آزمون تصویری بازشناسی انسان از ماشین مبتنی بر تبدیلات هندسی

مریم مهرنژاد، عباس قائمی بافقی، احد هراتی، احسان تورینی
دانشگاه فردوسی مشهد
هشتمین کنفرانس بین المللی انجمن رمز ایران
شهریور ۹۰- مشهد- ایران

فهرست مطالب

فهرست مطالب

مقدمه

- کپتچا مخفف Completely Automated Public Turing Test To Tell Computers And Humans Apart به معنی تست عمومی کاملاً خودکار تورینگ برای تشخیص انسان از کامپیوتر می-باشد.
- در واقع کپتچا یک نوع تغییر یافته تست معروف- آلن -تورینگ است.
- اولین کپچا در سال ۲۰۰۰ برای سایت یاهو و در دانشگاه کارنگی ملون ساخته شد. و پس از آن به صورت قابل ملاحظه-ای در ۱۰ سال گذشته مورد توجه- محققان قرار گرفته-اند.
- ما عبارت آزمون بازشناسی انسان از ماشین (آبام) را به عنوان معادل فارسی کپتچا انتخاب کرده و در این مقاله از آن استفاده می کنیم.

مقدمه ...

- در منابع مختلف برای ارزیابی آبام از ویژگی-های مختلفی از جمله موارد زیر استفاده شده است :
  - خودکار: سوال تست باید به راحتی توسط کامپیوتر قابل تولید و جواب آن قابل ارزیابی یا نمره-دهی باشد.
  - باز بودن: الگوریتم-ها و پایگاه داده-هایی که به منظور تولید سوال و ارزیابی جواب آبام بکار می-روند باید عمومی باشند. این ویژگی بر اساس اصل کرچفز می-باشد. اصل کرچفز بیان می-کند که یک سیستم حتی درصورتی که تمام اطلاعاتش به صورت عمومی منتشر شود، همچنان باید امن باقی بماند.
  - قابل استفاده: تست-ها باید در زمان معقولی و به آسانی توسط انسان قابل حل باشند. علاوه بر آن تست-ها معمولا طوری طراحی می-شوند که کمترین وابستگی را به زبان کاربر، مکان فیزیکی، تحصیلات و یا توانایی-های ادراکی وی داشته باشند.
  - امن: تست-ها باید برای ماشین سخت و بطور الگوریتمیک غیرقابل حل باشد.

مقدمه ...

- در حال حاضر آبامهای مبتنی بر متن به علت طراحی و پیاده-سازی ساده و بالا بودن قابلیت استفاده،- بطور قابل ملاحظه-ای در وب سایت-ها استفاده می-شوند.
- با توجه به پیشرفت علم پردازش تصویر روش-های حمله به آبام ها در قالب الگوریتم-های OCR گسترش یافته است.

مقدمه ...

- اولین ایده های استفاده از تصویر برای شناسایی انسان از ماشین در ESP-PIXبه کار برده شد. در این آبام از یک پایگاه داده محدود برچسب گذاری-شده، چند عکس با موضوع یکسان به کاربر نمایش داده می-شود و کاربر باید محتوای عکس را تشخیص و از یک لیست انتخاب کند.
- کپتچاهای تصویری به دلیل جذابیت ذاتی، در حال حاضر مورد استقبال کاربران و در نتیجه مورد توجه طراحان می-باشند.

مقدمه ...

- روش-های مبتنی بر تصویر متفاوتی جهت بازشناسی خودکار انسان از ماشین وجود دارد.
  - در برخی از این روش-ها یک عکس از یک مجموعه تصاویر به کاربر نمایش داده می-شود و از وی خواسته می-شود تا تصویر را شناسایی کند.
  - در روش-های پیشرفته-تر و امن-تر پس از اینکه عکس از یک مجموعه تصاویر انتخاب شد، مجموعه-ای از تبدیلات بر روی عکس اعمال شده و عکس تغییر-یافته به جای عکس اصلی به کاربر نمایش داده می-شود. در این مقاله یک روش جدید مبتنی بر تبدیلات هندسی پیشنهاد، پیاده-سازی و ارزیابی شده است.

فهرست مطالب

آبام پیشنهادی

- در این مقاله یک روش جدید برای توسعه یک آبام مبتنی بر تصویر ارائه شده است که در آن احتیاجی به یک پایگاه داده بزرگ عکس و یا مجموعه بزرگی از برچسب-های ذخیره شده نیست.
- در این مقاله از یک پایگاه داده عکس ثابت ۳۰ تایی استفاده شده است. هرکدام از این عکس ها با نام خود برچسب زده شده-اند.
  - این برچسب-ها برای انسان مبهم نبوده و قابل شناسایی می-باشند.
- این عکس-ها با استفاده از یکسری از تبدیلات هندسی بر روی یک شی سه-بعدی منتقل می-شوند و پس از اینکه از یک زاویه اتفاقی از این شی سه-بعدی یک عکس دوبعدی تهیه شد به کاربر نمایش داده می-شوند.
- این تبدیلات تاکنون در کار دیگری استفاده نشده-اند و گزینه خوبی برای تولید مجموعه-ای از عکس-های تغییریافته از عکس-های خام می-باشند.

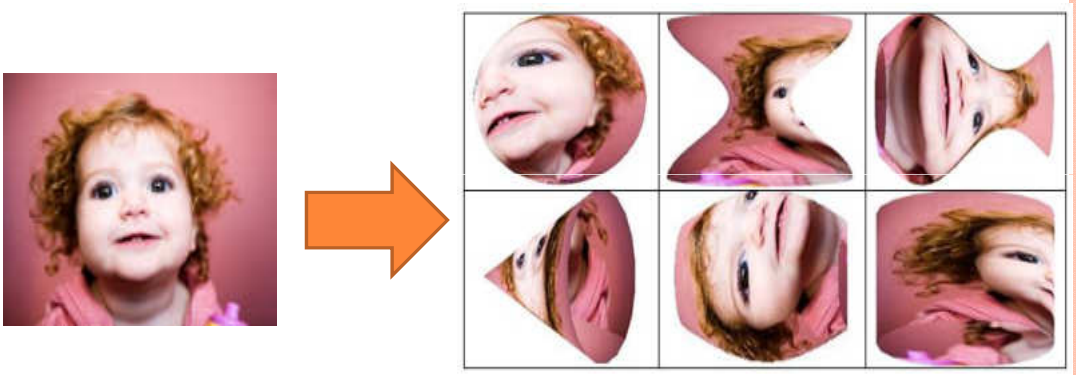
تبدیلات

- در این طرح از یک سری تبدیلات مطابق با الگوریتم زیر برای تغییر دادن عکس استفاده شده است.
  1. انتخاب یک عکس به صورت اتفاقی از پایگاه داده
  2. چرخاندن عکس به سمت-های مختلف به صورت اتفاقی
  3. انتخاب یک تبدیل حجمی اتفاقی و انتقال عکس بر روی آن
  4. انتخاب زاویه دید اتفاقی نسبت به شی سه بعدی و تهیه یک عکس دو بعدی از زاویه انتخاب شده

تبدیلات ...

- تبدیلات هندسی مجموعه از از تبدیلات ریاضی می-باشند. در این تبدیلات از یک تابع ریاضی برای انتقال پیکسل-های عکس خام به جای دیگری از صفحه یا فضا استفاده می-شود.
- این توابع بسیار متنوع بوده و دارای متغیرهای زیادی برای تغییر می-باشند.
- در این کار از ۶ تابع تبدیل هندسی حجمی ثابت که بر روی عکس پیچش فضایی ایجاد می-کنند، برای انتقال تصاویر استفاده شده است.

تبدیلات ...



تبدیلات ...

- پیاده سازی تبدیلات عکس ها در محیط متلب انجام شده-است.
- عکس-های اولیه در یک فایل ذخیره شده-اند.
- برای تست اولیه سیستم، به ازای هر تابع تبدیل سه-بعدی، ۴ عکس تصادفی برای هر عکس خام تهیه می-شود. پس به ازای هر عکس ۲۴ عکس نهایی تولید می-شود. بنابراین برای ۳۰ عکس خام اولیه ۷۲۰ عکس تغییریافته تولید می-شود.
- این ۷۲۰ عکس شامل عکس-های قابل-استفاده و غیرقابل-استفاده می-باشند. همانطور که مشخص است، این ۷۲۰ عکس تنها تعدادی از عکس-های ممکن قابل تولید توسط این الگوریتم می-باشند.

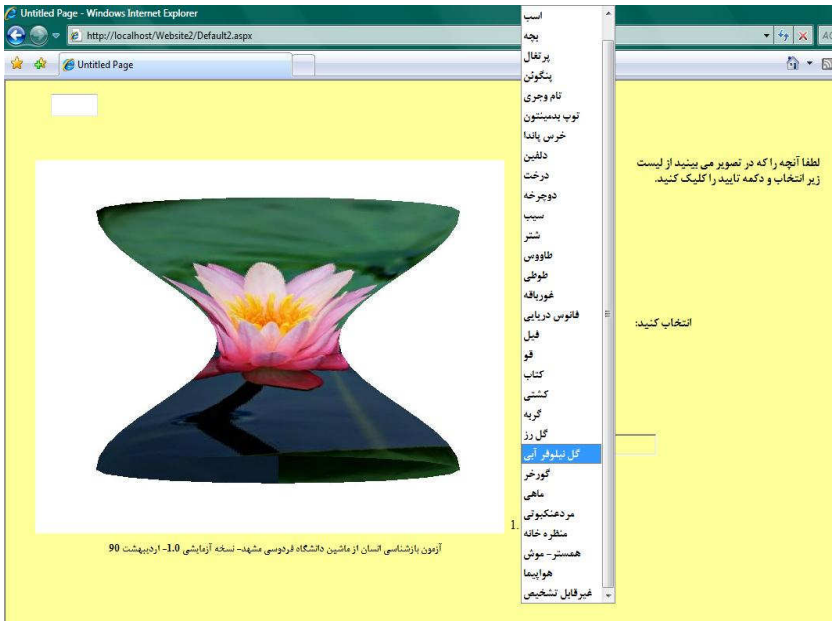
تبدیلات ...

- در قسمت تهیه عکس دوبعدی از یک زاویه تصادفی از یک شی سه-بعدی، فرض کرده ایم که نگاه دوربین همواره به سمت مرکز شی سه-بعدی تنظیم شده است و دوربین روی یک کره حول شی در حال حرکت است.
- ۳ درجه آزادی با بازه ۳۶۰ درجه برای ما ایجاد می شود.
- از این ۳ درجه آزادی برخی از زوایا به علت غیرقابل استفاده شدن عکس حذف شده-اند.
- برای رفع این مشکل و جلوگیری از تولید عکس-های غیرقابل استفاده یکی از زوایا بین -۵۰ تا ۵۰ تنظیم شده است.

نمایش تصویر و دریافت پاسخ

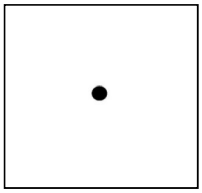
- رابط کابری سیستم در محیط ASP.NET طراحی شده است.
- در این تست از کاربر خواسته می شود که عکسی را که می بیند از یک لیست ۳۰تایی انتخاب کند و پس از کلیک کردن بر روی دکمه تایید به تست بعدی برود.
- برچسب انتخاب شده با جواب درست مقایسه می شود و جواب به کاربر اعلام می-شود.

رابط کاربری آبام



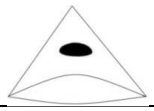
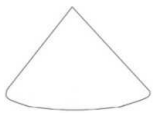
افزایش قابلیت استفاده

- در این آبام یک هیوریستیک برای بالا بردن میزان قابیلت استفاده شده است.
- در این هیوریستیک، ابتدا یک عکس کلید برای همه عکس ها تهیه شده است



- تغییراتی که روی عکس های خام انجام می-شود، بر روی این عکس هم انجام می-شود و چنانچه عکس نهایی متناظر فاقد قسمتی از دایره سیاه بود، عکس به عنوان غیرقابل استفاده در پایگاه داده برچسب می-خورد.

افزایش قابلیت استفاده ...

عکس و کلید تبدیل یافته قابل استفاده		
عکس و کلید تبدیل یافته غیرقابل استفاده		

فهرست مطالب

آزمایشات

- در این آزمایش از ۲۰ کاربر زن و مرد به طور مساوی استفاده شده است.
- سن افراد همگی بین ۱۸ تا ۳۰ سال بوده و رشته تحصیلی آن-ها مجموعه رشته-های کامپیوتر می- باشد.
- مقطع تحصیلی این افراد بین لیسانس و فوق لیسانس است.
- هیچ کدام از شرکت کنندگان قبلا در این تست شرکت نکرده و برای همه، این آزمون جدید می-باشد.

آزمایشات ...

- هر کاربر در دو دور مورد ارزیابی قرار گرفته است و در هر دور ۳۰ عکس از تمامی موارد به طور تصادفی به وی نمایش داده شده است.
- اطلاعات مربوط به بازخورد کابران نسبت به آزمون در یک پایگاه داده Access ذخیره می-شود
- شامل اطلاعات مربوط به کاربر (جنسیت، رده سنی، رشته تحصیلی و مقطع تحصیلی) و اطلاعات مربوط به تست (دور تست، شماره عکس نمایش داده شده، کارا (قابل استفاده) یا غیر کارا بودن (غیرقابل استفاده) عکس، عبور یا عدم عبور کاربر و زمان صرف شده برای پاسخگویی) می-باشند.
- جدول کاربران حاوی ۲۰ رکورد از شرکت کنندگان و جدول آزمون حاوی ۶۰ رکورد به ازای هر شرکت کننده و در نتیجه دارای ۱۲۰۰ رکورد است.

این رکوردها توسط یک برنامه برای ارزیابی پروژه مورد تحلیل قرار گرفته-اند.

تحلیل اولیه

- نتایج این بررسی ها فرضیات در نظر گرفته شده در مسئله را تایید می-کنند.
- احتمال اینکه پارامترهای دیگری در این نتایج تاثیر داشته باشند که در بررسی های ما شرکت نداشته-اند نیز وجود دارد.

تحلیل اولیه ...

- نتایج تحلیل های ما به همراه نظرات کاربران نشان می-دهد که:
  1. تابع هیوریستیک روی تصاویری که موضوع اصلی در وسط تصویر نمی-باشد، ضعیفتر کار می-کند. به طور مثال در تصویر فانوس دریایی به دلیل اینکه محتوای قابل تشخیص در سمت راست قرار گرفته است و در وسط تصویر قرار ندارد، اعمال هیوریستیک روی آن بر کارایی آن نمی-افزاید.
  2. تصاویری که علاوه بر موضوع اصلی دارای موضوی دیگری هم در عکس می-باشند کاربر را تشخیص نهایی دچار ابهام و خطا می-کنند. به طور مثال علاوه بر دلفین تعدادی ماهی نیز در عکس دیده می-شوند. کاربران در این مورد زمانی که به واسطه تبدیل نمی-توانند موضوع اصلی را تشخیص دهند، به اشتباه موضوع ثانویه را در عکس انتخاب می کنند.
  3. عکس-های دارای تکرار موضوع اصلی برای کاربر راحت-تر هستند. به طور مثال، چهار عکس ماهی در کنار هم قرار گرفته اند. این عکس با نرخ خوبی برای کاربران قابل تشخیص است. با رعایت موارد فوق می توان با طراحی هیورستیک کاراتر و یا انتخاب مجموعه عکس-های مناسب-تری برای آبام کارآمدی را بالا برد.

ارزیابی

- سنجه-های ارزیابی پروژه در دو دسته تقسیم میشوند
  - سنجه-های کاربر (قابلیت استفاده)
  - سنجه های ماشین (امنیت)

سنجه-های قابلیت استفاده

- در این قسمت متوسط زمان پاسخ به تست و نرخ پاسخ صحیح به عنوان سنجه درنظر گرفته می-شوند.
- منظور از تعداد عکس-ها در هر دور این است که در هر مرحله از نمایش آبام چند عکس به کاربر نمایش داده شود.

شماره دور نمایش عکسهای تغییر یافته	نرخ پاسخ صحیح		متوسط زمان پاسخ
	بدون هیورستیک	با هیورستیک	
دور اول	٪۷۶.۸۳	٪۸۲.۹۲	۸.۹۹ ثانیه
دور دوم	٪۸۴.۳۳	٪۹۱.۰۶	۶.۱ ثانیه

سنجه های قابلیت استفاده ...

- در دور دوم کاربر به علت آشنایی با آزمون و شکل-ها، بهتر از دور اول عمل می-کند و پیشبینی می-شود که در دورهای بعدی نیز بهتر عمل کند.
- دراین آزمون کاربر با یک بار انجام آزمون می تواند با نرخ ۹۱٪ و در ۶ ثانیه از تست عبور کند.
- این جواب ها، نتایج بسیار خوبی برای ویژگی قابلیت استفاده آبام می باشند.

سنجه-های امنیت سیستم

- این سنجه ها به سه دسته تقسیم میشوند:
  - حملات حدس اتفاقی
  - حملات تطابق مستقیم
  - حملات یادگیری

حملات حدس اتفاقی

- حمله اتفاقی در این آزمون یعنی، مهاجم برحسب اتفاق یکی از گزینه-های موجود در منو را انتخاب کند.
- از آنجایی که گزینه-های موجود در این منو ۳۰ برچسب می-باشند، احتمال حمله اتفاقی حدود ۳.۳ ٪ است. اگر این آزمون ۲ بار تکرار شود، احتمال این حمله به حدود ۰.۱٪ کاهش می یابد.
- چنانچه مثل کارهای مشابه، تعداد عکس-های نمایش داده شده را تا ۱۲ تا بالا ببریم، این احتمال به 1.66 e -18 کاهش می-یابد.

حملات تطابق مستقیم

- منظور از تطابق مستقیم این است که یک مهاجم می-تواند با استفاده- خیلی زیاد از تست یا دزدیدن پایگاه داده، با استفاده از تعدادی کاربر (در ازای پرداخت هزینه-ای معقول به آن-ها، معروف به Mechanical Turk Attack) تمامی برچسب-های متناظر با عکس-هایی که نمایش داده می-شوند را استخراج کند.
- ذخیره- عکس خام در پایگاه داده (به جای عکس تغییریافته آن)، احتمال این حمله را به طور قابل ملاحظه-ای کم می-کند.
- حال فرض کنید که مهاجم به هرطریقی قسمتی یا همه پایگاه داده را بدست آورده است و با تشکیل یک پایگاه داده- دیگر، تمام حالت-های تبدیلات الگوریتم را بر روی عکس-ها انجام دهد و در پایگاه داده- جدید ذخیره کند.
  - وی باید تمام حالات موجود را تولید کند و عکسی که آزمون نمایش می-دهد را با تمام جواب-های از قبل تولید شده خود مقایسه کند.
  - تعداد عملیات لازم برای تطابق دو عکس با استفاده از سریعترین حالت برابر لگاریتم تعداد پیکسل-های عکس در مبنای ۲ است.
  - عکس-هایی که برنامه ما تولید می کند ۱۲۰۰ در ۹۰۰ پیکسل می-باشند.
  - همچنین طبق آمارگیری حدود ۲۵٪ عکس-ها در اثر اعمال هیوریستیک حذف می-شوند.

حملات تطابق مستقیم ...

- جدول زیر کل عملیات لازم برای تطبیق مهاجم را محاسبه می-کند

نام متغیر	تعداد حالات
عکس-ها موجود در پایگاه داده	۳۰ عکس
چرخش در گام ۲	۳۶۰ درجه
تبدیلات هندسی	حداقل ۶
زاویه دید	۱۰۰ × ۳۶۰ × ۳۶۰
تعداد کل جواب-ها بدون اعمال هیوریستیک	۸۴۰ میلیارد
تعداد کل جواب-ها با اعمال هیوریستیک	۶۳۰ میلیارد
تعداد عملیات لازم برای تطابق دو عکس	$Log_2 (۹۰۰×۱۲۰۰) = ۲۰.۰۴۳$
کل عملیات لازم بدون اعمال هیوریستیک	$۱۶.۸×۱۰^{۱۲}$
کل عملیات لازم با اعمال هیوریستیک	$۱۲.۶×۱۰^{۱۲}$

حملات یادگیری ماشین

- در این نوع حمله یک سیستم هوش مصنوعی آموزش داده می-شود و در آن عکس-های تغییریافته به برچسب متناظر خود نگاشت داده می-شوند. این سیستم-های هوشمند از روش-های مختلفی برای یادگیری استفاده می-کنند.
- دو روش مطرح-تر عبارتند از:
  - استفاده از توپولوژی ویژگی-های نقطه-ای
  - استفاده از شکل-های تصویر.

حملات یادگیری ماشین ...

- برخی از روش-ها از توپولوژی نسبی ویژگی-های نقطه-ای پیکسل-های عکس برای شناسایی و یادگیری عکس ها استفاده می-کنند. در این کار این توپولوژی بهم ریخته می-شود. بنابراین این روش ضعیف می-شود.
- برخی دیگر از شکل موجود در عکس برای شناخت عکس استفاده می-کنند. این شکل-ها در تبدیلاتی مثل تغییر نور و چرخش از بین نمی-روند، اما در تبدیلات هندسی این شکل-ها تا حدود زیادی از بین می-روند.

مقایسه با کارهای دیگران

آیام / معیار مقایسه	Collage	2D CAPTCH As from 3D models	Assira	طرح پیشنهادی
نرخ پاسخ صحیح	منتشر نشده	منتشر نشده	٪ ۸۳.۴	٪۹۱
متوسط زمان پاسخ	منتشر نشده	منتشر نشده	۱۵ ثانیه	۶ ثانیه
احتمال حمله اتفاقی	٪۱۶	٪۳.۳	٪۰.۳۹ و ٪۰.۰۲۴ برای مجموعه ۸تایی و ۱۲تایی	٪۳.۳
مقاومت در برابر tin.eye	ضعیف	متوسط	ضعیف	قوی
میزان دانش منتشر شده	زیاد	متوسط	زیاد	کم

فهرست مطالب

کارهای آینده

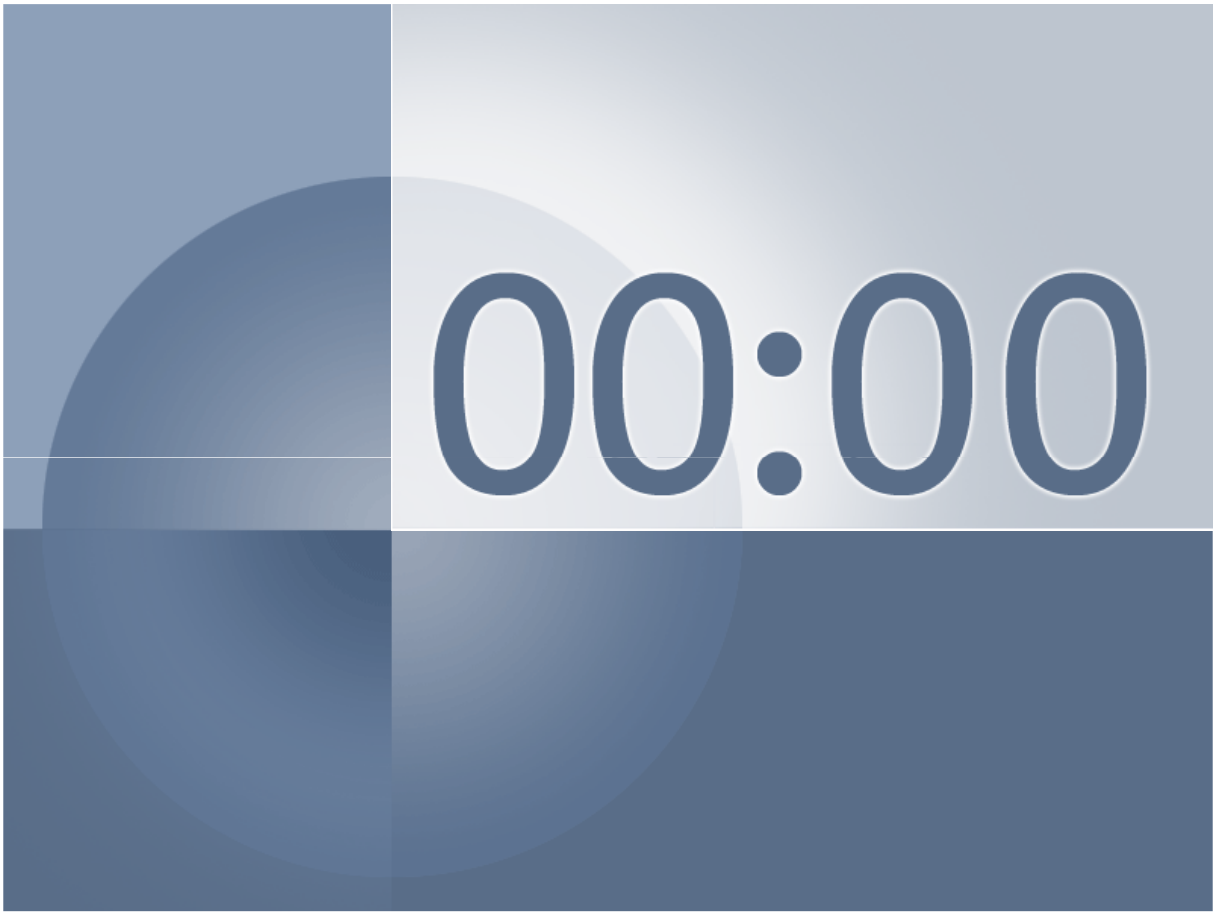
- در کارهای آینده به تبدیلات دیگر هندسی نیز توجه خواهیم کرد و تاثیرات هرکدام را بر روی ویژگی-های قابلیت استفاده و امنیت آبام بررسی می-کنیم.
- برای بهبود احتمال حمله تصادفی باید فضای پاسخگویی را افزایش دهیم. می-توان از طریق نمایش چند عکس به جای یک عکس و یا چند دور انجام آبام توسط کاربر احتمال حمله تصادفی را کاهش داد.
- برای تضعیف حملات یادگیری ماشین با استفاده از روش-های دیگر پردازش تصویر، می-توان پایگاه داده خام را به صورت دوره-ای به روز نمود.
  - بحث به روز نمودن پایگاه داده موضوعی است که به تازگی در زمینه آبام مورد توجه قرار گرفته است که در کارهای آینده به آن توجه می-کنیم.

فهرست مطالب

- مقدمه
- آبام پیشنهادی مبتنی بر تبدیلات هندسی
  - تبدیلات
  - نمایش تصویر و دریافت پاسخ
  - افزایش قابلیت استفاده
- آزمایشات
- نتیجه گیری و کارهای آینده
- مراجع

منابع

1. *Chandaval, A., Dr. Sapkal, A., Dr. Jalnekar, R.,* ***A Framework to analyze the security of Text-based CAPTCHAs****, International Journal of Computer Applications, by IJCA Journal, pages 127-139, 2010.*
2. *Ahn L., Blum M., Hopper N. J., Langford J.,* ***CAPTCHA: Using Hard AI Problems for Security****. On http://www.captcha.net, 2000.*
3. *Tariq Bandary, M., A. Shah, N.,* ***Image Flip Captcha****,* ISecure (The ASC Int'l Journal of Information Security, Volume1, Number1, Number2, pp. 105-123, July 2009.
4. http://www.tineye.com/faq
5. *Kluever, K., Zanibbi, R.,* ***Balancing Usability and Security in a Video CAPTCHA****, Symposium on Usable Privacy and Security (SOUPS), Mountain View, CA USA, 2009.*
6. *Pavlidis, T.,* ***Why Meaningful Automatic Tagging of Images Is Very Hard****, ICME, IEEE, Pages 1432-1435, 2009.*
7. *Hoque, M. E., Russomanno, D. J., and Yeasin, M.,* ***2D CAPTCHAs from 3D models****, Proc. of IEEE SoutheastCon 2006, Pages 165–170, 2006.*
8. *Elson, J., Douceur, J. R., Howell, J., and Saul, J.,* ***ASIRRA: a CAPTCHA that exploits interest-aligned manual image categorization****, Proc. of 14th ACM Conf. on Computer and Communications Security (CCS 2007), pp. 366–374, 2007.*
9. *The CAPTCHA Project, http://www.captcha.net/captchas/pix/*
10. Lowe, D. G., **Object recognition from local scale-invariant features,** *Proceedings of the International Conference on Computer Vision*. **2**. pp. 1150–1157, 1999.
11. Belongie, S. and Malik, J., **Matching with Shape Contexts,** *IEEE Workshop on Content based Access of Image and Video Libraries (CBAIVL-2000), 2000.*
12. *Shirali Shahreza, M., Shirali Shahreza, S.,* ***Advanced Collage Captcha****, fifth international conference on information technology ,pp. 1234-1235, 2008.*
13. *Sony, R., Tiwari, D.,* ***Improved CAPTCHA Method****, International Journal of Computer Applications, by IJCA Journal, pages 107-109, 2010.*
14. *Shirali , M., Shirali, M.,* ***Persian/Arabic Buffletext CAPTCHA,*** *Journal of Universal Computer Science (J.UCS), Vol. 12, No. 12, December 2006, pp. 1783-1796, 2006.*



धन्यवाद

Hindi

Спасибо

Russian

多謝

Traditional Chinese

ขอบคุณ

Thai

Gracias

Spanish

شكراً

Arabic

Thank You

Brazilian Portuguese

Grazie

Italian

Danke

German

Merci

French

நன்றி

Tamil

多谢

Simplified Chinese

Korean

متشكرم

Farsi

ありがとうございました