند شناسایی پلاک و دست نویسی ایفا می‌کند.

این مقاله بر روی پرکاربردترین تصاویر مبتنی بر کاراکتر کپچا تمرکز می‌کند که از اعداد تصادفی و حروف انگلیسی تشکیل شده‌است. تولید آن آسان است، و تحت‌تاثیر پس‌زمینه فرهنگی کاربر قرار نمی‌گیرد، و به سختی می توان آن را سرکوب کرد. ما می‌توانیم به وسیله زبان‌های برنامه‌نویسی اصلی [‏ ۳ ] تصویری ایجاد کنیم که شامل اعداد و حروف باشد. به منظور افزایش دشواری تشخیص توسط کامپیوتر، کپچا ها نیاز به اضافه کردن نویز پس‌زمینه و انجام پردازش کانتوگلوت پیچش کاراکترها دارند.

در زمینه پردازش سنتی تصویر، تکنولوژی تشخیص کپچا به پیش‌پردازش تصویر، موقعیت یابی، جداسازی کاراکتر، تشخیص کاراکتر و مراحل دیگر تقسیم می‌شود. با این حال، ایجاد یک مجموعه الگوی دقیق به دلیل کپچا پیچیده و چسبیده دشوار است. روش سنتی استخراج نقاط پیکسلی یک به یک و انطباق الگو، تنها می‌تواند کپچا های ساده راتشخیص دهدو تشخیصی برای کپچا های چسبیده و پیچیده وجود ندارد. بنابراین، یک روش کارآمدتر برای شناسایی این کپچا ها مورد نیاز است. امروزه، شبکه یادگیری عمیق به طور گسترده در تحقیقات علمی مورد استفاده قرار می‌گیرد. به عنوان یکی از نقاط مهم در زمینه تحقیقات هوش مصنوعی در سال‌های اخیر، در بسیاری از زمینه‌ها مانند تشخیص تصویر، تشخیص صحبت، پردازش زبان طبیعی و تشخیص هدف به موفقیت بزرگی دست یافته‌است. در مقایسه با روش تشخیص الگوی سنتی، بزرگ‌ترین مزیت یادگیری عمیق این است که می‌تواند ویژگی‌ها را به طور فعال بدون طراحی مصنوعی یاد بگیرد. براساس مشاهدات و الهامات بالا، یک الگوریتم شبکه عصبی کانولوشن (‏سی ان ان)‏[‏ ۴ ]‏ برای شناسایی کپچا ها پیشنهاد شده‌است. برای مساله نرخ هم‌گرایی مدل و راه‌حل بهینه سراسری، نرخ یادگیری تطبیقی برای بهبود توانایی یادگیری شبکه معرفی می‌شود و هم‌گرایی و مقاومت بهتری دارد. مدل آموزشی مشترک چندوظیفه‌ای برای سرعت بخشیدن به سرعت آموزش مدل و بهبود توانایی تعمیم مدل استفاده می‌شود. روش این مقاله به طور مستقیم از تصاویر به عنوان ورودی به سی ان ان استفاده می‌کند، لازم نیست تصویر را برای شخصیت‌ها، ویژگی‌های یادگیری فعال در فرآیند آموزش شبکه تقسیم کند. نتایج تجربی نشان می‌دهد که روش پیشنهادی اثر تشخیص خوبی بر کپچا با نویز پس‌زمینه و اعوجاج چسبندگی کاراکتر دارد.

پژوهش‌های مرتبط

روش سنتی، مکان‌یابی یک ناحیه یک عدد یا کاراکتر در یک تصویر و سپس بخش‌بندی و شناسایی کاراکترهای منفرد است [‏ ۵، ۶ ]‏. از طریق این دو مرحله، شخصیت‌ها در تصویر شناسایی می‌شوند. به عنوان مثال، یان و احمد، به طور موفقیت آمیزی کپچا های مایکروسافت را تقسیم‌بندی کردند و آن را با چندین طبقه بند با نرخ شناسایی ۶۰ % شناسایی کردند [‏ ۷ ]‏. موری و مالک با استفاده از روش بافت شکل، کپچا ها را در تصاویر تشخیص می‌دهند [‏ ۸ ]‏. همچنین شلپلیا و سیمارد کپچا را با بخش‌بندی کاراکترهای منفرد و شناسایی آن‌ها حل می‌کنند. محققان داخلی همچنین تحقیقاتی در مورد به رسمیت شناختن کپچا براساس روش تقسیم‌بندی انجام داده‌اند. وانگ یانگ و همکارانش استفاده ازK نزدیک‌ترین همسایه ‏KNN)‏)را پیشنهاد کردند. فن‌آوری برای تایید کد [‏ ۹ ]‏. ژانگ شویا و همکاران از طریق بخش‌بندی کپچا ها، بخش‌بندی نتایج توسط طبقه‌بندی کننده KNN، شبکه پس انتشار ‏BP)‏)و ماشین بردار پشتیبان ‏SVM)‏)شناسایی شدند و نرخ‌های تشخیص همگی بالای ۹۵ % بودند [‏ ۱۰ ]‏.

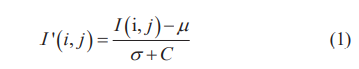
با این حال، به منظور جلوگیری از شناسایی خودکار کپچا توسط کامپیوتر و بهبود امنیت شبکه، کاراکترهای موجود در کپچا ها تا حدی با هم همپوشانی می‌کنند، به طوری که تقسیم یک کاراکتر بسیار دشوار می‌شود و در نتیجه بر دقت تشخیص تاثیر می‌گذاردبا توجه به مشکلات بالا، در مواجهه با محدودیت‌های روش‌های پردازش تصویر سنتی، لکان و همکارانش استفاده ازیادگیری عمیق را پیشنهاد کردند. برای استخراج ویژگی‌های تصویر از روش‌های یادگیری برای شناسایی ارقام دست‌نویس و برای طبقه‌بندی آن‌ها از شبکه‌های عصبی کانولوشن استفاده شد [‏ ۱۱ ]‏. با این حال، همه آن‌ها باید تصاویر را تقسیم کنند. در عوض، ما از کل تصاویر به عنوان ورودی استفاده می‌کنیم تا نتیجه را به طور مستقیم به دست آوریم.

روش پیشنهادی

1. نرمال سازی کنتراست

عادی‌سازی کنتراست می‌تواند از اشباع خروجی نورون ناشی از مقدار ورودی مطلق بیش از حد جلوگیری کند و اطمینان حاصل کند که مقادیر کوچک در داده‌های خروجی بلعیده نخواهند شد

این روش می‌تواند تعمیم شبکه را افزایش دهد، تاثیر روشنایی و واریانس کنتراست را به طور موثر در شبکه از بین ببرد، تا حد زیادی وابستگی بین عوامل همسایه را کاهش دهد و هم‌گرایی شبکه را شتاب بخشد.. قبل از آموزش شبکه، این مقاله تصویر را برای نرمال سازی کنتراست استخراج می‌کند. مقدار روشنایی تصویر(i,j) را به I(i,j) ، و مقدار روشنایی پس از نرمال‌سازی کنتراست محلی را به I’(I,j) تنظیم کنید، روش نرمال‌سازی کنتراست [‏ ۱۲ ]‏ را می توان به صورت زیر بیان کرد:

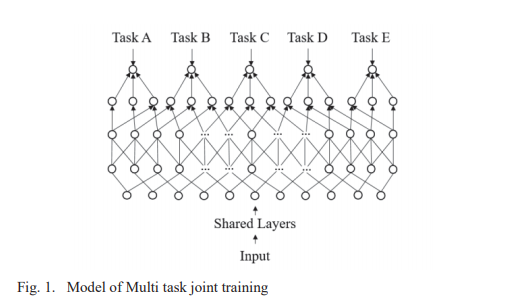


که در آن، i و M , N اندازه ابعاد بلاک تصویر هستند و C ثابت 1 است واز مخرج صفر جلوگیری می‌کند. ، میانگین و انحراف معیار مقادیر پیکسل تصویر است.

1. آموزش مشترک چند وظیفه‌ای

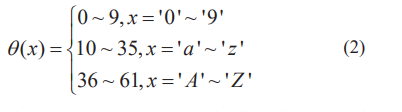
یادگیری چند وظیفه ای یک روش یادگیری ماشینی در مقابل یادگیری تک وظیفه است. هدف اصلی بهبود قابلیت تعمیم با استفاده از اطلاعات خاص دامنه در سیگنال‌های آموزشی پنهان در وظایف متعدد مرتبط است. یادگیری چند وظیفه‌ای می‌تواند این کار را با استفاده از نمایش مشترک برای آموزش موازی چند وظیفه انجام دهد. به اشتراک گذاری پارامترهای شبکه یادگیری چندوظیفه، و می‌تواند تعداد مدل‌ها را کاهش دهد، کارایی یادگیری را بهبود بخشد.

در طول آموزش مدل تشخیص کپچا، برچسب‌های تصاویر به چند وظیفه یادگیری تقسیم می‌شوند، هر وظیفه یک کاراکتر را آموزش می‌دهد و همه وظایف با هم آموزش داده می‌شوند. ساختار شبکه آموزشی مشترک چندوظیفه‌ای در شکل نشان‌داده شده‌است.

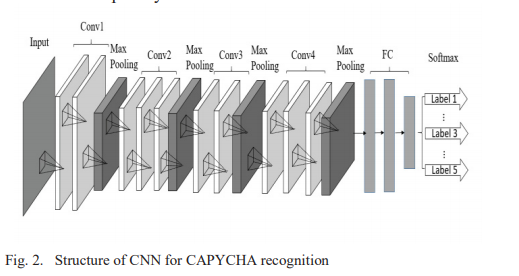


مدل شناخت CAPTCHA

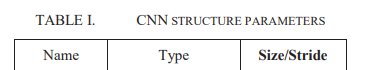
] VGG - Net 13]‏ یک شبکه عصبی کانولوشن است که توسط گروه هندسه بصری آکسفورد توسعه‌یافته است.. این مدل مبتنی بر معماری شبکه الکس –نت ] ۱۴ ] است ، که لایه convolutional را عمیق‌تر می‌سازد و اندازه هسته کانولوشن را کاهش می‌دهد . با بهبود این دو جنبه , عملکرد of - Net نیز به شدت بهبود یافته‌است . با توجه به مزایای شبکه VGG - Net , که با کار این مقاله ترکیب می‌شوند , ما یک روش عمیق سی ان ان را برای به رسمیت شناختن مجموعه‌ای از شخصیت‌ها بدون تقسیم‌بندی ارائه می‌کنیم . ساختار شبکه که ما از آن استفاده می‌کنیم در شکل ۱ نشان‌داده شده‌است . ۲ . هر تصویر CAPTCHA حاوی ۶ نویسه است . در لایه خروجی هر ۶۲ نورون یک کاراکتر را پیش‌بینی می‌کنندما یک (x) bijection را تعریف می‌کنیم که متصل میکند کارکترهای به اعداد :

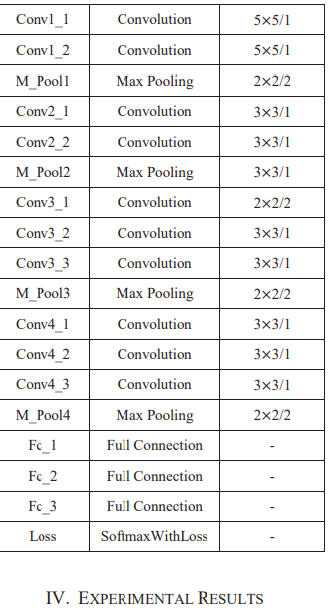


ما ۶۲ نورون خروجی اول را به کاراکتر اول توالی، ۶۲ نورون دوم را به کاراکتر دوم و غیره اختصاص می‌دهیم. لایه خروجی دارای 5\*62=310 نورون‌ است.



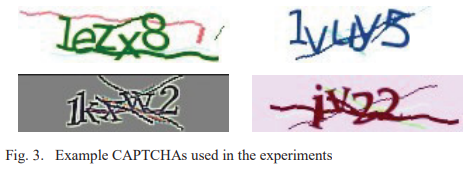
اندازه ورودی مجموعه آموزشی در این مقاله ۲۲۴ \* ۲۲۴ , لبه نقشه ویژگی ورودی بسط داده می‌شود , به طوری که اندازه نگاشت ویژگی خروجی همانند نگاشت ویژگی خروجی است . پارامترهای هر لایه از مدل در جدول.1



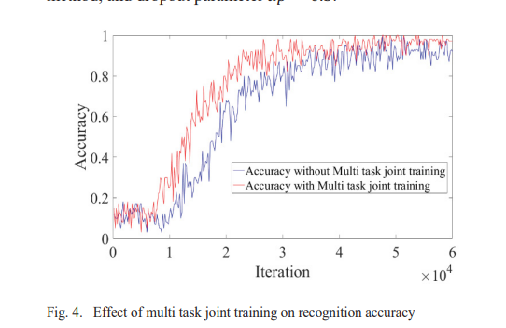


جدول 1محیط سخت‌افزار آزمایشی ویندوز ۱۰ 64 بیتی , CPU اینتر پنتیوم G3258، RAM ۸ گیگابایت و کارت گرافیکی NVIDIA GT980Ti است . محیط نرم‌افزاری که در این آزمایش استفاده می‌شود TensorFlow است . از آنجا که هیچ مجموعه داده کپچا عمومی وجود ندارد که بتواند در حال حاضر مورد استفاده قرار گیرد ، و آموزش مدل‌های شبکه عصبی به تعداد زیادی داده نیاز دارد . برای حل این مشکل ، از یک اسکریپت پیتون برای تولید تصاویر CAPTCHA با ۵ شخصیت استفاده می‌کنیم .

هر شخصیت به طور تصادفی از مجموعه‌ای از ۱۰ رقم و ۲۶ حرف انگلیسی برداشته می‌شود و شخصیت‌ها تحریف می‌شوند . در طی تولید CAPTCHA ، ما تصاویر تکراری را حذف کردیم تا قابلیت اطمینان مدل را تضمین کنیم . اندازه تصاویر 48\*128 است . مجموعه آموزشی شامل تصاویر ، مجموعه اعتبار سنجی شامل تصاویر و مجموعه تست شامل ۱۰۰۰ تصویر است . شکل ۳ نمونه‌هایی از CAPTCHA تولید شده ما را نشان می‌دهد .



در این مقاله یک الگوریتم گرادیان تصادفی SGD ) ) برای آموزش مدل مورد استفاده قرار می‌گیرد و راه‌حل بهینه کلی از طریق تعداد زیادی از تکرارها بدست می‌آید . از این مساله اجتناب می‌کند که تابع ضرر وقتی که مدل به حالت بهینه محلی همگرا می‌شود , کاهش نمی‌یابد . نرخ یادگیری تغییرات با توجه به تعداد تکرار ، و نرخ یادگیری از طریق فرمول ، که در آن نرخ یادگیری پایه ، ضریب میرایی نرخ یادگیری و iتعداد فعلی تکرار است ، تغییر خواهد کرد . لایه اتصال کامل از روش حذف و پارامتر حذف dp=0.5 استفاده می‌کند.

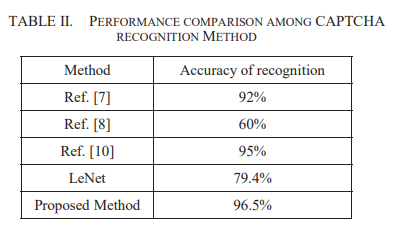


ما به بررسی تاثیر آموزش مشترک چند وظیفه‌ای و آموزش تک وظیفه‌ای بر روی مدل با استفاده از روش کنترل متغیر می‌پردازیم .

نتایج در شکل ۱ نشان‌داده شده‌است . نتایج نشان می‌دهد که استفاده از حالت آموزش مشترک چند وظیفه‌ای سرعت هم‌گرایی سرعت و دقت بالاتر را نسبت به مدل واحد آموزشی واحد دارد .

روش ارزیابی عملکرد ارائه‌شده توسط این روش , صحت تشخیص است . جدول Ⅱ عملکرد روش‌های مختلف برای شناسایی کپچا , از جمله شبکه‌های عصبی BP , SVM و الگوریتم‌های knn را نشان می‌دهد .

با این حال ، تمام روش‌های بالا نیاز به preprocess و بخش‌بندی تصاویر برای رسیدن به هدف شناسایی دارند . این مقاله همچنین عملکرد شبکه عصبی کانولوشن کلاسیک را با همان مجموعه داده‌ها مقایسه می‌کند . نتایج نشان می‌دهد که در مقایسه با روش‌های دیگر ، روش پیشنهادی نیازی به تجزیه کردن کاراکترها در تصاویر ندارد و عملکرد شناخت بهتری دارد .



.vنتیجه‌گیری و کاره‌ای آینده

کپچا یک روش آزمایشی است که برای تمایز بین انسان و ماشین در محیط شبکه به کار می‌رود.مطالعات انجام‌شده بر روی شناسایی CAPTCHA می‌تواند نقاط ضعف در امنیت را شناسایی کرده و در نتیجه مانع از نفوذ بدخواهانه ای در شبکه شود . در این مقاله , یک تکنولوژی تشخیص هویت مبتنی بر شبکه عصبی مصنوعی براساس مدل شبکه عصبی مصنوعی پیشنهاد شده‌است .تشخیص اختلال شخصیت تصاویر و چسبندگی , و همه حروف در تصویر را می‌توان بدون تقسیم‌بندی به رسمیت شناخت .

مدل آموزش مشترک چند وظیفه‌ای برای بهبود سرعت یادگیری شبکه و توانایی تعمیم مدل معرفی شده‌است و ساختار شبکه modularized است که می‌تواند طول کاراکتر متفاوت تصویر CAPTCHA را با تغییر جزیی تشخیص دهد . نتایج تجربی نشان می‌دهد که روش پیشنهادی دارای یک اثر تشخیص خوب است و دقت تشخیص به ۹۶.۵ % می‌رسد . در کار آینده ، به رسمیت شناختن شخصیت‌های چینی به رسمیت شناخته خواهد شد .