به نام خدا

عنوان مقاله:

فناوری تشخیص CAPTCHA مبتنی بر یادگیری عمیق

ارائه دهنده:

زهرامصلح

فهرست مطالب:

چکیده

- CAPTCHA، یک فناوری مهم ماشینی انسان برای وب سایت برای جلوگیری از حمله خودکار برنامه مخرب است.
- شناساییCAPTCHA می تواند فناوری های تشخیص پلاک و تشخیص دست خط را ارتقا دهد و نقض امنیت در CAPTCHAرا پیدا کند.
- این مقاله برای شناسایی CAPTCHAو جلوگیری از فناوری سنتی پردازش تصویر مانند مکان تقسیم بندی کپچا، روشی مبتنی بر مدل شبکه عصبی کانولوشن (CNN) را پیشنهاد داده است.

چکیده (ادامه)

- نرخ یادگیری انطباقی برای تسریع میزان همگرایی مدل، معرفی گردیده و به روش بهینه محلی حل شده است.
- از مدل آموزش مشترک چند وظیفه ای برای بهبود دقت و توانایی تعمیم شناخت مدل استفاده می شود .
- نتایج تجربی نشان می دهد که مدل دارای اثر تشخیص خوبی بر CAPTCHA با شلوغی پس زمینه و اعوجاج چسبندگی کاراکتر است.

۱- مقدمه

- فناوری کپچا طیف گسترده ای از برنامه ها را در محافظت از شبکه و امنیت اطلاعات دارد. به عنوان یک استراتژی امنیتی شبکه، عمدتا برای وب سایت ها استفاده می شود تا از حملات خودکار برنامه های مخرب مانند ثبت نام خودکار، هرزنامه، رای گیری خودکار و غیره جلوگیری کند.

- مزایای تحقیق در مورد CAPTCHAمی تواند نقایص کپچا را به موقع پیدا کند و پیشنهادات بهبودی را برای برنامه تولید کد ارائه دهد و امنیت کپچا را افزایش دهد.

۱- مقدمه (ادامه)

- برای انسان، دقت تشخیص CAPTCHAهای موثر حداقل ۸۰٪ است، اما برای رایانه ها، باید کمتر از یکصدم درصد باشد.
- این مقاله بربیشترین و پرکاربردترین تصاویر مبتنی بر کاراکتر CAPTCHAرا که از اعداد تصادفی و حروف انگلیسی تشکیل شده است متمرکز می شود.
- تولید CAPTCHAآسان است، تحت تأثیر زمینه فرهنگی کاربر قرار نمی گیرد.
- می توانیم توسط زبانهای اصلی برنامه نویسی تصویری حاوی اعداد و حروف ایجاد کنیم و به منظور افزایش دشواری تشخیص توسط رایانه، به CAPTCHA ها نویز پس زمینه را اضافه کرده و کاراکترهای پردازشی را پیچ و تاب دار کنیم.

۱- مقدمه (ادامه)

- در زمینه پردازش تصویر سنتی، فناوری تشخیص CAPTCHAبه مراحل پیش پردازش تصویر، موقعیت یابی، تقسیم کاراکتر، تشخیص کاراکتر و سایر مراحل تقسیم می شود. با این حال، ایجاد یک مجموعه الگوی دقیق به دلیل چسبیدگی و پیچیدگی CAPTCHAدشوار است.
- روش سنتی استخراج نقاط پیکسل یک به یک و تطبیق الگو، فقط می تواند CAPTCHAهای ساده را تشخیص دهد، در حالی که هیچ روش کارآمد برای شناسایی CAPTCHAچسبیده و پیچیده وجود ندارد. بنابراین، یک روش کارآمد تر برای شناسایی چنین CAPTCHAمورد نیاز است.

۱- مقدمه (ادامه)

- امروزه، شبکه یادگیری عمیق به عنوان یکی از نقاط مهم در زمینه تحقیقات هوش مصنوعی در سال های اخیر، در بسیاری از زمینه ها مانند شناسایی تصویر، تشخیص گفتار، ... پردازش زبان طبیعی و تشخیص هدف موفقیت زیادی کسب کرده است.

- در مقایسه با روش تشخیص الگوی سنتی، بزرگترین مزیت یادگیری عمیق این است که می توان بدون طراحی مصنوعی ویژگیها را به طور فعال یاد گرفت.

۲- تحقیقات مرتبط

- الگوریتم شبکه عصبی کانولوش(CNN) برای شناسایی کپچا پیشنهاد شده است. برای مسئله نرخ همگرایی مدل و راه حل بهینه جهانی، نرخ یادگیری انطباقی برای بهبود توانایی یادگیری شبکه معرفی شده است و از همگرایی و استحکام بهتری برخوردار است.روش این مقاله مستقیماً از تصاویر به عنوان ورودی استفاده می کند

- روش سنتی شناسایی کاراکتر:

- ۱) یک عدد یا مناطق مشخصه را در یک تصویر قرارداده می دهیم.
- ۲) کاراکترهای جداگانه را تقسیم و شناسایی می کنیم .

۲- تحقیقات مرتبط

- با این حال، به منظور جلوگیری از شناسایی CAPTCHAبه طور خودکار توسط رایانه و بهبود امنیت شبکه، کاراکترهای CAPTCHAفعلی تا حدی با هم همپوشانی دارند، به این ترتیب تقسیم کاراکتر منفرد بسیار دشوار می شود و در نتیجه بر دقت تشخیص تأثیر می گذارد.
- درمواجهه با محدودیت روشهای سنتی پردازش تصویر، پیشنهاد شد که از روشهای یادگیری عمیق برای شناسایی ارقام دست نویس استفاده شود و از شبکه های عصبی کانولوشن برای استخراج ویژگی های تصویر و سپس طبقه بندی آنها استفاده شود. با این حال، همه آنها باید تصاویر را تقسیم کنند. در عوض، از کل تصاویر به عنوان ورودی استفاده می کنیم تا مستقیماً نتیجه بگیریم.

۳- روش پیشنهادی

- الف - نرمال سازی کنتراست
- ب - آموزش مشترک چند وظیفه ای
- ج- مدل شناسایی CAPTCHA

الف – نرمال سازی کنتراست:

- نرمالسازی از اشباع خروجی نورون ناشی از مقدار ورودی مطلق بیش از حد جلوگیری میکند.
- اطمینان حاصل میکند که مقادیر کوچک در داده های خروجی ازبین نمیروند.
- تعمیم شبکه افزایش می یابد.
- تأثیر روشنایی و واریانس، کنتراست را به طور موثر بر روی شبکه از بین برده و می تواند وابستگی بین عوامل همسایه را بسیار کاهش دهد و همگرایی شبکه را تسریع کند.

الف - نرمال سازی کنتراست(ادامه)

- قبل از آموزش شبکه، این مقاله تصویر را برای نرمال سازی کنتراست استخراج می کند. مقدار روشنایی تصویر (i,j)را به I(i,j) تنظیم میکند و مقدار روشنایی پس از نرمال سازی کنتراست محلی I′(i,j) می شود، روش نرمال سازی کنتراست می تواند به صورت زیر بیان شود.
- i متعلق به مجموعه {1,2,3,…,M} و j متلعق به مجموعه {1,2,3,…,N} ، M,N ابعاد بلوک های تصویر است. C ثابت ۱ برای اجتناب از مخرج صفر است. μ وσ میانگین و انحراف معیار مقادیر پیکسل تصویر است.

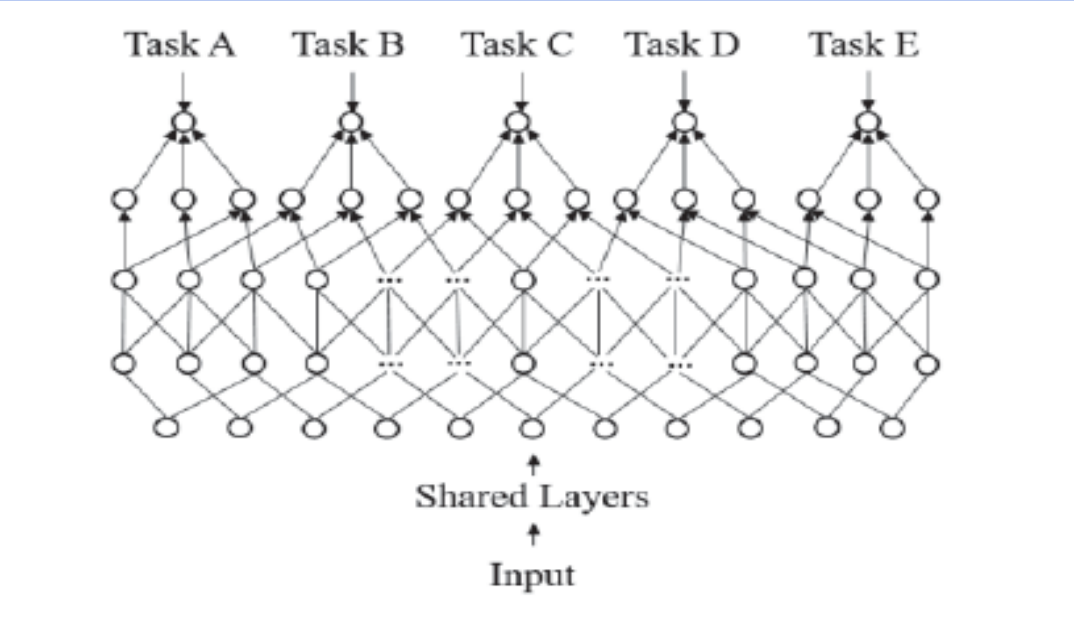
$$I'(i,j)=\frac{I(i,j)-\mu}{\sigma+C} \qquad (1)$$

ب – آموزش مشترک چند وظیفه ای

- یادگیری چند وظیفه ای روشی برای یادگیری ماشین در مقابل یادگیری تک وظیفه است.
- هدف اصلی بهبود توانایی تعمیم با استفاده از اطلاعات خاص دامنه در سیگنالهای آموزشی پنهان در چندین کار مرتبط است.
- اشتراک پارامتر شبکه یادگیری چند وظیفه ای، می تواند تعداد مدلها را کاهش دهد، بهره وری یادگیری را بهبود بخشد.

ب – آموزش مشترک چند وظیفه ای(ادامه)

- در طول آموزش مدل شناسایی CAPTCHA، برچسب های تصاویر به چندین وظیفه یادگیری تقسیم شده، هر کار یک کاراکتر را آموزش می دهد و همه وظایف را با هم آموزش می دهد.



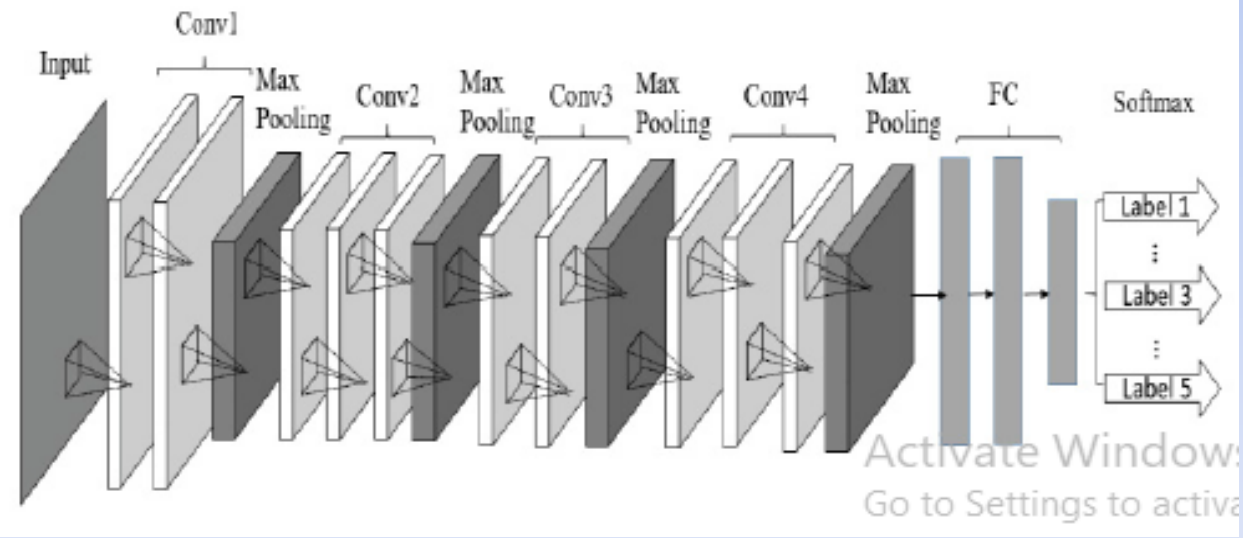
ج- مدل شناسایی CAPTCHA

- VGG Net یک شبکه عصبی کانولوشن است که توسط گروه هندسه بینایی آکسفورد ساخته شده است. این مدل براساس معماری شبکه Alex Net ساخته شده است که لایه کانولوشن را عمیقتر می کند و اندازه هسته کانولوشن را کاهش می دهد. از طریق بهبود این دو جنبه، عملکرد VGG Net بسیار بهبود یافته است. با توجه به مزایای VGG Net، همراه با کار این مقاله، ما یک روش CNN عمیق برای شناسایی یک سری از کاراکترها بدون تقسیم بندی قبل ارائه می دهیم.

$$\theta(x)=\begin{cases}0\sim 9, x='0'\sim'9'\\ 10\sim 35, x='a'\sim'z'\\ 36\sim 61, x='A'\sim'Z'\end{cases} \qquad (2)$$

ج- مدل شناسایی CAPTCHA (ادامه)

- هر تصویر CAPTCHA شامل ۶ کاراکتراست. در لایه خروجی، هر ۶۲ نورون یک کاراکتررا پیش بینی می کند. ما یک $\theta(x)$ انتخابی تعریف می کنیم که یک کاراکتر x متعلق است به {0,1,….9,a,b,….,z , A,B,...,Z} به یک عدد صحیح l که متعلق است به مجموعه {0,…,61}
- ۶۲ نورون اول خروجی را به کاراکتر اول، ۶۲ نورون دوم را به کاراکتر دوم و غیره اختصاص می دهیم. لایه خروجی دارای ۳۱۰=۶۲×۵ نورون است



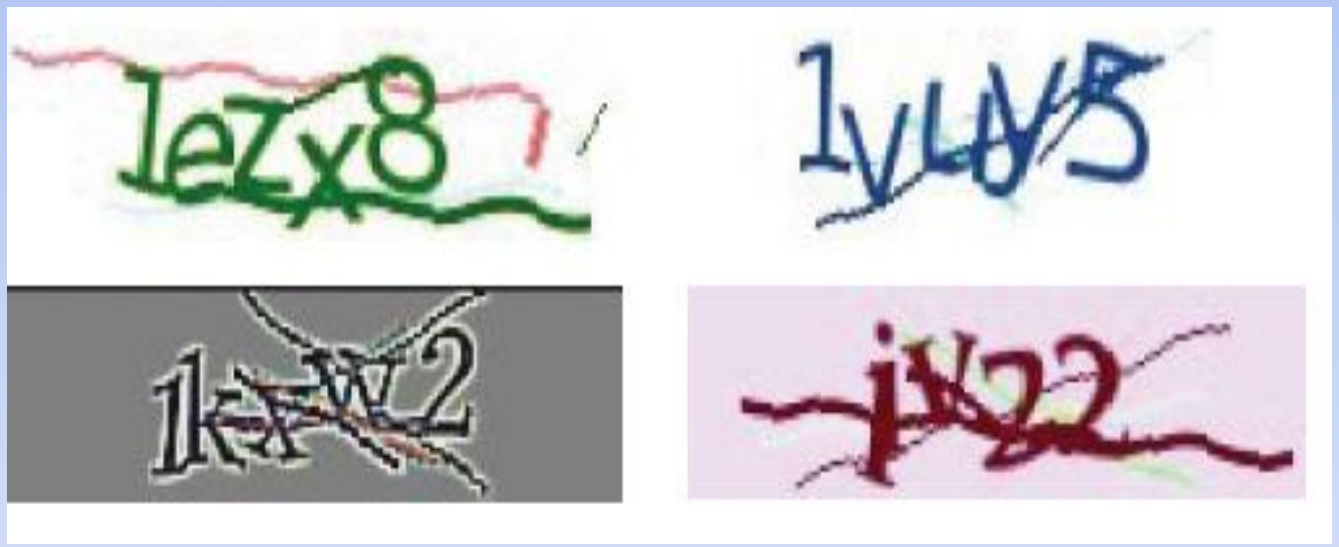
۴- نتایج تجربی

- از آنجا که هیچ مجموعه داده CAPTCHAعمومی وجود ندارد که بتوان در حال حاضر از آن استفاده کرد، و آموزش مدل های شبکه عصبی کانولوشن به تعداد زیادی داده نیاز دارد. برای حل این مشکل، ما از اسکریپت پایتون برای تولید تصاویر CAPTCHAبا ۵ کاراکتر استفاده می کنیم.

- هر کاراکتر به طور تصادفی از یک مجموعه ۱۰ رقمی و ۲۶ حرف انگلیسی گرفته می شود و کاراکترها تحریف می شوند. در طول تولید CAPTCHA، ما تصاویر تکراری را حذف کردیم تا از قابلیت اطمینان حاصل کنیم.

۴- نتایج تجربی(ادامه)

- مجموعه آموزش شامل 5×10^4تصاویر، مجموعه اعتبار سنجی شامل 2×10^4 تصویر و مجموعه آزمون شامل ۱۰۰۰ تصویر است.

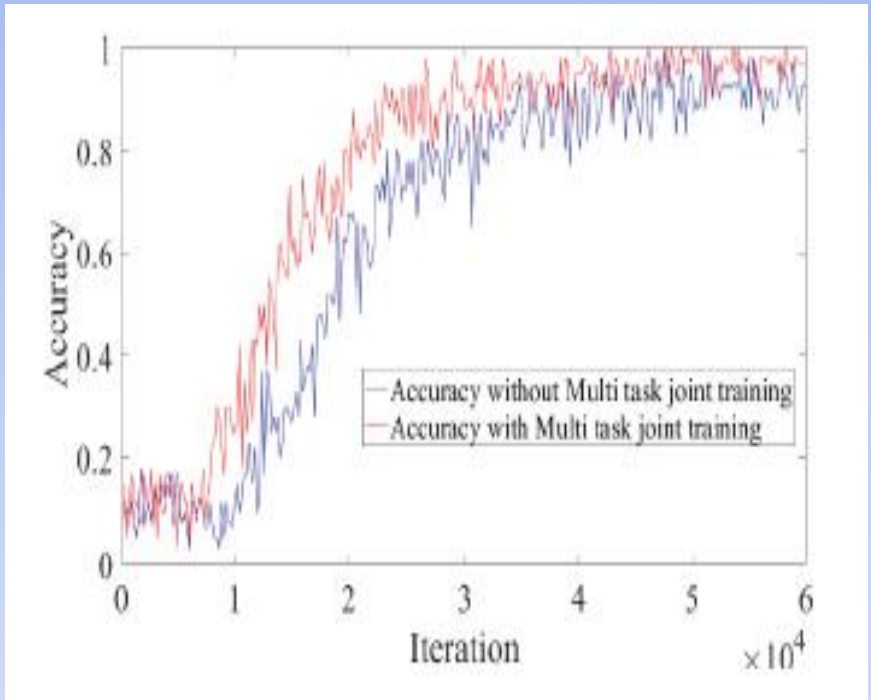


۴- نتایج تجربی(ادامه)

- در این مقاله، از الگوریتم نزول شیب تصادفی (SGD) برای آموزش مدل استفاده شده است و راه حل بهینه جهانی با تعداد زیادی تکرار حاصل می شود. با اینکار از این مسئله جلوگیری می شود که وقتی مدل به یک بهینه محلی می رسد، عملکرد از دست دادن کاهش نمی یابد و میزان یادگیری به صورت سازگار است.
- با توجه به تعداد تکرار تغییر می کند، و میزان یادگیری با فرمول $lr=lr_o\times(1/(1+decay\times i))$ تغییر می کند، جایی که نرخ یادگیری پایه $lr_0=0.001$ عامل کاهش میزان یادگیری $decay=0.0001$ و i تعداد فعلی تکرار است.

۴- نتایج تجربی(ادامه)

تأثیر آموزش مشترک چند وظیفه ای بر دقت تشخیص



با استفاده از روش کنترل متغیر، تأثیر آموزش مشترک چند وظیفه ای و آموزش تک وظیفه را بر روی مدل بررسی می کنیم.نتایج نشان می دهد که استفاده از حالت آموزش مشترک چند وظیفه ای(نمودارقرمز) دارای سرعت همگرایی سریعتر و دقت بالاتری نسبت به مدل آموزش تک وظیفه است.

۴- نتایج تجربی(ادامه)

مقایسه عملکرد در بین روش شناسایی CAPTCHA

Method	Accuracy of recognition
Ref. [7]	92%
Ref. [8]	60%
Ref. [10]	95%
LeNet	79.4%
Proposed Method	96.5%

روش ارزیابی عملکرد ارائه شده توسط روش، دقت تشخیص است. جدول عملکرد روشهای مختلف برای شناسایی CAPTCHAرا نشان می دهد، از جمله شبکه های عصبی BP، الگوریتم های SVMو KNN.با این وجود، برای دستیابی به هدف شناسایی، همه روش های فوق نیاز به پیش پردازش و تقسیم تصاویر دارند. این مقاله همچنین عملکرد شبکه عصبی کانولوشن کلاسیک LeNetرا با همان مجموعه داده مقایسه می کند. نتایج نشان می دهد، در مقایسه با سایر روش ها، روش پیشنهادی نیازی به تقسیم کاراکترها در تصاویر ندارد و عملکرد بهتری دارد.

۵- نتیجه گیری و کار آینده

- CAPTCHAیک روش آزمایشی است که برای تمایز بین انسان و ماشین در محیط شبکه استفاده می شود. مطالعات مربوط به شناسایی CAPTCHAمی تواند آسیب پذیری های امنیتی CAPTCHAرا بهتر تشخیص دهد، در نتیجه از برخی از نفوذهای مخرب در شبکه جلوگیری می کند. در این مقاله، یک فناوری شناسایی CAPTCHمبتنی بر شبکه عصبی کانولوشن با توجه به CAPTCHAاز اعوجاج و چسبیدگی کاراکتر تصاویر است و همه کاراکترهای تصویر بدون تقسیم بندی قابل تشخیص هستند. مدل آموزش مشترک چند وظیفه ای برای بهبود سرعت یادگیری شبکه و توانایی تعمیم مدل معرفی شده است که میتواند با تغییر اندکی طول کاراکتر متفاوت تصویر CAPTCHAرا تشخیص دهد. نتایج تجربی نشان می دهد که روش پیشنهادی اثر تشخیص خوبی دارد و دقت تشخیص به ۹۶.۵ درصد می رسد. در کار آینده، تشخیص حروف چینی CAPTCHAاضافه خواهد شد.

تصدیق این کار توسط بنیاد علوم طبیعی ملت چین پشتیبانی شد.

مقاله های مرتبط با این مقاله

A CAPTCHA recognition technology based on deep learning

Y Hu, L Chen, J Cheng - 2018 13th IEEE Conference on …, 2018 - ieeexplore.ieee.org

1) Versatile CAPTCHA Generation Using Machine Learning and Image Processing

V Deshmukh, S Deshmukh… - 2020 IEEE 5th …, 2020 - ieeexplore.ieee.org

2) CAPTCHA Recognition Using Deep Learning with Attached Binary Images

A Thobhani, M Gao, A Hawbani, STM Ali… - Electronics, 2020 - mdpi.com

3)A novel CAPTCHA scheme based on facial expression reconstruction

M Moradi, MR Keyvanpour- International Journal of ..., 2020 - inderscienceonline.com

سپاس از همراهی شما عزیزان