

ارائه یک کپچای تصویری جدید با استفاده از مورفولوژی

احمد رضا ثابت اقلیدی^۱، علی محمد لطیف^{۲*}، علی محمد اسمعیلی زینی^۳

۱- کارشناسی ارشد، ۲- دانشیار، ۳- دانشجوی دکتری، دانشگاه یزد

(دریافت: ۹۵/۰۴/۲۷، پذیرش: ۹۵/۱۰/۲۳)

چکیده

امروزه با رشد گسترده کاربران اینترنت، سرویس‌های اینترنتی زیادی از قبیل رایانامه، موتورهای جستجو و شبکه‌های اجتماعی به صورت رایگان ارائه می‌شود. با توسعه سرویس‌های اینترنت، از کار انداختن خدمات توسط برنامه‌های مخرب خودکار، مانند ربات‌های اینترنتی و هکرها، تبدیل به مشکل اصلی سرویس‌های اینترنتی شده است. کپچا، یک سازوکار تأیید انسانی است که آزمون‌هایی را برای تشخیص اینکه آیا کاربر یک انسان است یا یک برنامه رایانه‌ای مخرب، تولید و نتایج آن را ارزیابی می‌کند. حل این آزمون‌ها برای انسان راحت و برای ربات‌های اینترنتی مشکل است. روش‌های کپچای کنونی سعی در افزایش سختی این آزمون‌ها برای برنامه‌های خودکار با استفاده از افزایش تحریف و پارازیت دارند، در نتیجه حل آن برای انسان نیز مشکل می‌شود. در این مقاله یک کپچای تصویری با استفاده از عملیات مورفولوژی ریاضی ارائه می‌شود که هدف از ارائه این راهکار افزایش امنیت و دفاع در مقابل حملات مخرب‌ها و هکرها است. در این روش یک الگوی باینری با توجه به تصویر ورودی دچار گسترش و فرسایش می‌شود. سپس با انجام تغییراتی بر روی تصویر به کاربر ارائه شده و کاربر باید تصویر اولیه را تشخیص دهد. طبق ارزیابی‌های انجام شده، برای کپچای چهره ۹۶ درصد و برای کپچای غیر چهره ۹۰/۵ درصد از انسان‌ها آزمون کپچا را با موفقیت گذراندند و متوسط زمان پاسخگویی برای کپچای غیر چهره ۱۶/۸ و برای کپچای چهره برابر با ۷/۶ ثانیه است.

کلیدواژه‌ها: امنیت، برنامه‌های مخرب، تشخیص تصویر، کپچا، مورفولوژی

Presenting a New Photographic CAPTCHA Using Morphology

A. Sabeteghlidi, A. Latif*, A. Esmailizaini

Yazd university

(Received: 17/07/2016; Accepted: 12/01/2017)

Abstract

Today by the increasingly growth of internet users, many internet services such as electronic mails, search engines and social networks are presented. Due to developments in internet services, disabling the services through automatic programs such as internet robots and hackers has become a main problem. CAPTCHA is a mechanism that confirms whether the user is a human or a computer program. This task is performed through some tests. Performing these tests is easy for human but it is difficult for robots. CAPTCHA techniques are trying to increase the mentioned difficulties in automatic programs and it is performed through increasing the deviations and parasite. Then solving it will become difficult for human. In this research an image CHAPTCHA is presented and it is done through mathematical morphology the purpose of this solution to increase security and to defend against malicious attacks and hackers. In this method by the input image, a binary model is developed and worn. Then by making some changes, the image is presented to the user and he should recognize the early image. According to these estimations, 96% human have passed the face CAPTCHA and 90.5% human have passed the non-face CAPTCHA, and the average of required time to answer is 16.8 for non-face CAPTCHA and 7.6 second for face CAPTCHA.

Keywords: Security, Malicious Programs, Image Recognition, CAPTCHA, Morphology

*Corresponding Author E-mail: Alatif@yazd.ac.ir

۱. مقدمه

امروزه با افزایش خدمات اینترنتی رایگان، مشکل سوء استفاده از این خدمات توسط اسپمرها^۱ و ربات‌های نرم‌افزاری به شدت در حال افزایش است؛ بنابراین ایجاد تمایز بین انسان و برنامه‌های رایانه‌ای بسیار مهم است؛ به طوری که بتوان با ایجاد یک سازوکار تدافعی مناسب در مقابل نفوذ و حمله هکرها، سرویس‌های اینترنتی را مقاوم و محافظت نمود. کیچاها^۲ روشی را برای تمایز قائل شدن بین انسان و عامل مصنوعی و خودکار ارائه می‌دهند. تاکنون افراد مختلف روش‌های متفاوتی برای کیچا ارائه کرده‌اند که هر کدام با وجود معایب و مزایایی سعی در محافظت از خدمات اینترنتی دارند.

در سال‌های اخیر مفهومی به نام HIP^۳ مطرح شد که به معنی اثبات تعامل انسانی است. HIP برنامه‌ای است که به نوعی از فعل و انفعال‌ها از طرف انسان نیاز دارد تا وی به عنوان انسان شناخته شود. این برنامه به طور مؤثری قادر به جلوگیری از دسترسی برنامه‌های خرابکار به خدمات اینترنتی است. کیچا که به معنی آزمون همگانی خودکار شده تورینگ برای مجزا کردن انسان و رایانه است، نوعی از آزمون HIP است و حل آن برای انسان آسان و برای ربات‌های اینترنتی مشکل‌تر است.

کیچا یک سازوکار تأیید انسان بودن است که آزمون‌هایی را برای تشخیص اینکه آیا کاربر یک انسان است یا یک برنامه رایانه‌ای مخرب، تولید و ارزیابی می‌کند و سعی می‌کند فراتر از قابلیت‌های برنامه‌های رایانه‌ای کنونی باشد. روش‌های کیچای کنونی سعی در افزایش سختی آزمون برای برنامه‌های خودکار با استفاده از افزایش خرابی و نویز دارند. در نتیجه پاسخ به آن برای انسان نیز مشکل‌تر خواهد شد. نمونه بارزی از کیچا، تصویری از حروف و اعداد در صفحات مختلف وب است که به صورت کج و ناواضح رسم شده‌اند و از کاربر خواسته می‌شود تا آن را به شکل صحیح خوانده و با دقت در یک جعبه متن وارد کند.

کیچا به طور معمول یک آزمون یا جورچین ساده بصری است که یک انسان می‌تواند بدون مشکل زیادی به آن پاسخگو باشد، اما یک برنامه خودکار قادر به این کار نیست. این آزمون به طور معمول از حروف، اعداد یا ترکیبی از آن‌ها که با هم تداخل دارند و متقاطع هستند تشکیل شده است. تصاویر کیچا ممکن است به

گونه‌ای تحریف^۴ شده باشد یا در یک پس‌زمینه پیچیده نشان داده شود تا به راحتی توسط سامانه‌های تشخیص حروف^۵ خوانده نشود. سامانه‌های تشخیص حروف برای خواندن خودکار متون استفاده می‌شوند، ولی اینگونه نرم‌افزارها در خواندن متون چاپ شده با کیفیت پایین یا متون دست‌نویس با مشکل مواجه شده و فقط قادر به تشخیص متون تائیدی که از کیفیت بالایی برخوردار بوده و از قالب‌های رایج و استاندارد پیروی می‌کنند، هستند. پس می‌توان از این نقص نرم‌افزارهای تشخیص حروف استفاده کرد و تصویر یک کلمه را به شکلی تغییر داد که توسط انسان قابل خواندن باشد، ولی نرم‌افزارهای تشخیص حروف قادر به بازیابی و تشخیص آن نباشند [۱].

کیچا دارای طیف گسترده‌ای از کاربرد در وب است که از جمله کاربردهای آن می‌توان به موارد زیر اشاره کرد:

- ۱- مشخص کردن کرم‌ها و اسپم‌ها در شناسایی رایانامه،
- ۲- نظرسنجی بر خط،
- ۳- خدمات رایانامه رایگان،
- ۴- پیام‌های بر خط،
- ۵- محدود کردن میزان استفاده.

خصوصیت‌های کیچا به شرح زیر هستند:

- ۱- آزمون کیچا باید به صورت خودکار توسط یک ماشین تولید و ارزیابی شود. این خصوصیت، حداقل نیاز یک سامانه کیچا است.
- ۲- این آزمون باید به سرعت و به راحتی توسط یک کاربر انسانی پاسخ داده شود. هر آزمون کیچایی که به بیش از ۳۰ ثانیه زمان برای پاسخگویی نیاز داشته باشد، در عمل مفید نیست.
- ۳- این آزمون باید همه انسان‌ها و یا گروهی از انسان‌ها را پذیرا باشد [۲].

کیچا را می‌توان به چهار دسته تقسیم کرد:

- ۱- کیچای مبتنی بر متن،
- ۲- کیچای مبتنی بر تصویر،
- ۳- کیچای مبتنی بر صدا،
- ۴- کیچای مبتنی بر ویدئو.

تصاویر شکل (۱) نمونه‌ای از کیچاهای معروف مبتنی بر متن را نشان می‌دهد.

^۱ Spammers

^۲ CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart)

^۳ Human Interaction Proof (HIP)

^۴ Distortion

^۵ Optical Character Recognition (OCR)



شکل ۴. نمونه‌ای از کپچای مبتنی بر ویدئو [۶]

۲. الگوریتم پیشنهادی

الگوریتم پیشنهادی شامل مراحل زیر است:

شکل (۵) نمای کلی از ارائه یک کپچای تصویری با استفاده از مورفولوژی را نشان می‌دهد.



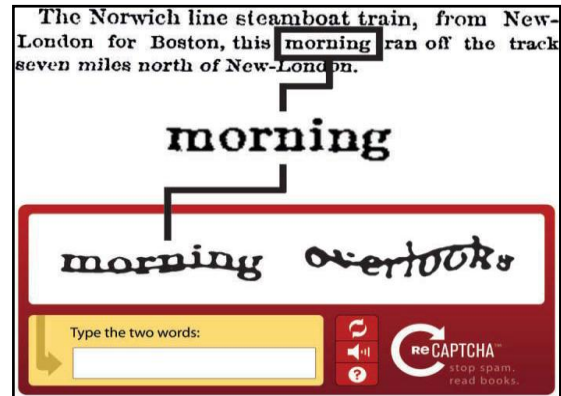
شکل ۵. روند نمای تولید کپچای تصویری با استفاده از مورفولوژی

پیش‌پردازش: قبل از اعمال پردازش برای ساخت کپچا از هر تصویر ورودی، ابتدا لازم است تصویر ورودی به یک تصویر سطوح خاکستری تبدیل و سپس کیفیت ظاهری آن از نظر کنتراست بهبود یابد [۷]. در روش پیشنهادی از روش تعدیل هیستوگرام به منظور افزایش سطح کنتراست استفاده شده است. تعدیل هیستوگرام یکی دیگر از کاربردهای هیستوگرام در افزایش کنتراست تصاویر با کنتراست پایین است. زمانی که گفته می‌شود کنتراست تصویری کم است این بدان معناست که اختلاف بین کمترین و بیشترین شدت روشنایی تصویر کم است. تعدیل سازی هیستوگرام موجب می‌شود که کنتراست تصویر ورودی تا حد ممکن افزایش یابد؛ به این معنا که اگر مقادیر شدت در قسمتی تجمع دارد مقادیر را به گونه‌ای بسط می‌دهد تا توزیع شدت تقریباً یکسان شود [۸]. شکل (۶) یک تصویر ورودی رنگی را به همراه نسخه سطوح خاکستری و تعدیل شده آن نشان می‌دهد

ساخت الگو: در روش پیشنهادی از الگوی نشان داده شده در شکل (۷) استفاده شده است. ایده اصلی این الگو از چندین آزمون هوش برای تشخیص تصویر گرفته شده است. در این روش خطوط ترسیم شده به دلیل نزدیک بودن در پایین و فاصله‌دار شدن در بالا می‌توانند تصویر را به گونه‌ای مناسب تحریف کنند که تنها توسط انسان قابل شناسایی باشد. با توجه به تحقیقات انجام شده به نظر می‌رسد ربات‌های تشخیص تصویر با توجه به



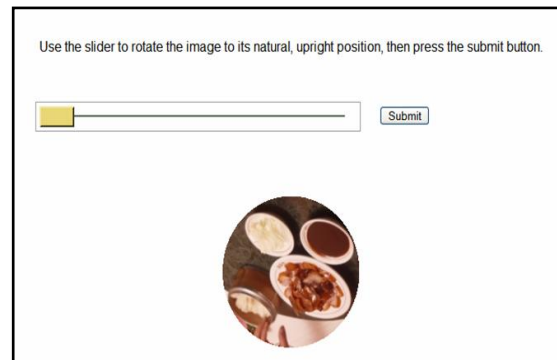
الف) کپچاهای مبتنی بر متن معتبر GIMPY [۱]



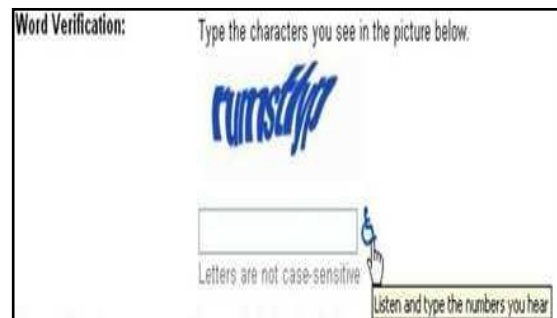
ب) معروف‌ترین کپچاهای مبتنی بر متن، reCAPTCHA [۳]

شکل ۱. نمونه‌ای از کپچاهای معروف مبتنی بر متن

شکل‌های (۴-۲) به ترتیب نمونه‌ای از کپچاهای تصویری، صوتی و ویدئویی را نشان می‌دهند.



شکل ۲. نمونه‌ای از کپچای مبتنی بر تصویر [۴]



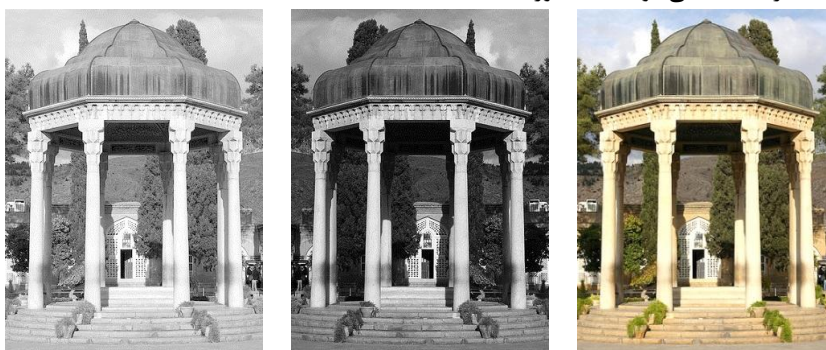
شکل ۳. نمونه‌ای از کپچای مبتنی بر صوت [۵]

تصویر الگو از روابط مثلثاتی تانژانت معکوس موقعیت هر پیکسل که بیانگر زاویه آن پیکسل نسبت به مبدأ است، استفاده شده است [۷].

$$\theta = \text{Arctg}\left(\frac{y}{x}\right) \quad (1)$$

در رابطه (۱)، x و y ، بیانگر موقعیت هر پیکسل از تصویر است. شکل (۷-الف)، تصویر الگو را پس از مشخص شدن زاویه هر پیکسل نشان می‌دهد. پس از آن پیکسل‌های تصویر جدید آستانه‌گذاری می‌شوند. شکل (۷) مراحل تولید الگوی روش پیشنهادی را نشان می‌دهد.

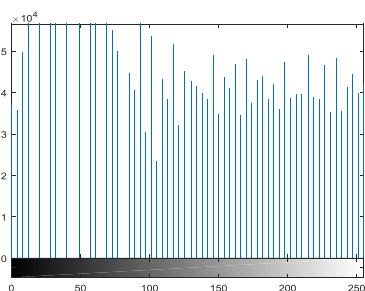
اینکه بر مبنای رنگ عمل می‌کنند و در تشخیص تصاویر رنگی نسبت به سیاه و سفید قدرت بیشتری دارند و همچنین برای تشخیص تصویر تحریف شده، تصویر مورد نظر را با رنگی متمایز از پس‌زمینه جدا می‌کنند، در تشخیص تصویر با این نوع الگوی پیشنهادی با مشکل مواجه می‌شوند. به منظور ساخت الگوی نشان داده شده در شکل (۷) از روابط ریاضی استفاده شده است. به دلیل تقارن تصویر تنها نیمه راست آن ایجاد و سپس با تبدیل هندسی نیمه چپ آن تولید شده است. برای ساخت الگو، تصویری با تعداد سطر برابر با تصویر مرجع و نصف تعداد ستون‌های تصویر مرجع با مقداره‌ی اولیه صفر ساخته می‌شود. به منظور ساخت



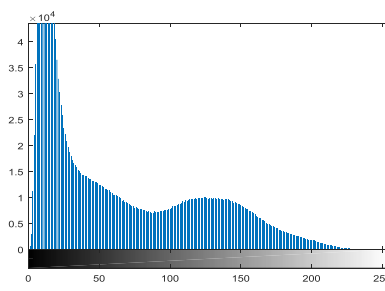
پ) تصویر متعادل شده

ب) تصویر سطوح خاکستری

الف) تصویر ورودی

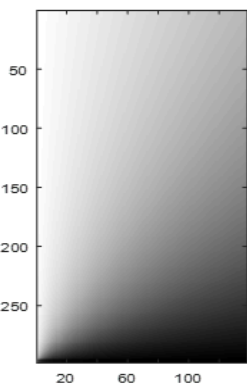


ث) هیستوگرام تصویر خاکستری بعد از تبدیل

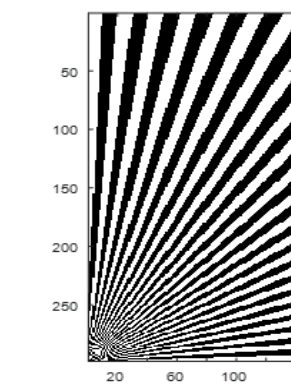


ت) هیستوگرام تصویر خاکستری قبل از تبدیل

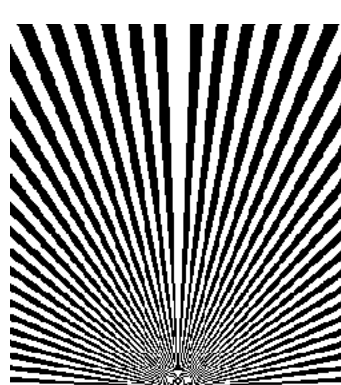
شکل ۶. پیش‌پردازش



پ) آستانه گذاری تصویر تانژانت معکوس

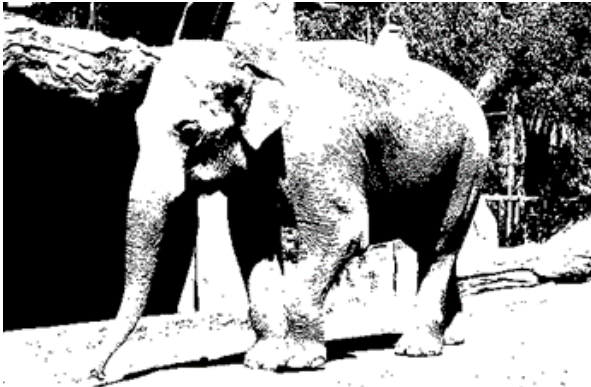


ب) تصویر حاصل از محاسبه تانژانت معکوس

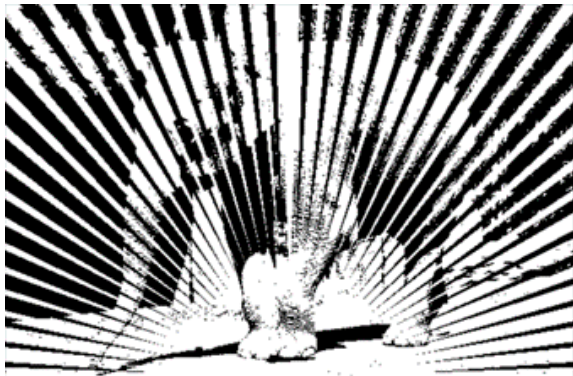


الف) تصویر الگوی مورد نظر

شکل ۷. مراحل تولید الگوی روش پیشنهادی



الف) تصویر حیوان



ب) کپچای پیشنهادی مبتنی بر غیرچهره

شکل ۹. ساخت کپچای مبتنی بر غیر چهره

ویژگی‌های سامانه پیاده‌سازی الگوریتم: برنامه‌های مربوط به شبیه‌سازی الگوریتم، در فضای نرم‌افزار متلب ۲۰۱۵ نوشته شده و توسط یک لپ‌تاپ با پردازشگر Core i7 با حافظه 8GB اجرا شده است.

۳. ارزیابی کپچای روش پیشنهادی

معیارهای موفق بودن کپچاها شامل تولید خودکار آن‌ها توسط رایانه، پاسخ سریع و آسان به آزمون کپچا توسط انسان‌ها، پذیرش همه انسان‌ها و یا گروهی از انسان‌ها و مقاومت در برابر حمله برنامه‌های رایانه‌ای است. هر کپچایی که قادر به برآورده کردن این نیازها نباشد، در عمل کاربردی نخواهد بود. در ادامه این معیارها در کپچای پیشنهادی مورد بررسی قرار خواهد گرفت.

تولید و ارزیابی خودکار کپچا توسط رایانه: کپچای تولید شده به صورتی که در قسمت‌های قبل شرح داده شد، به طور خودکار توسط رایانه در مدت زمانی مشابه مدت زمان تولید کپچاهای متداول یعنی در حدود ۱ یا ۲ ثانیه تولید می‌شود. همچنین ارزیابی پاسخ کاربران نیز به صورت خودکار انجام می‌شود.

ساخت کپچا با استفاده از عملیات ریخت‌شناسی: در روش پیشنهادی پس از ساخت الگو، الگوریتم پیشنهادی برای ساخت کپچا اجرا می‌شود. به این منظور ابتدا تصویر ورودی با استفاده از آستانه‌گذاری اتسو [۷] به یک تصویر باینری به نام B تبدیل می‌شود. سپس با استفاده از یک المان ساختاری ۳×۳ تصویر الگو که P نام دارد به صورت رابطه (۲) پویش می‌شود.

$$\text{If } B(x,y)=P(x,y)=1 \quad (2)$$

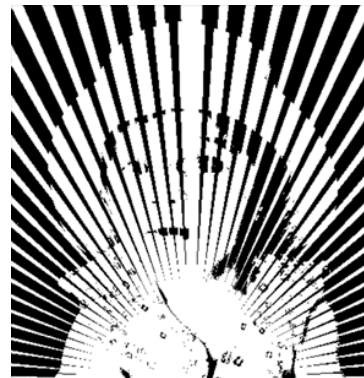
Template Dilatation
Else
Erosion Templat

شکل‌های (۸ و ۹) ساخت کپچای مبتنی بر چهره و غیر چهره را نشان می‌دهد.

کپچای نهایی در قالب یک واسط کاربر در HTML و با زبان‌های JavaScript و PHP آماده شده و به کاربر ارائه می‌شود. در کپچای مبتنی بر تصاویر غیر چهره کاربر می‌بایست نام شیء یا موجودی را که در کپچا می‌بیند در یک جعبه متنی وارد کند. اگر پاسخ کاربر صحیح باشد، آنگاه آزمون کپچا را با موفقیت گذرانده است و در نتیجه انسان بودن کاربر ثابت شده و در غیر این صورت کاربر یک ربات است.



الف) تصویر کودک



ب) کپچای پیشنهادی مبتنی بر چهره

شکل ۸. ساخت کپچای مبتنی بر چهره

خاصی نیاز نیست. تنها گروهی از انسان‌ها که قادر به حل این کپچا نیستند، افرادی با مشکلات بینایی شدید هستند.

مقایسه کپچای پیشنهادی با سایر روش‌ها: در جدول (۲) مقایسه‌ای بین چند کپچا از نظر درصد موفقیت انسان و زمان پاسخگویی به کپچا انجام شده است. لازم به ذکر است زمان‌های پاسخگویی گزارش نشده به دلیل این است که در مرجع مربوطه از این زمان صحبتی نشده است.

شکل (۱۰) واسط کاربری آزمایش کپچای روش پیشنهادی را نشان می‌دهد.



شکل ۱۰. واسط کاربری آزمایش کپچای روش پیشنهادی

جدول ۲. زمان متوسط پاسخ به آزمون کپچا بر حسب ثانیه

نام کپچا	درصد موفقیت انسان‌ها	زمان پاسخگویی انسان‌ها (ثانیه)
ARTiFACIAL [۹]	۹۹/۷	۱۴
Asirra [۱۰]	۹۹	-
Face Recognition CAPTCHA [۱۱]	۹۶	-
FaceDCAPTCHA [۱۲]	۹۲/۴۷	-
FaceCAPTCHA [۱۳]	۹۰/۲	۱۰/۰۹
مبتنی بر ویدئو [۱۴]	۹۰	۱۷
Face Detection CAPTCHA [۱۵]	۷۱/۷۱	-
کپچای پیشنهادی مبتنی بر غیر چهره	۹۰/۵۰	۱۶/۸
کپچای پیشنهادی مبتنی بر چهره	۹۶	۷/۶

۵. نتیجه‌گیری

در معرض خطر بودن سرویس‌های اینترنتی، همواره می‌طلبد تا با ارائه یک راهکار در عین حال کارآمد این سرویس‌ها را در مقابل حمله و تخریب توسط هکرها محافظت و از آن‌ها همه جانبه دفاع نمود. در روش پیشنهادی یک کپچای تصویری با استفاده از عملیات مورفولوژی بر روی یک تصویر الگو با توجه به تصویر

پاسخ سریع و آسان به آزمون کپچا توسط انسان: برای ارزیابی این کپچا در بین نمونه‌های مختلف کاربری، از تعداد ۱۰۰ نفر نظرسنجی به عمل آمد. این ۱۰۰ نفر، کاربران اینترنت در رده سنی ۱۰ تا ۶۰ سال بودند. فرایند ارزیابی به صورت زیر انجام شد:

۱- یک لپ‌تاپ در اختیار کاربر قرار می‌گیرد و از او خواسته می‌شود که لپ‌تاپ را به گونه‌ای که بتواند به راحتی با آن کار کند تنظیم نماید.

۲- در مورد کپچای مبتنی بر غیر چهره دستورالعمل زیر به کاربر داده می‌شود: یک تصویر شامل یک شیء یا یک صحنه به کاربر نشان داده می‌شود و کاربر می‌بایست نام شیء یا نام صحنه را در کادر متنی وارد کند.

۳- برنامه تولید کپچا بر روی لپ‌تاپ شروع به کار می‌کند و به صورت تصادفی یک تصویر کپچا را از میان تصاویر کپچا نمایش می‌دهد. کاربر، نام شیء را وارد می‌کند. با این کار مدت زمانی که طول می‌کشد تا کاربر کار را به پایان برساند، برای تجزیه و تحلیل‌های بعدی ثبت می‌شود.

۴- برنامه کپچا بسته می‌شود و رضایت فرد از این کپچا مورد بررسی قرار می‌گیرد.

۴. نتایج و بحث

هر کدام از ۱۰۰ کاربر مورد بررسی، به چهار آزمون کپچا (دو آزمون مبتنی بر چهره و دو آزمون مبتنی بر غیر چهره) پاسخ دادند. بر اساس پاسخ کاربران و زمان پاسخگویی به آزمون کپچا، نتایج نظرسنجی از کاربران را می‌توان به صورت زیر خلاصه کرد: زمان متوسط برای تشخیص شیء و تایپ نام آن در کپچای مبتنی بر غیر چهره و همچنین بر روی چهره در جدول (۱) آمده است. این زمان برای حل یک آزمون کپچا، زمان مناسب و مطلوبی است.

جدول ۱. زمان متوسط پاسخ به آزمون کپچا بر حسب ثانیه

کپچای مبتنی بر غیر چهره	کپچای مبتنی بر چهره
۱۶/۸ ثانیه	۷/۶ ثانیه

از میان ۱۰۰ نفر، ۸۷ نفر آزمون را به طور کامل با موفقیت پشت سر گذاشتند. طبق نظرسنجی انجام شده، از میان ۱۰۰ کاربر، ۹۲ نفر از کپچای پیشنهادی رضایت داشتند.

پذیرش همه انسان‌ها و یا گروهی از انسان‌ها: همان‌گونه که مشاهده می‌شود، برای پاسخگویی به کپچای پیشنهادی به دانش

- [6] Kluever, K. A.; Zanibbi, R. "Balancing Usability and Security in a Video CAPTCHA"; Proc. 5th Symposium on Usable Privacy and Security, 2009, 14.
- [7] Rafael, C. G.; Woods, R. E. "Digital Image Processing"; 2002.
- [8] Wang, Y.; Chen, Q.; Zhang, B. "Image Enhancement Based on Equal Area Dualistic Sub-Image Histogram Equalization Method"; IEEE Trans. Consumer Electronics 1999, 45, 68-75.
- [9] Zhu, B. B.; Yan, J.; Li, Q.; Yang, C.; Liu, J.; Xu, N. "Attacks and Design of Image Recognition CAPTCHAs"; Proc. 17th ACM Conf. Comput. Commun. Secur. 2010, 187-200.
- [10] Golle, P. "Machine Learning Attacks Against the Asirra CAPTCHA"; Proc. of the 15th ACM Conf. on Computer and Communications Security, 2008, 535-542.
- [11] Goswami, G.; Singh, R.; Vatsa, M.; Powell, B.; Noore, A. "Face Recognition Captcha"; IEEE Fifth Int. Conf. Biometrics: Theory, Applications and Systems 2012, 412-417.
- [12] Goswami, G.; Powell, B. M.; Vatsa, M.; Singh, R.; Noore, A. "FaceDCAPTCHA: Face Detection Based Color Image CAPTCHA"; Future Generation Computer Syst. 2014, 31, 59-68.
- [13] Kim, J.; Kim, S.; Yang, J.; Ryu, J.-H.; Wahn, K. "FaceCAPTCHA: A CAPTCHA that Identifies the Gender of Face Images Unrecognized by Existing Gender Classifiers"; Multimedia Tools and Applications 2014, 72, 1215-1237.
- [14] Cui, J.-S.; Mei, J.-T.; Wang, X.; Zhang, D.; Zhang, W.-Z. "A Captcha Implementation Based on 3D Animation"; Int. Conf. Multimedia Information Networking and Security 2009, 179-182.
- [15] Day, A. C. "Designing a Face Detection CAPTCHA"; West Virginia University, 2010.

اصلی ارائه شد. از آنجا که تشخیص عناصر چهره و یا اشیاء از آشناترین موضوعات برای تمام کاربران انسانی است، کپچای پیشنهادی کاملاً همگانی است. همچنین مطالعاتی بر روی ۱۰۰ کاربر انسانی با پیشینه‌های گوناگون انجام شد و اکثریت این افراد از کپچای ارائه شده رضایت داشتند. بنابراین سهولت تشخیص کپچای ارائه شده توسط انسان، کاربر پسند بودن و همگانی بودن کپچا برای بیشتر کاربران انسانی به دلیل تصویر قابل فهم و شناخته شده از مزایای این نوع کپچای ارائه شده است. همچنین با توجه به مطالعات و تحقیقات انجام شده ضعف ربات‌ها و برنامه‌های مخرب در یافتن تصویر تحریف شده توسط الگوی پیشنهادی با این روش و مدت زمان پاسخگویی توسط کاربر را می‌توان از مزایای روش مذکور نسبت به سایر روش‌ها بر شمرد.

۶. مراجع

- [1] Von Ahn, L.; Blum, M.; Hopper, N. J.; Langford, J. "CAPTCHA: Using Hard AI Problems for Security"; Advances in Cryptology—Eurocrypt. 2003, 294-311.
- [2] Pinkas, B.; Sander, T. "Securing Passwords against Dictionary Attacks"; Proc. 9th ACM Conf. on Comput. Commun. Secur. 2002, 161-170.
- [3] Von Ahn, L.; Maurer, B.; McMillen, C.; Abraham, D.; Blum, M. "Recaptcha: Human-Based Character Recognition via Web Security Measures"; Sci. 2008, 321, 1465-1468.
- [4] Elson, J.; Douceur, J. R.; Howell, J.; Saul, J. "Asirra: A CAPTCHA that Exploits Interest-aligned Manual Image Categorization"; ACM Conf. Comput. Commun. Secur. 2007, 366-374.
- [5] Viola, P.; Jones, M. "Rapid Object Detection Using a Boosted Cascade of Simple Features"; Computer Vision & Pattern Recognition, CVPR 2001. Proc. IEEE Comput. Soc. Conf. 2001, 1, 511-518.