مطالعات علوم کاربردی در مهندسی

دوره ۲، شماره ۲، تابستان ۱۳۹۵

صفحات ۷۱- ۸۰

ISSN: ۲۴۷۶-۴۵۰۷

www.irijournals.com

ارائه‌ی کپچای خطای دید جهت بهبود امنیت

علی شمسایی[۱]، دکتر محسن سرداری[۲]

[۱] دانشگاه ازاد اسلامی یزد

[۲] دانشگاه میبد

چکیده

در این مقاله، به ارائه روش جدیدی در ایجاد کپچا می‌پردازیم. در این روش که ما آن را کپچای خطای دید می‌نامیم، با استفاده از حس بینایی در انسان کپچایی را ایجاد می‌کنیم که انسان به‌راحتی آن را تشخیص دهد و ربات‌ها نمی‌توانند آن را به‌سادگی تشخیص دهند. ما می‌توانیم با استفاده از چند روش مختلف در این ضمیمه کپچاهای مختلفی تولید کنیم که هرکدام از آن‌ها به‌تنهایی می‌توانند قابل‌استفاده باشند. روش سؤال و جواب که یک روش امنیتی اما بدون تصویر بود در اینجا به‌صورت سؤال و تصویر ارائه می‌شود و کاربر باید با توجه به تصویر به سؤال پاسخ دهد ولی ربات از تشخیص تصویر عاجز خواهد بود. درروش دوم ما با استفاده از خطای دید جدولی ایجاد می‌کنیم که کاربر باید تصاویر بارنگ موردنظر را انتخاب کند که بسیار ساده است اما به دلیل اینکه تمامی رنگ‌ها از دید کامپیوتر یکسان است غیرقابل‌تشخیص است. در این روش‌ها ما روش‌های انتخاب تصادفی در ربات را نیز بررسی کردیم که معمولاً احتمال ان کمتر از ۱٪ است.

واژه‌های کلیدی: کپچای خطای دید، امنیت کپچا، کپچای تصویر، حمله تصادفی در کپچا.

دوره ۲، شماره ۲، تابستان ۱۳۹۵، صفحات ۷۱- ۸۰

۱. مقدمه

با پیشرفته‌تر شدن دنیای فنّاوری و سرعت انتقال اطلاعات، گسترش مجامع مجازی و وب سایت‌ها، حملات به سایت‌ها از طریق ربات‌ها و اسکریپت‌های از پیش نوشته‌شده رو به افزایش است و هکرها هرروزه سعی می‌کنند تا با استفاده از روش‌های مختلف به اطلاعات مهم وب‌سایت‌ها و پایگاه‌های اطلاعاتی دسترسی پیدا کنند. در نمونه‌های کوچک‌تر آن‌ها می‌توانند با نوشتن برنامه‌ای ساده پسوردهای امنیتی کاربران را حدس زده و از اطلاعات محرمانه آن‌ها استفاده کنند، پس ازاین‌رو نیاز به روشی برای مقابله با این مشکل است.

Completely Automated Public Turing Test To Tell Computers And Humans Apart یا به عبارتی تست عمومی کاملاً خودکار تورینگ برای تشخیص انسان از کامپیوتر» یک سامانه‌ی امنیتی و روند ارزیابی است که برای جلوگیری از برخی حمله‌های خرابکارانه‌ی ربات‌های اینترنتی به کار می‌رود. این روند می‌تواند مشخص کند که مراجعه‌کنندگان به یک وب‌سایت و یا سایر خدمات آنلاین انسان هستند یا کامپیوتر است (پندی و لوت[1]، ۲۰۱۴). بدین منظور برنامه‌ی کپچا آزمون‌هایی را تولید می‌کند که تنها انسان‌ها قادر به پاسخ‌گویی به آن‌ها باشند و کامپیوترها و نرم‌افزارهای فعلی نمی‌توانند پاسخ درستی به این آزمون‌ها بدهند، پس هر کاربری که آن را به‌درستی حل کند، انسان فرض می‌شود (لوویس و همکاران[2]).

با پیشرفت شاخه‌های علم کامپیوتر ازجمله پردازش تصویر راهکارهای متعددی جهت کشف متن کپچا از پس‌زمینه و افکت‌های موجود در آن ارائه شد که تا درصد قابل قبولی به‌درستی متن کپچا را حدس می‌زد (ون و همکاران[3]، ۲۰۰۴). ازآن‌پس کپچا های مختلفی از قبیل کپچای تصویر و صدا ارائه شد تا امنیت آن را بالا ببرد اما همان‌طور که گفته شد با گذر زمان آن‌ها نیز تا حدودی آسیب‌پذیر معرفی شدند (لوویس و همکاران[4]). ازآنجاکه پیشرفت علم در عرصه‌های پردازش تصویر و هوش مصنوعی منجر به شکستن راحت‌تر کپچاهای متن و تصاویر شده پس باید راهکاری را ارائه کرد که با پیشرفته‌تر کردن کپچاها مانع از شکستن آن‌ها شویم و این موضوع را هم باید در نظر بگیریم که استفاده نادرست از کپچا و عدم رعایت اصول آن می‌تواند موجب کاهش ارتباط کاربران با سایت گردد. همه‌روزه به دلیل ضعف کپچا حملات متعددی به سرورها و سایت‌ها می‌شود که ازاین‌رو با پیاده‌سازی این روش می‌توان تا حد زیادی ضعف کپچا را برطرف کرد و از آن حملات جلوگیری کرد.

در صورت ادامه این مشکل سرویس‌دهندگان متقبل هزینه‌های سنگینی می‌شوند، در تحقیقات به‌عمل‌آمده کپچاهای موجود توسط الگوریتم‌های تشخیص متن و پردازش تصویر به‌راحتی قابل‌حل است و شکسته می‌شود که راه ورود هکرها و ربات‌ها را به سایت‌ها و سرورها باز می‌کند. در تحقیقات گذشته نیز سعی در پیچیده کردن کپچا شده اما به‌مرورزمان باز روش‌هایی جهت شکستن آن‌ها نیز ارائه‌شده که تا درصد بالایی در حدود ۹۴٪ عملی بوده است (استاروستنکو[5]، ۲۰۱۵).

آزمون تورینگ برای اولین بار توسط التا ویستا در سال ۱۹۹۷ برای کاهش هرزنامه‌ها استفاده شد که کلمه‌ای به کاربر نشان داده و از کاربر خواسته می‌شد که آن را وارد کند (اگیجنکو و کلوپوو[6]، ۲۰۰۸). در سال ۲۰۰۰ لویس ون در دانشگاه ملون ایده کپچا را پیشنهاد داد و اولین بار در سایت یاهو برای جلوگیری از نفوذ ربات‌ها به چت روم‌ها به کار گرفته شد. کپچای gimpy توسط لویس ون و بلوم پیشنهاد داده شد که به دلیل اینکه از لغات دیکشنری استفاده‌شده بود توسط موری و مالیک با استفاده از

[1] Pandey and Lothe
[2] Luis et al.
[3] Von et al.
[4] Luis et al.
[5] Starostenko
[6] Ogijenko and Kolupaev

الگوریتم تشخیص تا ۹۹٪ به‌درستی تشخیص داده شد (بندی و شاه[1]، ۲۰۰۸). ریکپچا که توسط ون نیز پیشنهادشده بود به دلیل استفاده از کلمات ناخوانا توسط OCR در نسخه های خطی دارای امنیت بیشتری بود (احمد و همکاران[2]، ۲۰۱۲). تکنیک های متن برجسته و دست خطی نیز ارائه شدند که تا حدودی کاربران را دچار مشکل می‌ساختند (شاه و بندی[3]، ۲۰۰۸).

سیستم بینایی ما طوری تنظیم‌شده است که ما بتوانیم در محیطی سه‌بعدی و سرشار از نور، سایه، رنگ، بافت و اشیاء و اشکالی متنوع و متعدد در فواصل دور و نزدیک ببینیم. بسیاری از ما بدون توجه به اینکه ایجاد تصویری صحیح از جهان اطراف ما برای سیستم بینایی و مغز چه عملیات پیچیده‌ای به همراه دارد، دیدن را امری ساده و پیش‌پاافتاده تلقی می‌کنیم.

خطای دید یا خطای چشم به احساس دیدن تصاویری گفته می‌شود که فریبنده یا گمراه‌کننده هستند. در این حالت اطلاعاتی که به‌وسیله چشم جمع‌آوری‌شده و توسط مغز پردازش می‌گردد منجر به درک تصویری می‌شود که با واقعیت آن تصویر تطابق ندارد. مغز انسان بااین‌همه قدرت شگرفی که دارد در برخی موارد به چالش کشیده می‌شود و آن‌طور که فکر می‌کنیم مصون از خطا و لغزش نیست. یکی از این موارد خطاهای دید هستند. مغز ما با دریافت انبوهی از تصاویر در اطرافمان تلاش دارد مفهوم واقعیت را برای ما نمایان کند و این تجزیه‌وتحلیل در کسری از ثانیه انجام می‌گیرد. در این میان گاهی مغز نمی‌تواند آنچه را که دریافت می‌کند به‌درستی نمایان کند و واقعیتی که خودش دریافت می‌کند را به‌خوبی نشان نمی‌دهد این اتفاق را توهم بصری می‌نامیم. درواقع درک ما از جهان، بر اساس ترجمه اطلاعات بصری توسط مغز شکل می‌گیرد و این ترجمه، گاه به خطای چشم منجر می‌شود. به‌این‌ترتیب که ذهن ما نسبت به اطلاعات رسیده منفعل نیست و برای ترجمه این اطلاعات بسیار مبتکرانه عمل کرده و درنتیجه هرازگاهی اطلاعات وارده را به شکلی نامتعارف معنا می‌کند. با استفاده از این مفهوم می‌توان سعی در تولید کپچایی کرد که می‌تواند ما را در نحوه تشخیص انسان از ربات یاری کند. انسان‌ها برخلاف کامپیوترها خطای دید را به همراه خواهند داشت که می‌توان از این خصیصه جهت تولید کپچای خطای دید استفاده کرد.

۲. کپچای خطای دید

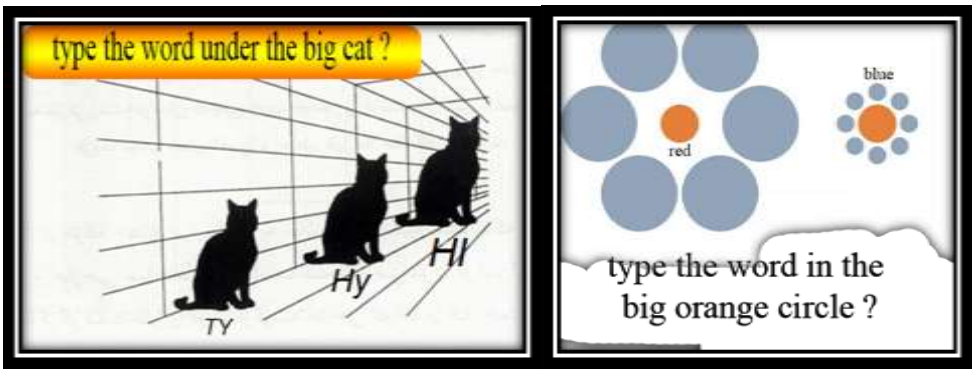
این کپچا با استفاده از خطای دید در انسان سعی در ایجاد تمایز بین انسان و ماشین شده است به‌گونه‌ای که فقط انسان قادر به تشخیص آن است و کامپیوتر فقط به‌صورت تصادفی می‌تواند تلاش به حدس زدن این کپچا کند.

تولید کپچای خطای دید

درروش پیشنهادی اول جهت ایجاد کپچای خطای دید نیاز به یک پایگاه داده از تصاویر خطای دید و سؤالات درج‌شده مربوط به آن‌ها داریم. شاید یکی از ضعف‌های این کپچا را بتوان محدود بودن تصاویر دانست اما می‌توان باکمی تغییر درروند نمایش تصاویر این مشکل را کمرنگ‌تر نشان داد. جهت ایجاد این کپچا در ابتدا بانکی از تصاویر خطای دید را به‌عنوان پس‌زمینه ذخیره می‌کنیم. پس‌ازآن قسمت متمایز مربوط به هر تصویر را مشخص مس کنیم. در مرحله بعد سؤالات مربوط به هر تصویر را در بانک اطلاعاتی ذخیره می‌کنیم. سپس با ایجاد کلمات تصادفی در نقاط مشخص‌شده می‌توانیم یک کپچا را ایجاد کنیم. کلمات ایجادشده در تصاویر کاملاً به‌صورت تصادفی هستند و حتی می‌توان از اعوجاج و افکت در آن کلمات بهره برد. سؤالات ایجادشده مربوط به هر تصویر نیز همانند کلمات باید تصادفی بوده و مربوط به تصویر باشد به‌طوری‌که هر تصویر دارای تعدادی سؤال باشد. هر بار که کپچا به‌روزرسانی می‌شود، حتی در صورت تکراری بودن تصویر، سؤالات و کلمات تولیدشده کاملاً متفاوت است و از تکراری بودن

[1] Banday and Shah
[2] Ahmad et al.
[3] Shah and Banday

کپچا جلوگیری می‌کند. هرچند این روش محدود بودن پایگاه تصاویر را جبران نکند اما تا حدود زیادی آن را بهبود می‌بخشد و می‌تواند ضعف آن را جبران کند. نمونه هایی از کپچای خطای دید در شکل ۱ نشان داده شده است.



شکل (۱): کپچای خطای دید

امنیت در کپچای خطای دید

در این قسمت می‌خواهیم چند روش پیشنهادی را در کپچای خطای دید ارائه دهیم که امنیت کپچای فوق را بالابرده و هم بهبودی درزمینه امنیت کپچای متنی باشد به‌طوری‌که بتوان به‌صورت مجزا و جدا از کپچای تلفیقی مورداستفاده قرار گیرد.

کپچای نوع اول

مراحل ایجاد کپچای خطای دید را به‌صورت بالا طی کرده ولی در قسمت ایجاد کلمه تصادفی و جایگذاری آن در تصویر از کپچای متن استفاده می‌کنیم و آن را در تصویر جایگذاری می‌کنیم. اگر بخواهیم مراحل حل کپچا را توسط کاربر بررسی کنیم به این شرح است:

۱. دیدن عکس و خواندن سؤال مطرح‌شده
۲. دیدن عکس و تشخیص خطای دید و پیدا کردن کلمه موردنظر
۳. خواندن کپچا و تشخیص درست آن
۴. واردکردن آن در کادر پاسخ

حال اگر بخواهیم آن را ازنظر پردازش تصویر و ربات بررسی کنیم:

۱. باز شدن عکس و ذخیره کردن
۲. بازخوانی سؤال و تحلیل آن
۳. تحلیل شکل به دلیل یکسان بودن رنگ مشکل‌ساز می‌شود
۴. استفاده از حمله تصادفی
۵. تشخیص کپچا و مراحل شکست کپچای متنی

دوره ۲، شماره ۲، تابستان ۱۳۹۵، صفحات ۷۱- ۸۰

شکل (۲): استفاده از کپچای متن در کپچای خطای دید

ربات می‌تواند با ریسک ۵۰ درصد یکی از کپچا ها را وارد کرده و از مراحل یک تا ۳ عبور کند که خود می‌تواند نقطه‌ضعف بزرگی باشد. در این صورت ما می‌توانیم فضای حالت را از ۲ تا به ۱۰ یا بیشتر افزایش دهیم کاربر به‌راحتی می‌تواند تفاوت در رنگ را ببیند ولی از دید ربات به دلیل یکسان بودن ناچار است تمامیِ کپچاهای موجود را بررسی کرده و با فرمول احتمال زیر یکی از آن‌ها را انتخاب کرده و وارد کند:

۱. در حالت عادی با ضریب $OPI = \frac{100}{\text{تعداد حالتها}}\%$

۲. در حالت استفاده از کپچا $OPIC = \frac{OPI}{\text{ضریب شکست}}\%$

به‌عنوان‌مثال نرخ تشخیص در حالت تصادفی درصورتی‌که متن عادی در کپچا استفاده‌شده باشد و درصورتی‌که از کپچای متن با در صد تشخیص ۲۰٪ با نرم‌افزارهای تشخیص استفاده‌شده باشد.

جدول (۱): درصد شکست در حالت تصادفی بدون کپچا و با کپچا

تعداد حالتها و تعداد متون	درصد شکست	
	متن عادی	با کپچا
۲	٪۵۰	٪۱۰
۵	٪۲۰	٪۴
۱۰	٪۱۰	٪۲
۲۰	٪۵	٪۱
۵۰	٪۲	٪۰.۴
۱۰۰	٪۱	٪۰.۲

همان‌طور که در جدول ۱ مشخص است، هر چه تعداد تصاویر افزایش یابد درصد تشخیص کاهش پیدا می‌کند. همین‌طور اگر از کپچای متن به‌جای متن استفاده کنیم نیز امنیت بالاتری خواهد داشت. در این روش استفاده از تعداد حالات بالا ازنظر اقتصادی، فضای اشغال‌شده و زمان تشخیص توسط کاربر به‌صرفه نیست. در این صورت باید حد متعادل آن را در نظر گرفت که قابل‌استفاده و به‌صرفه باشد که در اینجا می‌توان گفت تعداد حالات کمتر از ۱۰ دارای این شرایط هستند. پس در فضای حالت ده‌تایی و با استفاده از کپچای متن می‌توان نرخ تشخیص تصادفی توسط ربات را تا ۲٪ رساند. استفاده ازاین‌روش تا حدودی می‌تواند نرخ تشخیص را کاهش دهد و احتمال شکست کپچا را نیز پایین بیاورد.

کپچای نوع دوم

استفاده از روش کلیک و انتخاب به‌طوری‌که از کاربر خواسته می‌شود که موارد خواسته‌شده را با کلیک بر روی آن‌ها انتخاب کند. به‌طور مثال در تصویر خواسته می‌شود که اسب‌هایی بارنگ سیاه انتخاب شوند درصورتی‌که از دید کامپیوتر همه اسب‌ها به یکرنگ هستند ولی به دلیل خطای دید اسب‌ها از دید کاربر دارای رنگ متفاوت هستند و به‌راحتی قابل‌تشخیص هستند. می‌توان از اشکال مختلف در هر عکس استفاده کرد در این تصاویر از اسب استفاده‌شده.

شکل (۳): روش انتخابی در کپچای خطای دید، انتخاب اسب‌های سیاه در تصویر

در این روش به دلیل بدیهی بودن تعداد اسب‌های تیره برای انسان و مکان آن‌ها به‌راحتی قابل‌حل است و کاربر با چند کلیک می‌تواند از آن عبور کند. ولی برای ربات به دلیل مشخص نبودن اختلاف در رنگ‌ها و تعداد تصاویر انتخابی، احتمال انتخاب صحیح بسیار پایین است. یکی از دلایل آن وجود فضای حالت بسیار بزرگ است. حال اگر تعداد تصاویر را از ۹ حالت به بالاتر افزایش دهیم تعداد حالات بسیار بزرگ‌شده به‌طوری‌که احتمال انتخاب درست نزدیک به صفر می‌رسد. در محاسبه تعداد حالات، از حالت صفر و کل حالات یکسان صرفه نظر می‌شود، زیرا حداقل نیاز به یک انتخاب وجود دارد.حداقل یک وجه تفاوت نیز بین تصاویر باید موجود باشد. بر اساس قانون احتمالات ترکیب بین انتخاب‌ها را محاسبه می‌کنیم و در آخر احتمال انتخاب صحیح به‌طور تصادفی را در حالت کلی محاسبه می‌کنیم. به‌عنوان‌مثال در رابطه ۳ احتمال انتخاب تصادفی در حالتی که ۳ انتخاب صحیح از ۹ حالت وجود دارد بررسی می‌شود.

$$Case\ n = \frac{\binom{n}{Cn}}{\binom{AP}{n}} = \frac{\binom{3}{3}}{\binom{9}{3}} = \frac{1}{\frac{9\times8\times7\times6!}{3!\times6!}} = \frac{1}{84} \times 100 = 1.1\% \quad (۳)$$

با توجه به جدول ۲ تعداد تصاویر ثابت ولی تعداد انتخاب‌ها متغیر است. اگر تعداد انتخاب‌ها نصف تعداد تصاویر باشد، درصد شکست تصادفی بسیار کم می‌شود. پس می‌توان گفت هر چه تعداد تصاویر انتخابی جهت حل پازل کپچا به حد میانه نزدیک شود امنیت افزایش میابد.

جدول (۲): میزان درصد شکست در حمله‌ای با انتخاب تصادفی

تعداد تصاویر	تعداد انتخاب	درصد شکست با انتخاب تصادفی	
9	1	$1/9$	**11%**
9	2	$1/36$	**2.7%**
9	3	$1/84$	**1.1%**
9	4	$1/126$	**0.7%**
9	5	$1/126$	**0.7%**
9	6	$1/84$	**1.1%**
9	7	$1/36$	**2.7%**
9	8	$1/9$	**11%**

حال اگر بخواهیم میانگین درصد شکست در انتخاب تصادفی در همه‌ی حالت‌های انتخاب از ۱ حالت تا ۹ حالت را محاسبه کنیم و به یک درصد کلی برسیم از رابطه ۴ استفاده می‌کنیم. در این رابطه که شبیه به رابطه ۷ است، احتمال شکست را در همه‌ی حالات محاسبه می‌کند و جدول ۲ را به‌صورت یک درصد کل نمایش می‌دهد. در محاسبه احتمال انتخاب حالت صحیح در انتخاب تصادفی کل، از حالت صفر و حالت کلی یعنی AllPic صرف‌نظر می‌شود. تعداد کلیک و یا انتخاب‌ها با Click Number و تعداد انتخاب‌های صحیح با Correct Choice نشان می‌دهیم. با جایگذاری اعداد در رابطه احتمال ۴ به رابطه احتمال ۵ می‌رسیم. بعد از محاسبه حالت کلی انتخاب‌ها در ۹ تصویر به‌احتمال در صد شکست ۰.۱۹٪ در حالت انتخاب تصادفی می‌رسیم.

$$Total = \frac{\binom{CCh!}{CN!}}{\sum_{NC=1}^{NC=AP-1}\binom{AP!}{CN!}} = \frac{1}{2^{AP}-2} \qquad (۴)$$

$$Total = \frac{1}{\sum_{NC=1}^{NC=8}\binom{9!}{CN!}} = \frac{1}{2^9-2} = \frac{1}{510} \times 100 = 0.19\% \qquad (۵)$$

حال می‌خواهیم درصد شکست تصادفی را توسط رابطه احتمال ۴ برای کل تعداد تصاویر مورداستفاده و فضای حالت انتخابی از ۳ حالت تا ۱۶ حالت را محاسبه کنیم. بعدازاینکه همه‌ی حالت‌ها را محاسبه و جایگذاری کردیم، جدول ۳ ایجاد می‌شود.

جدول (۳): درصد شکست کپچا در سایزهای مختلف

تعداد تصاویر	تعداد انتخاب	درصد شکست با انتخاب تصادفی	
3	1-2	$1/6$	**16.6%**
6	1-5	$1/62$	**1.6%**
9	1-8	$1/510$	**0.19%**
12	1-11	$1/4094$	**0.02%**
16	1-15	$1/65534$	**0.001%**

با توجه به این جدول مشخص می‌شود که هر چه تعداد تصاویر زیاد شود درصد شکست نیز کاهش پیدا می‌کند. درست است که هر چه تعداد تصاویر افزایش یابد درصد شکست کاهش پیدا می‌کند اما باید فضای استفاده و دیدگاه کاربر را نیز در نظر داشت. پس

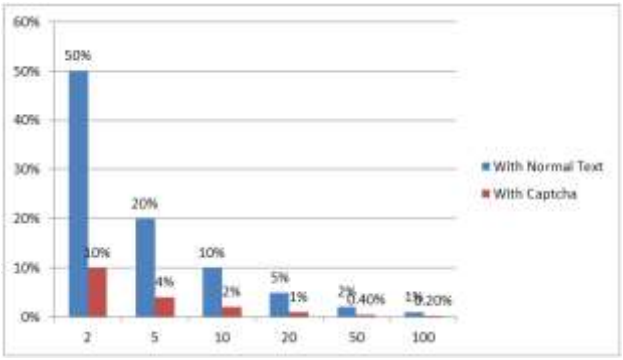
دوره ۲، شماره ۲، تابستان ۱۳۹۵، صفحات ۷۱- ۸۰

در این حالت نیز همانند روش قبل باید حد متعادل را جهت کاربردی بودن آن حفظ کنیم و می‌توان، تعداد تصاویر کمتر از ۹ و بیشتر از ۶ را ازنظر امنیت و کاربری مناسب دانست.

نتیجه

کامپیوترها و بینایی ماشین تابه‌حال قادر به تشخیص خطای دید نیست لذا فقط یک حالت به وجود می‌آید که ماشین‌ها بتوانند به‌درستی این کپچا را حل کنند. این حالت این است که به‌صورت کاملاً تصادفی یکی از حالت‌ها را انتخاب کرده و از راه کاملاً تصادفی گزینه درست را انتخاب کنند که بااین‌حال احتمال انتخاب گزینه صحیح بسیار کم است. در حالت اول که همان تشخیص و ورود کپچا بود در تعداد دوتایی ربات می‌تواند با ریسک ۵۰ درصد یکی از کپچا ها را وارد کرده و از مراحل یک تا ۳ عبور کند که خود می‌تواند نقطه‌ضعف بزرگی باشد. در این صورت ما می‌توانیم فضای حالت را از ۲ تا به ۱۰ یا بیشتر افزایش دهیم کاربر به‌راحتی می‌تواند تفاوت در رنگ را ببیند ولی از دید ربات به دلیل یکسان بودن ناچار است تمامیِ کپچاهای موجود را بررسی کرده و با فرمول احتمال ۱ و۲ یکی از آن‌ها را انتخاب کرده و وارد کند. در حالت استفاده از هر نوع کپچا درصد تشخیص در حالت تصادفی در حالت عادی را بر نرخ تشخیص کپچا تقسیم می‌کنیم. به‌عنوان‌مثال نرخ تشخیص در حالت تصادفی درصورتی‌که متن عادی در کپچا استفاده‌شده باشد و درصورتی‌که از کپچای متن با در صد تشخیص ۲۰٪ استفاده‌شده باشد به‌صورت زیر است.

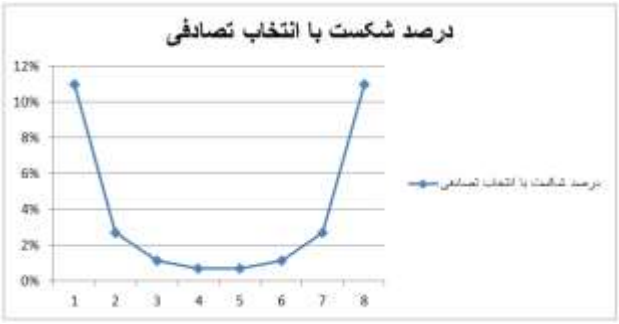
نمودار ۱: درصد شکست کپچای خطای دید در حالت تصادفی بدون کپچا و همراه با کپچا



همان‌طور که مشاهده می‌شود استفاده ازاین‌رو تا حدود می‌تواند نرخ تشخیص را کاهش دهد و احتمال شکست کپچا را نیز پایین بیاورد.

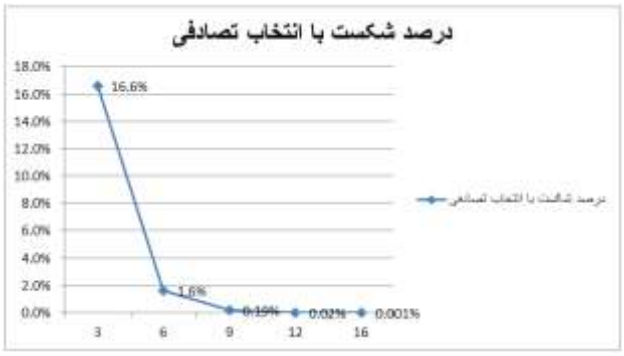
حالت دوم کلیک و انتخاب در این روش به دلیل بدیهی بودن تعداد اسب‌های تیره برای انسان و مکان آن‌ها به‌راحتی قابل‌حل است و کاربر با چند کلیک می‌تواند از آن عبور کند ولی برای ربات به دلیل مشخص نبودن اختلاف در رنگ‌ها و تعداد درست چون فضای حالت بسیار بزرگ است احتمال انتخاب صحیح بسیار پایین است حال اگر تعداد تصاویر را از ۹ حالت به بالاتر افزایش دهیم تعداد حالات بسیار بزرگ‌شده به‌طوری‌که احتمال انتخاب درست نزدیک به صفر می‌شود. در محاسبه تعداد حالات از صفر و کل حالات یکسان صرفه نظر می‌شود زیرا حداقل نیاز به یک انتخاب وجود دارد و حداقل یک وجه تفاوت نیز بین تصاویر باید موجود باشد. بر اساس قانون احتمالات ترکیب بین انتخاب‌ها را محاسبه می‌کنیم و در آخر احتمال انتخاب صحیح به‌طور تصادفی را در حالت کلی محاسبه می‌کنیم. به‌عنوان‌مثال احتمال انتخاب تصادفی در حالتی که ۳ انتخاب وجود دارد.

نمودار۲: میزان درصد شکست در حمله‌ای با انتخاب تصادفی



در محاسبه احتمال انتخاب حالت درست در انتخاب تصادفی کل از حالت صفر و حالت کلی یعنی AllPic صرف‌نظر می‌شود. تعداد کلیک و یا انتخاب‌ها با Click Number و تعداد انتخاب‌های صحیح با Correct Choice نشان می‌دهیم در فرمول ۴ و ۵.

نمودار ۳: درصد شکست کپچا با استفاده از تعداد تصاویر مختلف در کپچا



مراجع

1. Ahmad El Ahmad, Jeff Yan and Wai-Yin Ng , “CAPTCHA Design Color, , and Security,” IEEE Computer Society, 1089-7801,March – April 2012 IEEE.
2. Ahn, L. Von., Blum M., Hopper N. (2004) .CAPTCHA: Telling humans and computers apart automatically , communication of the ACM, Vol. 47,No.2
3. J.Ogijenko and A.Kolupaev, “Captchas: Humans vs Bots.” IEEE Computer Security, vol.6, pp.68-70, Feb. 2008.
4. M. Tariq Banday and Nisar A. Shah, “Drag and Drop Image CAPTCHA.” Sprouts 4th J&K Science congress, 2008 .
5. N. A. Shah and M. Tariq Banday, “A Study of CAPTCHAs for Securing Web Services.” IJSDIA International Journal of Secure Digital Information Age, Vol. 1. No. 2, December 2009.
6. Starostenko, O., Cruz-Perez, C., Uceda-Ponga, F., & Alarcon-Aquino, V. (2015). Breaking text-based CAPTCHAs with variable word and character orientation. Pattern Recognition, 48(4), 1101-1112. doi:http://dx.doi.org/10.1016/j.patcog.2014.09.006
7. Von Ahn Luis, B. Manuel and L. John, “Telling Humans and Computer Apart Automatically,” CACM, V47, No2.

8. Von Ahn Luis, B. Manuel and L. John, "Telling Humans and Computer Apart Automatically," CACM, V47, No2
9. Yogdhar Pandey and Darshika Lothe, "Evaluating the Usability and Security of a Spelling Based Captcha System," International Journal of Computer Science and Information Technologies, Vol. 5 (3), 2014, 4728-4731.