مقاله پژوهشی

# راهکاری نوین در پیشگیری از تقلب در آزمون‌های آنلاین حضوری دانشگاه صنعتی اصفهان، با بهره‌گیری از تکنیک YOLO و سیستم‌های چندعاملی

Doi: 10.30508/kdip.2025.499404.1125

طاهره رحیم پور[1]
۱-دانشجوی دکتری حرفه‌ای مدیریت کسب و کار، دانشگاه صنعتی اصفهان، اصفهان، ایران

تاریخ دریافت: ۱۴۰۳/۱۰/۲۳
تاریخ پذیرش: ۱۴۰۳/۱۱/۲۸
صفحه: ۷۴ - ۶۰

## چکیده

با گسترش سریع آموزش‌های آنلاین، حفظ صداقت علمی در آزمون‌های مجازی به چالشی اساسی برای مؤسسات آموزشی تبدیل شده است. این تحقیق که در دانشگاه صنعتی اصفهان و در محیط آزمایشگاهی ویژه آزمون‌های آنلاین حضوری شبیه‌سازی شده است، سیستمی نوآورانه را معرفی می‌کند که از ترکیب الگوریتم شناسایی اشیاء YOLO و سیستم‌های چندعاملی (MAS) برای شناسایی و پیشگیری از تقلب استفاده می‌نماید. در این سیستم، الگوریتم YOLO به‌منظور شناسایی اشیاء غیرمجاز مانند تلفن‌های همراه و تبلت‌ها از تحلیل ویدئویی بهره می‌برد، در حالی‌که سیستم MAS با ارزیابی رفتارهای غیرعادی دانشجویان، همچون کلیک‌های مشکوک ماوس، تأخیرهای غیرعادی در پاسخ‌دهی، تغییرات غیرطبیعی در حرکت نگاه و باز کردن تب‌های غیرمجاز در مرورگر، به شناسایی الگوهای احتمالی تقلب می‌پردازد. این سیستم در آزمون‌های تستی دروس عمومی پرجمعیت دانشگاه صنعتی اصفهان از جمله معارف اسلامی، فارسی و اخلاق شبیه‌سازی شده است و نتایج نشان می‌دهد که با دقت ۸۷٫۹ درصد قادر به شناسایی تقلب است. همچنین، با سرعت پردازش ۰٫۱ تا ۰٫۱۵ ثانیه برای هر فریم، این سیستم امکان اجرای آن در زمان واقعی را فراهم می‌آورد. یافته‌های این تحقیق تأکید دارند که ترکیب الگوریتم‌های یادگیری عمیق و سیستم‌های مبتنی بر عامل می‌تواند راهکاری مؤثر و مقیاس‌پذیر برای تقویت امنیت آزمون‌های آنلاین حضوری ارائه دهد و در نهایت به ارتقای اعتماد به فرآیندهای ارزیابی آنلاین و تضمین عدالت آموزشی کمک نماید.

**کلمات کلیدی:** تقلب، آزمون آنلاین، YOLO، سیستم چندعاملی، یادگیری عمیق

## ۱- مقدمه

در دنیای امروز، فناوری‌های آنلاین نه تنها روش‌های آموزش و یادگیری را تغییر داده‌اند، بلکه چالش‌های جدیدی را در زمینه ارزیابی و آزمون‌های تحصیلی ایجاد کرده‌اند. یکی از اصلی‌ترین مشکلاتی که در این راستا پدید آمده، تقلب در آزمون‌های آنلاین است. با توجه به اینکه آزمون‌های آنلاین به طور فزاینده‌ای در حال تبدیل شدن به یک روش استاندارد در ارزیابی دانش‌آموزان و دانشجویان هستند، شناسایی و جلوگیری از تقلب به یکی از دغدغه‌های مهم در سیستم‌های آموزشی تبدیل شده است (هوو، جیانگ، وو ووانگ[1]، ۲۰۲۴). استفاده از ابزارهای نظارتی سنتی مانند نظارت انسانی یا روش‌های مبتنی بر پایش آنلاین به‌تنهایی قادر به مقابله با این مشکل در مقیاس‌های بزرگ و محیط‌های پیچیده نیستند.

در این راستا، هوش مصنوعی به‌عنوان یک راهکار نوین و کارآمد برای حل این مشکل مطرح شده است. الگوریتم‌های یادگیری عمیق و بینایی کامپیوتری می‌توانند به شناسایی تقلب در زمان واقعی کمک کنند و ابزارهای جدیدی را برای نظارت دقیق و خودکار بر آزمون‌های آنلاین فراهم کنند (علی، منظور، مسعود، و عباس[2]، ۲۰۲۴).

یکی از برجسته‌ترین تکنیک‌ها در این زمینه، الگوریتم YOLO[3] است که به دلیل سرعت و دقت بالای خود در تشخیص اشیاء، به‌طور گسترده‌ای در پروژه‌های نظارتی مورد استفاده قرار می‌گیرد. YOLO قادر است با پردازش ویدئوهای زنده و شناسایی اجسام مشکوک، به سرعت تقلب‌های مختلف مانند استفاده از گوشی موبایل، کپی‌برداری از منابع خارجی و یا حرکت غیرطبیعی دانشجویان را شناسایی کند. (ردمون و فرهادی[4]، ۲۰۱۸).

علاوه بر این، استفاده از سیستم‌های چندعاملی (MAS) می‌تواند قدرت تحلیل این داده‌ها را به‌طور قابل توجهی افزایش دهد. سیستم‌های چندعاملی به‌طور معمول از چندین عامل مستقل استفاده می‌کنند که به‌طور همزمان به تحلیل و پردازش داده‌ها می‌پردازند و به این ترتیب توانایی سیستم در تشخیص رفتارهای پیچیده و غیرمنتظره افزایش می‌یابد. در این مقاله، با ترکیب این دو تکنیک پیشرفته، یعنی YOLO و MAS، یک سیستم نوین برای پیشگیری از تقلب در آزمون‌های آنلاین معرفی می‌شود که قادر است با دقت بالا و در زمان واقعی، تقلب‌های ممکن را شناسایی و گزارش کند.

هدف این پژوهش ارزیابی توانایی این رویکرد ترکیبی در شناسایی تقلب در آزمون‌های آنلاین، بررسی کارایی سیستم در شرایط مختلف، و تحلیل چالش‌ها و محدودیت‌های استفاده از این تکنولوژی می باشد.

این تحقیق در دانشگاه صنعتی اصفهان و در محیط آزمایشگاهی ویژه آزمون‌های آنلاین حضوری در آزمون‌های تستی دروس عمومی پرجمعیت از جمله معارف اسلامی، فارسی، اخلاق و نظایر آن شبیه‌سازی شده است و با هدف بررسی دقیق و همه‌جانبه موضوع مورد مطالعه، طراحی و اجرا شد. فرآیند اجرای پژوهش به‌صورت گروهی و در فضای علمی سالن آزمایشگاه کامپیوتر این دانشگاه انجام گرفت. برای دستیابی به داده‌های معتبر و قابل استناد، آزمون‌ها به‌صورت آنلاین طراحی شدند و در چارچوب سناریوهای متنوع و هدفمند برگزار گردیدند. این سناریوها به‌گونه‌ای برنامه‌ریزی شده بودند که شرایط مختلفی را شبیه‌سازی کنند و امکان تحلیل نتایج در موقعیت‌های گوناگون را فراهم آورند. چنین رویکردی این امکان را داد تا نتایج به‌دست‌آمده را از منظرهای مختلف ارزیابی کرده و به یافته‌هایی جامع‌تر و دقیق‌تر دست پیدا کرد.

## ۲- مبانی نظری

در سال‌های اخیر، تحقیقات گسترده‌ای در زمینه استفاده از هوش مصنوعی برای نظارت و شناسایی تقلب در آزمون‌های آنلاین صورت گرفته است. یکی از نخستین پژوهش‌ها در این حوزه به‌کارگیری الگوریتم‌های بینایی کامپیوتری برای شناسایی تقلب در محیط‌های آموزشی است. به‌عنوان مثال در تحقیقی (وینیکی، پاولیکی، پاولیکا، کوزیک، و کروآس[5]، ۲۰۲۵) از مدل‌های یادگیری عمیق برای تشخیص تقلب در آزمون‌های آنلاین استفاده کردند.

1- Hu, Jing, Wu, & Wang
2- Ali, Manzoor, Masood, & Abbas
3- You Only Look Once
4- Redmon,- & Farhadi
5- Winiecki, Pawlicki, Pawlicka, Kozik, & Chora

نتایج این مطالعه نشان داد که مدل‌های CNN قادر به شناسایی تغییرات غیرعادی در رفتار و موقعیت کاربران هستند و می‌توانند در شناسایی تقلب به‌طور قابل توجهی مؤثر باشند.

در پژوهش‌های دیگری نیز، (آسیپ[1]، ۲۰۱۹) به بررسی چالش‌ها و مشکلات اخلاقی ناشی از استفاده از نظارت هوش مصنوعی در آزمون‌های آنلاین پرداخته‌اند. آن‌ها استدلال می‌کنند که استفاده از سیستم‌های هوشمند باید با دقت و در نظر گرفتن حریم خصوصی کاربران صورت گیرد تا از سوءاستفاده‌های احتمالی جلوگیری شود.

(وینیال، بلوندل، لیلیکارپ، و ویرستارا[2]، ۲۰۱۶) در تحقیقی به‌کارگیری سیستم‌های چندعاملی برای حل مسائل پیچیده در محیط‌های آموزشی را بررسی کردند و به این نتیجه رسیدند که ترکیب MAS با الگوریتم‌های بینایی کامپیوتری می‌تواند باعث افزایش دقت و سرعت پردازش در سیستم‌های نظارتی شود.

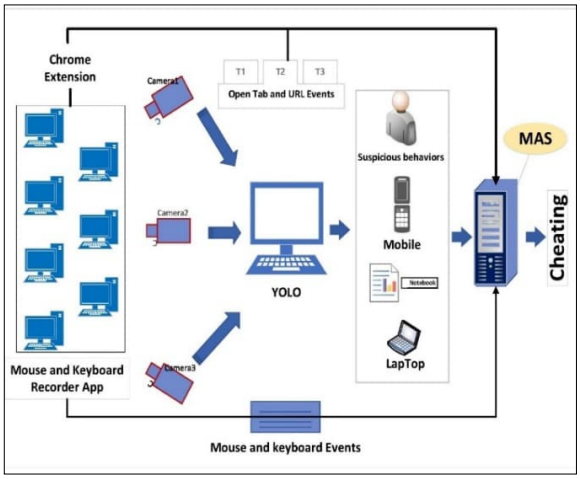
پژوهش‌های اخیر در زمینه‌های مختلف نیز نشان داده‌اند که ترکیب الگوریتم‌های YOLO با سیستم‌های MAS نه تنها دقت را بهبود می‌بخشد بلکه توانایی شناسایی تقلب‌های پیچیده و نوآورانه را افزایش می‌دهد. این تحقیق‌ها بیشتر بر روی بهبود الگوریتم‌ها و کاربرد آن‌ها در سناریوهای واقعی تمرکز دارند و در حال گسترش هستند (فاطیما، جنینگ، و وولدرینگ[3]، ۲۰۲۴).

## ۳- روش تحقیق

روش‌شناسی این تحقیق به منظور ارزیابی و طراحی یک سیستم هوشمند برای پیشگیری از تقلب در آزمون‌های آنلاین با استفاده از ترکیب الگوریتم YOLO و سیستم‌های چندعاملی (MAS) طراحی شده است. این سیستم به‌طور خودکار و در زمان واقعی رفتارهای مشکوک در محیط‌های آنلاین را شناسایی کرده و از وقوع تقلب جلوگیری می‌کند. در این بخش، جزئیات مراحل مختلف تحقیق، از طراحی سیستم تا ارزیابی آن، به تفصیل توضیح داده خواهد شد.

### طراحی سیستم تشخیص تقلب

هدف اصلی این تحقیق طراحی یک سیستم مبتنی بر هوش مصنوعی است که بتواند با استفاده از الگوریتم YOLO و سیستم‌های چندعاملی، تقلب در آزمون‌های آنلاین را شناسایی کند. در این سیستم، بخش‌های مختلف، شامل شناسایی اشیاء مشکوک (مانند گوشی موبایل، کتاب و یا مواد تقلبی)، تحلیل رفتار دانشجویان، و تصمیم‌گیری در زمان واقعی برای شناسایی تقلب طراحی شده‌اند (شکل ۱).




شکل (۱): طراحی سیستم تشخیص تقلب

1- Asep
2- Vinyals, Blundell, Lillicrap, & Wierstra
3- Fatima, Jennings, & Wooldridge

تعریف الگوریتم YOLO: بخش اصلی سیستم برای شناسایی اشیاء مشکوک از الگوریتم YOLO استفاده شده است. این الگوریتم از معماری شبکه عصبی کانولوشنی (CNN) برای شناسایی سریع و دقیق اشیاء مختلف در تصاویر و ویدئوها بهره می‌برد. در این تحقیق، نسخه YOLOv۹ به‌عنوان نسخه‌ای با عملکرد بالا انتخاب شد. الگوریتم به‌طور پیوسته و در زمان واقعی تصاویر مربوط به آزمون آنلاین را پردازش می‌کند و اشیاء مشکوک مانند گوشی‌های موبایل یا دیگر ابزارهای تقلب را شناسایی می‌کند (اردیم، و کاراباتاک[1]، ۲۰۲۵؛ سینگه، نایر، بابو، و دوراسیمای[2]، ۲۰۲۴).

## قابلیت‌های الگوریتم YOLOv۹:

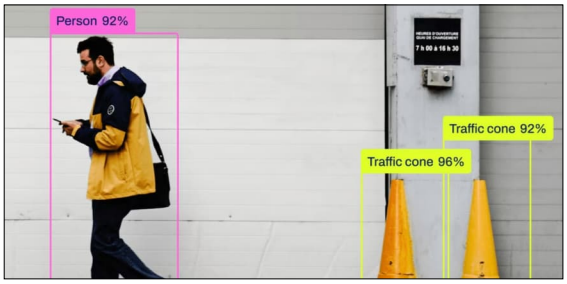
### طبقه‌بندی تصویر[3]

به تکنیک تخصیص لیبل به تصاویر بر اساس ویژگی‌های آنها، طبقه‌بندی تصویر گفته می‌شود (شکل ۲) که این لیبل در واقع همان مفهوم عکس است. طبقه‌بندی تصاویر بر اساس ویژگی‌های مشترک آن‌ها، یعنی شناسایی و دسته‌بندی محتوای موجود در تصاویر، به شکلی که ماشین‌ها بتوانند آن‌ها را درک کرده و تشخیص دهند.


شکل (۱): طبقه‌بندی تصویر

### تشخیص اشیا[4]

تشخیص اشیاء یکی از زمینه‌های مهم در بینایی کامپیوتر است که وظیفه آن شناسایی و تعیین مکان اشیای خاص در تصاویر یا ویدئوها است. این فرآیند شامل دو مرحله اصلی است: شناسایی کلاس شیء: تشخیص می‌دهد که هر شیء به چه دسته یا کلاسی (خودرو، انسان، حیوان و غیره) تعلق دارد. تعیین مکان شیء: مختصات دقیق ناحیه‌ای که هر شیء در تصویر یا ویدئو قرار دارد (شکل ۳).

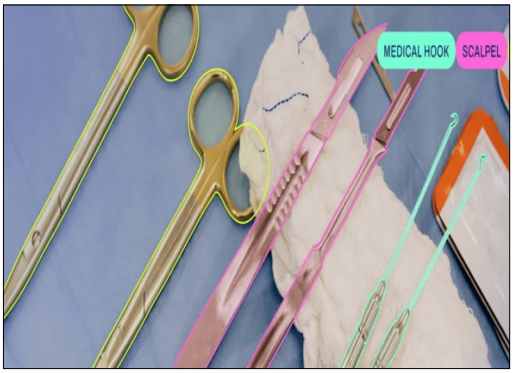



شکل (۳): تشخیص اشیا

### بخش‌بندی تصویر[5]

یک تکنیک پیشرفته در بینایی کامپیوتر است که فراتر از طبقه‌بندی و تشخیص اشیا عمل می‌کند. این روش وظیفه شناسایی، طبقه‌بندی و تفکیک هر نمونه از یک شیء در یک تصویر را بر عهده دارد و به هر نمونه یک ناحیه دقیق اختصاص می‌دهد.

به جای استفاده از کادرهای مستطیلی، شکل دقیق هر شیء با استفاده از پیکسل‌های تصویر مشخص می‌شود (شکل ۴).



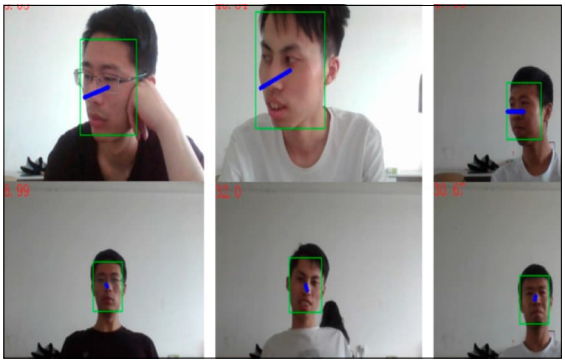

شکل (۴): بخش‌بندی تصویر

1- Erdem, & Karabatak
2- Singh, Nair, Babu, & Duraisamy
3- Image Classification
4- Object Detection
5- Instance Segmentation

### تشخیص حالت بدن انسان[1]

یک تکنیک در بینایی کامپیوتر است که هدف آن شناسایی موقعیت و جهت اجسام، به ویژه انسان‌ها، در تصاویر یا ویدئوها است. در واقع، این تکنیک به سیستم‌ها کمک می‌کند تا وضعیت هندسی و موقعیت دقیق اعضای بدن یا اجسام را شناسایی کنند (شکل ۵ و ۶).

شکل(۵): تشخیص حالت بدن انسان



شکل (۶): تشخیص حالت بدن انسان

سیستم چندعاملی (MAS): پس از شناسایی اشیاء مشکوک توسط YOLO، سیستم چندعاملی وارد عمل می‌شود،MAS ، از چندین عامل مستقل تشکیل شده است که به‌طور همزمان وظایف مختلفی مانند تجزیه و تحلیل رفتار دانشجویان (شبیه به شبیه‌سازی‌های رفتارشناسی،کلیک‌های موس و صفحه کلید و نیز باز کردن تب‌های غیرمجاز)، و مدیریت داده‌های مختلف از محیط آزمون آنلاین را انجام می‌دهند. این سیستم با تحلیل و ترکیب اطلاعات به‌دست‌آمده از عامل‌های مختلف، تصمیم‌گیری دقیق‌تری در خصوص تقلب یا عدم تقلب می‌کند (جنینگس و وودریج[2]، ۱۹۹۸).

## ۴- یافته‌های تحقیق

برای ارزیابی سیستم، از داده‌های ویدئویی و رفتاری دانشجویان در شرایط آزمایشی استفاده شده است شکل(۶ و ۷). این داده‌ها شامل ویدئوهای ضبط‌شده از آزمون‌های آنلاین هستند که در آن‌ها دانشجویان در حال انجام آزمون در یک محیط شبیه‌سازی شده قرار دارند.

داده‌های ویدئویی: ویدئوهای ضبط شده از دوربین‌های وب‌کم به‌طور مداوم بررسی می‌شوند تا رفتارهای مشکوک مانند استفاده از گوشی موبایل، نگاه کردن به منابع خارجی و یا حرکت غیرعادی بدن را شناسایی کنند. داده‌های ویدئویی به‌طور مستقیم به الگوریتم YOLO ارسال می‌شوند تا اشیاء مشکوک شناسایی شوند.

داده‌های رفتاری: علاوه بر داده‌های تصویری، از داده‌های رفتاری شامل تغییرات در سرعت تایپ، زمان پاسخ‌دهی به سوالات، باز کردن تب‌های غیرمجاز و حرکات ماوس نیز استفاده می‌شود.

این داده‌ها توسط عامل‌های MAS تحلیل می‌شوند تا الگوهای غیرعادی رفتار دانشجو شناسایی شود. در این پژوهش سرعت پردازش سیستم با ۰٫۱ تا ۰٫۱۵ ثانیه برای هر فریم، آن را برای استفاده در زمان واقعی مناسب ساخته است.

در این پژوهش، بر روی کلیه سیستمهای آزمون گیرنده، نرم‌افزاری جهت ثبت وقایع[3] موس و صفحه کلید نصب شده است که این وقایع را به سامانه MAS برای تصمیم‌گیری ارسال می‌کند، همچنین ابزار افزونه کروم[4] جهت تشخیص باز کردن تب‌های غیرمجاز استفاده شده است. این اطلاعات نیز برای تصمیم‌گیری نهایی به سامانه

1- Pose Estimation
2- Jennings & Wooldridge
3- Events
4- Chrome Extension

MAS ارسال می‌گردد.

شکل (۶): تصاویر ضبط‌شده توسط دوربین‌ها

شکل (۷): تصاویر ضبط‌شده توسط دوربین‌ها

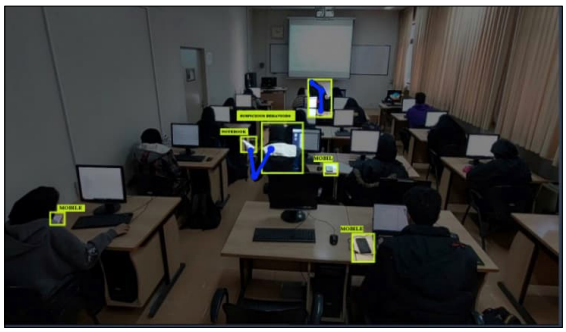
## پردازش و تحلیل داده‌ها

پیش‌پردازش داده‌ها: داده‌های ویدئویی قبل از ارسال به الگوریتم YOLO باید پیش‌پردازش شوند. این پیش‌پردازش شامل عملیات‌هایی مانند تغییر اندازه تصاویر به ابعاد استاندارد، حذف نویز و بهبود کیفیت تصویر است (ژنگ[1]، ۲۰۲۴). همچنین داده‌های رفتاری مانند کلیک‌های ماوس باید به‌صورت ویژگی‌های عددی آماده شوند تا بتوانند به‌طور موثر توسط عامل‌های MAS تحلیل شوند (هوو، جیانگ، وو، و وانگ[2]، ۲۰۲۴).

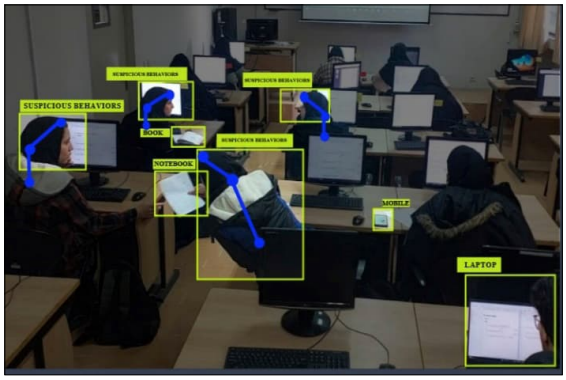
شناسایی اشیا با YOLO: پس از پیش‌پردازش، داده‌های ویدئویی به الگوریتم YOLO ارسال می‌شوند، YOLO با استفاده از معماری شبکه عصبی، اشیاء مختلف را شناسایی کرده و در صورت شناسایی اشیاء مشکوک مانند گوشی موبایل، بلافاصله آن‌ها را علامت‌گذاری می‌کند (سلیم و همکاران[3] ، ۲۰۲۴).

تحلیل رفتار توسط MAS: پس از شناسایی اشیاء مشکوک توسط YOLO، اطلاعات رفتاری دانشجو توسط سیستم MAS تجزیه و تحلیل می‌شود. عوامل MAS برای تحلیل رفتار از مدل‌های یادگیری ماشین و آمار استفاده می‌کنند تا شواهد تقلب را از رفتارهای طبیعی تمایز دهند.

شکل (۸ و ۹) مربوط به شناسائی تقلب با استفاده از ابزار YOLO و تحلیل MAS می باشد:



شکل (۸): شناسایی تقلب با استفاده از تکنیک YOLO




شکل (۹): شناسایی تقلب با استفاده از تکنیک YOLO

## سیستم تصمیم‌گیری

سیستم تصمیم‌گیری مبتنی بر سیستم‌های چندعاملی (MAS) که با استفاده از کتابخانه JADE در محیط جاوا پیاده‌سازی شده است، یکی از نوآوری‌های کلیدی این پژوهش است. MAS با ترکیب چندین عامل مستقل

1- Zeng
2- Hu, Jing, Wu, & Wang
3- Saleem etal

که هر یک وظیفه‌ای خاص دارند، امکان تحلیل جامع داده‌ها و تصمیم‌گیری خودکار را فراهم می‌کند. در این سیستم، عامل‌های مختلف وظیفه پردازش و تحلیل داده‌های رفتاری (مانند کلیک‌های ماوس، ضربات کیبورد، و باز کردن تب‌های غیرمجاز) و داده‌های بصری (مانند تصاویر پردازش‌شده از دوربین‌ها که رفتارهای مشکوک یا استفاده از موبایل، لپ‌تاپ و کتاب را شناسایی کرده‌اند) را بر عهده دارند.

الگوریتم تصمیم‌گیری MAS، پس از جمع‌آوری و تحلیل داده‌ها از عامل‌های مختلف، احتمال وقوع تقلب را بر اساس شواهد جمع‌آوری‌شده محاسبه می‌کند. این فرآیند به‌صورت یکپارچه و با هماهنگی عامل‌ها انجام می‌شود، به‌طوری که هر عامل نقش ویژه‌ای در تحلیل جنبه خاصی از داده‌ها دارد. برای مثال، یک عامل به تحلیل تعاملات کاربر با سیستم می‌پردازد، درحالی‌که عامل دیگری داده‌های بصری دریافتی از تکنیک YOLO را پردازش و رفتارهای مشکوک را شناسایی می‌کند.

نتایج نهایی توسط MAS پردازش‌شده و به‌طور خودکار برای ناظران یا مدرسین ارسال می‌شود. این ساختار چندعاملی باعث افزایش سرعت، دقت، و مقیاس‌پذیری سیستم شده و نشان می‌دهد که چگونه ترکیب MAS با تکنیک‌های هوش مصنوعی مانند YOLO می‌تواند راهکاری مؤثر برای نظارت بر آزمون‌های آنلاین و شناسایی تقلب ارائه دهد. در عامل کلیک، کلیک‌های مشکوک شناسایی می‌شود. برای مثال، اگر کاربر بیش از ۳ بار روی دکمه‌ای کلیک کند که نباید کلیک شود، رفتار مشکوک تلقی می‌شود، همینطور در عمل صفحه کلید، الگوهای تایپ بررسی می‌شود. اگر تایپ شامل عبارات خاصی مانند URL یا نام فایل باشد، سیستم هشدار می‌دهد. و نیز عامل تب، این عامل تعداد و نوع تب‌های باز را ثبت و تحلیل می‌کند. باز کردن تب‌هایی با آدرس غیرمجاز یا مرتبط با منابع خارجی نشانه تقلب است.

هر رفتار مشکوک یک امتیاز (score) دریافت می‌کند، تعداد کلیک‌های مشکوک با ($C_{Mouse}$)، تعداد ضربات غیرمجاز با ($K_{Keyboard}$)، تعداد تب‌های غیرمجاز با ($Tab_T$) و وزن‌هایی که اهمیت هر رفتار را مشخص می‌کنند با (W) مشخص می‌شوند. اگر مجموع امتیازات رفتارها ($S_{Behavior}$) از یک آستانه فراتر رود، رفتار به‌عنوان تقلب ثبت می‌شود.

برای هر تعامل، الگوریتم تصمیم‌گیری زیر اعمال می‌شود:

$$S_{Behavior} = Tab_T * W_1 + K_{Keyboard} * W_2 + C_{Mouse} * W_3 \quad (1)$$

نمونه کد برنامه:

```
import jade.core.Agent;
import jade.core.behaviours.Behaviour;

public class FraudDetectionAgent extends Agent {
    @Override
    protected void setup() {
        System.out.println("Agent " + getLocalName() + " is starting.");
        addBehaviour(new FraudDetectionBehaviour());
    }

    @Override
    protected void takeDown() {
        System.out.println("Agent " + getLocalName() + " is shutting down.");
    }
}

class FraudDetectionBehaviour extends Behaviour {
    private boolean isDone = false;
```

```
@Override
public void action() {
    // data collection
     int mouseClicks = collectMouseClicks();
    int keyPresses = collectKeyPresses();
    int tabsOpen = collectTabs();

    // YOLO output
     double yoloScore = getYOLOScore();

    // Combine results
     double fraudScore = calculateFraudScore(mouseClicks, keyPresses, tabsOpen,
 yoloScore);

    System.out.println("Fraud Score: " + fraudScore);

    // Decision
     if (fraudScore > 3.0) {
        System.out.println("Fraud detected!");
    } else {
        System.out.println("No fraud detected.");
    }

    isDone = true;
}

@Override
public boolean done() {
    return isDone;
}

private int collectMouseClicks() {
    // my mouse click collection codes...
     return 5; // 5 suspicious clicks
}

private int collectKeyPresses() {
    // my key press collection codes...
     return 3; // 3 suspicious key presses
}

private int collectTabs() {
    // my open tab collection codes...
     return 2; // 2 suspicious tabs
}

private double getYOLOScore() {
    // YOLO outputs (e.g., detected phone or book or face or ...)
     return 1.5; // Score from YOLO
}

private double calculateFraudScore(int mouseClicks, int keyPresses, int tabsOpen, double yoloScore) {
```

```
        double wMouse = 0.3;
        double wKeyPress = 0.3;
        double wTabs = 0.4;
        return (mouseClicks * wMouse) + (keyPresses * wKeyPress) + (tabsOpen * wTabs) +
    yoloScore;
      }
}
```

ارتباط Java با YOLO (REST API) از Java برای ارسال تصویر به YOLO استفاده می‌شود:

خود بخش YOLO در Python اجرا می‌شود و به دوربین‌های نظارت بر جلسه متصل شده، نتایج و داده‌های تشخیص داده شده را به همراه احتمال و موقعیت آنها از طریق REST API به جاده (Jade) ارسال می‌کند.

لازم به ذکر است که بخش کدهای پایتون در اینجا آورده نشده است. همچنین در این مقاله از ذکر نحوه مدل سازی و آموزش YOLO و نیز نحوه annotation تصاویر آموزش داده شده در مدل و دیگر مباحث مربوطه چشم پوشی شده است.

```
import java.io.File;
import java.io.FileInputStream;
import java.io.OutputStream;
import java.net.HttpURLConnection;
import java.net.URL;

public class YOLOClient {
    public static double getYOLOScore(File imageFile) {
        try {
            // ارتباط JADE با YOLO (REST API)
             URL url = new URL("http://localhost:5000/detect");
            HttpURLConnection connection = (HttpURLConnection) url.openConnection();
            connection.setDoOutput(true);
            connection.setRequestMethod("POST");
            connection.setRequestProperty("Content-Type",
    "multipart/form-data; boundary=---");

            OutputStream out = connection.getOutputStream();
            FileInputStream in = new FileInputStream(imageFile);

            byte[] buffer = new byte[1024];
            int bytesRead;
            while ((bytesRead = in.read(buffer)) != -1) {
                out.write(buffer, 0, bytesRead);
            }

            in.close();
            out.close();

            if (connection.getResponseCode() == 200) {
                // Parse the response to get the YOLO score
                 return Double.parseDouble(new
    String(connection.getInputStream().readAllBytes()));
            }
        } catch (Exception e) {
            e.printStackTrace();
```

```
        }
        return 0.0; // Default score if error occurs
    }
}
```

لیست تب‌های باز (openTabs):

```
private int collectTabs() {
    // Simulate the list of currently open tabs (in a real system, fetch this
 dynamically)
    String[] openTabs = {
        "https://math.iut.ac.ir/lms",  // Example: Allowed tab
        "https://iut.ac.ir/library",   // Example: Allowed tab
        "https://192.168.1.300/test",  // Example: Unauthorized tab
        "https://192.168.1.400/proxy"  // Example: Unauthorized tab
    };

    // Define a list of allowed URLs
    String[] allowedUrls = {
        "https://192.168.1.100/lms",
        "https://math.iut.ac.ir/lms"
    };

    // Count unauthorized tabs
    int unauthorizedTabCount = 0;

    for (String tab : openTabs) {
        boolean isAuthorized = false;
        for (String allowedUrl : allowedUrls) {
            if (tab.equalsIgnoreCase(allowedUrl)) {
                isAuthorized = true;
                break;
            }
        }
        if (!isAuthorized) {
            unauthorizedTabCount++;
        }
    }

    return unauthorizedTabCount; // Return the count of unauthorized tabs
}
```

**تشریح بخش تشخیص تب های باز غیر مجاز:**

جمع‌آوری تب‌های باز: از افزونه‌های مرورگر (افزونه Chrome و Firebox) برای ارسال تب‌های باز به سرور جاده (Jade) استفاده می شود.

ارتباط با سرور: از طریق REST API، نیز می‌توان تب‌های باز را به برنامه Java ارسال کرده و آنها را تحلیل کرد.

اتصال به لاگ‌های شبکه: اگر از فایروال یا ابزارهای پایش شبکه داخلی استفاده می‌شود، تب‌های باز کاربران را می‌توان از این طریق نیز دریافت نمود.

این روش ساده قابل گسترش است و می‌تواند در کلیه محیط‌های واقعی استفاده شود.

### ارزیابی سیستم

برای ارزیابی عملکرد سیستم طراحی‌شده، از معیارهای مختلفی مانند دقت، زمان پردازش، و نرخ مثبت کاذب استفاده شده است. آزمایش‌ها در محیط شبیه‌سازی‌شده آزمون آنلاین انجام شده و نتایج آن مورد تحلیل قرار گرفته است.

دقت: دقت سیستم در شناسایی تقلب با مقایسه تعداد تقلب‌های شناسایی‌شده با تعداد تقلب‌های واقعی محاسبه می‌شود. هدف این است که دقت سیستم حداقل ۸۰ درصد باشد. دقت نشان‌دهنده درصد مواردی است که سیستم به درستی شناسایی کرده است.

در اینجا شناسایی‌های درست با (TP)، تعداد پیش‌بینی‌های اشتباه منفی با (FN)، شناسایی‌های نادرست (وقتی که سیستم به‌درستی نشان داده تقلبی انجام نشده است) با (TN)، تعداد شناسایی‌های مثبت کاذب (وقتی که سیستم اشتباه تقلب را شناسایی کرده است) با (FP) نشان داده شده‌اند.

فرمول محاسبه دقت (Accuracy):

$$Accuracy = \frac{TP}{TP + FN} * 100 \qquad (۲)$$

زمان پردازش: زمان پردازش هر فریم ویدئویی و شناسایی اشیاء مشکوک به‌طور پیوسته اندازه‌گیری می‌شود تا اطمینان حاصل شود که سیستم قادر است در زمان واقعی عمل کند.

نرخ مثبت کاذب: نرخ مثبت کاذب (False Positive Rate) به‌عنوان یکی از معیارهای ارزیابی سیستم در نظر گرفته می‌شود. این نرخ نشان می‌دهد که که سیستم تا چه حد در شرایطی که تقلبی وجود ندارد، به اشتباه آن را به‌عنوان تقلب شناسایی کرده است که در آن:

FP تعداد مواردی است که سیستم به‌اشتباه وجود تقلب را گزارش کرده است.

TN تعداد مواردی است که سیستم به‌درستی عدم وجود تقلب را شناسایی کرده است.

فرمول نرخ مثبت کاذب (FPR):

$$FPR = \frac{FP}{FP + TN} * 100 \qquad (۳)$$

## ۵- نتیجه‌گیری

در این بخش، آزمایش‌ها و نتایج ارزیابی سیستم پیشنهادی برای تشخیص تقلب در آزمون‌های آنلاین با استفاده از ترکیب الگوریتم YOLO و سیستم‌های چندعاملی (MAS) مورد بررسی قرار می‌گیرد. برای این منظور، آزمایش‌ها در یک محیط شبیه‌سازی‌شده طراحی شده است که شرایط آزمون آنلاین را در مقیاس کوچک شبیه‌سازی کند. در این آزمایش‌ها، هدف بررسی کارایی سیستم در شناسایی تقلب‌های مختلف، از جمله استفاده از گوشی موبایل، کپی بردار از منابع خارجی و تغییرات غیرعادی در رفتار دانشجویان است.

### شرح آزمایش‌ها

برای ارزیابی سیستم، سه سناریوی اصلی در یک محیط شبیه‌سازی‌شده طراحی شد که هر کدام طی پنج آزمون مجزا اجرا و تکرار شدند.

سناریوی ۱: شبیه‌سازی تقلب با استفاده از گوشی موبایل

سناریوی ۲: شبیه‌سازی تقلب با کپی‌برداری از منابع خارجی (کتاب یا اینترنت)

سناریوی ۳: شبیه‌سازی تقلب با تغییرات غیرعادی در رفتار (مانند نگاه کردن به‌طور مداوم به‌یک سمت خاص یا حرکت‌های غیرعادی بدن)

در هر سناریو، یک مجموعه داده ویدئویی از چندین دانشجو ضبط شد که در حال انجام آزمون آنلاین بودند. داده‌ها شامل ویدئوهای ۱۰ دقیقه‌ای با رزولوشن ۱۰۸۰p از دانشجویانی بودند که در شرایط مختلف آزمون قرار داشتند. به‌علاوه، داده‌های رفتاری دانشجویان مانند کلیک‌های ماوس و حرکات بدن نیز ضبط شدند.

### نتایج و تحلیل آزمایش‌ها

در این بخش، نتایج آزمایش‌ها برای هر سناریو به تفصیل بررسی می‌شود.

سناریوی ۱: شبیه‌سازی تقلب با استفاده از گوشی موبایل

در این سناریو، دانشجویان در حین آزمون آنلاین، گوشی موبایل خود را برای مشاهده منابع غیرمجاز به‌کار بردند. سیستم مبتنی بر YOLO این اشیاء را شناسایی کرد و آن‌ها را به‌عنوان اشیاء مشکوک علامت‌گذاری کرد. سیستم MAS همچنین رفتار غیرعادی دانشجویان مانند نگاه کردن مکرر به‌سمت پایین یا سمت گوشی موبایل را شناسایی کرده و آن‌ها را به‌عنوان الگوهای تقلب به سیستم گزارش داد.

در این سناریو، سیستم به‌خوبی توانست گوشی‌های موبایل را شناسایی کرده و رفتارهای مرتبط با تقلب را علامت‌گذاری کند. نرخ مثبت کاذب نسبتاً پایین بود و سیستم در زمان واقعی توانست این تقلب‌ها را شناسایی کند.

سناریوی ۲: شبیه‌سازی تقلب با کپی‌برداری از منابع خارجی

در این سناریو، دانشجویان به‌طور غیرقانونی از منابع خارجی مانند کتاب یا اینترنت برای پاسخ‌دهی به سوالات استفاده کردند.

سیستم MAS قادر بود با تحلیل رفتار دانشجویان، حرکت‌های غیرعادی بدن و تغییرات در سرعت تایپ را شناسایی کند.

در این آزمایش، سیستم MAS توانست به‌خوبی رفتارهای غیرعادی مانند تغییرات سرعت تایپ و حرکات بدن را شناسایی کند.

سناریوی ۳: شبیه‌سازی تقلب با تغییرات غیرعادی در رفتار

در این سناریو، دانشجویان به‌طور عمدی حرکات غیرعادی انجام دادند، مانند نگاه کردن به‌طور مداوم به یک سمت خاص یا تکان دادن بدن. این نوع رفتارهای مشکوک می‌توانند نشانه‌ای از استفاده از منابع تقلبی یا تعامل با دیگر افراد باشند.

سیستم MAS به‌خوبی توانست رفتارهای غیرطبیعی را شناسایی کند، از جمله نگاه کردن به سمت خاص یا تکان‌های غیرعادی بدن، که معمولاً نشانه‌هایی از تقلب هستند. نتایج نشان داد که این سیستم برای شناسایی تقلب‌های غیرمستقیم نیز بسیار مؤثر است، اما دقت سیستم در شناسایی منابع خارجی کمی کاهش داشت.

نتایج تحلیل عملکرد سیستم از دو جنبه‌ی مهم دقت شناسایی و نرخ مثبت کاذب (FPR) در قالب دو جدول ۱ و ۲ بصورت مجزا ارائه و بررسی شده است.

جدول نخست به بررسی دقت شناسایی سیستم در شرایط مختلف و تحت سه سناریوی اصلی و ۵ بار تکرار آزمون آنلاین، پرداخته و توانایی سیستم در شناسایی تقلب را با توجه به رفتارهای شبیه‌سازی‌شده ارزیابی می‌کند.

جدول دوم نرخ مثبت کاذب را که نشان‌دهنده خطاهای سیستم در شناسایی تقلب‌های غیرواقعی است به تفصیل تحلیل می‌کند.

این تحلیل‌ها کمک می‌کنند تا ضمن درک نقاط قوت و ضعف سیستم، عوامل مؤثر بر عملکرد آن شناسایی شده و راهکارهای بهبود ارائه شوند. این ارزیابی‌ها نشان‌دهنده توانمندی سیستم در شناسایی دقیق تقلب‌ها و کاهش خطاهای مثبت کاذب، به‌ویژه در شرایط شبیه‌سازی‌شده آزمون‌های آنلاین، است.

جدول (۱): محاسبه دقت شناسایی تقلبها

| سناریوی ۱: گوشی موبایل | آزمون ۱ | آزمون ۲ | آزمون ۳ | آزمون ۴ | آزمون ۵ | کل نتایج |
|---|---|---|---|---|---|---|
| تعداد کل تقلب‌ها | ۱۰ | ۲۰ | ۳۰ | ۱۵ | ۲۵ | ۱۰۰ |
| True Positives (TP) | ۹ | ۱۸ | ۲۸ | ۱۴ | ۲۱ | ۹۰ |
| False Negatives (FN) | ۱ | ۲ | ۲ | ۱ | ۴ | ۱۰ |
| دقت شناسایی (Accuracy) | ٪۹۰ | ٪۹۰ | ٪۹۳ | ٪۹۳ | ٪۸۴ | ٪۹۰ |

| سناریوی ۲: منابع خارجی | آزمون ۱ | آزمون ۲ | آزمون ۳ | آزمون ۴ | آزمون ۵ | کل نتایج |
|---|---|---|---|---|---|---|
| تعداد کل تقلب‌ها | ۵ | ۱۰ | ۲۰ | ۱۲ | ۸ | ۵۵ |
| True Positives (TP) | ۴ | ۹ | ۱۸ | ۱۰ | ۷ | ۴۸ |
| False Negatives (FN) | ۱ | ۱ | ۲ | ۲ | ۱ | ۷ |
| دقت شناسایی (Accuracy) | ٪۸۰ | ٪۹۰ | ٪۹۰ | ٪۸۳٫۳ | ٪۸۷٫۵ | ٪۸۷٫۲ |
| سناریوی ۳: حرکات رفتاری | آزمون ۱ | آزمون ۲ | آزمون ۳ | آزمون ۴ | آزمون ۵ | کل نتایج |
| تعداد کل تقلبها | ۸ | ۱۲ | ۲۰ | ۱۰ | ۲۵ | ۷۵ |
| True Positives (TP) | ۷ | ۱۱ | ۱۷ | ۸ | ۲۳ | ۶۵ |
| False Negatives (FN) | ۱ | ۱ | ۳ | ۲ | ۲ | ۱۰ |
| دقت شناسایی (Accuracy) | ٪۸۷٫۵ | ٪۹۱٫۶ | ٪۸۵ | ٪۸۰ | ٪۸۸ | ٪۸۶٫۶ |

دقت کلی سیستم در شناسایی تقلب‌ها با توجه به جدول (۱) برابر است با: ٪۸۷٫۹

| جدول (۲): محاسبه نرخ مثبت کاذب | | | | |
|---|---|---|---|---|
| سناریو | آزمون | FP | TN | FPR |
| گوشی موبایل | آزمون ۱ | ۱ | ۹ | ٪۱۰ |
| | آزمون ۲ | ۲ | ۲۳ | ٪۸ |
| | آزمون ۳ | ۳ | ۳۷ | ٪۷ |
| | آزمون ۴ | ۲ | ۲۰ | ٪۹ |
| | آزمون ۵ | ۱ | ۱۵ | ٪۶ |
| | کلی | - | - | ٪۸ |
| منابع خارجی | آزمون ۱ | ۲ | ۱۴ | ٪۱۲ |
| | آزمون ۲ | ۳ | ۲۷ | ٪۱۰ |
| | آزمون ۳ | ۴ | ۳۶ | ٪۹ |
| | آزمون ۴ | ۳ | ۲۲ | ٪۱۱ |
| | آزمون ۵ | ۲ | ۲۴ | ٪۸ |
| | کلی | - | - | **٪۱۰** |

| | | | | |
|---|---|---|---|---|
| حرکات رفتاری | آزمون ۱ | ۳ | ۱۸ | ٪۱۴ |
| | آزمون ۲ | ۴ | ۳۰ | ٪۱۱ |
| | آزمون ۳ | ۵ | ۳۵ | ٪۱۰ |
| | آزمون ۴ | ۴ | ۲۵ | ٪۱۲ |
| | آزمون ۵ | ۳ | ۲۷ | ٪۹ |
| | کلی | - | - | ٪۱۱٫۲ |

برای محاسبه میانگین نرخ مثبت کاذب (FPR) کل از جدول (۲)، مراحل زیر انجام می‌شود:

جمع کل FPRها برای تمام آزمون‌ها در هر سه سناریو:

سناریوی ۱ (گوشی موبایل): ۴۰=۶+۹+۷+۸+۱۰

سناریوی ۲ (منابع خارجی): ۵۰=۱۲+۱۰+۹+۱۱+۸

سناریوی ۳ (حرکات رفتاری): ۵۶=۱۴+۱۱+۱۰+۱۲+۹

جمع کل مقادیر FPR: ۴۰+۵۰+۵۶=۱۴۶

تعداد کل آزمون‌ها: ۵ آزمون برای هر سناریو= ۱۵

بنابراین نرخ مثبت کاذب کل: ۹٫۷۳=۱۴۶/۱۵

نرخ مثبت کاذب کل (FPR): ٪۹٫۷۳

نتایج به‌دست‌آمده نشان می‌دهند که سیستم ترکیبی YOLO و MAS قادر است تقلب‌های مختلف در آزمون‌های آنلاین را با دقت بالا شناسایی کند. مهم‌ترین دستاورد این تحقیق، توانایی سیستم در شناسایی تقلب‌های پیچیده مانند استفاده از گوشی موبایل و تغییرات غیرعادی در رفتار است.

این نتایج نشان می‌دهند که سیستم می‌تواند به‌طور مؤثر تقلب را در زمان واقعی شناسایی و به‌طور مؤثر نرخ منفی کاذب را کاهش داده و اطلاعات دقیق‌تری در مورد رفتارهای مشکوک در اختیار ناظران قرار دهد.

**چالش‌ها:** اگرچه نتایج سیستم مثبت بودند، چالش‌هایی در برخی سناریوها وجود داشت. یکی از بزرگترین چالش‌ها شبیه‌سازی دقیق شرایط دنیای واقعی بود. در بعضی موارد، سیستم دقت کمتری در شناسایی تقلب‌هایی داشت که در محیط‌های واقعی ممکن است با تغییرات جزئی در رفتار دانشجویان همراه باشند. همچنین، نرخ مثبت کاذب در برخی موارد به‌ویژه در سناریوهای پیچیده، کمی بالا بود که نیاز به بهبود در پردازش داده‌ها و الگوریتم‌ها دارد.

**پیشنهادها:** در نهایت، این تحقیق نشان داد که ترکیب الگوریتم YOLO برای شناسایی اشیاء و سیستم MAS برای تحلیل رفتار می‌تواند یک راه‌حل مؤثر و کارا برای شناسایی تقلب در آزمون‌های آنلاین باشد. سیستم ترکیبی توانسته است دقت بالایی در شناسایی تقلب‌های مختلف از جمله استفاده از گوشی موبایل، کپی‌برداری از منابع خارجی و تغییرات غیرعادی در رفتار دانشجویان به‌دست آورد. در سناریوهای مختلف، دقت شناسایی تقلب‌ها به‌طور متوسط ۸۷٫۹ درصد بود که نشان‌دهنده کارایی بالای الگوریتم YOLO در شناسایی اشیاء و سیستم MAS در تحلیل رفتار بود. این دقت بالا به‌ویژه در شناسایی تقلب‌های پیچیده مانند استفاده از گوشی موبایل و تغییرات غیرعادی در رفتار که معمولاً توسط سیستم‌های ساده‌تر شناسایی نمی‌شود، بسیار چشمگیر است. سیستم پیشنهادی در مقایسه با دیگر روش‌های شناسایی تقلب آنلاین، که بیشتر به تجزیه و تحلیل تصویری و یا پردازش تک‌عاملی وابسته‌اند، از دقت بالاتر و انعطاف‌پذیری بیشتری برخوردار است. استفاده از ترکیب YOLO برای شناسایی اشیاء و MAS برای تحلیل رفتار دانشجویان توانسته است یک راه‌حل جامع و دقیق برای شناسایی تقلب در آزمون‌های آنلاین فراهم کند.

برای بهبود بیشتر سیستم، پیشنهاد می‌شود که از داده‌های بیشتر و متنوع‌تری برای آموزش سیستم (مدل‌سازی) استفاده شود و طراحی سیستم‌هایی که قادر به پشتیبانی از تعداد زیادی دانشجو به‌طور همزمان باشند تا بهینه‌سازی‌های لازم برای کاهش نرخ مثبت کاذب و زمان پردازش انجام گیرد.

## منابع:

1-Ali, L., Manzoor, N., Masood, H. A., & Abbas, A. (2024). Nanotechnology-Enabled Approaches to Mitigating Abiotic Stresses in Agricultural Crops. In *Molecular Dynamics of Plant Stress and its Management* (pp. 621-650). Singapore: Springer Nature Singapore.
2-Asep, H. S. (2019, July). A design of continuous user verification for online exam proctoring on M-learning. In *2019 international conference on electrical engineering and informatics (ICEEI)* (pp. 284-289). IEEE.
3-Erdem, B., & Karabatak, M. (2025). Cheating Detection in Online Exams Using Deep Learning and Machine Learning. *Applied Sciences (2076-3417), 15*(1).
4-Fatima, S., Jennings, N. R., & Wooldridge, M. (2024). Learning to resolve social dilemmas: a survey. *Journal of Artificial Intelligence Research*, *79*, 895-969.
5-Hu, Z., Jing, Y., Wu, G., & Wang, H. (2024). Multi-Perspective Adaptive Paperless Examination Cheating Detection System Based on Image Recognition. *Applied Sciences*, *14*(10), 4048.
6-Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, *5*(4), 533-561.
7-Singh, T., Nair, R. R., Babu, T., & Duraisamy, P. (2024). Enhancing academic integrity in online assessments: Introducing an effective online exam proctoring model using yolo. *Procedia Computer Science*, *235*, 1399-1408.
8-Redmon, J., & Farhadi, A. (2018). YOLOv3: An incremental improvement. *arXiv preprint*, arXiv:1804.02767.
9-Vinyals, O., Blundell, C., Lillicrap, T., & Wierstra, D. (2016). Matching networks for one shot learning. *Advances in neural information processing systems*, *29*.
10-Winiecki, E., Pawlicki, M., Pawlicka, A., Kozik, R., & Chora, M. (2025, April). Evaluation of Selected Few-Shot Learning Methods in Network Intrusion Detection. In *International Conference on Advanced Information Networking and Applications* (pp. 10-20). Cham: Springer Nature Switzerland.
11-Zeng, W. (2024). Image data augmentation techniques based on deep learning: A survey. *Mathematical BiosciencesandEngineering*, *21*(6),6190-6224.